

# CIP Evidence Request Tool v3.0

# Agenda



- Questions?
- History
- ERT Version 3.0 User Guide
- Using the ERT
  - ERT Level 1
  - NPCC Tab
  - ERT Level 2
  - Sample Sets Example
- Submitting the ERT and responses
  - Naming Conventions
  - Folder Structure
  - Handling of evidence
- Tips for evidence
- ERT & RSAW

# Questions?

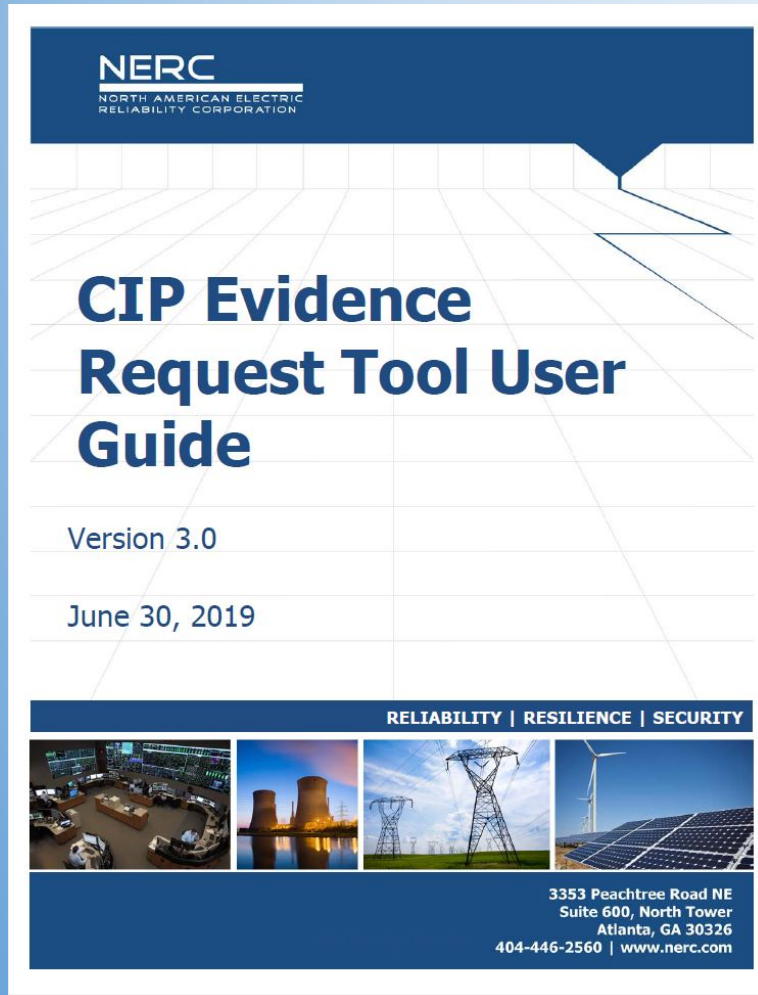
Please send all questions to [cip@npcc.org](mailto:cip@npcc.org)

