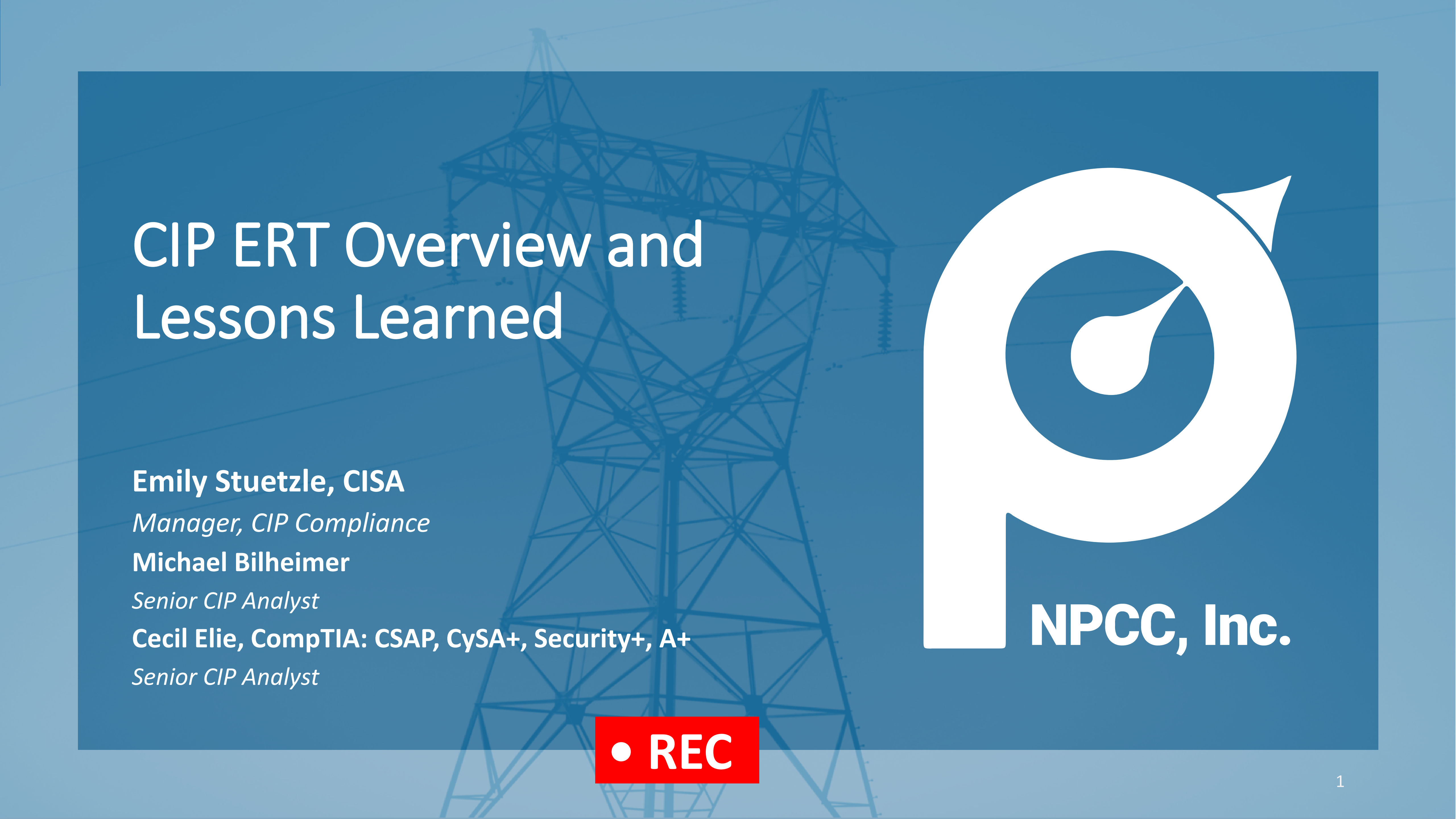


# CIP ERT Overview and Lessons Learned

**Emily Stuetzle, CISA**

*Manager, CIP Compliance*

**Michael Bilheimer**

*Senior CIP Analyst*

**Cecil Elie, CompTIA: CSAP, CySA+, Security+, A+**

*Senior CIP Analyst*

NPCC, Inc.

● REC

# Agenda

Tool Overview

Engagement Timeline

v7 Update

Common Errors

CIP-014 Evidence Options

Future SEL Integration

Demo and Tab Notes

# CIP ERT Tool Overview

| | |
|---|---|
| What is it? | • The Evidence Request Tool is an elaborate Excel workbook used to communicate and organize CIP compliance evidence |
| Who develops and updates it? | • An ERO team with representatives from each region and NERC |
| How often are new versions published? | • Annually |
| How are changes proposed? | • Members of the ERT team provide suggested improvements using input from the region and registered entities |
| Are RSAWs still required? | • Yes |

