

[Registered Entity Name]

NERC ID: [NCRXXXXX]

CIP-003-8 – Cyber Security – *Security Management Controls*

[QX] [20XX] Guided Self-Certification Worksheet

# Instructions

1. Populate the cover page by adding your Registered Entity name, NERC compliance registry (NCR) number, and the quarter and year indicated for the Guided Self-Certification in Align.
2. Complete the tasks listed under Assessment Guidance. Only complete tasks listed for the Requirements and Sections in scope.
3. Log into Align and complete your Guided Self-Certification response.
4. Where random sampling is required, use an objective tool such as Microsoft Excel or random.org. If you have questions, reference NERC’s [Compliance Monitoring and Enforcement Manual](https://www.nerc.com/pa/comp/CAOneStopShop/ERO%20Enterprise%20Compliance%20Monitoring%20and%20Enforcement%20Manual%20v6.pdf) (2021 Version 6, p. 151) or contact your Self-Certification lead for assistance.
5. Submit the following to the Secure Evidence Locker (SEL):
	1. This completed worksheet; and
	2. The specific evidence annotated for the requested Requirements and/or Attachment 1 Sections.
		1. Please use unique file names and identify which evidence file(s) support each conclusion.
		2. Direct references and unique file names help facilitate an expedited review of the Guided Self-Certification.
6. The Guided Self-Certification request in Align includes the monitoring period and the timeframe to perform the assessment and respond.
7. For the purpose of this document all capitalized terms have the meaning ascribed to them in the NERC *Glossary of Terms Used in NERC Reliability Standards* ([Available Here](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf)) unless otherwise indicated.

# Requirements

The scope of this CIP-003-8 Guided Self-Certification is listed below:

|  |  |
| --- | --- |
| CIP-003-8 Requirement | In Scope |
| **R1** | *Requirement is included within the scope of this SC* |
| **R2 Attachment 1**  | *Requirement is included within the scope of this SC* |
|  | **Section 1** | *Section is included within the scope of this SC* |
|  | **Section 2** | *Section is included within the scope of this SC* |
|  | **Section 3** | *Section is included within the scope of this SC* |
|  | **Section 4** | *Section is included within the scope of this SC* |
|  | **Section 5** | *Section is included within the scope of this SC* |
| **R3** | *Requirement is not included within the scope of this SC* |
| **R4** | *Requirement is not included within the scope of this SC* |

# Assessment Guidance - Compliance

## R1

* + - 1. Per Requirement R1, provide the current version of the cyber security policy(ies) developed to collectively address the required topics. Please identify where the cyber security policy(ies) specifically address the required topics of Part 1.1 and/or Part 1.2.

|  |
| --- |
| Evidence of Cyber Security Policy(ies) |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Provide evidence demonstrating the review and CIP Senior Manager approval of the cyber security policy(ies) occurred within the previous 15 calendar months.

|  |
| --- |
| Evidence of Review and Approval  |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

## R2

Provide a list of all BES assets containing low impact BES Cyber Systems (LIBCS) for which you have or share compliance responsibility. The listing should include (a) the BES asset type (e.g., Control Centers, Transmission Stations and substations, Generation resources, Systems and facilities critical to system restoration, Special Protection Systems, Distribution Provider Protection Systems) and (b) whether the BES asset uses electronic access controls pursuant to Sections 3.1 and 3.2.

|  |
| --- |
| List of BES assets Containing LIBCS |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

## Attachment 1: Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

#### Attachment 1 Section 1

1. Per Attachment 1 Section 1, please identify where the cyber security plan(s) shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

|  |
| --- |
| Cyber Security Awareness Plan(s) |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Provide evidence of the reinforcement materials provided within the previous 15 calendar months to personnel who have access to BES assets containing a LIBCS.

|  |
| --- |
| Evidence of Cyber Security Awareness Reinforcement |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

