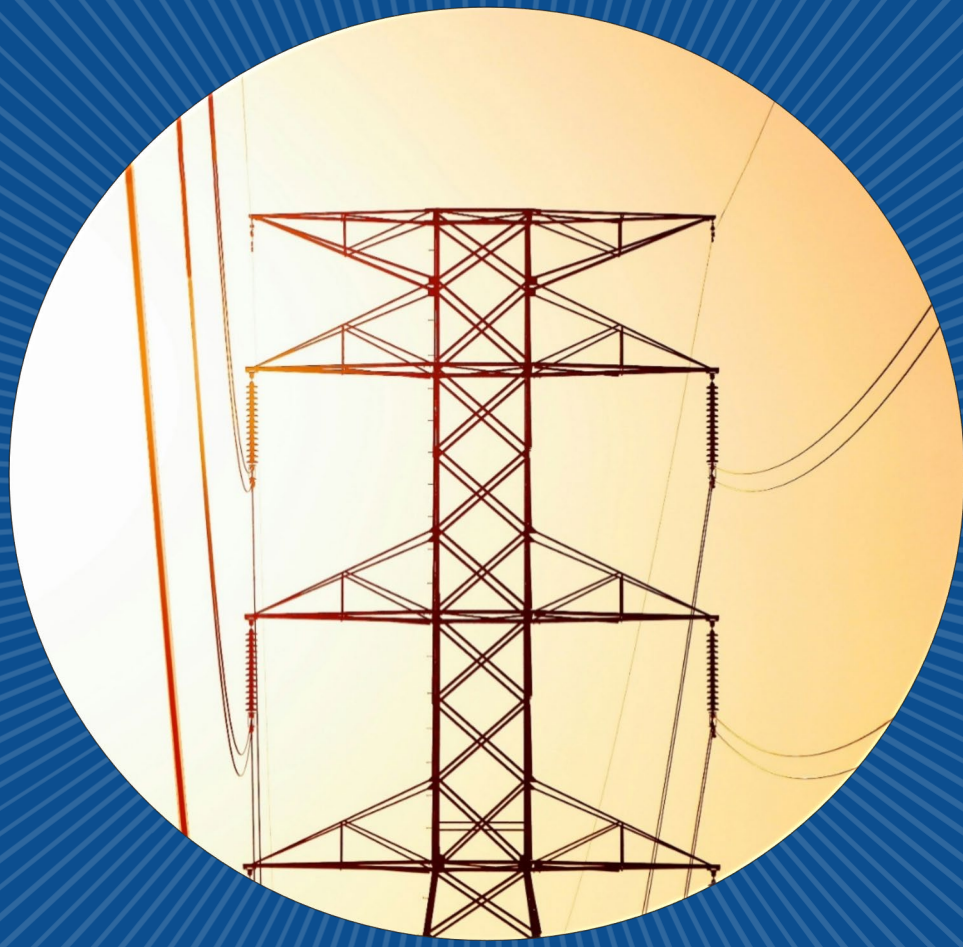
NPCC

CIP Evidence Request Tool (ERT) Overview



Compliance Monitoring & Enforcement

Spring 2026

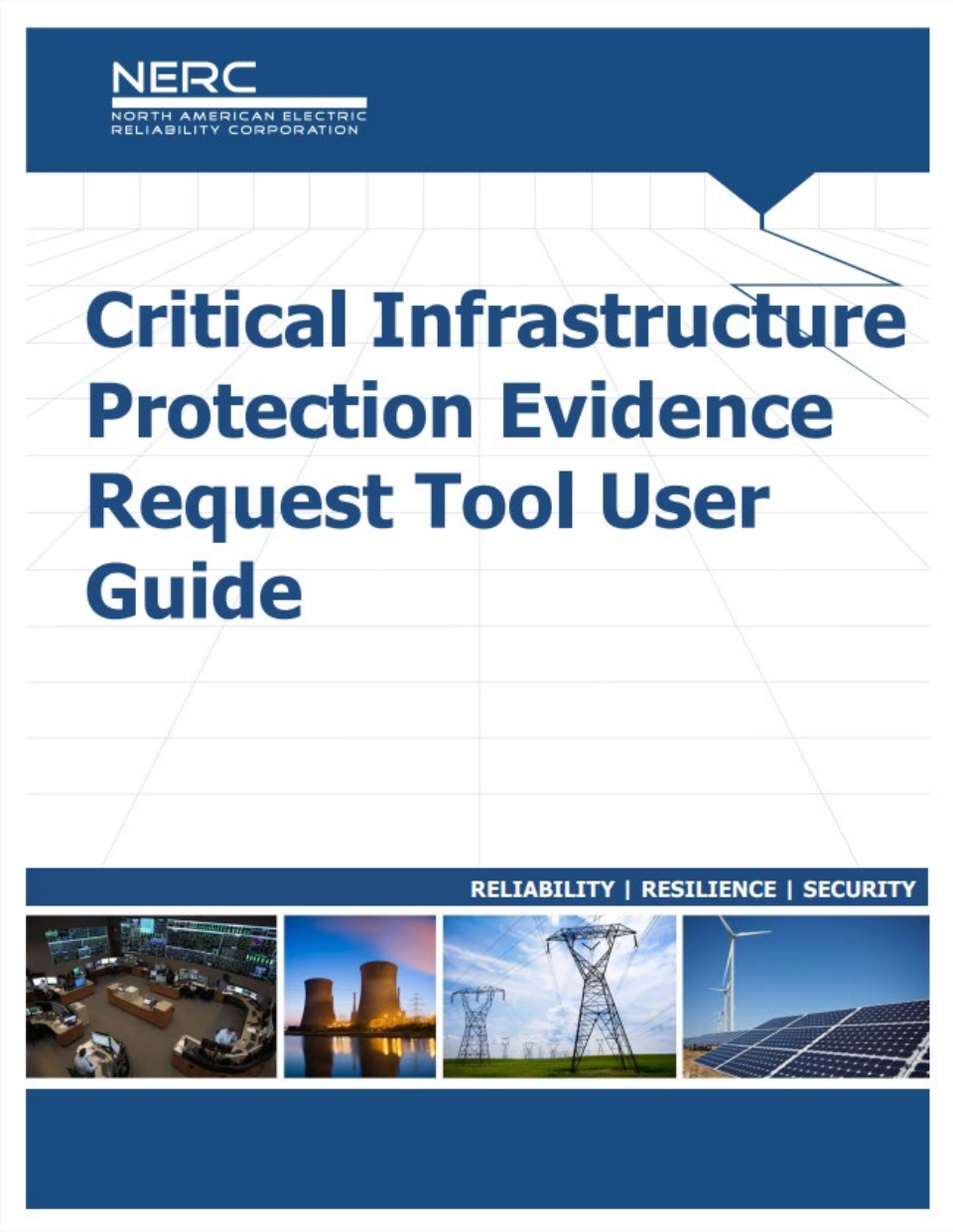
Public

Overview

- CIP ERT v10 User Guide
- Using the ERT
- Submitting the ERT & Responses
- Common Issues
- Tips for Evidence
- Resources
- Questions

CIP ERT v10 User Guide

- Key resource when completing the ERT
- Sent with Audit Notification Package (ANP)
- Available on NERC's Website



Using the ERT:
Level 1 – Initial Evidence Request

Detail Tab or Request ID	Standard	Requirement	Evidence Request
BES Assets	CIP-002 CIP-003 CIP-012		Provide a listing of all BES assets, select type from the drop down list in the *Asset Type* field, in service during the audit period for which you have or share compliance responsibility by using the BES Assets tab of this spreadsheet. Include data center(s) associated with each Control Center.
CA	CIP-002 CIP-005 CIP-006 CIP-007 CIP-010		Provide a listing of all Applicable Systems that are included in or associated with a high or medium impact BES Cyber System on the CA tab of this spreadsheet, ensure to include VMs and their associated host or cluster.
Low CA	CIP-002		Provide evidence of BES Cyber Assets that are included in or associated with low impact BES Cyber System, one-line diagrams, network configuration files, or other documentation. 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.
Personnel	CIP-004		Provide a complete listing of individuals who are currently, or have been at any time during the audit period, authorized for: 1. electronic access; 2. unescorted physical access; 3. provisioned access to BCSI, whether physical or electronic, for BCSI, using the Personnel Tab.
ESP	CIP-005		Provide a list of all defined Electronic Security Perimeters (ESPs) in the ESP tab of this spreadsheet.
EAP	CIP-005		Provide a list of all Electronic Access Points (EAPs) and identify the interfacing ESP(s) and its configured EACMS on the EAP tab.
PSP	CIP-006		Provide a list of Physical Security Perimeters (PSPs) and physical access points on the PSP tab.