# NPCC ERT Subgroup Members

Emily Stuetzle

estuetzle@npcc.org

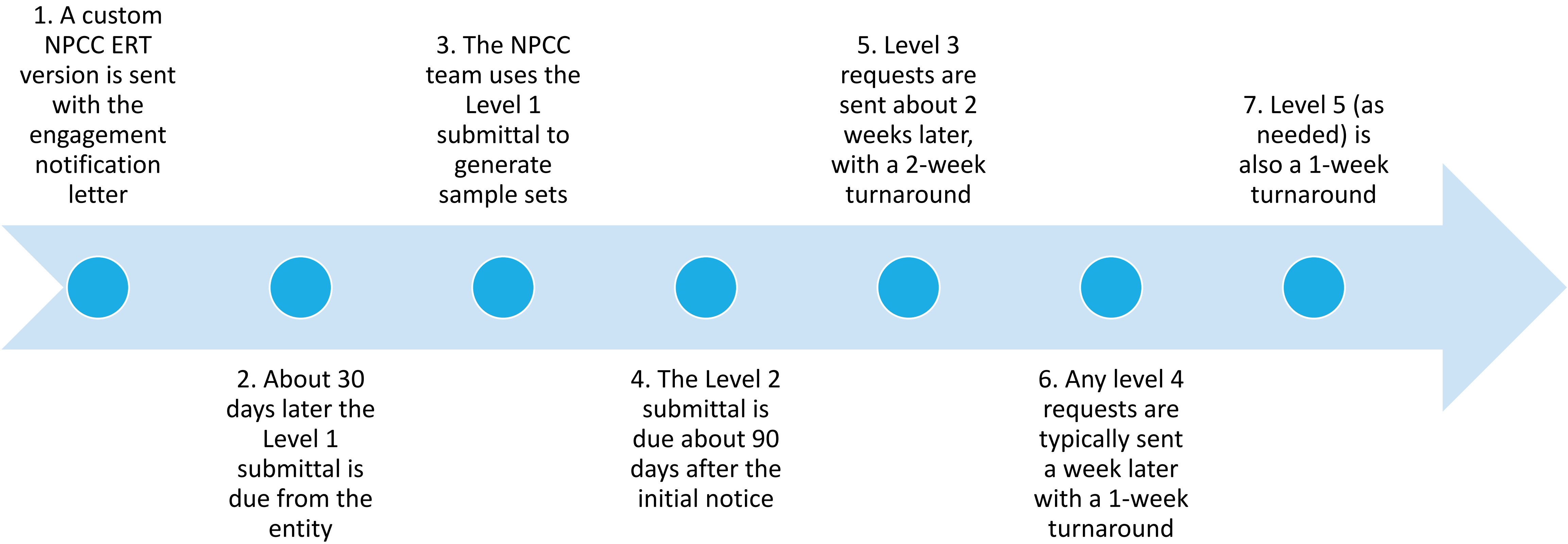
Cecil Elie

celie@npcc.org

Anil Rauniyar

arauniyar@npcc.org

# CIP ERT Engagement Timeline



1. A custom NPCC ERT version is sent with the engagement notification letter

2. About 30 days later the Level 1 submittal is due from the entity

3. The NPCC team uses the Level 1 submittal to generate sample sets

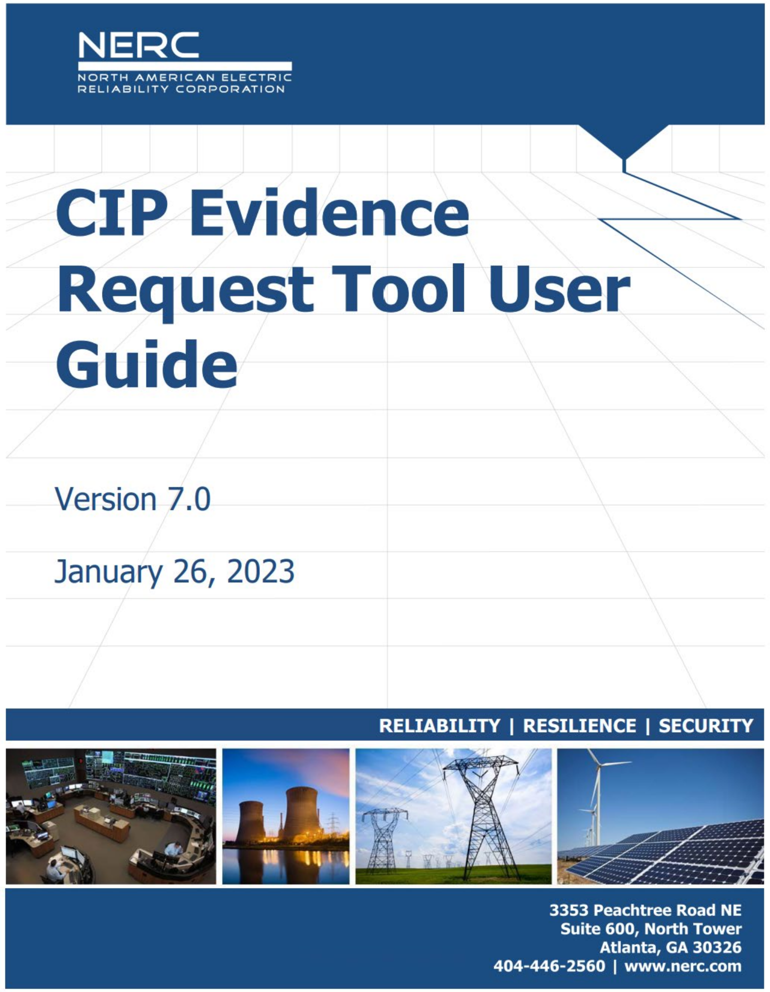
4. The Level 2 submittal is due about 90 days after the initial notice

5. Level 3 requests are sent about 2 weeks later, with a 2-week turnaround

6. Any level 4 requests are typically sent a week later with a 1-week turnaround

7. Level 5 (as needed) is also a 1-week turnaround

# CIP ERT v7 Update



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Evidence Request Tool User Guide

Version 7.0

January 26, 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

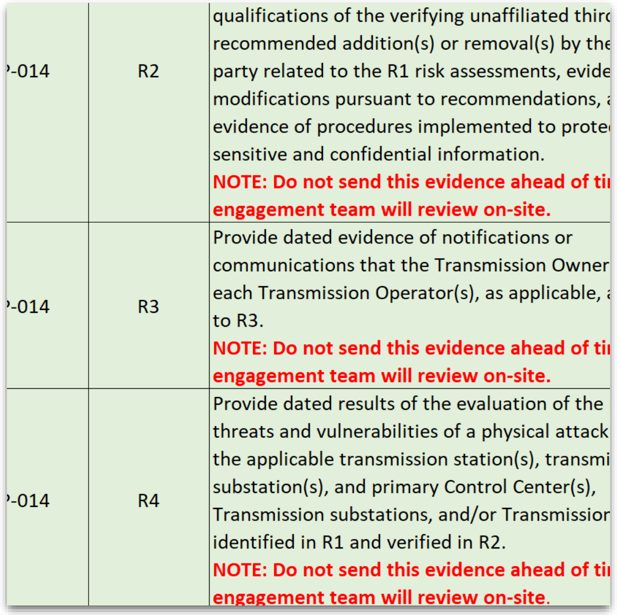
Guide and ERT sent with audit notification package