#### Attachment 1 Section 2

1. Per Attachment 1 Section 2, please identify where the cyber security plan(s) shall control physical access, based on need as determined by your entity, to (1) the BES asset or the locations of the LIBCS within the BES asset, and (2) the Cyber Asset(s) that provide electronic access control(s) implemented for Section 3.1, if any.

|  |
| --- |
| Physical Security Plan(s) |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Select a random sample from the population identified in (R2) step 1, above.
2. Per Attachment 1 Section 2, for each BES asset containing a LIBCS selected in the sample above from (R2) step 5, provide evidence that physical security controls were implemented to control physical access to (1) the asset or the locations of the LIBCS in the asset; and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

|  |
| --- |
| Evidence of Physical Security Controls |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

#### Attachment 1 Section 3

1. Per Attachment 1 Section 3.1, please identify where the cyber security plan(s) shall implement electronic access controls to permit only necessary inbound and outbound electronic access as determined by your entity for any communications that are: (i) between a LIBCS and a Cyber Asset(s) outside the BES asset containing LIBCS; (ii) using a routable protocol when entering or leaving the BES asset containing the LIBCS; and (iii) not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

|  |
| --- |
| Electronic Access Control Plan(s) |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 3.2, please identify where the cyber security plan(s) shall implement electronic access controls to authenticate all Dial-up Connectivity, if any, that provides access to a LIBCS, per Cyber Asset capability. Please indicate N/A in the filename and comments if there is no use of Dial-up Connectivity to access LIBCS.

|  |
| --- |
| Dial-up Connectivity Plan(s) |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Select random samples from the population identified in (R2) step 1, above, as follows:
	1. Select a random sample from the population of the BES assets containing a LIBCS with routable protocol communication entering or leaving the BES asset containing the LIBS (Section 3.1).
	2. Select a random sample from the population of the BES assets containing a LIBCS with Dial-up Connectivity (Section 3.2).
2. Per Attachment 1 Section 3.1, for each BES asset containing a LIBCS selected in the sample above from (R2) step 9(a), provide representative diagram(s), if any, of the specific implementation of electronic access control(s) for each sampled BES asset.

|  |
| --- |
| Diagrams of Electronic Access Controls |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 3.1, for each BES asset containing a LIBCS selected in the sample above from (R2) step 9(a), provide evidence of the inbound and outbound electronic access permissions (e.g., firewall policy or rules) at each sampled BES asset.

|  |
| --- |
| Evidence of Electronic Access Permissions |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 3.1, for each BES asset containing a LIBCS selected in the sample above from (R2) step 9(a), provide documentation identifying why the enabled inbound and outbound electronic permissions are necessary at each sampled BES asset.

|  |
| --- |
| Evidence Electronic Access Permissions are Necessary |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 3.2, for each BES asset containing a LIBCS selected in the sample above from (R2) step 9(b), provide representative diagram(s) of the specific implementation of Dial-up Connectivity for each sampled BES asset.

|  |
| --- |
| Diagrams of Dial-up Connectivity |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 3.2, for each BES asset containing a LIBCS selected in the sample above from (R2) step 9(b), provide either: (a) documentation of the incapability of LIBCS to perform authentication; or (b) documentation that authentication of Dial-up Connectivity has been implemented.

|  |
| --- |
| Evidence of Dial-up Connectivity Authentication |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

#### Attachment 1 Section 4

1. Per Attachment 1 Section 4.1, please identify where the Cyber Security Incident response plan(s) (CSIRP(s)) include the process to identify, classify, and respond to Cyber Security Incidents.

|  |
| --- |
| Cyber Security Incident Response Plan(s) |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 4.2, please identify where the CSIRP(s) include the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and the subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law.

|  |
| --- |
| Cyber Security Incident Notification |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 4.3, please identify where the CSIRP(s) include roles and responsibilities for the Cyber Security Incident response by groups or individuals.

|  |
| --- |
| CSIRP Roles & Responsibilities |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 4.4, please identify where the CSIRP(s) details the incident handling processes for Cyber Security Incidents.

