NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Evidence Request Tool (ERT) v4.0 to v4.5 Change List

June 17, 2020

List of Changes

Instructions tab

- Row 2
  - Changed Version 4.0 to 4.5

Level 1 tab

- CIP-002-R1-L1-03
  - Removed “Special Protection Systems and” from item 6.
  - Added, “neighboring responsible entities” in item 7.
- CIP-004-R1-L1-02
  - Removed “reinforcement materials”
  - Added “security awareness”

BES Assets tab

- Added “SS-012-R1-L2-01” column S for CIP-012

CA tab

- Removed “Real-time Assessment and/or Real-time Monitoring Protected?” column O for CIP-012.
- Removed “SS-012-R1-L2-01” column AR for CIP-012

PSP tab

- Added “SS-007-R1-L2-02” column L for CIP-007 R1 Part 1.2.

CSI tab

- Added, “Was the Incident responding to a Cyber Security Incident that attempted to compromise a system?” to column F for CIP-008-6, effective on January 01, 2021.

Ref tab

- Removed “IP/Serial Converter” from Function column
- Added “Serial/IP Converter” to Function column
- Added “Integrated Dell Remote Access Controller (iDRAC)” to Function column
- Added “Integrated Lights-Out (iLO)” to Function column
- Added “Intelligent Platform Management Interface (IPMI)” to Function column
- Added “Management Console” to Function column

Sample Sets L2 tab

- SS-005-R1-L2-02
  - Population
    - Modified to “BES Cyber Assets not residing within a defined ESP (where "ESP Identifier [If Any]" column is blank on CA tab) that are members of high impact BES Cyber Systems or medium impact BES Cyber Systems”
  - Description
    - Modified to “Sample of BES Cyber Assets not residing within a defined ESP”
- SS-006-R1-L2-03
  - Request ID
    - Removed CIP-007-R1-L2-02
- SS-006-R1-L2-04
  - Request ID
    - Removed CIP-007-R1-L2-02
- SS-007-R1-L2-02
  - Sample Set
    - Added SS-007-R1-L2-02
  - Request ID
    - Added CIP-007-R1-L2-02
  - Source Tab
    - PSP
  - Population

    - Physical Security Perimeters that are associated with PCAs and nonprogrammable communication components located inside both a PSP and an ESP associated with high impact BES Cyber Systems or medium impact BES Cyber Systems at Control Centers
  - Description
    - Physical Security Perimeters that are associated with PCAs and nonprogrammable communication components located inside both a PSP and an ESP associated with high impact BES Cyber Systems or medium impact BES Cyber Systems at Control Centers
- SS-008-R2-L2-02
  - Request ID
    - Added CIP-008-R4-L2-01 for CIP-008-6 R4 Part 4.1
    - Added CIP-008-R4-L2-02 for CIP-008-6 R4 Part 4.2
    - Added CIP-008-R4-L2-03 for CIP-008-6 R4 Part 4.3
- Population
    - Modified to “Reportable Cyber Security Incidents (entries on the CSI tab where "Was the Incident a Test?" is blank and "Was the Incident Reportable?" is TRUE and/or "Was the Incident responding to a Cyber Security Incident that attempted to compromise a system?" is TRUE)”
- Description
    - Modified to “Sample of Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system”
- SS-008-R3-L2-01
  - Request ID
    - Removed CIP-008-R3-L2-02 combined into CIP-008-R3-L2-01
    - Removed CIP-008-R3-L2-03 combined into CIP-008-R3-L2-01
- SS-012-R1-L2-01
  - Source Tab
    - Removed CA
    - Added BES Assets
  - Population
    - Removed “Cyber Assets with TRUE in the "Real-time Assessment and/or Real-time monitoring protected?" column”
    - Added “BES Assets with Control Center in the "Asset Type" column”
  - Description

- Removed "*Cyber Assets*"
- Added "*BES Assets*"