Both available on the NERC website

[CIP ERT Version 7.0 User Guide]

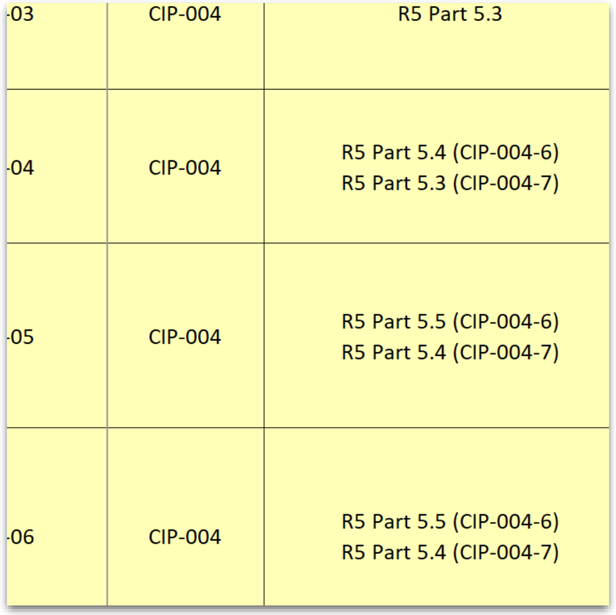
**[v6.0 to v7.0 Change List]**

# CIP ERT v7 Update



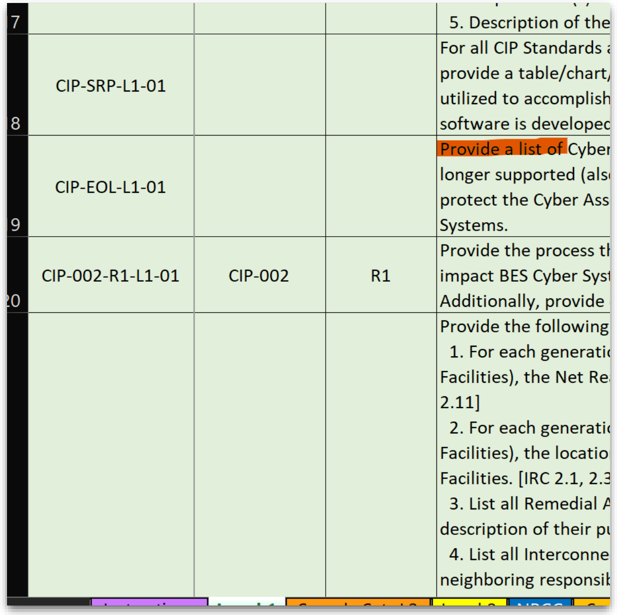
| | | |
|---|---|---|
| -014 | R2 | qualifications of the verifying unaffiliated thir recommended addition(s) or removal(s) by the party related to the R1 risk assessments, evide modifications pursuant to recommendations, evidence of procedures implemented to prote sensitive and confidential information.<br>**NOTE: Do not send this evidence ahead of ti engagement team will review on-site.** |
| -014 | R3 | Provide dated evidence of notifications or communications that the Transmission Owner each Transmission Operator(s), as applicable, to R3.<br>**NOTE: Do not send this evidence ahead of ti engagement team will review on-site.** |
| -014 | R4 | Provide dated results of the evaluation of the threats and vulnerabilities of a physical attack the applicable transmission station(s), transmi substation(s), and primary Control Center(s), Transmission substations, and/or Transmissior identified in R1 and verified in R2.<br>**NOTE: Do not send this evidence ahead of ti engagement team will review on-site.** |

Removed the CIP-014 "NOTE: Do not send this evidence ahead of time…" and added/edited requests for all CIP-014



| | | |
|---|---|---|
| -03 | CIP-004 | R5 Part 5.3 |
| -04 | CIP-004 | R5 Part 5.4 (CIP-004-6)<br>R5 Part 5.3 (CIP-004-7) |
| -05 | CIP-004 | R5 Part 5.5 (CIP-004-6)<br>R5 Part 5.4 (CIP-004-7) |
| -06 | CIP-004 | R5 Part 5.5 (CIP-004-6)<br>R5 Part 5.4 (CIP-004-7) |

Added requests for future CIP-004-7 and CIP-011-3 and added instructions for a few existing requests



| | | | | |
|---|---|---|---|---|
| 7 | | | | 5. Description of the |
| 8 | CIP-SRP-L1-01 | | | For all CIP Standards provide a table/chart, utilized to accomplish software is developec |
| 9 | CIP-EOL-L1-01 | | | Provide a list of Cyber longer supported (als protect the Cyber Ass Systems. |
| 20 | CIP-002-R1-L1-01 | CIP-002 | R1 | Provide the process th impact BES Cyber Syst Additionally, provide |
| | | | | Provide the following<br>1. For each generati Facilities), the Net Re 2.11]<br>2. For each generati Facilities), the locatio Facilities. [IRC 2.1, 2.3<br>3. List all Remedial A description of their pu<br>4. List all Interconne neighboring responsi |

