

# Evidence Request Tool (ERT) v3.0 to v4.0 Change List

February 10, 2020

## List of Changes

### Instructions tab

- Row 2
  - Changed Version 3.0 to 4.0

### Level 1 tab

- CIP-002-R1-L1-01
  - Added *“Additionally, provide evidence of the implementation of that process.”*
- CIP-002-R1-L1-03
  - Removed
    - 4. For each Transmission station or substation, list the number of lines to other Transmission stations or substations at each voltage level at or above 200 kV.
    - 5. System-level one-line diagram(s) depicting each BES Transmission Line for voltage levels at or above 200 kV.
    - 6. List of each BES reactive resource or group of resources at a single location with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities).
    - 9. For systems and facilities critical to system restoration, system restoration plan(s) covering all applicable assets.
    - 10. If not otherwise included in the system restoration plan(s), system-level one-line diagrams depicting any Cranking Path used by the restoration plan(s).
    - 11. Provide the UFLS and/or the UVLS plan, including the expected load shed at each voltage or frequency level. For each voltage or frequency level that will shed an aggregate of more than 300 MW, provide a breakdown of the amount of load shed by each common control system without human operator initiation.
    - Re-numbered question 7 to 4
  - Added *“(either owned or connected to the entity's Transmission Facilities)”*
  - Re-numbered question 7 to 5

- Added “(either owned or connected to the entity's Transmission Facilities)”
- Added
  - 6. List all Special Protection Systems and Remedial Action Schemes which relate to the entity's Facilities along with a description of their purpose.
  - 7. List all Interconnection Reliability Operating Limits which include the entity or its neighbors along with a description of their purpose.
  - 8. Explain in detail if any Cyber Assets located in other countries have the capability to monitor and/or control generation resources in the United States.
  - 9. Explain in detail if there are any Cyber Assets that you own that have the capability to monitor and/or control Facilities owned by other Registered Entities.
  - 10. Provide evidence as to whether the Reliability Coordinator, Planning Coordinator, or Transmission Planner has identified generation at a single plant location or Transmission Facilities at a single station or substation location as being critical to derivation of Interconnection Reliability Operating Limits and their associated contingencies.
  - 11. Provide evidence as to whether any Special Protection Systems and Remedial Action Schemes, or automated switching Systems that operate BES Elements, if destroyed degraded misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits violations or cause a reduction in one or more Interconnection Reliability Operating Limits.
  - 12. Provide evidence as to whether the Planning Coordinator or Transmission Planner has identified generation Facilities (either owned or connected to the entity's Transmission Facilities) as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
- CIP-002-R1-L1-04
  - Modified to address only Transmission assets
  - Removed
    - Provide the following supporting information for medium impact criteria:
    - 2.3. Provide evidence as to whether the Planning Coordinator or Transmission Planner has identified generation Facilities as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
    - 2.6. Provide evidence as to whether the Reliability Coordinator, Planning Coordinator, or Transmission Planner has identified generation at a single plant location or Transmission Facilities at a single station or substation location as being critical to derivation of Interconnection Reliability Operating Limits and their associated contingencies.
    - 2.7. Provide evidence of the agreed upon Nuclear Plant Interface Requirements for Transmission Facilities with one or more Agreements in effect with a Nuclear Plant

- Generator Operator that include mutually agreed to Nuclear Plant Interface Requirements (per NUC-001-3 R2).
- 2.9. Provide evidence as to whether any Special Protection Systems and Remedial Action Schemes, or automated switching Systems that operate BES Elements, if destroyed degraded misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits violations or cause a reduction in one or more Interconnection Reliability Operating Limits.
- 2.11. Provide evidence as to whether there is a Control Center or backup Control Center, not already included in High Impact Rating, that performs the functional obligations of the Generator Operator (which includes dispatching) for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.
- Added
  - Provide the following supporting information for each listed Transmission asset on the BES Assets tab:
    - 1. For each Transmission station or substation, list the number of lines to other Transmission stations or substations at each voltage level at or above 200 kV.
    - 2. System-level one-line diagram(s) depicting each BES Transmission Line for voltage levels at or above 200 kV.
    - 3. List all BES reactive resources including locations (excluding generation Facilities).
    - 4. For systems and facilities critical to system restoration, system restoration plan(s) covering all applicable assets.
    - 5. If not otherwise included in the system restoration plan(s), system-level one-line diagrams depicting any Cranking Path used by the restoration plan(s).
    - 6. Provide the UFLS and/or the UVLS plan, including the expected load shed at each voltage or frequency level. For each voltage or frequency level that will shed an aggregate of more than 300MW, provide a breakdown of the amount of load shed by each common control system without human operator initiation.
    - 7. Provide evidence of the agreed upon Nuclear Plant Interface Requirements for Transmission Facilities with one or more Agreements in effect with a Nuclear Plant Generator Operator that include mutually agreed to Nuclear Plant Interface Requirements (per NUC-001-3 R2).
- CIP-002-R1-L1-05
  - Added this Request ID for CIP-002 for Generation assets
  - Added
    - Provide the following supporting information for each listed Generation asset on the BES Assets tab:

