NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Evidence Response Tool (ERT) v2.0 to v3.0 Change List

July 1, 2019

List of Changes

Instructions tab

- Row 1
  - Removed “Version 5 (Revised)”
  - Added “Tool”
- Row 2
  - Removed “<INSERT DATE>, 2019”
- Row 3
  - Removed “EV5R”
  - Added “Tool”
- Row 10
  - Added font red, bold, black box outline
- Row 12
  - Added font red, bold, black box outline
  - Added “The Low CA tab of this spreadsheet is included for those entities that have chosen to have a list. This tab is NOT MANDATORY and is ONLY OPTIONAL.”

Level 1 tab

- Removed Standard Version for all Standards (e.g. CIP-002-5.1a to CIP-002) to accommodate future changes to Versions.
- CIP-002-R1-L1-03
  - Added “for each listed BES asset on the BES Assets tab:”
- CIP-003-R2-L1-07
  - Added this Request ID for CIP-003-7 Section 5
  - Added R2 Sect 5.1

    - Added R2 Sect 5.2
    - Added R2 Sect 5.3
        - Added “Provide all Transient Cyber Asset and Removable Media plans for low impact BES Cyber Systems.”
- CIP-003-R2-L1-08
    - Added this Request ID for CIP-003-7 Section 5
    - Added R2 Sect 5.1
    - Added R2 Sect 5.2
    - Added “For each TCA managed or not managed by the Responsible Entity provide the information requested on the TCA tab.”
- CIP-003-R2-L1-09
    - Added this Request ID for CIP-003-7 Section 5
    - Added R2 Sect 5.3
    - Added “For each location where use of Removable Media is authorized, provide the information requested on the RM tab.”
- CIP-006-R1-L1-03
    - Added “for those instances when cabling and components used for connection between applicable Cyber Assets within the same ESP are located outside of a PSP.”
- CIP-008-R1-L1-02
    - Removed “to the E-ISAC”
- CIP-010-R4-L1-02
    - Added “For each TCA managed or not managed by the Responsible Entity provide the information requested on the TCA tab.” Accommodated the combining of the “TCA” and TCA Non-RE” tabs
- CIP-010-R4-L1-03
    - Removed this Request ID to accommodate the combining of the “TCA” and TCA Non-RE” tabs
- CIP-010-R4-L1-04
    - Changed to Request ID CIP-010-R4-L1-03
- CIP-012-R1-L1-01
    - Added this Request ID for CIP-012-1
    - Added R1

  - Added “Provide each documented plan(s) that addresses the applicable requirement parts in CIP-012 R1.”
- CIP-012-R1-L1-02
  - Added this Request ID for CIP-012-1
  - Added R1
  - Added “Provide evidence of the documented specification for data necessary to perform Real-time Assessments and Real-time monitoring, per IRO-010 and/or TOP-003.”
- CIP-013-R1-L1-01
  - Added this Request ID for CIP-013-1
  - Added R1
  - Added “Provide each documented plan(s) that addresses the applicable requirement parts in CIP-013 R1.”
- CIP-013-R1-L1-02
  - Added this Request ID for CIP-013-1
  - Added R1
  - Added “Provide a listing of all planned procurements 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
  - Added this Request ID for CIP-013-1
  - Added R1
  - Added “Provide a listing of all procurements in effect for high and/or medium impact BES Cyber Systems, during the audit period by using the Procurement tab of this spreadsheet.”
- CIP-013-R3-L1-01
  - Added this Request ID for CIP-013-1
  - Added R3
  - Added “Provide evidence that the documented plan(s) in CIP-013 R1 and its parts were reviewed and approved at least once every 15 calendar months during the audit period. Also provide evidence of the most recent review and approval performed prior to the audit period. Include the date of each review and the results, if any, of the review.”

BES Assets tab

- Column L
  - Added “External Routable Connectivity?”