We will be compiling the questions and producing a FAQ

# History

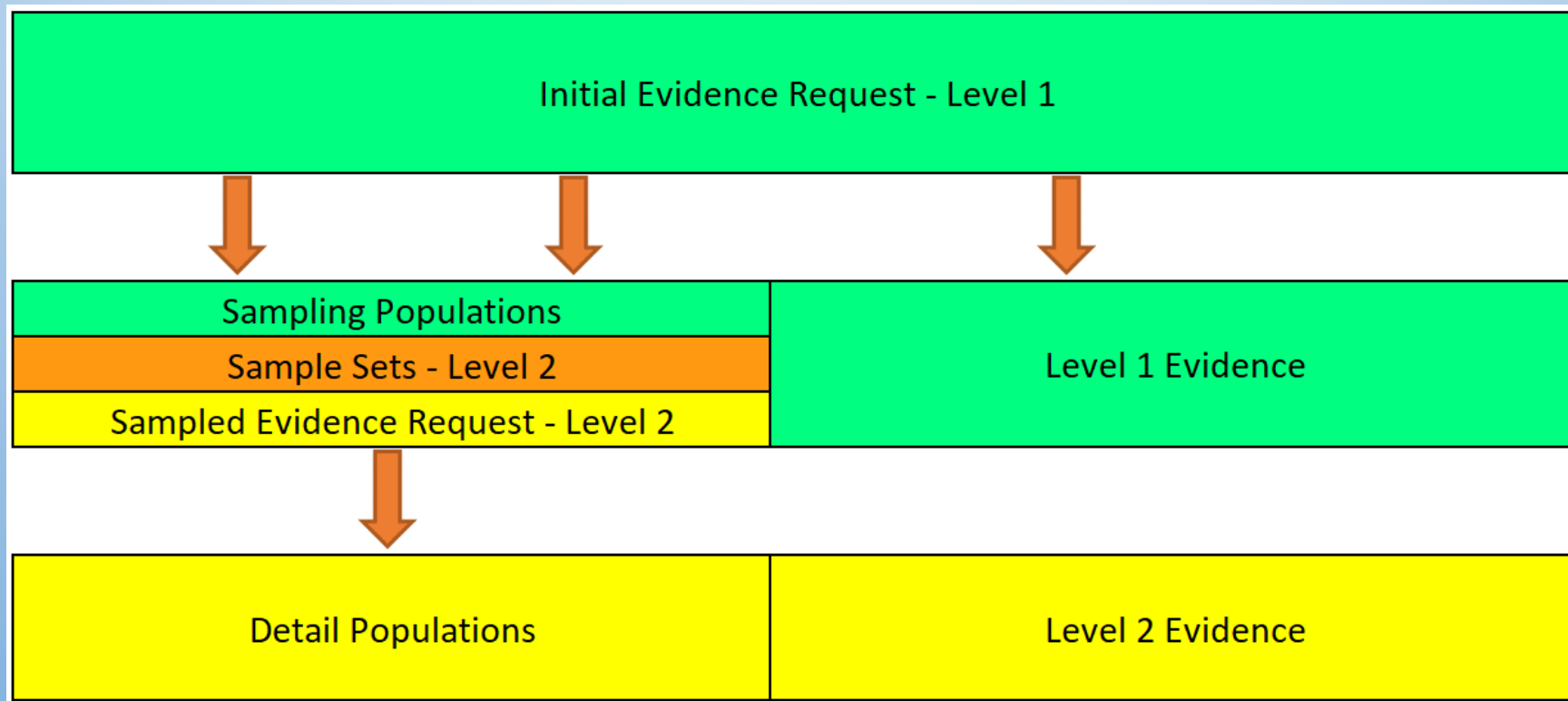
- Evidence Request Tool (ERT) released December 2015
- Used by FERC during CIP audits
- ERO initiated an update in late 2017 (v2) and 2019 (v3)
- Used by NPCC for CIP audits starting in 2019

# ERT Version 3.0 User Guide



- Key resource when completing the ERT
- Sent with audit notification package
- Available on NERC website: CIP v5 Transition Program

## Evidence Request Flow



# Using the ERT

## ERT Level 1 – Initial Evidence Request

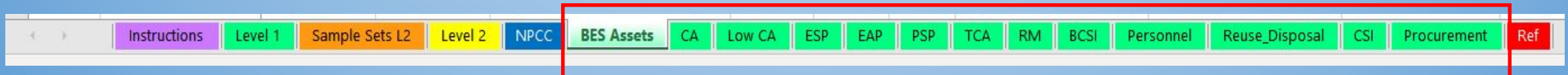
|    | A                | B        | C           | D                                                                                                                                                                                                                                                                                        |
|----|------------------|----------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Request ID       | Standard | Requirement | Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet                                                                                                                                                                                                          |
| 32 | CIP-004-R4-L1-01 | CIP-004  | R4          | Provide each documented program that addresses the applicable requirement parts in CIP-004 R4.                                                                                                                                                                                           |
| 33 | CIP-004-R4-L1-02 | CIP-004  | R4 Part 4.4 | Provide a <u>list</u> of designated storage locations for BES Cyber System Information in the <u>BCSI</u> tab.                                                                                                                                                                           |
| 34 | CIP-004-R5-L1-01 | CIP-004  | R5          | Provide each documented program that addresses the applicable requirement parts in CIP-004 R5.                                                                                                                                                                                           |
| 35 | CIP-005-R1-L1-01 | CIP-005  | R1          | Provide each documented process that addresses the applicable requirement parts in CIP-005 R1.                                                                                                                                                                                           |
| 36 | CIP-005-R1-L1-02 | CIP-005  | R1 Part 1.1 | Provide a <u>list</u> of all defined Electronic Security Perimeters (ESPs) in the <u>ESP</u> tab of this spreadsheet.                                                                                                                                                                    |
| 37 | CIP-005-R1-L1-03 | CIP-005  | R1 Part 1.1 | Please provide ESP network topology overview diagram(s), showing the relationship(s) among ESP(s).                                                                                                                                                                                       |
| 38 | CIP-005-R1-L1-04 | CIP-005  | R1 Part 1.2 | Provide a <u>list</u> of all Electronic Access Points (EAPs), the ESP it interfaces with, and the EACMS its configured, on the <u>EAP</u> tab.                                                                                                                                           |
|    |                  |          |             | Provide configuration files for each network device type (router, firewall, switch, etc.) Cyber Asset on the CA tab in the format(s) specified in the NP-View Instructions. Please follow link below for instructions.                                                                   |
|    | CIP-005-R1-L1-05 | CIP-005  | R1 Part 1.3 | Supported devices / instruction for providing configs for NP-View:<br><a href="http://www.network-perception.com/supported-devices/">http://www.network-perception.com/supported-devices/</a><br><br>If the device is not supported per the website above, please provide the equivalent |