Figure 1: Level 1 Tab of the ERT

- Approximately 100 requests, depending upon scope
- Documentation-focused:
  - Policies
  - Programs
  - Procedures
  - Diagrams
  - Configurations
  - Other supporting documentation
- Bright Green rows indicate there is an accompanying tab to be completed

Using the ERT: Level 1 – Sampling Population Tabs

- Approximately 13 Sampling Populations, depending upon scope
- Each population has a tab that must be completed. All fields within each tab should be completed or left blank as appropriate
  - For requests associated with standards or requirements that are not in scope for the audit, simply state “Not in scope”
- The CIP Evidence Request Tool User Guide (hosted on the NERC website) has detailed instructions for completing each tab
- Ensure all True/False drop-downs and pick list selections are reviewed for accuracy
- When in doubt, reach out to your Audit Team Lead (ATL) for clarification

Figure 2: Tabs Used For Sampling

Using the ERT: NPCC Tab

NCR # NCR00000 Align Engagement # ME25-00000

Level	RFI #	Standard	Req.	Internal Control Question	CURRENT Auditor Request	Entity Response	Document Reference
2	CP1	CIP-002-5.1a	R1		For any High or Medium impact BES assets, explain in detail, if consideration was given to VoIP, UPS, and HVAC Cyber Assets, or any other supporting system for BES Cyber Systems, for CIP-002 applicability.		
2	CP2	CIP-002-5.1a	R1		Provide any letters or documents from your RC/ISOs notifying you that any of your generators and/or Transmission Facilities meet Attachment 1 - Criteria 2.3, 2.6 or 2.9. If no notifications were made, a letter or document from the RC/ISOs supporting this is required.		
2	CP3	CIP-002-5.1a	R1		Are there Cyber Assets utilized by operators at Control Centers that are not categorized as BES Cyber Assets? If so, list them, explain their function, justification for categorization and impact rating assigned, and the BES asset they are located at.		
2	CP4	CIP-003-8	R2		Provide a detailed narrative around how protections for Low Impact BCS are applied to permit *only necessary* inbound and outbound electronic access.		
2	CP5	CIP-003-8	R2		If utilizing a Medium or High impact incident response plan for Low Impact BES Cyber Systems, provide a narrative explaining the relationship between the roles and responsibilities of the plan and how it incorporates the Low Impact Cyber Systems.		
2	CP6	CIP-005-7	R1		If applicable, please describe the communication protocols used for any external connectivity (routable and/or non-routable) in use at High and Medium Impact assets.		

Level 1 | Sample Sets L2 | Level 2 | Sample Sets Table | NPCC | BES Assets | CA | Low CA | ESP

Figure 3: NPCC Tab

- The NPCC tab is used during the level 2 of the audit process by the Audit Team to request additional information outside of the standard Level 1 and Level 2 tabs
- Begins being utilized at Level 2 and continues to be used throughout the audit
- Each request is assigned a unique RFI# & SEL ID

Using the ERT: Sampling Process Overview

The audit team generates Level 2 sampled indexes, dates & date ranges based off the Level 1 ERT data provided by the entity

Samples are selected according to the population Filtering Instructions in the Sample Sets L2 tab

All sampling is performed in accordance with the Electric Reliability Organization (ERO) Sampling Handbook

	BCSI-L2-01	BES-Assets-L2-01	BES-Assets-L2-02	BES-Assets-L2-03	BES-Assets-L2-04
Population Size	5	23	7	19	16
Sample Size	5	16	7	9	9
SAMPLES					
1	1	1	1	5	6
2	2	7	3	8	7
3	3	8	5	9	12

Formulas are used to auto-populate sampled indexes and dates from the Sample Sets Table tab into the Level 2 tab

Sample Set Evidence Request
For each BES asset containing a low impact BES Cyber System in Index Sample Set BES-Assets-L2-01, provide evidence that physical security controls were implemented to control physical access, based on need as determined by entity, to: 1. The asset or the locations of the low impact BES Cyber Systems within 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.