- Column N
  - Removed “FRCC”

CA tab

- Removed Standard Version for all Standards (e.g. CIP-002-5.1a to CIP-002) to accommodate future changes to Versions.
- Column M
  - Added for CIP-005-6 Parts 2.4-2.5
  - Added “Is Vendor Remote Access Enabled to this CA?”
    - Drop-down with TRUE and a blank as choices.
- Column O
  - Added for CIP-012-1
  - Added “Real-time Assessment and/or Real-time Monitoring Protected?”
    - Drop-down with TRUE and a blank as choices.
- Column Y
  - Removed “FRCC”
- Column AA
  - Removed “active”
- Columns AC-AT
  - Modified to adjust new and revised Sample Sets

Low CA

- Column I
  - Removed “FRCC”

ESP tab

- Column H
  - Removed SS-010-R3-L2-01 (Sample Set was consolidated)

EAP tab

- Column H
  - Removed SS-005-R1-L2-06 (Sample Set was consolidated)

TCA tab

    - Row 1
    - Added “Transient Cyber Assets Managed by the Responsible Entity or by a Party Other Than the Responsible Entity”
- Column C
    - Added “Ongoing/On-demand” as a Drop-down choice
- Column E
    - Added “Managed by”
        - Drop-down with Entity and Other Party as choices.
- Column F
    - Added “Asset ID Where Used”
- Column G
    - Added “For on-demand Cyber Asset ID of BCA/PCA or Low Impact BES Cyber System Accessed”
- Column H
    - Added “"For on-demand Date and Time of Access"
- Column N
    - Removed SS-010-R4-L2-04 (Sample Set was consolidated)

TCA Non-RE tab

- Removed (Data was consolidated in the TCA tab)

Procurement tab

- Added for CIP-13-1
- Column B
    - Added “Procurement ID"
- Column C
    - Added “BES Cyber System Impact Level”
        - Drop-down with High, Medium and High and Medium as choices.
- Column D
    - Added “Description of Products or Services by Vendor or Vendor Transition(s)”
- Column E
    - Added “Status”
        - Drop-down with Planning and Procuring as choices.

- Column F
  - Added “Start Date”
- Column G
  - Added “End Date”
- Column H
  - Added SS-013-R1-L2-01
- Column I
  - Added SS-013-R1-L2-02

Sample Sets L2 tab

- SS-003-R2-L2-04
  - Added this Sample Set for CIP-003-7
  - Added Source Tab “TCA”
  - Added Population “Transient Cyber Assets managed by the Responsible Entity (TCA in the TCA tab with "Entity" in the "Managed By" and "Asset ID" that contains low impact BES Cyber System" columns)”
  - Added Description “Sample of Transient Cyber Assets managed by the Responsible Entity for BES Assets which contain a Low Impact BES Cyber System”
- SS-003-R2-L2-05
  - Added this Sample Set for CIP-003-7
  - Added Source Tab “TCA”
  - Added Population “Transient Cyber Assets not managed by the Responsible Entity (TCA in the TCA tab with "Other Party" in the "Managed By" and "Asset ID" that contains low impact BES Cyber System" columns)”
  - Added Description “Sample of Transient Cyber Assets not managed by the Responsible Entity for BES Assets which contain a Low Impact BES Cyber System”
- SS-003-R2-L2-06
  - Added this Sample Set for CIP-003-7
  - Added Source Tab “RM”
  - Added Population “Locations authorized for Removable Media use (RM in the RM tab with "Asset ID Where Removable Media is Authorized for Use" that contains low impact BES Cyber Systems column)”
  - Added Description “Sample of locations authorized for Removable Media use BES Assets which contain a Low Impact BES Cyber System”

- SS-004-R4-L2-02
  - Column B
    - Added Request ID CIP-004-R4-L2-03
- SS-004-R4-L2-03
  - Removed SS-004-R4-L2-03 (Sample Set was consolidated into SS-004-R4-L2-02)
- SS-004-R4-L2-04
  - Re-numbered to SS-004-R4-L2-03 because of consolidation
- SS-005-R1-L2-02
  - Column D
    - Added “Cyber Assets not connected to an ESP (where "ESP Identifier [If Any]" column is blank on CA tab) that are members of, or PCA associated with, high impact BES Cyber Systems or medium impact BES Cyber Systems”
- SS-005-R1-L2-05
  - Added SS-005-R1-L2-06 (Sample Set was consolidated into SS-005-R1-L2-05)
  - Added Description “Sample of EAPs on ESPs with high impact BES Cyber Systems and/or medium impact BES Cyber Systems located at Control Centers”
- SS-005-R1-L2-06
  - Removed SS-005-R1-L2-06 (Sample Set was consolidated into SS-005-R1-L2-05)
- SS-005-R2-L2-01
  - Column B
    - Added Request ID’s CIP-005-R2-L2-02 and CIP-005-R2-L2-03 (Sample Set was consolidated)
- SS-005-R2-L2-02
  - Added this Sample Set for CIP-005-6
  - Added Request ID’s CIP-005-R2-L2-04 and CIP-005-R2-L2-05
  - Added Source Tab “CA”
  - Added Population “Cyber Assets with TRUE in the "Is vendor remote access enabled to this CA?" column”
  - Added Description “Sample of Cyber Assets accessible via vendor remote access (including Interactive Remote Access and system-to-system remote access)”
- SS-006-R1-L2-02
  - Added Request ID’s CIP-006-R1-L2-07 and CIP-006-R1-L2-08 (Sample Set was consolidated)