- 86 requests depending upon scope
- Also requested in RSAW
- Documentation focused:
  - Policies
  - Programs
  - Procedures
  - Processes
  - Diagrams
  - Configurations
  - Etc.
- Populations of Cyber Assets, etc., that will be used for generating the Sample Sets in the Level 2 Evidence Request. Bright Green rows indicate that there is a tab to be completed.

# Using the ERT

## ERT Level 1 - Sampling Population Tabs

- 13 Sampling Populations depending upon audit scope.
- Each population has a tab that must be completed. All fields on the tab should be completed or blank as appropriate.
- The CIP Evidence Request Tool User Guide v3.0 has detailed instructions for completing each tab and each column in the ERT.
- Pay attention to true/blank drop downs, pick lists and date of activation/deactivation.
- When in doubt, contact your Audit Team Lead.



# Using the ERT

## NPCC TAB

Used by audit team to ask questions and request evidence that may not be covered by the ERT or RSAW. This tab is also used to document onsite questions

- Each request is assigned a unique number
- Multiple rounds of questions will be separated by a yellow bar

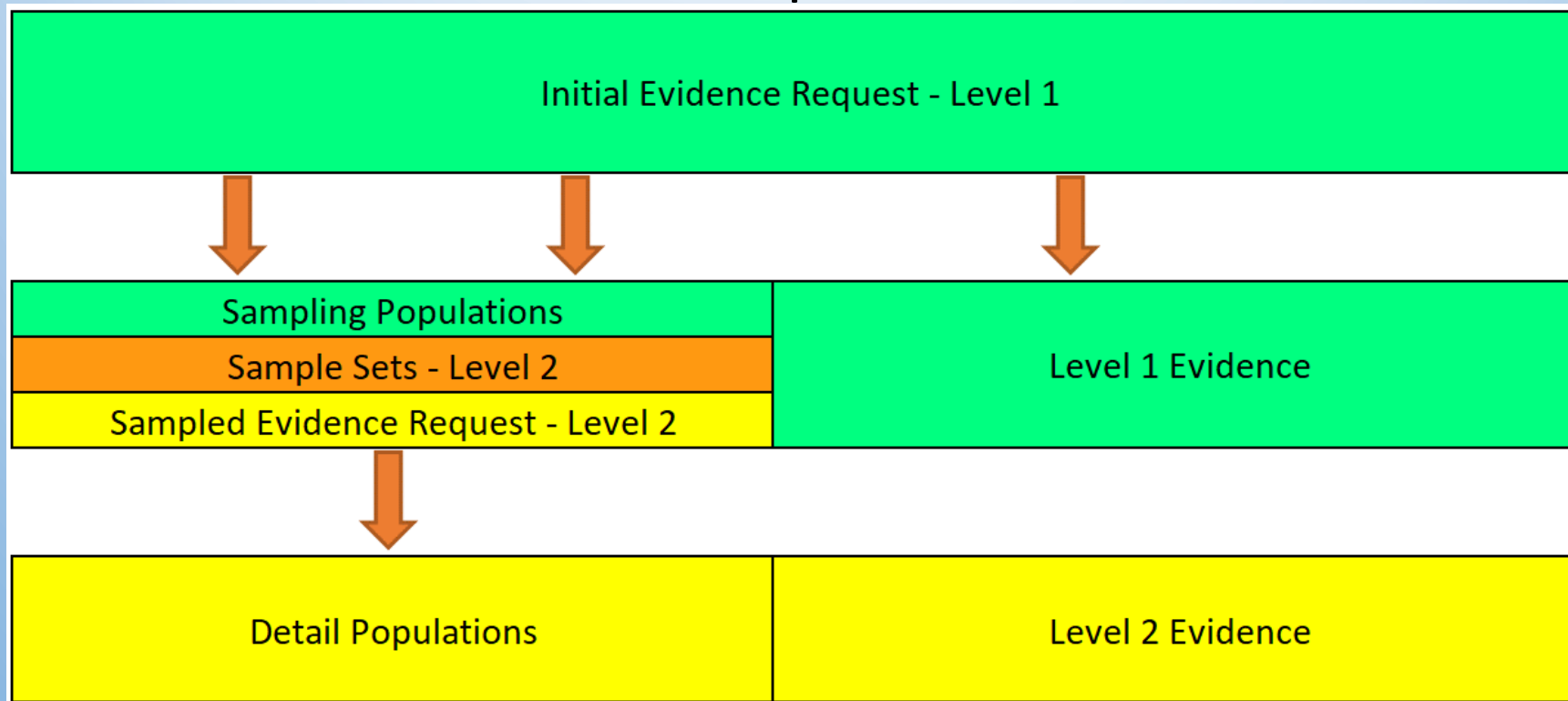
|    | A    | B        | C    | D               | E               | F                  | G                |
|----|------|----------|------|-----------------|-----------------|--------------------|------------------|
|    | DR # | Standard | Req. | Auditor Request | Entity Response | Document Reference | Status (Ok / No) |
| 1  |      |          |      |                 |                 |                    |                  |
| 2  | 1    | CIP-002  | R1   | Question 1      |                 |                    |                  |
| 3  | 2    | CIP-002  | R1   | Question 2      |                 |                    |                  |
| 4  | 3    | CIP-002  | R1   | Question 3      |                 |                    |                  |
| 5  |      |          |      | Level 2         |                 |                    |                  |
| 6  | 4    | CIP-005  | R1   | Question 4      |                 |                    |                  |
| 7  | 5    | CIP-005  | R1   | Question 5      |                 |                    |                  |
| 8  | 6    | CIP-005  | R1   | Question 6      |                 |                    |                  |
| 9  | 7    | CIP-005  | R1.3 | Question 7      |                 |                    |                  |