- 1. For each generating station that generates over 1500 MW at a single plant location, provide all analysis documents which identify the BES Cyber Assets (or absence of any such assets) which can impact 1500 MW of generation in less than 15 minutes.
- 2. Provide evidence as to whether there is a Control Center or backup Control Center, not already included in High Impact Rating, that performs the functional obligations of the Generator Operator (which includes dispatching) for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.
- CIP-002-R1-L1-05
  - Changed to Request ID CIP-002-R1-L1-06
- CIP-002-R1-L1-06
  - Changed to Request ID CIP-002-R1-L1-07
- CIP-003-R1-L1-01
  - Modified to *“Provide evidence that the cyber security policies that address compliance with CIP-003 R1 were approved by a CIP Senior Manager.”*
- CIP-003-R1-L1-09
  - Modified to *“For each location where use of Removable Media is used, provide the information requested on the RM tab.”*
- CIP-005-R1-L1-02
  - Removed *“please”*
- CIP-005-R1-L1-05
  - Removed *“please”*
- CIP-005-R2-L1-02
  - Added *“Provide detailed explanation on the use of remote access for third-parties.”*
- CIP-005-R2-L1-03
  - Added *“Provide what electronic access controls (multi-factor, encryption, etc.) and Cyber Asset(s) are used to authenticate individuals for remote access?”*
- CIP-007-R3-L1-02
  - Removed Request ID
    - Consolidated into the Sample Sets L2 and Level 2 tabs
- CIP-008-R3-L1-02

- Added *“Provide evidence supporting what the entity has considered to be “technology determined to impact the ability to execute the plan.” Has the entity had any changes to such technology during the audit period?”*
- CIP-009-R2-L1-02
  - Modified to address R2 Part 2.2
  - Added *“Provide evidence of each test of a representative sample of information used to recover BES Cyber System functionality and that the information is useable and compatible with current configurations during the audit period.”*
- CIP-009-R2-L1-03
  - Modified from CIP-009-R2-L1-02 to CIP-009-R2-L1-03
- CIP-009-R3-L1-02
  - Added *“For any change to roles and responsibilities, responders, or technology determined to impact the ability to execute the recovery plan provide dated evidence showing:*
    - *The update to the recovery plan(s)*
    - *The notification to each person or group with a defined role in the recovery plan with the corresponding updatesCIP-010-R4-L1-03”*
- CIP-009-R3-L1-03
  - Added *“Provide evidence supporting what the entity has considered to be “technology determined to impact the ability to execute the plan.” Has the entity had any changes to such technology during the audit period?”*
- CIP-010-R2-L1-02
  - Removed Request ID
    - Consolidated into the Sample Sets L2 and Level 2 tabs
- CIP-013-R1-L1-02
  - Modified to CIP-013-R2-L1-01
  - Modified “Requirement” column to “R2”
    - Added *“Provide a listing of each procurement of 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) during the audit period for high and/or medium impact BES Cyber Systems, during the audit period by using the Procurement tab of this spreadsheet.”*
- CIP-013-R1-L1-03
  - Removed Request ID
    - No longer needed

- CIP-013-R3-L1-01
  - Add *“by the CIP Senior Manager or delegate(s)”*
- CIP-014-R1-L1-01
  - Removed *“please”*
  - Modified to *“1. Provide dated results of assessment of substations for applicability under CIP-014-2, to include planned and existing Transmission stations/substations meeting the criteria specified in CIP-014 Section 4.1.1. If provided in an O&P standard please indicate and identify the evidence.*
  - *2. Provide the list of planned and existing Transmission stations/substations that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection. Include a list of primary Control Center(s) that operationally control each identified Transmission station/substation. If provided in an O&P standard please indicate and identify the evidence.”*
- CIP-014-R1-L1-02
  - Removed *“please”*
- CIP-014-R2-L1-01
  - Modified to *“Provide dated results of the third party review of the results of the assessment of substations in R1 for applicability under CIP-014. Include the documented qualifications of the verifying third party, recommendations of the verifying party related to the R1 risk assessments, evidence of modifications pursuant to recommendations, and evidence of procedures implemented to protect sensitive and confidential information.”*
- CIP-014-R3-L1-01
  - Modified to *“Provide dated evidence of notifications or communications that the Transmission Owner notified each Transmission Operator(s), as applicable, according to R3.”*