|  |
| --- |
| Cyber Security Incident Handling |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 4.5, please identify where the CSIRP(s) include testing the plan(s) at least once every 36 calendar months.

|  |
| --- |
| CSIRP Testing |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 4.6, please identify where the CSIRP(s) detail updating the plan(s), if needed, within 180 calendar days after completion of a CSIRP test or actual Reportable Cyber Security Incident.

|  |
| --- |
| CSIRP Updates |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Has your entity had to activate its CSIRP(s) during the monitoring period? [ ]  Yes [ ]  No

If yes, provide documentation of each activation of the CSIRP for a LIBCS, including the date of activation and evidence that the CSIRP was followed.

|  |
| --- |
| Evidence of CSIRP Activation |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Provide evidence related to Reportable Cyber Security Incidents for BES assets containing a LIBCS, including the date E-ISAC was notified. Please indicate N/A in the filename and comments if there have been no Reportable Cyber Security Incidents during the monitoring period.

|  |
| --- |
| Evidence of Reportable Cyber Security Incidents |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 4.5, provide evidence CSIRP testing was completed within the last 36 calendar months, and indicate the date of completion for each test, including: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident.

|  |
| --- |
| Evidence of CSIRP Testing |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 4.6, if updates to the CSIRP were needed, provide evidence the CSIRP was updated within 180 calendar days of the test or actual Reportable Cyber Security Incident.

|  |
| --- |
| Evidence of CSIRP Updates |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

#### Attachment 1 Section 5

1. Pursuant to Attachment 1 Section 5, please provide a list of any CIP Exceptional Circumstances (CEC) and include the beginning date of the CEC, ending date of the CEC, BES assets affected and a description of the situation which triggered the CEC.

|  |
| --- |
| CIP Exceptional Circumstances |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 5.1, please identify where the cyber security plan(s) annotate Transient Cyber Assets (TCAs) are managed in an ongoing, on-demand, or combination or both manners and the method(s) for mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of TCAs managed by your entity.

|  |
| --- |
| Plan(s) for TCAs Managed by Entity |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Provide a list of TCAs managed by your entity for use with LIBCSs. Please indicate N/A in the filename and comments if there have been no TCAs used during the monitoring period.

|  |
| --- |
| List of TCAs Managed by Entity |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Select a random sample from the population identified in (R2) step 27, above.
2. Per Attachment 1 Section 5.1, for each TCA selected in the sample above from (R2) step 28, provide evidence: (i) the TCA was managed in an ongoing, on-demand, or combination of both and (ii) evidence that each TCA uses: (1) antivirus software, including manual or managed updates of signatures or patterns; (2) application whitelisting; or (3) other method(s) to mitigate the introduction of malicious code.

|  |
| --- |
| Evidence of Mitigation Methods for TCAs Managed by Entity |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 5.2, please identify where the cyber security plan(s) annotate method(s) for mitigating the risk of the introduction of malicious code to a LIBCS through the use of Transient Cyber Assets managed by a party other than your entity.

|  |
| --- |
| Plan(s) for TCAs Managed by Parties Other than Entity |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Provide a list of TCAs managed by a party other than your entity for use with a LIBCS. Please indicate N/A in the filename and comments if there have been no TCAs managed by other parties used during the monitoring period.

|  |
| --- |
| List of TCAs Managed by Parties Other than Entity |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Select a random sample from the population identified in (R2) step 31, above.
2. Per Attachment 1 Section 5.2.1, for each TCA selected in the sample above from (R2) step 32, provide evidence, including the date and time performed, of the: (1) review of antivirus update level; (2) review of antivirus update process used by the party; (3) review of application whitelisting used by the party; (4) review use of live operating system and software executable only from read-only media; (5) review of system hardening used by the party; or (6) other method(s) to mitigate the introduction of malicious code.

|  |
| --- |
| Evidence of Mitigation Methods for TCAs Managed by Parties Other than Entity |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 5.2.2, for each TCA selected in the sample above from (R2) step 32, provide evidence of any determinations of additional mitigation actions deemed necessary and implemented prior to connecting the TCA.