| 10 |      |          |      | Onsite          |                 |                    |                  |
| 11 | 8    | CIP-005  | R2   | Question 8      |                 |                    |                  |
| 12 | 9    | CIP-005  | R2   | Question 9      |                 |                    |                  |

Initial questions may be available with the L1 requests.

# Using the ERT

## ERT Level 2

## Evidence Request Flow



Level 2 requests additional detail about compliance for specific Cyber Assets, specific personnel, and other individual items that are subject to the Standards.

# Using the ERT

## Sample Sets Example – CA Tab – CIP-005-6 R2

| CIP-005 R1 Part 1.1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | CIP-005 R1 Part 1.4 |  |  | CIP-005 R2 |  | CIP-005 R3 |  | CIP-012 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|---------------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|---------------------|--|--|------------|--|------------|--|---------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|---------------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|---------------------|--|--|------------|--|------------|--|---------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

|   | A     | B              | J                  | K                                         | L                                | M                                                       |
|---|-------|----------------|--------------------|-------------------------------------------|----------------------------------|---------------------------------------------------------|
| 1 |       |                |                    | CIP-005 R1 Part 1.4                       | CIP-005 R2                       |                                                         |
| 2 | Index | Cyber Asset ID | ESP ID<br>[If Any] | Accessible via<br>Dial-up<br>Connectivity | Is IRA<br>Enabled to<br>this CA? | Is Vendor<br>Remote<br>Access<br>Enabled to<br>this CA? |
| 3 | 1     | Server_1       | MKHESP             |                                           | TRUE                             |                                                         |
| 4 | 2     | Server_2       | MKHESP             |                                           |                                  |                                                         |

Instructions

Level 1

Sample Sets L2

Level 2

NPCC ...