#### **CA tab**

- Modified *“Included in an OEA or self-log ID(s)?”* column to *“OEA or self-log ID(s)”* column
- Modified *“SS-012-R2-L2-01”* column to *“SS-012-R1-L2-01”*
- Removed *“SS-009-R2-L2-01”* column because it was consolidated in to a Level 1 Request

#### **TCA tab**

- Modified *“TCA Description of Use”* column to *“Description of Use”* column

#### **RM tab**

- Modified *“Asset ID Where Removable Media is Authorized for Use”* column to *“Asset ID Where Used”* column

- Modified “CIP-003-R2-L2-06” to “SS-003-R2-L2-06”

### **Procurement tab**

- Modified “Procurement ID” column to “Unique ID” column
- Removed “Status” column and drop down list
- Added “Planning Start Date” column
- Added “Planning End Date” column
- Modified “Start Date” column to “Procuring Start Date”
- Modified “End Date” column to “Procuring End Date”
- Modified “SS-013-R1-L2-01” column to “SS-013-R2-L2-01”
- Removed “SS-013-R1-L2-02” column

### **Ref tab**

- Removed “Supply Chain” column
- Removed “CA in BCS” from CA Type Column

### **Sample Sets L2 tab**

- SS-003-R2-L2-02
  - Population
    - Modified to “Connected to a Network Via a Routable Protocol?”
- SS-003-R2-L2-06
  - Population
    - Removed “authorized”
    - Description
      - Removed “authorized”
- SS-006-R1-L2-03
  - Source Tab
    - Removed reference to CA
- SS-006-R1-L2-04
  - Source Tab
    - Removed reference to CA
- SS-007-R3-L2-01

- Population
  - Modified to *“Instances of detected malicious code”*
- Description
  - Modified to *“Instances of detected malicious code”*
- SS-009-R2-L2-01
  - Removed this Sample Set because it was consolidated in to a Level 1 Request
- SS-010-R2-L2-02
  - Population
    - Modified to *“Detected unauthorized changes to a bassline configuration”*
  - Description
    - Modified to *“Detected unauthorized changes to a baseline configuration of a Cyber Asset that is a member of, or EACMS or PCA associated with, a high impact BES Cyber System.”*
- SS-010-R3-L2-01
  - Request ID
    - Modified to reference correct request id SS-010-R3-L2-03
- SS-013-R1-L2-01
  - Modified to SS-013-R2-L2-01
  - Request ID
    - Modified to CIP-013-R2-L2-01
  - Population
    - Removed *“with Planning in the “Status” column”*
      - This column was removed from the Procurement tab
    - Modified to *“Unique IDs”*
    - Description
      - Modified to *“Sample of Unique IDs”*
- SS-013-R1-L2-02
  - Removed this Sample Set because there is no longer a *“Status”* column on the Procurement tab

## Level 2 tab

- CIP-003-R2-L2-05
  - Sample Set Evidence Request



- Added *“7. Review to determine whether additional mitigation was necessary and was implemented prior to connecting.”* For CIP-003-8, effective on April 1, 2020.
- CIP-003-R2-L2-06
  - Sample Set Evidence Request
    - Modified *“permitted”* to *“utilized”*
- CIP-007-R2-L2-01
  - Sample Set Evidence Request
    - Added *“and any revisions.”* to d)
    - Added *“3. For instances of no patches being released, indication that an assessment for patches was completed at least every 35 calendar days.”*
- CIP-007-R3-L2-02
  - Sample Set Evidence Request
    - Modified to *“For each instance(s) of detected malicious code during the audit period, provide evidence that the threat of the detected malicious code was mitigated.”*
- CIP-009-R2-L2-01
  - Removed this Request ID because it was consolidated into a Level 1 Request
- CIP-010-R2-L2-02
  - Sample Set Evidence Request
    - Modified to *“For each occurrence(s) of a detected unauthorized change to a baseline configuration during the audit period, provide evidence of the investigation of the occurrence(s), to include:”*
- CIP-010-R3-L2-03
  - Sample Set
    - Modified to reference correct sample set SS-010-R3-L2-01
  - Sample Set Evidence Request
    - Modified to reference correct sample set SS-010-R3-L2-01
    - Added *“and any revisions.”* to 3.
    - Added *“the completion of the”*
- CIP-012-R1-L2-01
  - Sample Set
    - Modified to reference correct sample set SS-012-R1-L2-01
  - Sample Set Evidence Request