Population Filtering Instructions
"Low Impact" = TRUE
"Low Impact" = TRUE "Low Routable" = TRUE
"Low Impact" = TRUE "Dial-up Connectivity" = TRUE

The audit team populates sampled indexes, dates, and date ranges into the Sample Sets Table tab

Sample Set Index Numbers
1, 7, 8, 22, 23, 25, 31, 36, 37, 38, 41, 42, 45, 48, 55, 61

Entities then respond to each applicable evidence request within the Level 2 tab

Submitting the ERT & Responses: Naming Conventions

- Each line of the Level 1 and Level 2 tabs contains a “Request ID,” which uniquely identifies each request
- The Request ID Syntax is structured as follows:
  - Three-digit CIP Reliability Standard number
  - Standard version number
  - Requirement number within the Standard
  - Level of the evidence request (either “L1” for Level 1, or “L2” for Level 2
  - Two-digit request index, unique to each Standard, Requirement and Level

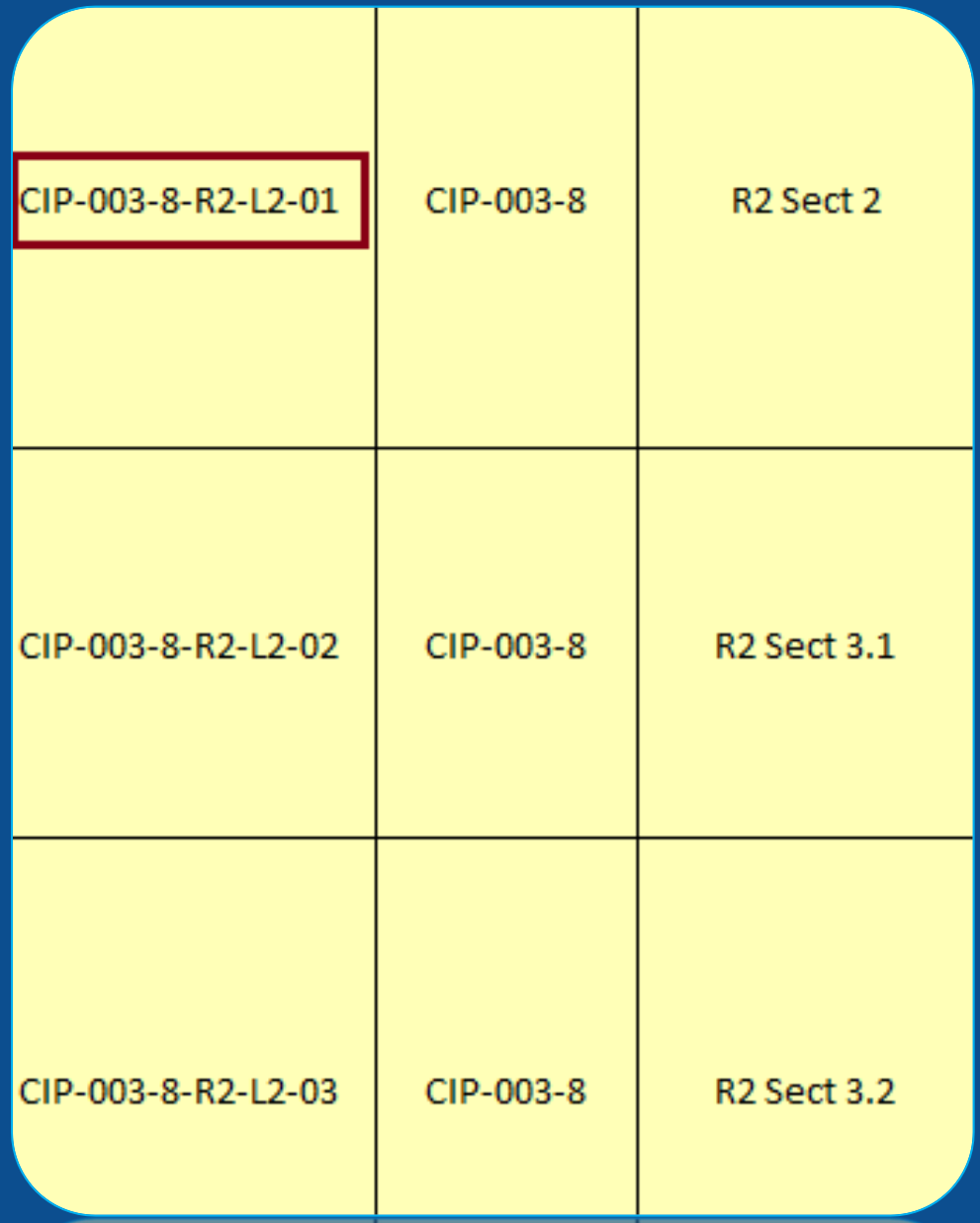
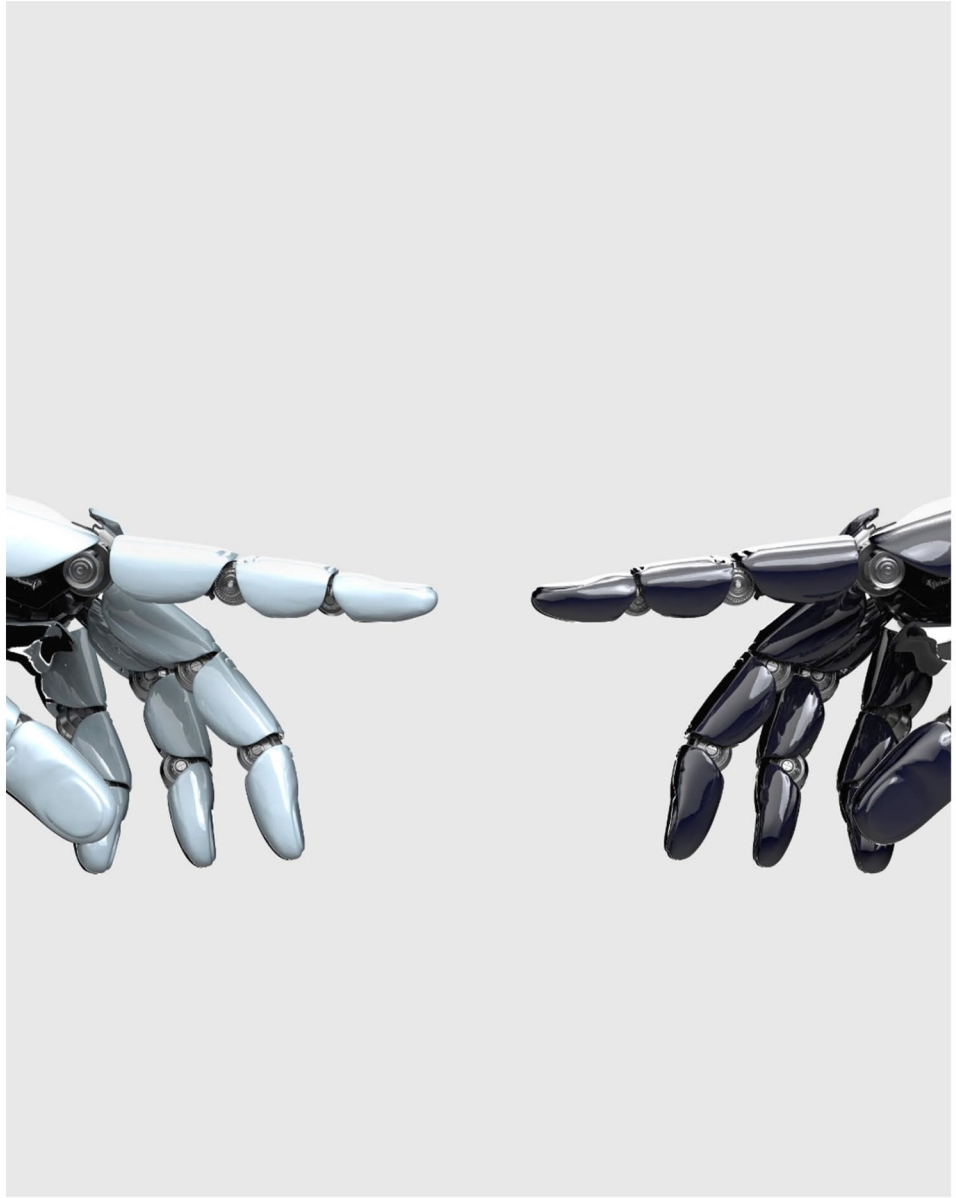