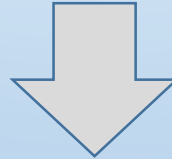
Ready

100%

## Sample Sets Example – CA Tab – CIP-005-6 R2 (cont'd)

|    | A               | B                                                        | C      | D                                                                 | E                                                               |
|----|-----------------|----------------------------------------------------------|--------|-------------------------------------------------------------------|-----------------------------------------------------------------|
| 1  | Sample Set      | Request ID                                               | Source | Population                                                        | Description                                                     |
| 20 | SS-005-R2-L2-01 | CIP-005-R2-L2-01<br>CIP-005-R2-L2-02<br>CIP-005-R2-L2-03 | CA     | Cyber Assets with TRUE in the "Is IRA enabled to this CA?" column | Sample of Cyber Assets accessible via Interactive Remote Access |

Instructions
Level 1
Sample Sets L2
Level 2
NPCC
BES Assets
CA
Low CA
ESP
EAP

[illegible]

- \* Sampling performed in alignment with the ERO Sampling Handbook

# Using the ERT

## Sample Sets Example – CA Tab – CIP-005-6 R2 (cont'd)

### Level 2 Evidence Requests

|    | A                | B        | C           | D               | E                                                               | F                                                                                                                                                                                                                                                                                                                     |
|----|------------------|----------|-------------|-----------------|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Request ID       | Standard | Requirement | Sample Set      | Sample Set Description                                          | Sample Set Evidence Request                                                                                                                                                                                                                                                                                           |
| 24 | CIP-005-R2-L2-01 | CIP-005  | R2 Part 2.1 | SS-005-R2-L2-01 | Sample of Cyber Assets accessible via Interactive Remote Access | For each Cyber Asset in Sample Set SS-005-R2-L2-01, provide evidence that an Intermediate System is used such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset, or that an approved TFE is applicable to this Cyber Asset.                                |
| 25 | CIP-005-R2-L2-02 | CIP-005  | R2 Part 2.2 | SS-005-R2-L2-01 | Sample of Cyber Assets accessible via Interactive Remote Access | For each Cyber Asset in Sample Set SS-005-R2-L2-01, provide evidence that communications between the Cyber Asset initiating Interactive Remote Access and the Intermediate System are encrypted and that encryption terminates at the Intermediate System, or that an approved TFE is applicable to this Cyber Asset. |
| 26 | CIP-005-R2-L2-03 | CIP-005  | R2 Part 2.3 | SS-005-R2-L2-01 | Sample of Cyber Assets accessible via Interactive Remote Access | For each Cyber Asset in Sample Set SS-005-R2-L2-01, provide evidence that all Interactive Remote Access sessions require multi-factor authentication, or that an approved TFE is applicable to this Cyber Asset.                                                                                                      |

Ready Filter Mode

Instructions Level 1 Sample Sets L2 Level 2 NPCC BES Assets CA Low CA ESP EAP PSP TCA RM BCSI Personnel Reuse\_Disposal CSI ...

Request IDs CIP-005-R2-L2-01 to CIP-005-R2-L2-03 apply to the cyber assets selected in SS-005-R2-L2-01

# Using the ERT

## Sample Sets Example – Sampling Dates

|    | A          | B                                                                                                                    | C      | D          | E                                                                                  |
|----|------------|----------------------------------------------------------------------------------------------------------------------|--------|------------|------------------------------------------------------------------------------------|
| 1  | Sample Set | Request ID                                                                                                           | Source | Population | Description                                                                        |
|    | SS-DATE-04 | CIP-007-R2-L2-01<br>CIP-010-R1-L2-02<br>CIP-010-R1-L2-03<br>CIP-010-R1-L2-04<br>CIP-010-R1-L2-05<br>CIP-010-R1-L2-06 | N/A    | N/A        | Range or ranges of dates throughout the audit period for baseline and patch review |
| 55 |            |                                                                                                                      |        |            |                                                                                    |
| 56 | SS-DATE-05 | CIP-010-R2-L2-01                                                                                                     | N/A    | N/A        | Range or ranges of dates throughout the                                            |

