CIP Evidence Request Tool v3.0
• 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

We will be compiling the questions and producing a FAQ
• 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 v3.0
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

- Initial Evidence Request - Level 1
  - Sampling Populations
  - Sample Sets - Level 2
  - Sampled Evidence Request - Level 2

- Level 1 Evidence

- Level 2 Evidence

- Detail Populations
ERT Level 1 – Initial Evidence Request

- 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.
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.
ERT v3.0

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

Initial questions may be available with the L1 requests.
Level 2 requests additional detail about compliance for specific Cyber Assets, specific personnel, and other individual items that are subject to the Standards.
### Sample Sets Example – CA Tab – CIP-005-6 R2

#### Using the ERT

<table>
<thead>
<tr>
<th>Index</th>
<th>Cyber Asset ID</th>
<th>ESP ID</th>
<th>Accessible via Dial-up Connectivity</th>
<th>Is IRA Enabled to this CA?</th>
<th>Is Vendor Remote Access Enabled to this CA?</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Server_1</td>
<td>MKHESP</td>
<td></td>
<td>TRUE</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Server_2</td>
<td>MKHESP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ERT v3.0

Using the ERT

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

* 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

<table>
<thead>
<tr>
<th>Request ID</th>
<th>Standard</th>
<th>Requirement</th>
<th>Sample Set</th>
<th>Sample Set Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-005-R2-L2-01</td>
<td>CIP-005</td>
<td>R2 Part 2.1</td>
<td>SS-005-R2-L2-01</td>
<td>Sample of Cyber Assets accessible via Interactive Remote Access</td>
</tr>
<tr>
<td>CIP-005-R2-L2-02</td>
<td>CIP-005</td>
<td>R2 Part 2.2</td>
<td>SS-005-R2-L2-01</td>
<td>Sample of Cyber Assets accessible via Interactive Remote Access</td>
</tr>
<tr>
<td>CIP-005-R2-L2-03</td>
<td>CIP-005</td>
<td>R2 Part 2.3</td>
<td>SS-005-R2-L2-01</td>
<td>Sample of Cyber Assets accessible via Interactive Remote Access</td>
</tr>
</tbody>
</table>

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.

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
Sample Sets Example – Sampling Dates

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.

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.
ERT v3.0

Submitting the ERT and responses

Folder Structure

- Response Level
- ERT Request ID
- NPCC Data Request #
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
• 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