Very minor wording changes for better clarity throughout

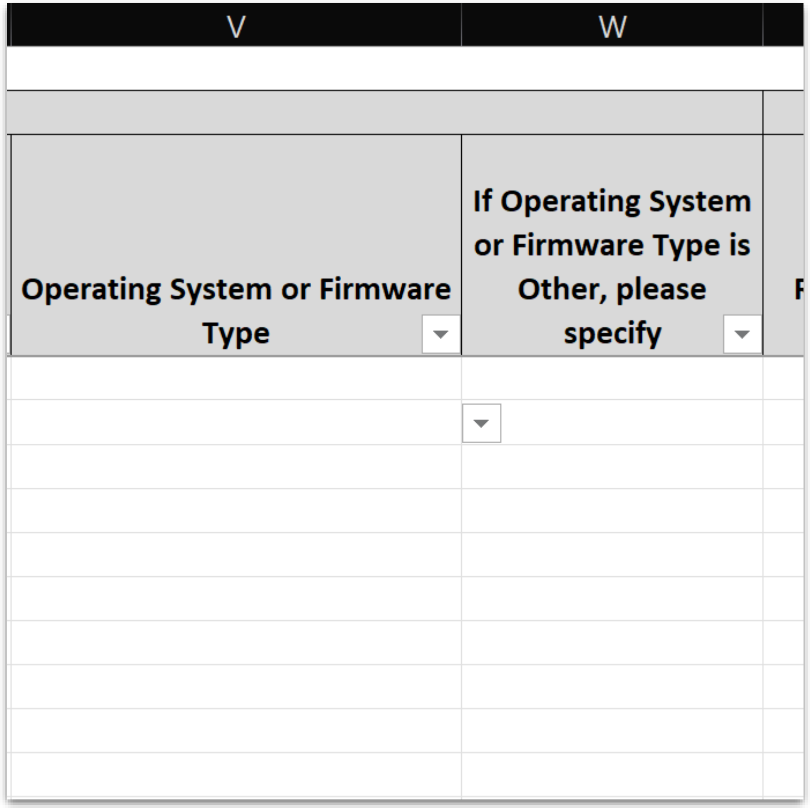
# CIP ERT v7 Update

## CIP-014 R1 Level 1 Request Changes

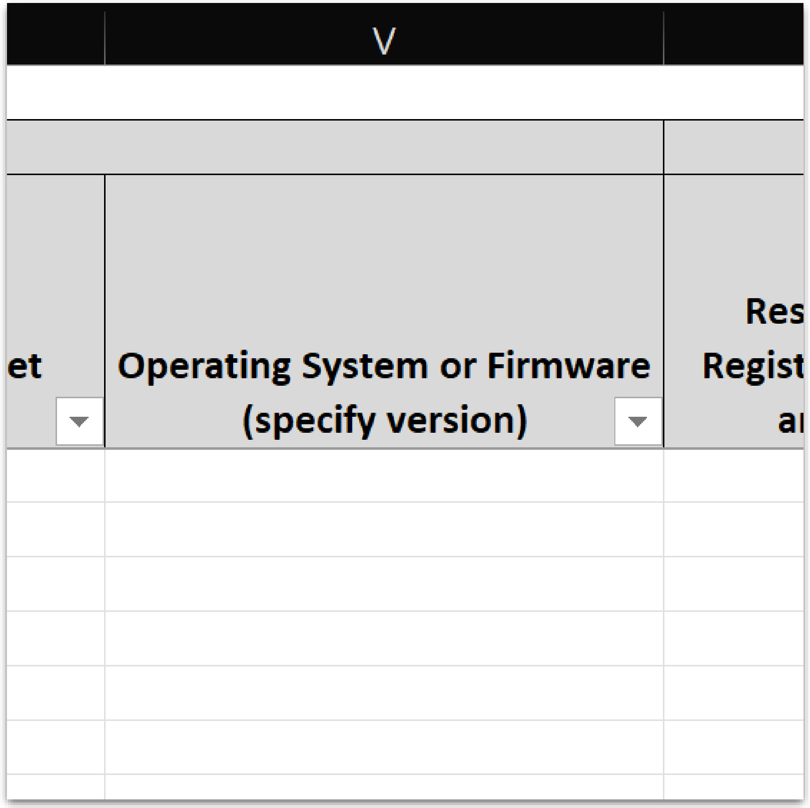
| v6 | | v7 | | Note |
|---|---|---|---|---|
| | | CIP-014-R1-L1-01 | | Moved from 2 to 1 and greatly expanded upon |
| CIP-014-R1-L1-01 | | CIP-014-R1-L1-02 | | Moved from 1 to 2 |
| CIP-014-R1-L1-02 | | | | |
| | | CIP-014-R1-L1-03 | | New request |
| | | CIP-014-R1-L1-04 | | New request |
| | | CIP-014-R1-L1-05 | | New request |

# CIP ERT v7 Update

## CA tab change



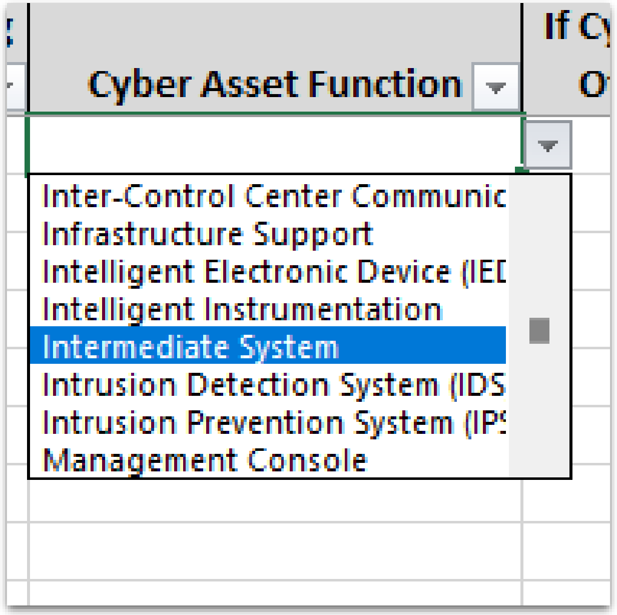
| V | W | |
|---|---|---|
| Operating System or Firmware Type | If Operating System or Firmware Type is Other, please specify | F |



| | V | |
|---|---|---|
| et | Operating System or Firmware (specify version) | Res Regist ar |