|  |
| --- |
| Additional Mitigation for TCAs Managed by Parties Other than Entity |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Per Attachment 1 Section 5.3, please identify where the cyber security plan(s) annotate method(s) to detect malicious code on Removable Media (RM) using a Cyber Asset other than a BES Cyber System [5.3.1] and the mitigation of the threat of detected malicious code prior to connecting RM to a LIBCS [5.3.2].

|  |
| --- |
| Plan(s) for Removable Media |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Provide a list of RM used with LIBCSs during the monitoring period. Please indicate N/A in the filename and comments if there have been no RM used during the monitoring period.

|  |
| --- |
| List of Removable Media |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Select a random sample from the population identified in (R2) step 36, above.
2. Per Attachment 1 Section 5.3, for each RM selected in the sample above from (R2) step 37, provide evidence of: (1) using method(s) to detect malicious code on RM using a Cyber Asset other than a BES Cyber System; and (2) mitigation of the threat of detected malicious code on the RM, if any, during the monitoring period, prior to connecting the RM to a LIBCS.

|  |
| --- |
| Mitigation Evidence for Removable Media |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

## R3

* + - 1. Please provide evidence demonstrating identification of a CIP Senior Manager by name, including the date of designation.

|  |
| --- |
| CIP Senior Manager Identification |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Provide evidence of any changes to the CIP Senior Manager identification, if any, were documented within 30 calendar days of the change.

|  |
| --- |
| Changes to CIP Senior Manager Identification |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Provide evidence the CIP Senior Manager is a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards.

|  |
| --- |
| CIP Senior Manager Authority |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

## R4

* + - 1. If delegations are used, please provide the documented process that addresses the delegation of the CIP Senior Manager’s authority.

|  |
| --- |
| CIP Senior Manager Authority Delegation Process |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Provide documentation for each delegation and identify where the documentation includes the name or title of the delegate, specific actions for which authority is delegated, the date of delegation, and approval of the CIP Senior Manager.

|  |
| --- |
| Evidence of Delegations |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

* + - 1. Provide evidence that changes to delegates were documented within 30 calendar days of the change.

|  |
| --- |
| Changes to Delegations of CIP Senior Manager Authority |
| **File Name** | **Document Title** | **Revision** **Or Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

# Assessment Guidance – Controls

**Controls Instructions:**

In this section of the document, WECC asks you to identify/describe the controls your entity put in place to mitigate the risk(s) addressed by this Standard. When WECC asks you to "provide associated evidence," you should provide any evidence (examples include checklists, processes, procedures, training, sign-in sheets, etc.) demonstrating your entity *created* a control and *implemented* the control.

If you have any questions, please reach out to WECC at internalcontrols@wecc.org.

**Controls Questions:**

1. (a) Describe the controls your entity uses to ensure all applicable employees and contractors understand cyber security policies (e.g., training, communications plans); (b) describe how your entity confirms training or communications plans are effective; and provide supporting evidence for your responses to (a) and (b), above.

|  |
| --- |
| Narrative  |
| Response:(a)(b) |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Describe the method your entity uses to provide training to employees on the cyber security policies (e.g., online, in person, etc.); and provide supporting evidence for your response.

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. (a) Describe additional security measures to supplement physical access controls (e.g., key management program(s), Closed Circuit Television (CCTV), on-site security; (b) describe response procedures in the event of an unauthorized access attempt or physical breach; and provide supporting evidence for your responses to (a) and (b), above.

|  |
| --- |
| Narrative  |
| Response:(a)(b) |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. (a) Describe how your entity determines appropriate electronic access controls to BES assets containing LIBCS (e.g., risk assessment process); (b) describe how your entity monitors for changes to its electronic access controls that would affect the BES Cyber System (e.g., additions, replacements); and provide supporting evidence for your responses to (a) and (b), above.

|  |
| --- |
| Narrative  |
| Response:(a)(b) |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Describe how your entity ensures electronic access is limited to only necessary traffic (i.e., grant, review, revoke, monitor electronic access) and provide supporting evidence for your response.