- SS-006-R1-L2-04
  - Removed Request ID CIP-006-R1-L2-08 (Sample Set was consolidated)
- SS-010-R1-L2-01
  - Added Request ID CIP-010-R3-L2-02 (Sample Set was consolidated)
  - Removed Request ID CIP-010-R3-L2-03 (Sample Set was consolidated)
- SS-010-R1-L2-02
  - Added this Sample Set for CIP-010-3
  - Added Request ID CIP-010-R1-L2-06
  - Added Source Tab “CA”
  - Added Population “Cyber Assets that are members of a high impact BES Cyber Systems or medium impact BES Cyber Systems”
  - Added Description “Sample of Cyber Assets that are members of a high impact BES Cyber Systems or medium impact BES Cyber Systems”
- SS-010-R4-L2-01
  - Added Population “Transient Cyber Assets managed by the Responsible Entity (TCA in the TCA tab with "Entity" in the "Managed By" and "Asset ID" that contains high or medium impact BES Cyber System" columns)”
- SS-010-R4-L2-02
  - Removed Request ID’s CIP-010-R4-L2-03 and CIP-010-R4-L2-04 (Sample Set was consolidated)
  - Added Population “Transient Cyber Assets managed by the Responsible Entity in an ongoing, on-demand, or combination of both (TCA in the TCA tab with "Entity" in the "Managed By" and "On-going" or "On-demand" or "On-demand/On-going" in the "TCA Management Type" and "Asset ID" that contains high or medium impact BES Cyber System" columns)”
  - Added Description ”Sample of Transient Cyber Assets managed by the Responsible Entity in an in an ongoing, on-demand, or combination of both”
- SS-010-R4-L2-03
  - Removed SS-010-R4-L2-03 (Sample Set was consolidated into SS-010-R4-L2-02)
- SS-010-R4-L2-03
  - Added Source Tab “TCA”
  - Added Population “Transient Cyber Assets not managed by the Responsible Entity (TCA in the TCA tab with "Other Party" in the "Managed By" and "Asset ID" that contains high or medium impact BES Cyber System" columns)”
  - Added Description “Sample of Transient Cyber Assets not managed by the Responsible Entity”

- SS-010-R4-L2-05
  - Re-numbered to SS-010-R4-L2-04 because of consolidation
  - Added Request ID CIP-010-R4-L2-04
  - Removed Request ID CIP-010-R4-L2-12
  - Added Population “Locations authorized for Removable Media use (RM in the RM tab with "Asset ID Where Removable Media is Authorized for Use" that contains high or impact BES Cyber Systems column)”
- SS-012-R1-L2-01
  - Added this Sample Set for CIP-012-1
  - Added Source Tab “CA”
  - Added Population “Cyber Assets with TRUE in the "Real-time Assessment and/or Real-time monitoring protected?" column”
  - Added Description “Sample of Cyber Assets that have security protection applied for Real-time Assessment and Real-time monitoring data between Control Centers”
- SS-013-R1-L2-01
  - Added this Sample Set for CIP-013-1
  - Added Source Tab “Procurement”
  - Added Population “Cyber Assets with Planning in the "Status" column”
  - Added Description “Sample of Cyber Assets that are planned for procurement”
- SS-013-R1-L2-02
  - Added this Sample Set for CIP-013-1
  - Added Source Tab “Procurement”
  - Added Population “Cyber Assets with Planning in the "Status" column”
  - Added Description “Sample of Cyber Assets that are being procured”
- SS-DATE-01
  - Added Request ID’s CIP-007-R4-L2-04 and CIP-007-R4-L2-05 (Sample Set was consolidated)
  - Description
    - Removed word “retention”
- SS-DATE-03
  - Removed SS-DATE-03 (Sample Set was consolidated into SS-DATE-01)
- SS-DATE-04