Changed the operating system column to be free-form and removed the column for "if OS type is other"

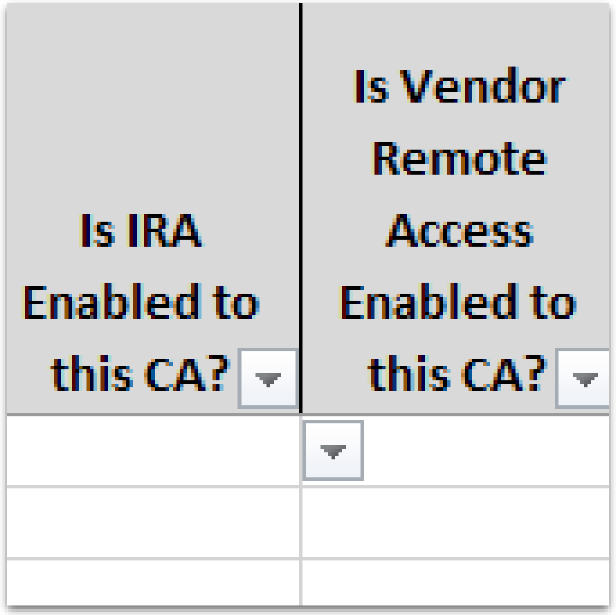
# ERT Common Errors



| Cyber Asset Function | If Cy<br>O |
|---|---|
| | |

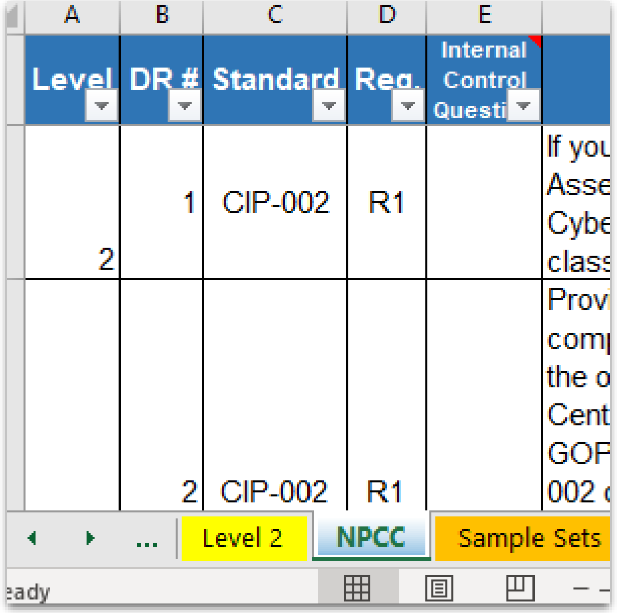
- Inter-Control Center Communic
- Infrastructure Support
- Intelligent Electronic Device (IEI
- Intelligent Instrumentation
- Intermediate System
- Intrusion Detection System (IDS
- Intrusion Prevention System (IPS
- Management Console

Cyber Asset Function – Intermediate System



| Is IRA Enabled to this CA? | Is Vendor Remote Access Enabled to this CA? |
|---|---|
| | |
| | |
| | |

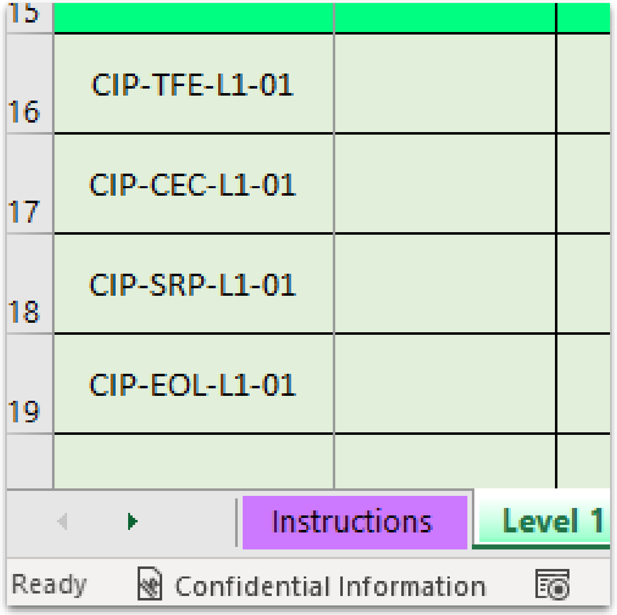
Is IRA Enabled to this CA?



| A | B | C | D | E | |
|---|---|---|---|---|---|
| Level | DR # | Standard | Req. | Internal Control Questi | |
| 2 | 1 | CIP-002 | R1 | | If you<br>Asse<br>Cybe<br>class |
| | 2 | CIP-002 | R1 | | Prov<br>comp<br>the o<br>Cent<br>GOP<br>002 c |