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. (a) Describe how your entity identifies and assesses risks associated with Cyber Security Incidents related to LIBCS; (b) describe how your entity ensures personnel are prepared to respond to identified threats (training, incident handling procedures, checklists, contact lists); (c) describe how Cyber Security Incident response exercises are developed; and provide supporting evidence for your responses to (a) through (c), above.

|  |
| --- |
| Narrative  |
| Response:(a)(b)(c) |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Describe the controls your entity has in place to verify methods to mitigate the risk of introduction of malicious code are properly employed on all relevant Transient Cyber Assets (TCAs); and provide supporting evidence for your responses.

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

1. Describe how your entity controls the use of removable media (e.g., restricting ports, USB hubs, standards of behavior); and provide supporting evidence for your response.

|  |
| --- |
| Narrative  |
| Response: |

|  |
| --- |
| Evidence (if available) |
| **File Name** | **Document Title** | **Revision/****Version** | **Document Date** | **Relevant Page(s) or Section(s)** |
|  |  |  |  |  |
|  |  |  |  |  |
| Comments: |

# Evidence Submittal

Please submit the following evidence with the Guided Self-Certification response to the Secure Evidence Locker (SEL):

|  |  |
| --- | --- |
| CIP-003-8 Requirement | Evidence |
|  | This completed worksheet |
| **R1** | *Requirement is included within the scope of this SC:*Cyber Security Policy(ies)Review and Approval |
| **R2 Attachment 1**  | *Requirement is included within the scope of this SC*List of BES assets Containing LIBCS |
|  | **Section 1** | *Section is included within the scope of this SC*Cyber Security Awareness Plan(s)Cyber Security Awareness Reinforcement |
|  | **Section 2** | *Section is included within the scope of this SC*Physical Security Plan(s)Physical Security Controls |
|  | **Section 3** | *Section is included within the scope of this SC*Electronic Access Control Plan(s)Dial-up Connectivity Plan(s)Diagrams of Electronic Access ControlsElectronic Access PermissionsElectronic Access Permissions are NecessaryDiagrams of Dial-up ConnectivityDial-up Connectivity Authentication |
|  | **Section 4** | *Section is included within the scope of this SC*CSIRP(s)Cyber Security Incident NotificationCyber Security Incident Response Roles & ResponsibilitiesCyber Security Incident HandlingCSIRP TestingCSIRP UpdatesActivation of CSIRPReportable Cyber Security IncidentsTesting of CSIRPUpdates to CSIRP |
|  | **Section 5** | *Section is included within the scope of this SC*CIP Exceptional CircumstancesPlan(s) for TCAs Managed by EntityList of TCAs Managed by EntityMitigation Methods for TCAs Managed by EntityPlan(s) for TCAs Managed by Parties Other than EntityList of TCAs Managed by Parties Other than EntityMitigation Methods for TCAs Managed by Parties Other than EntityAdditional Mitigation for TCAs Managed by Parties Other than EntityPlan(s) for RMList of RMMitigation Evidence for RM |
| **R3** | *Requirement is not included within the scope of this SC*CIP Senior Manager IdentificationChanges to CIP Senior Manager IdentificationCIP Senior Manager Authority |
| **R4** | *Requirement is not included within the scope of this SC*CIP Senior Manager Authority Delegation ProcessDelegationsChanges to Delegations of CIP Senior Manager Authority |

# Revision Table

|  |  |
| --- | --- |
| Revision Date | Description of Revision |
| 8/30/2021 | Initial version of CIP-003-8 Guided Self-Certification Worksheet |
| 2/28/2023 | Revisions include: * Reference to Compliance Monitoring and Enforcement Manual (version 6)
* Revised language in *Assessment Guidance – Controls* section
* Moved “Evidence Submittal” to end of worksheet
* Added Revision Table
 |