  - Removed SS-DATE-04 (Sample Set was consolidated into SS-DATE-01)
- SS-DATE-05
  - Re-numbered to SS-DATE-03 because of consolidation
- SS-DATE-06
  - Re-numbered to SS-DATE-04 because of consolidation
  - Added Request ID CIP-010-R1-L2-06 (Sample Set was consolidated)
- SS-DATE-07
  - Re-numbered to SS-DATE-05 because of consolidation

Level 2 tab

- Removed Standard Version for all Standards (e.g. CIP-002-5.1a to CIP-002) to accommodate future changes to Versions.
- CIP-003-R2-L2-01
  - Sample Set Evidence Request
    - Removed "*asset*"
    - Added "*For each low impact BES Cyber System*"
- CIP-003-R2-L2-02
  - Sample Set Evidence Request
    - Removed "asset"
    - Added "For each low impact BES Cyber System"
- CIP-003-R2-L2-03
  - Sample Set Evidence Request
    - Removed "asset"
    - Added "For each low impact BES Cyber System"
- CIP-003-R2-L2-04
  - Added this Request ID for CIP-003-7
  - Added Sample Set Description "Sample of Transient Cyber Assets managed by the Responsible Entity for BES Assets which contain a Low Impact BES Cyber System"
  - Added Sample Set Evidence Request "For the TCA managed in an ongoing, on-demand, or combination of both in Sample Set SS-003-R2-L2-04, provide evidence that each TCA has performed:

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*."

- CIP-003-R2-L2-05
  - Added this Request ID for CIP-003-7
  - Added Sample Set Description "Sample of Transient Cyber Assets not managed by the Responsible Entity for BES Assets which contain a Low Impact BES Cyber System"
  - Added Sample Set Evidence Request ""For each access to a low Impact BES Cyber System by a TCA not managed by the Responsible Entity in Sample Set SS-003-R2-L2-05, provide evidence, including the date and time performed, that each TCA implemented:
    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.*"
- CIP-003-R2-L2-06
  - Added this Request ID for CIP-003-7
  - Added Sample Set Description "Sample of locations authorized for Removable Media use BES Assets which contain a Low Impact BES Cyber System"
  - Added Sample Set Evidence Request ""For each location where use of Removable Media is permitted in Sample Set SS-003-R2-L2-06, provide:
    1. *Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and*
    2. *Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.*"."
- CIP-004-R2-L2-01
  - Sample Set Evidence Request
    - Added "for the audit period"
    - Added "2. Evidence that training was completed at least once every 15 calendar months for all personnel."
- CIP-004-R4-L2-02

- Sample Set Description
  - Fixed and Added Reference "='Sample Sets L2'!E10"

- CIP-004-R4-L2-03
  - Sample Set Description
    - Fixed and Added Reference "='Sample Sets L2'!E10"
  - Sample Set Evidence Request
    - Removed "For each BES Cyber System, EACMS, and PACS in Sample Set SS-004-R4-L2-03, provide:
      1. *Evidence that the authorization records for each enabled user of each Cyber Asset of the BES Cyber System, EACMS, or PACS match the actual implemented permissions.*
      2. *Evidence that evaluations of authorization records against actual account privileges were performed at least once every 15 calendar months for the audit period.*"
- CIP-005-R1-L2-01
  - Sample Set Evidence Request
    - Added "and/or"
- CIP-005-R1-L2-03
  - Sample Set Evidence Request
    - Added "most recent version available"
    - Removed "generated no more than 30 days prior to the date of this request"
- CIP-005-R1-L2-05
  - Sample Set Description
    - Added "Sample of EAPs on ESPs with high impact BES Cyber Systems and/or medium impact BES Cyber Systems located at Control Centers"
  - Sample Set Evidence Request
    - Added "For each EAP in Sample Set SS-005-R1-L2-05, provide evidence that method(s) for detecting known or suspected malicious communications have been implemented."
- CIP-005-R1-L2-06
  - Consolidated Request ID CIP-005-R1-L2-06 into CIP-005-R1-L2-05
- CIP-005-R2-L2-04
  - Added this Request ID for CIP-005-6
  - Sample Set Evidence Request

    - Added “For each Cyber Asset in Sample Set SS-005-R2-L2-02, provide evidence that method(s) for determining active vendor remote access sessions have been implemented.”