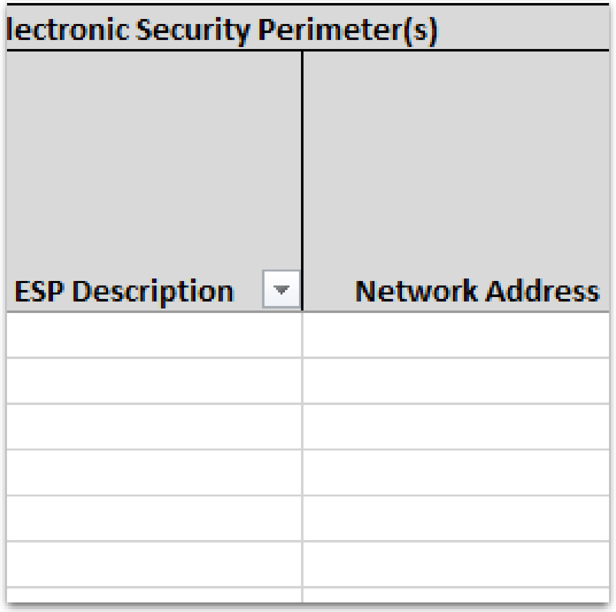
NPCC tab Level 2 requests

# ERT Common Errors



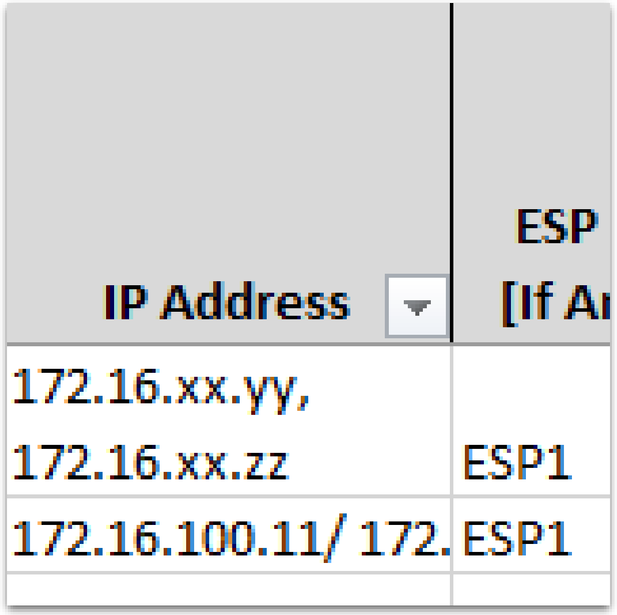
| | | | |
|---|---|---|---|
| 15 | | | |
| 16 | CIP-TFE-L1-01 | | |
| 17 | CIP-CEC-L1-01 | | |
| 18 | CIP-SRP-L1-01 | | |
| 19 | CIP-EOL-L1-01 | | |
| | | | |

Missing the four general Level 1 requests



| lectronic Security Perimeter(s) | |
|---|---|
| ESP Description | Network Address |
| | |
| | |
| | |
| | |
| | |
| | |

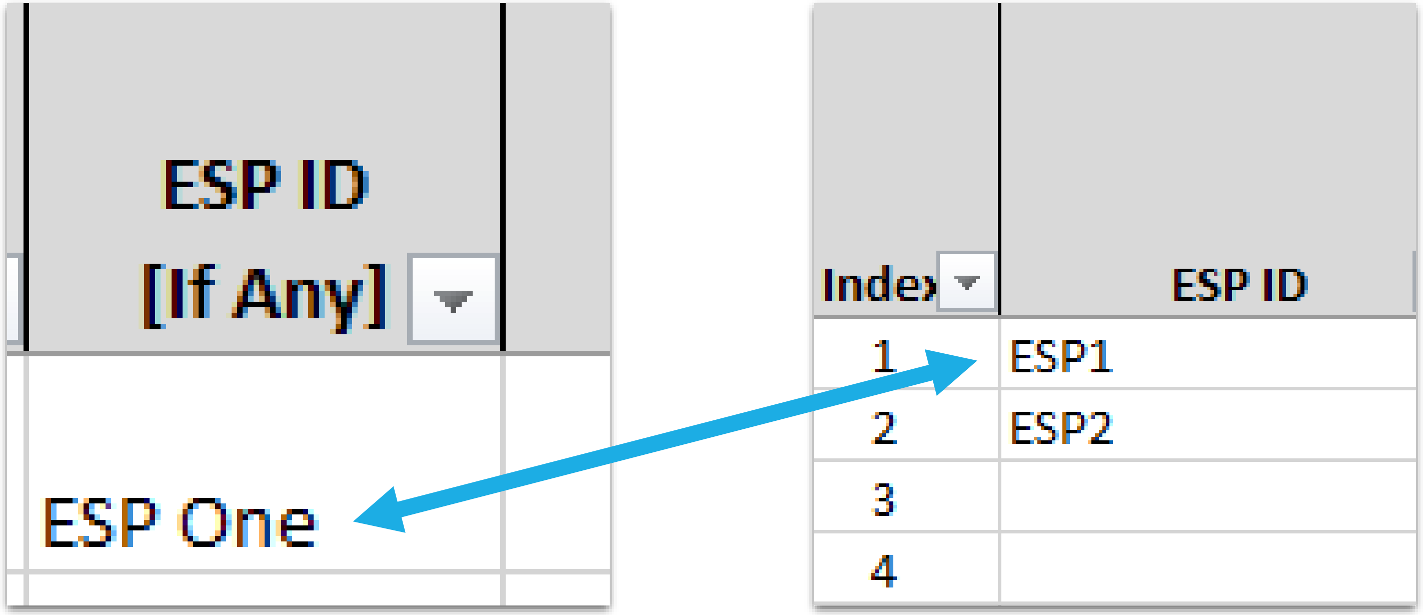
Missing ESP address spaces



| IP Address | ESP<br>[If A |
|---|---|
| 172.16.xx.yy,<br>172.16.xx.zz | ESP1 |
| 172.16.100.11/ 172. | ESP1 |
| | |

Multi-line entries

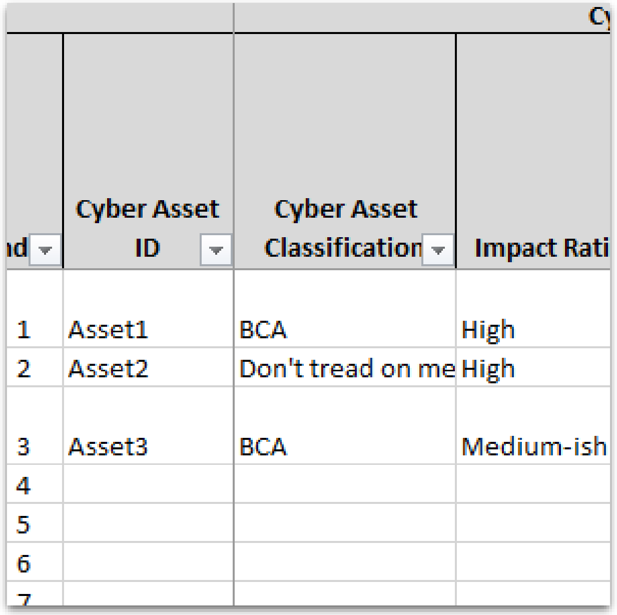
# ERT Common Errors



| ESP ID [If Any] |
|---|
| ESP One |

| Index | ESP ID |
|---|---|
| 1 | ESP1 |
| 2 | ESP2 |
| 3 | |
| 4 | |

CA tab ESP ID not matching an entry on the ESP tab



| ıd | Cyber Asset ID | Cyber Asset Classification | Impact Rati |
|---|---|---|---|
| 1 | Asset1 | BCA | High |
| 2 | Asset2 | Don't tread on me | High |
| 3 | Asset3 | BCA | Medium-ish |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |

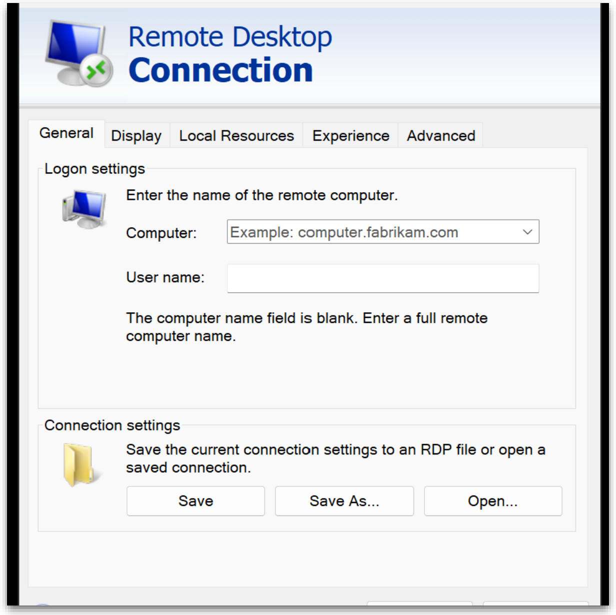
Altering the ERT

PUBLIC

# CIP-014 Evidence Options

Microsoft SharePoint

The entity can share evidence on a system that would permit the NPCC audit team to view files directly



Remote Desktop **Connection**

Logon settings

Enter the name of the remote computer.

Computer: Example: computer.fabrikam.com

User name:

The computer name field is blank. Enter a full remote computer name.

Connection settings

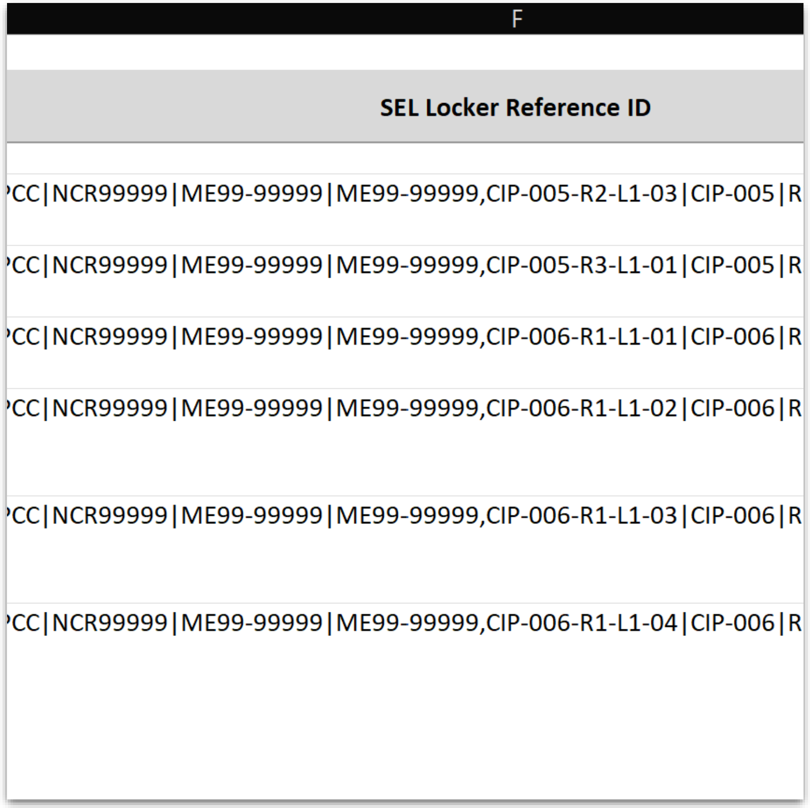
Save the current connection settings to an RDP file or open a saved connection.

The entity can grant remote desktop access to a system where NPCC Auditors can log in and view the evidence files

**ERO SEL**

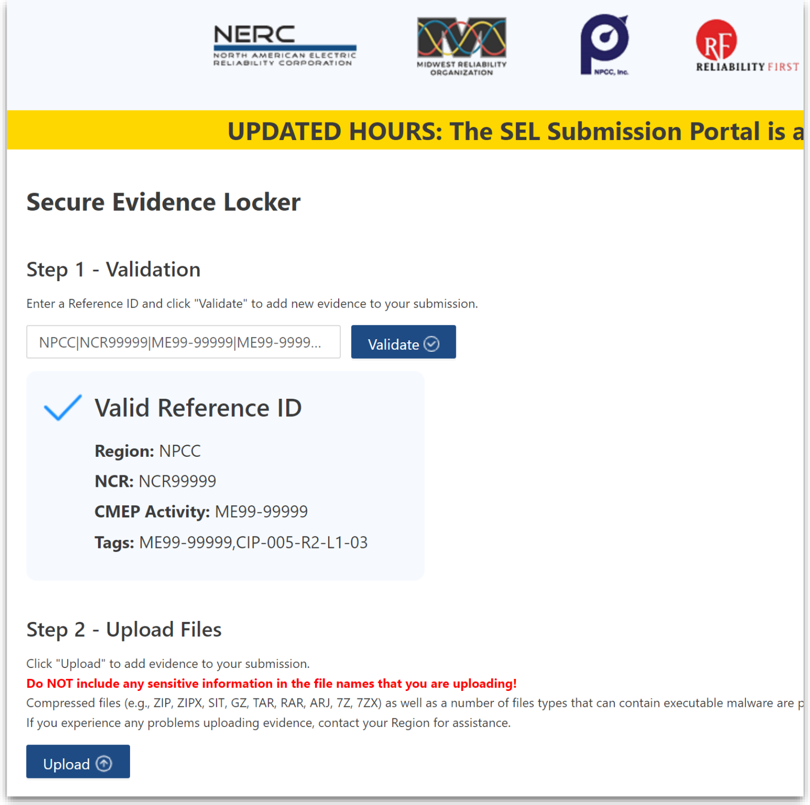
An SEL locker ID can be created for the entity to use to upload evidence files to