Figure 4: Request ID Syntax

Submitting the ERT & Responses: Secure Evidence Locker (SEL)

- Ensure that all evidence is submitted to the appropriate SEL ID provided within the Level 1, Level 2, and NPCC tabs
- The ERT itself should be uploaded to the “General” SEL ID for the engagement (provided in Align)



ERT Common Issues

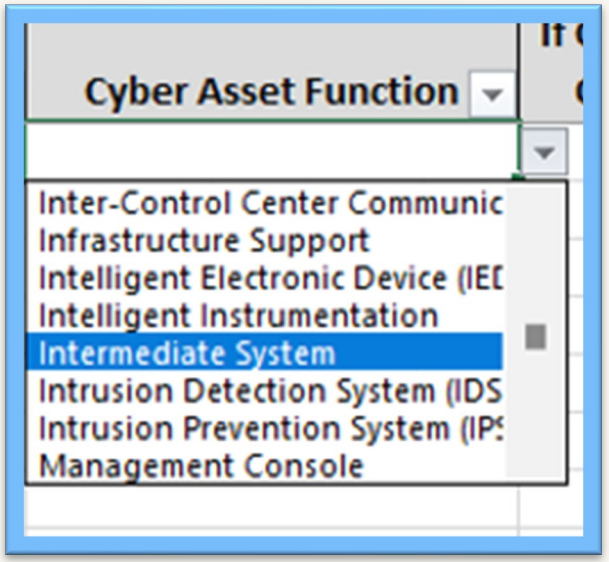


Figure 5: Cyber Asset Function drop-down list

- Verify that all Intermediate Systems have been identified for audit engagements where CIP-005 R2 is in scope

ERT Common Issues Cont'd

- Ensure responses to the Level 1 and Level 2 tabs match the CIP Standard version being audited