- CIP-005-R2-L2-05
  - Added this Request ID for CIP-005-6
  - Sample Set Evidence Request
    - Added “For each Cyber Asset in Sample Set SS-005-R2-L2-02, provide evidence that method(s) to disable active vendor remote access have been implemented.”
- CIP-007-R1-L2-01
  - Sample Set Evidence Request
    - Added “need for”
    - Removed “to be needed”
- CIP-007-R2-L2-01
  - Sample Set
    - Added SS-DATE-04
- CIP-007-R4-L2-04
  - Sample Set
    - Added SS-DATE-01
    - Sample Set Evidence Request
      - Added SS-DATE-01
- CIP-007-R4-L2-05
  - Sample Set
    - Added SS-DATE-01
    - Sample Set Evidence Request
      - Added SS-DATE-01
- CIP-010-R1-L2-01
  - Sample Set
    - Added SS-DATE-03
  - Sample Set Evidence Request
    - Added SS-DATE-03

- CIP-010-R1-L2-02
  - Sample Set
    - Added SS-DATE-04
  - Sample Set Evidence Request
    - Added SS-DATE-04
- CIP-010-R1-L2-03
  - Sample Set
    - Added SS-DATE-04
  - Sample Set Evidence Request
    - Added SS-DATE-04
- CIP-010-R1-L2-04
  - Sample Set
    - Added SS-DATE-04
  - Sample Set Evidence Request
    - Added SS-DATE-04
- CIP-010-R1-L2-05
  - Sample Set
    - Added SS-DATE-04
  - Sample Set Evidence Request
    - Added SS-DATE-04
- CIP-010-R1-L2-06
  - Added this Request ID for CIP-010-3
  - Sample Set
    - Added SS-010-R1-L2-02 and SS-DATE-04
  - Sample Set Evidence Request
    - Added "For each Cyber Asset in Sample Set SS-010-R1-L2-02, for the range of dates in SS-DATE-04, provide the following evidence for each change that deviated from the then-existing baseline configuration for baseline items in Parts 1.1.1, 1.1.2, and 1.1.5:
      1. *The date of the change.*
      2. *Evidence of the verification of:*

1) *The identity of the software source; and*
2) *The integrity of the software obtained from the software source*."

- CIP-010-R2-L2-01
  - Sample Set
    - Added SS-DATE-05
  - Sample Set Evidence Request
    - Added SS-DATE-05
- CIP-010-R3-L2-01
  - Sample Set Evidence Request
    - Removed "and included:
      a) *Network port and Service identification;*
      b) *Vulnerability review or scanning; and*
      c) *Wireless review or scanning*"
- CIP-010-R3-L2-02
  - Sample Set Evidence Request
    - Removed "and included:
      a) *Network discovery; and*
      b) *Wireless review or scanning.*"
- CIP-010-R3-L2-03
  - Sample Set
    - Added SS-010-R3-L2-05
    - Removed SS-010-R1-L2-01
  - Sample Set Evidence Request
    - Removed "and included:
      a) *Network port and Service identification;*
      b) *Vulnerability review or scanning; and*
      c) *Wireless review or scanning*"
- CIP-010-R4-L2-02
  - Requirement
    - Added R4 Sect 1.3, R4 Sect 1.4, and R4 Sect 1.5

- Sample Set Evidence Request
  - Added "For the TCA managed in an ongoing, on-demand, or combination of both in Sample Set SS-010-R4-L2-02, provide evidence that each TCA has performed:
    1) *Software vulnerability mitigation;*
    2) *Mitigation steps to prevent introduction of malicious code; and*
    3) *Methods in place to prevent unauthorized use*."