Ready

Instructions Level 1 Sample Sets L2 Level 2 NPCC BES Assets CA Low CA ESP EAP P

|   | A                | B        | C           | D                             | E                                                                                                                                                                                                                          | F                                                                                                                                                                                           | G               |
|---|------------------|----------|-------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| 1 | Request ID       | Standard | Requirement | Sample Set                    | Sample Set Description                                                                                                                                                                                                     | Sample Set Evidence Request                                                                                                                                                                 | Entity Response |
|   | CIP-010-R2-L2-01 | CIP-010  | R2 Part 2.1 | SS-010-R2-L2-01<br>SS-DATE-05 | Sample of Cyber Assets that are members of, or EACMS or PCA associated with, a high impact BES Cyber System<br><br>Range or ranges of dates throughout the audit period examined for monitoring for baseline modifications | For each Cyber Asset in Sample Set SS-010-R2-L2-01, provide evidence that monitoring for unauthorized changes in the baseline configuration was occurring during the date range SS-DATE-05. |                 |

Ready 1 of 83 records found

Instructions Level 1 Sample Sets L2 Level 2 NPCC BES Assets CA Low CA ESP EAP PSP TCA RM BCSI Personnel Reuse\_Disposal CSI Procurement Re ...

These can be a range or ranges of dates throughout the audit period.

SS-Date-XX will be documented on the NPCC Tab of the ERT and sent with the Level 2 requests.

# Submitting the ERT and responses

## Naming Conventions

- Each line of the Level 1 and Level 2 tabs contains a “Request ID,” which uniquely identifies each request.

Level 1 Tab

|    | A                | B        | C                                         | D                                                                                                                                                                                                          |
|----|------------------|----------|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Request ID       | Standard | Requirement                               | Initial Evidence Request Required in RSAW and N Spreadsheet                                                                                                                                                |
| 1  |                  |          |                                           |                                                                                                                                                                                                            |
| 17 | CIP-003-R2-L1-05 | CIP-003  | R2 Sect 4.5                               | For each Cyber Security incident response plan for low impact BES Cyber Systems, provide evidence of each test of the incident response plan.                                                              |
| 18 | CIP-003-R2-L1-06 | CIP-003  | R2 Sect 4.6                               | Provide evidence of changes to a Cyber Security Incident Response Plan for BES Cyber Systems in response to a test or activation of the plan, documented within 180 calendar days of the test or incident. |
| 19 | CIP-003-R2-L1-07 | CIP-003  | R2 Sect 5.1<br>R2 Sect 5.2<br>R2 Sect 5.3 | Provide all Transient Cyber Asset and Removable Media printouts for BES Cyber Systems.                                                                                                                     |