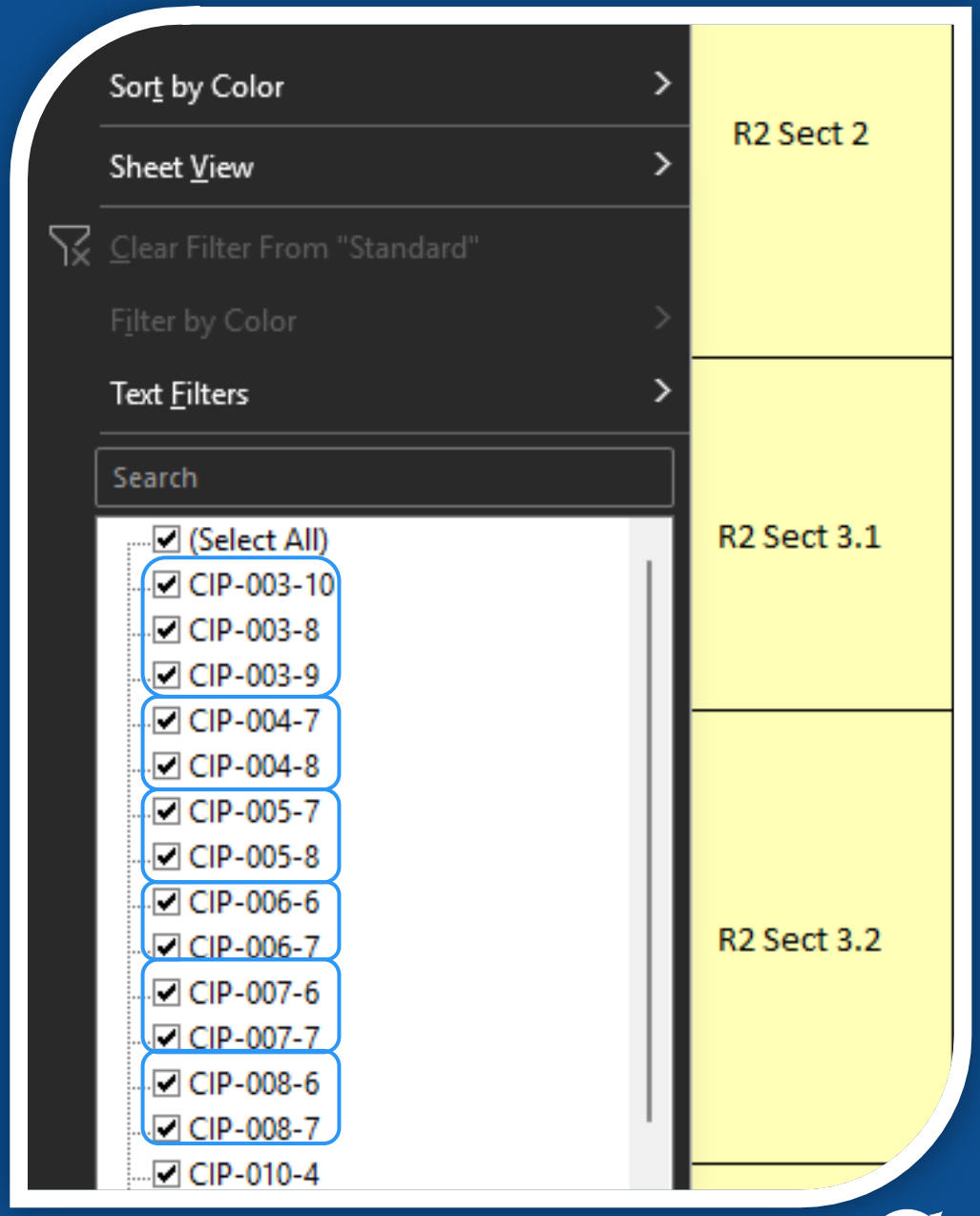


Figure 6: Various Standard Versions

ERT Common Issues Cont'd

Level 1 General Requests:

Often overlooked, be sure to respond to them

Detail Tab or Request ID	Standard
CIP-TFE-L1-01	All Standards
CIP-CEC-L1-01	All Standards
CIP-SRP-L1-01	All Standards
CIP-EOL-L1-01	All Standards

Complete & Accurate ESP Tab:

Ensure that all IP-based networks containing BCAs and PCAs are listed

B	C	D
	CONFIDENTIAL	
	Electronic Security Perimeter(s)	
ID	Description	Address Spaces

Sufficient EAP Tab Data:

Content from the ESP tab, column B (ESP ID), should be used to populate the EAP tab, column E (ESP ID)

C	D	E
CONFIDENTIAL		
Electronic Access Points		
IP Addresses	EACMS ID	ESP ID

Tips for Evidence

- Submit supporting narrative documents describing how each evidence file meets compliance
- Annotate screenshot/photographic evidence
- For larger file quantities, include a matrix indicating which files address specific requests
- Include the L1, L2 or CP Request ID in the name of each evidence file
- Verify the accuracy of all data provided within all applicable tabs

Resources

- ERT v10: https://www.nerc.com/globalassets/programs/compliance/cmep-resources/cip-evidence-request-tool-master-v10.xlsx
- ERT v10 User Guide: https://www.nerc.com/globalassets/programs/compliance/cmep-resources/cip-evidence-request-tool-user-guide-v10.pdf
- ERT v10 Release Notes: https://www.nerc.com/globalassets/programs/compliance/cmep-resources/cip-evidence-request-tool-release-notes-v10.pdf

NPCC

Questions?

Contact Us: npcc.org/contact

Compliance Monitoring & Enforcement