- CIP-010-R4-L2-03
  - Consolidated Request ID CIP-010-R4-L2-03 into CIP-010-R4-L2-02
- CIP-010-R4-L2-04
  - Consolidated Request ID CIP-010-R4-L2-04 into CIP-010-R4-L2-02
- CIP-010-R4-L2-05
  - Consolidated Request ID CIP-010-R4-L2-05 into CIP-010-R4-L2-02
- CIP-010-R4-L2-06
  - Consolidated Request ID CIP-010-R4-L2-06 into CIP-010-R4-L2-02
- CIP-010-R4-L2-07
  - Consolidated Request ID CIP-010-R4-L2-07 into CIP-010-R4-L2-02
- CIP-010-R4-L2-08
  - Consolidated Request ID CIP-010-R4-L2-08 into CIP-010-R4-L2-02
- CIP-010-R4-L2-03
  - Requirement
    - Added R4 Sect 2.1, R4 Sect 2.2, and R4 Sect 2.3
  - Sample Set
    - Added SS-010-R4-L2-03
  - Sample Set Evidence Request
    - Added "For each access to a BCA/PCA by a TCA not managed by the Responsible Entity in Sample Set SS-010-R4-L2-03, provide evidence, including the date and time performed, that each TCA implemented:
      1) *Software vulnerability mitigation;*
      2) *Mitigation steps to prevent introduction of malicious code; and*
      3) *The determination of whether any additional mitigation actions were necessary, the actions implemented, and the date and time the actions were implemented*."

- CIP-010-R4-L2-10
  - Consolidated Request ID CIP-010-R4-L2-10 into CIP-010-R4-L2-03
- CIP-010-R4-L2-11
  - Consolidated Request ID CIP-010-R4-L2-11 into CIP-010-R4-L2-03
- CIP-010-R4-L2-12
  - Re-numbered to CIP-010-R4-L2-04 because of consolidation
- CIP-012-R1-L2-01
  - Added this Request ID for CIP-012-1
  - Requirement
    - Added R1 Part 1.1, R1 Part 1.2, R1 Part 1.3
  - Sample Set
    - Added SS-012-R2-L2-01
  - Sample Set Evidence Request
    - Added "For each Cyber Asset in Sample Set SS-012-R2-L2-01, for Real-time Assessment and Real-time monitoring data being transmitted between Control Centers, provide the following evidence:
      1) *Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification;*
      2) *Identification of where the Responsible Entity applied security protection for transmitting; and*
      3) *If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission*."
- CIP-013-R1-L2-01
  - Added this Request ID for CIP-013-1
  - Requirement
    - Added R1 Part 1.1
  - Sample Set
    - Added SS-013-R1-L2-01
  - Sample Set Evidence Request
    - Added "For each Cyber Asset in Sample Set SS-013-R1-L2-01, provide evidence of the identification and assessment of cyber security risk(s) to the Bulk Electric System from

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)."

- CIP-013-R1-L2-02
  - Added this Request ID for CIP-013-1
  - Requirement
    - Added R1 Part 1.2
  - Sample Set
    - Added SS-013-R1-L2-02
  - Sample Set Evidence Request
    - Added "For each Cyber Asset in Sample Set SS-013-R1-L2-02, related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity, provide the following evidence:
      1) *Notification by the vendor of vendor-identified incidents;*
      2) *Coordination of responses to vendor-identified incidents;*
      3) *Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*
      4) *Disclosure by vendors of known vulnerabilities;*
      5) *Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*
      6) *Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)."*

User Guide

- Removed Standard Version for all Standards (e.g. CIP-002-5.1a to CIP-002) to accommodate future changes to Versions.
- Renamed CIP Version 5 (Revised) Evidence Request User Guide Version 2.0 to CIP Evidence Request Tool User Guide Version 3.0
  - Changed several references throughout
- Modified Date of User Guide
- Modified Footer with new date and ERT reference
- Updated Table of Contents
- Removed references of FRCC