Level 2 tab

- CIP-007-R1-L2-02
  - Sample Set
    - Removed SS-006-R1-L2-03
    - Removed SS-006-R1-L2-04
    - Added SS-007-R1-L2-02
  - Sample Set Evidence Request
    - Removed "*in Sample Sets SS-006-R1-L2-03 and SS-006-R1-L2-04*"
- CIP-008-R2-L2-02
  - Sample Set Evidence Request
    - Modified to *"For each selected Reportable Cyber Security Incident and Cyber Security Incident that attempted to compromise a system in Sample Set SS-008-R2-L2-02, provide evidence that the records related to the Reportable Cyber Security Incident and Cyber Security Incident that attempted to compromise a system were retained."* For CIP-008-86, effective on January 01, 2021.
- CIP-008-R3-L2-01
  - Sample Set Evidence Request
    - Modified to *"For each test of a Cyber Security Incident response plan and each actual Reportable Cyber Security Incident response in Sample Set SS-008-R3-L2-01, provide the following evidence:*
      - *Any lessons learned were documented, or the absence of any lessons learned was documented, and the date of documentation;*
      - *The Cyber Security Incident response plan was updated based on the lessons learned associated with the plan and the date updated; and*
      - *That each person or group with a defined role in the Cyber Security Incident response plan was notified of the update, and the date of notification."*
- CIP-008-R3-L2-02
  - Removed and combined into CIP-008-R3-L2-01
- CIP-008-R3-L2-03
  - Removed and combined into CIP-008-R3-L2-01
- CIP-008-R4-L2-01

- Added CIP-008-R4-L2-01 for CIP-008-6 R4 Part 4.1
- Sample Set Evidence Request
  - *Added "For each selected Reportable Cyber Security Incident and Cyber Security Incident that attempted to compromise a system in Sample Set SS-008-R2-L2-02, provide the following evidence:*
    - The date E-ISAC and NCCIC was notified and updated;
    - The functional impact;
    - The attack vector used; and
    - The level of intrusion that was achieved or attempted."

- CIP-008-R4-L2-02
  - Added CIP-008-R4-L2-01 for CIP-008-6 R4 Part 4.2
  - Sample Set Evidence Request
    - *Added "For each selected Reportable Cyber Security Incident and Cyber Security Incident that attempted to compromise a system in Sample Set SS-008-R2-L2-02, provide the following evidence:*
      - The date the Responsible Entity's determination was made pursuant to the documented process(es) in Requirement R1, Part 1.2,
      - Initial notification to E-ISAC and NCCIC was completed within the following timelines:
        * *One hour after the determination of a Reportable Cyber Security Incident,*
        * *By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system*."

- CIP-008-R4-L2-03
  - Added CIP-008-R4-L2-01 for CIP-008-6 R4 Part 4.3
  - Sample Set Evidence Request
    - *Added "For each selected Reportable Cyber Security Incident and Cyber Security Incident that attempted to compromise a system in Sample Set SS-008-R2-L2-02, provide the following evidence:*
      - The date the Responsible Entity determined new or changed attribute information required in Part 4.1,
      - Updates were provided to E-ISAC and NCCIC within 7 calendar days of the determination."

- CIP-012-R1-L2-01
  - Sample Set Evidence Request

- Removed "*Cyber*"
- Added "*BES Asset*"

User Guide

- Changed Version 4.0 to 4.5
- Chapter 3: Detail Tabs Instructions
  - Cyber Asset (CA)
    - Cyber Asset Classification
      - Removed "*CA in BCS – Cyber Asset that is not a BES Cyber Asset but is included in a BES Cyber System*"
        * Removed "***Real-time Assessment and/or Real-time Monitoring Protected?*** *This column contains a pull-down list. TRUE should be selected if security protection(s) for transmitting Real-time Assessment and Real-time monitoring data between Control Centers is applied to this Cyber Asset. Otherwise leave blank*."
  - Cyber Security Incident (CSI)
    - Added, *"**Was the Incident responding to a Cyber Security Incident that attempted to compromise a system?***
      This column contains a pull-down list. TRUE should be selected if this activation of the CSIRP was due to responding to a Cyber Security Incident that attempted to compromise a system. Otherwise leave blank."