Level 2 Tab

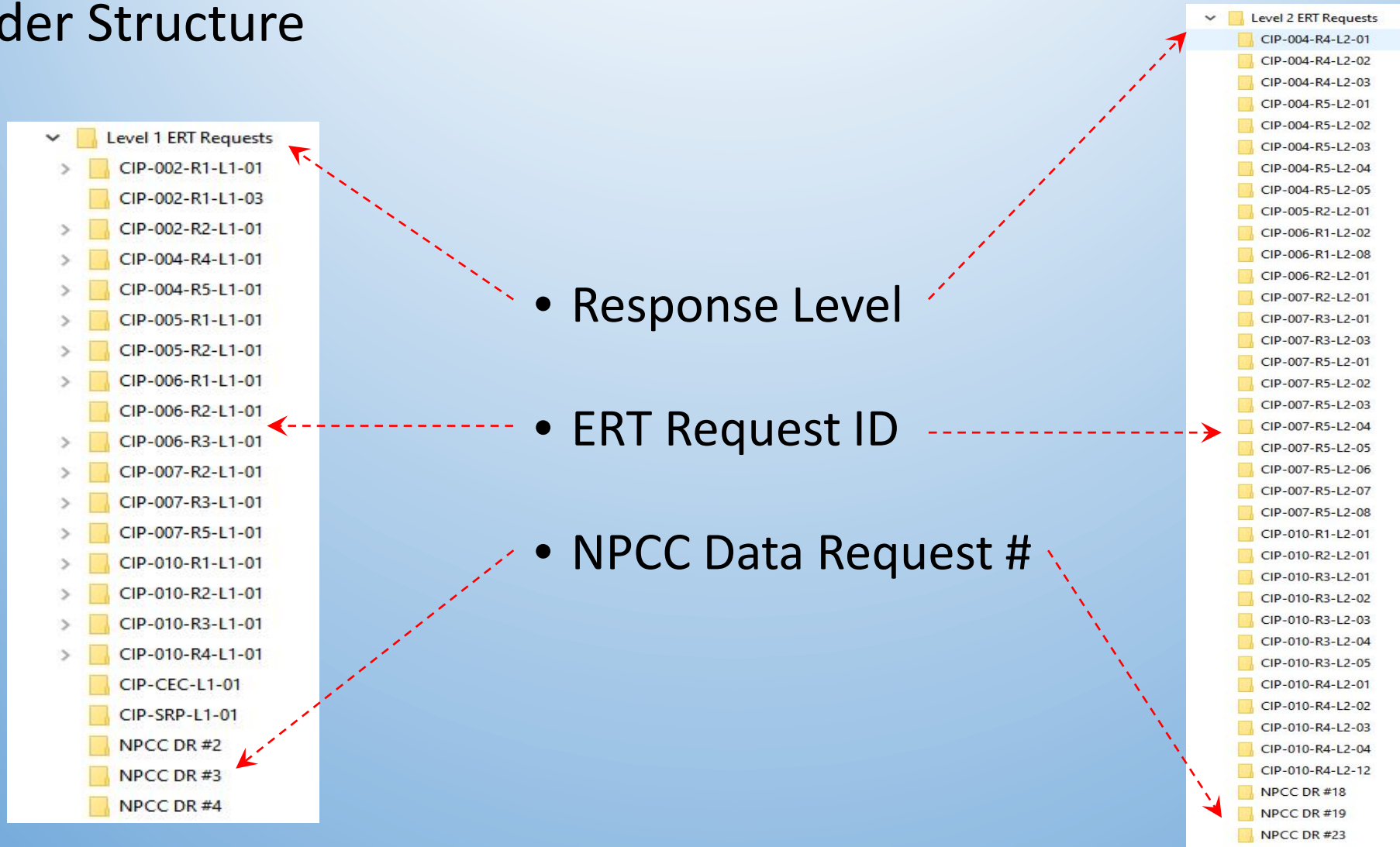
|   | A                | C           | D               | E                                                                                                                                                                    |
|---|------------------|-------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | Request ID       | Requirement | Sample Set      | Sample Set Description                                                                                                                                               |
| 1 |                  |             |                 |                                                                                                                                                                      |
|   | CIP-003-R2-L2-01 | R2 Sect 2   | SS-003-R2-L2-01 | BES Assets which contain a Low Impact BES Cyber System                                                                                                               |
| 2 |                  |             |                 |                                                                                                                                                                      |
|   | CIP-003-R2-L2-02 | R2 Sect 3.1 | SS-003-R2-L2-02 | BES Assets which contain a Low Impact BES Cyber System with routable protocol communication entering or leaving the asset containing the low impact BES Cyber System |
| 3 |                  |             |                 |                                                                                                                                                                      |

### CIP-sss-Rr-Lm-nn

- sss** is the three-digit CIP Reliability Standard number;
- r** is the Requirement number within the Standard;
- m** is the level of the evidence request, either “1” for Level 1 or “2” for Level 2 corresponding to Level 1, etc.;
- nn** is a two-digit request number within the Standard, Requirement, and Level.

# Submitting the ERT and responses

## Folder Structure



# Submitting the ERT and responses



## Handling of Evidence

- All audit submittals including the ERT will be uploaded to NPCC Drive
- The Audit Team Lead will move the Entities submittal to a secure server that is owned, maintained and physically resides in a protected zone within NPCC's office
- Access (electronic and physical) to this server is highly restricted
- Evidence is handled in accordance with applicable NPCC policies and procedures
- Evidence will be securely deleted after completion of the audit
- The Entity will maintain the official audit record on an encrypted USB Key

# Tips for Evidence



- It can be helpful to submit supporting documents with brief explanations of evidence files (i.e., README files or narratives).
- Screen Shot Evidence
  - Annotate if possible
  - Cyber Asset Name/Identifier
  - Date & Time
- Photographic Evidence
  - Annotate if possible
  - Front and back of device
  - Cyber Asset Name/Identifier Tag
  - Date & Time

- ERT, ERT responses and RSAWS must be submitted.
- Please cite ERT responses in RSAW if the same evidence is being used to demonstrate compliance.
- In addition to any cited ERT evidence in the RSAW, additional evidence may be required to submittal to support RSAW responses.

# Thank you !

Please send all questions to [cip@npcc.org](mailto:cip@npcc.org)