- Made minor formatting and spacing changes throughout
- Made minor grammar corrections
- Added reference to new Procurement tab
- Section Audit Evidence Submission
  - Added “letter (ANL)”
- Section Referenced Documents within a Process or Procedure
  - Added “Cyber Security”
- Section Request ID
  - Added “Note: A brighter green color is used for Request ID’s that require an associated detailed tab to be populated.”
- Added ”Index
  This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.”
- Modified
  - Location
  - Provide a brief description of the location of the asset, such as city and/or state name, latitude/longitude, or floor within a building
- Modified
  - Connected to a Network Via a Routable Protocol?
  - This column contains a pull-down list. TRUE should be selected if the asset contains any BES Cyber System with connected to a network via a routable protocol communication, or blank if it does not.
- Modified
  - External Routable Connectivity?
  - This column contains a pull-down list. TRUE should be selected if the asset contains any BES Cyber System that has External Routable Connectivity, or blank if it does not.
- Modified
  - Is Dial-up Connectivity present at this asset?
  - This column contains a pull-down list. TRUE should be selected if the asset contains any BES Cyber System that is accessible via Dial-up Connectivity, or blank if it does not.
- Cyber Asset (CA)
  - Added “CIP-002 through CIP-013-1”

- Added
  - Is Vendor Remote Access Enabled to this CA?
  - This column contains a pull-down list. TRUE should be selected if vendor IRA or system-to-system remote access is permitted to this Cyber Asset. Otherwise leave blank.
- Added
  - 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.
- Modified
  - Included in an Open Enforcement Action (OEA) or self-log?
  - This column contains a pull-down list. TRUE should be selected if this Cyber Asset is associated with an OEA or self-log. Otherwise leave blank.
- Modified
  - Physical Security Perimeter (PSP)
  - The PSP tab is requested by Per request CIP-006-R1-L1-02, and contains information about enter each PSP within scope of CIP-006 for which the Responsible Entity has compliance responsibility. Enter each PSP and physical access point(s) identified.
- Modified
  - Transient Cyber Asset (TCA)
  - The TCA tab is requested by CIP-003-R2-L1-08 and CIP-010-R4-L1-02, and contains information about each TCA managed or not managed by the Responsible Entity within the scope of CIP-003 and CIP-010-2 for which the Responsible Entity has compliance responsibility. Provide one row for each TCA managed by the Responsible Entity or a party other than the Responsible Entity during the audit period.
- Modified
  - TCA Management Type
  - This column contains a pull-down list. Select the management type used for this Transient Cyber Asset (Ongoing, or On-demand, or Ongoing/On-demand).
- Removed
  - TCA Non-RE
  - TCA ID
- Modified

  - Managed by
  - This column contains a pull-down list. Select the managed by for this Transient Cyber Asset (Entity or Other Party).
- Modified
  - For on-demand, Cyber Asset ID of BCA/PCA or Low Impact BES Cyber System ID Accessed
  - For on-demand, provide the Cyber Asset ID of the Cyber Asset (as referenced on the CA tab) or the low impact BES Cyber System ID being accessed by the Transient Cyber Asset.
- Modified
  - For on-demand, Date and Time of Access
  - For on-demand, date and time the Transient Cyber Asset accessed the Cyber Asset or low impact BES Cyber System indicated in the "For on-demand, Cyber Asset ID of BCA/PCA or Low Impact BES Cyber System ID Accessed" column.
- Modified
  - Removable Media (RM)
  - The RM tab is requested by CIP-003-R2-L1-09 and CIP-010-R4-L1-04, and contains information about RM within the scope of CIP-003 and CIP-010 for which the Responsible Entity has compliance responsibility. Provide one row for each location where RM is authorized for use.
- Added
  - Procurement
  - The Procurement tab is requested by CIP-013-R1-L1-02 and CIP-013-R1-L1-03, and contains information about each procurement within the scope of CIP-013 for which the Responsible Entity has compliance responsibility. Provide one row for each procurement during the audit period.
  - Index
  - This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.
  - Procurement ID
  - A unique identifier or name associated with the procurement.
  - BES Cyber System Impact Level
  - This column contains a pull-down list. Select either High, Medium, or High and Medium for the impact rating(s) of the BES Cyber System(s) associated with this procurement.
  - Description of Products or Services by Vendor or Vendor Transition(s)

  - Provide a brief description of the products or services or vendor transition(s) associated with this procurement.
  - Status
  - This column contains a pull-down list. Select either Planning or Procuring for the status associated with this procurement.
  - Start Date
  - Specify the start date associated with this procurement.
  - End Date
  - Specify the end date associated with this procurement.
- Section Chapter 4: Sample Sets L2
  - Added “Note: For any system-generated evidence; the Responsible entity should generate evidence in a manner that does not impact Real-Time operations.”