# Future SEL Integration



| F |
|---|
| SEL Locker Reference ID |
| 'CC\|NCR99999\|ME99-99999\|ME99-99999,CIP-005-R2-L1-03\|CIP-005\|R |
| 'CC\|NCR99999\|ME99-99999\|ME99-99999,CIP-005-R3-L1-01\|CIP-005\|R |
| 'CC\|NCR99999\|ME99-99999\|ME99-99999,CIP-006-R1-L1-01\|CIP-006\|R |
| 'CC\|NCR99999\|ME99-99999\|ME99-99999,CIP-006-R1-L1-02\|CIP-006\|R |
| 'CC\|NCR99999\|ME99-99999\|ME99-99999,CIP-006-R1-L1-03\|CIP-006\|R |
| 'CC\|NCR99999\|ME99-99999\|ME99-99999,CIP-006-R1-L1-04\|CIP-006\|R |

SEL Locker ID column


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
MIDWEST RELIABILITY ORGANIZATION
NPCC, Inc.
RELIABILITY FIRST

UPDATED HOURS: The SEL Submission Portal is a

Secure Evidence Locker

Step 1 - Validation

Enter a Reference ID and click "Validate" to add new evidence to your submission.

NPCC|NCR99999|ME99-99999|ME99-9999... Validate

✓ Valid Reference ID

**Region:** NPCC

**NCR:** NCR99999

**CMEP Activity:** ME99-99999

**Tags:** ME99-99999,CIP-005-R2-L1-03

Step 2 - Upload Files

Click "Upload" to add evidence to your submission.

**Do NOT include any sensitive information in the file names that you are uploading!**

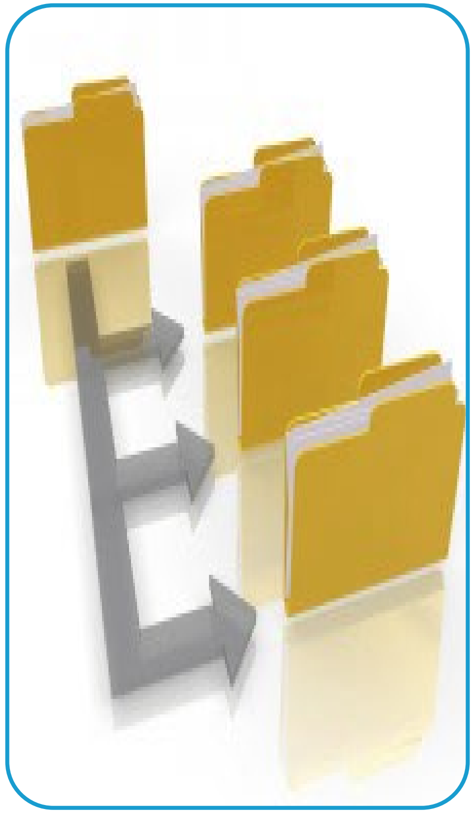
Compressed files (e.g., ZIP, ZIPX, SIT, GZ, TAR, RAR, ARJ, 7Z, 7ZX) as well as a number of files types that can contain executable malware are p

If you experience any problems uploading evidence, contact your Region for assistance.

Upload

SEL upload site

# Evidence Creation, Submission, and Handling



All submittals must be uploaded to the ERO Secure Evidence Locker (SEL) utilizing the appropriate SEL Reference ID for the Standard and Requirement or RFI. **Each in scope Standard and Requirement has its own SEL Reference ID.** Refer to the ***ANP*** tab for the audit in Align.

For example, **For evidence related to CIP-006-6 R2. use:**

**NPCC|NCR99999|ME23-99999|ME23-99999|CIP-006-6|R2.|**

It is important that only evidence for the applicable Standard and Requirement is placed in the corresponding SEL Reference ID for the Standard and Requirement. Please note that ZIP files are not compatible with the SEL and cannot be used for submittals.

**Uploads can be submitted from 6am-11pm Eastern Standard Time (EST) Monday – Friday**

Visit the NERC Training Site for access to all Align and ERO SEL training materials, including training videos and user guides.

***Failure to utilize the appropriate SEL Reference ID for uploading evidence can result in extended auditor review time prolonging the completion of the audit and re-submission of data utilizing appropriate SEL Reference IDs.***

# CIP ERT Demo and Tab Notes

| | |
|---|---|
| Level 1 | • Green requests correlate to green tabs<br>• Only complete requests for in-scope standards/requirements |
| Sample Sets L2 | • Primarily for NPCC |
| Level 2 | • ERT L2 requests and the associated sample sets for each |
| NPCC | • Prepopulated with our standard L2 requests and later the subsequent levels<br>• Enter a narrative for each and reference any evidence files |
| Sample Sets Table | • Primarily for formulas and checking |
| Green Tabs | • The bulk of an entity’s data goes here |

# Questions

Emily Stuetzle
estuetzle@npcc.org

Michael Bilheimer
mbilheimer@npcc.org

Cecil Elie
celie@npcc.org