TEXAS RE
Ensuring electric reliability for Texans

CIP Evidence Request Tool v.6

Benjamin Gregson, Texas RE
CIP Cyber and Physical Security Analyst

Evidence Request Tool - General

- Goal of the ERO is to have updated versions to be released at the Q1 of each year as necessary.
- Some of the edits are clarifications learned from field experience. Some are feedback from the Security Working Group (SWG).
- Some of the edits are clarifications to more closely mirror requirement language.
- Some consolidations were made where appropriate.
- Other more specific additions, removals, and modifications are being covered in this presentation.

Addition – CIP-002-R1-L1-08

Provide further details on each Transmission station(s) or substation(s) with both medium and low impact ratings, if any. Specifically, explain in detail how the applicable BES Cyber Systems are physically and logically segmented to ensure that the low impact BES Cyber System cannot impact the BES reliability operating services of the medium impact BES Cyber System.

Addition – CIP-002-R1-L1-09

Explain in detail if and where serial/IP converters are used to convert TCP/IP packets to serial data and serial data to TCP/IP packets.

Modifications to CIP-004-6 R4 Level 1 and Level 2 Requests

- Quarterly reviews in P4.2 and Annual reviews in P4.3 and P4.4 have been moved from Level 2 requests to Level 1 requests.
- Entity evidence to prove compliance has almost exclusively been providing evidence of all reviews anyway. Moving to level 1 is expected to reduce the burden by asking for all instead of sampling on personnel samples.

Addition – CIP-005-R3-L1-01

- **“Provide each documented process that collectively includes each of the applicable requirement parts in CIP-005 R3.”**
- **Standard becomes applicable on October 1, 2022**

Modification – CIP-007-R2-L1-01

Provide each documented process that collectively includes each of the applicable requirement parts in CIP-007 R2. For each applicable Cyber Asset that is updateable and for which a patching source exists, include the identification of a source or sources that are tracked for the release of cyber security patches.

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

Removal of CIP-008-R3-L1-02 and CIP-009-R3-L1-03

- **Incremental value of these requests has been viewed as low from regional perspective (few findings identified related to these).**
- **Entities should consider still having a good answer to these as they could be potential risk areas.**

CIP-008-R3-L1-02	CIP-008	R3 Part 3.2	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-R3-L1-03	CIP-009	R3 Part 3.2	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?

Sample set naming conventions

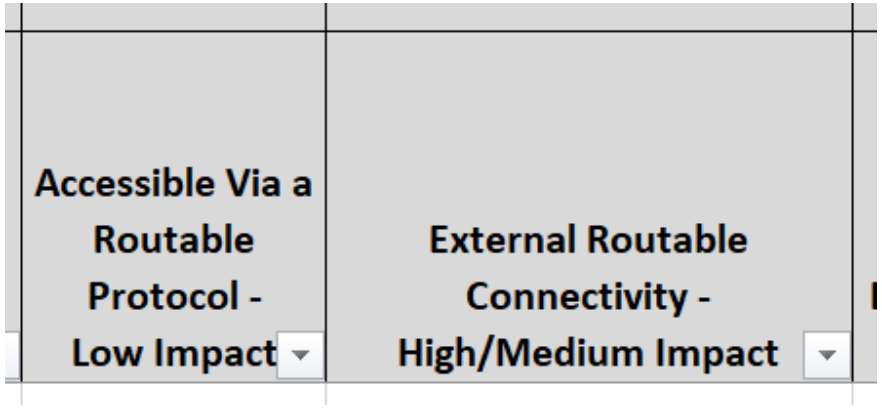
- For example, changed from SS-007-R1-L2-01 to CA-L2-09.
- Sample sets may be linked to more than one standard or requirement, so identifying sample sets based upon the ERT source tab seemed like a more clear means of identifying sample sets going forward.
- This makes it easier to identify duplication in sample sets.

Addition – CIP-004-R2-L2-02

For each individual in Personnel-L2-02, who had authorized electronic access or authorized unescorted physical access to applicable Cyber Assets during the audit period, provide evidence that training was completed at least once every 15 calendar months.

- **Separating out the ongoing periodic training (P2.3) from the training prior to granting access (P2.2)**

Clarification – BES Assets Tab (K&L)



Goal is to clearly separate out Low Impact from High/Medium Impact columns

Modification – ESP and EAP Tabs

- Added column of “Were modifications made to [ESP / EAP] during the audit period?”
- Answer may be TRUE or blank
- Identify risk related to major modifications of infrastructure design (used to help inform sample sets; based on historical compliance issues)

Modifications – Personnel Tab

- **Modified columns N, O, and P modified from dates of access authorization to being TRUE or blank.**
  - Significant input that these dates have been burdensome and required manual insertion
- **Added a column Q for "Was access authorized during the audit period?" Any access, not just initial. Allow filtering for some sample sets.**

Modification – Procurement Tab

- **Added column C to identify the vendor for the specific procurements. This allows better sampling as procurements become more numerous.**

User Guide

- The ERT User Guide has been updated and posted to the NERC website along with the ERT version 6.
- The ERT User Guide provides guidance on how to complete and interpret the meaning of specific questions and fields.

Additional Information

- One-Stop Shop (Compliance Monitoring & Enforcement Program) (nerc.com)
  - Compliance
    - CIP ERT & User Guide
      - CIP Evidence Request Tool User Guide v6
      - CIP Evidence Request Tool v6
      - CIP Evidence Request Tool v6 Changes

Any comments or concerns can be directed to Texas RE at:

CIP@TEXASRE.org

TEXAS RE
Ensuring electric reliability for Texans