- Modified to reference correct sample set SS-012-R1-L2-01
- CIP-013-R1-L2-01
  - Modified to CIP-013-R2-L2-01
  - Requirement
    - Modified to R2
  - Sample Set
    - Modified to SS-013-R2-L2-01
  - Sample Set Evidence Request
    - Modified “Procurement” to “Unique”
    - Modified to reference correct sample set SS-013-R2-L2-01
- CIP-013-R1-L2-02
  - Modified to CIP-013-R2-L2-02
  - Requirement
    - Modified to R2
  - Sample Set
    - Modified to SS-013-R2-L2-01
  - Sample Set Evidence Request
    - Modified “Procurement” to “Unique”
    - Modified to reference correct sample set SS-013-R2-L2-01

## User Guide

- Changed Version 3.0 to 4.0
- Chapter 1: General Instructions
  - Referenced Documents within a Process or Procedure
    - Modified “incident” to “Incident”
- Chapter 2: Level 1 Instructions
  - Request ID
    - Added *“All associated detail tabs that are associated with enforceable CIP Standards should be populated regardless of scope. The Responsible Entity should work with their Region(s) for clarification or exceptions to associated detail tabs.”*
    - Added *“Note: The Request ID abbreviations TFE, CEC, and SRP stand for Technical Feasibility Exception, CIP Exceptional Circumstance, and Standards Requirements Parts.”*
- Chapter 3: Detail Tabs Instructions

- Cyber Asset (CA)
  - Added *“Additionally, CAs could include iDRAC (Integrated Dell Remote Access Controller), iLO (Integrated Lights-Out), Intelligent Platform Management Interface (IPMI), or other management consoles. Include iDRAC(s), iLO(s), IPMI(s), or other management consoles on this tab.”*
  - Included in an Open Enforcement Action (OEA) or self-log?
    - Modified to *“Open Enforcement Action (OEA) or self-log ID(s)”*
    - Added *“If this Cyber Asset is associated with an OEA or self-log, provide the identification number. If the applicable Cyber Asset is associated with more than one ID, include them all. Otherwise leave blank. Use Alt+Enter to break lines of text in a single cell.”*
- Transient Cyber Asset (TCA)
  - TCA Description
    - Modified to *“Description of Use”*
    - Added *“Additionally, provide information if the TCA was used for high, medium, and/or low impact BES Cyber System(s), associated ESP(s), or PCA(s).”*
- Removable Media (RM)
  - Description of Use
    - Added *“Additionally, provide information if the RM was used for high, medium, and/or low impact BES Cyber System(s), associated ESP(s), or PCA(s).”*
- Procurement
  - Modified *“Provide one row for each procurement during the audit period.”* to *“Provide one row for each procurement of 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) during the audit period.”*
  - Procurement ID
    - Modified to Unique ID
    - Added *“For example, a change request ticket identification number, project plan identification number, request for proposal identification number, or “EMS upgrade” could be used.”*
    - Added Planning Start Date
      - \* *“Specify the planning start date associated with this procurement. Otherwise leave blank if the date is unknown.”*
    - Added Planning End Date

- \* *“Specify the planning end date associated with this procurement. Otherwise leave blank if the date is unknown.”*
  - Modified Start Date to Procuring Start Date
    - \* *Added “Specify the procuring start date associated with this procurement. Otherwise leave blank if the date is unknown.”*
  - Modified End Date to Procuring End Date
    - \* *Added “Specify the procuring end date associated with this procurement. Otherwise leave blank if the date is unknown.”*
- Chapter 5
  - Note
    - *Modified to “When submitting Level 2 evidence provide a summary overview of the various pieces of evidence, how/why they were collected and how they fit together to demonstrate compliance. Samples/Examples using the tools and features in PDF such as comment blocks/bubbles lassos, highlighter, arrows, etc. are always helpful. A recommendation is to give the same evidence to someone within your organization who is less familiar with it to determine if you have provided sufficient context or explanation.”*