NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Critical Infrastructure Protection Evidence Request Tool User Guide

RELIABILITY | RESILIENCE | SECURITY



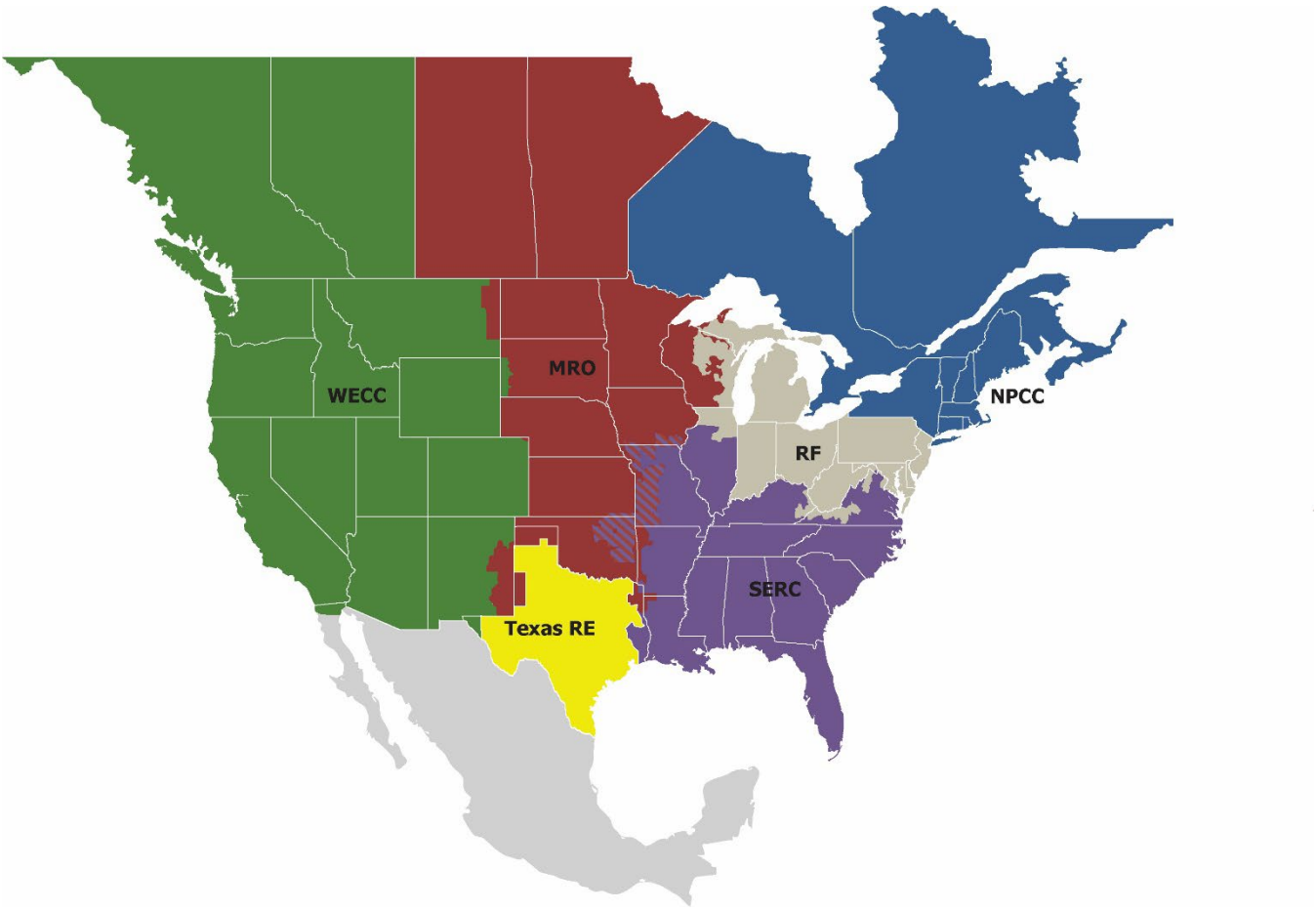

Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Introduction

A component of performing a compliance audit is the gathering of evidence to support audit findings. The Regional Entities, as delegates of NERC, perform compliance audits and exercise a degree of independence; historically, this meant each Region issued a request for information prior to the audit and the Responsible Entity provided the requested information.

The *Critical Infrastructure Protection (CIP) Evidence Request Tool* (ERT) is a common request for information that will be available for use by all of the Regions. This document will help the ERO Enterprise be more consistent and transparent in its audit approach. It will also help Responsible Entities (especially those that operate in multiple regions) fulfill these requests more efficiently by understanding what types of evidence are useful in preparation for an audit.

Evidence Request Flow

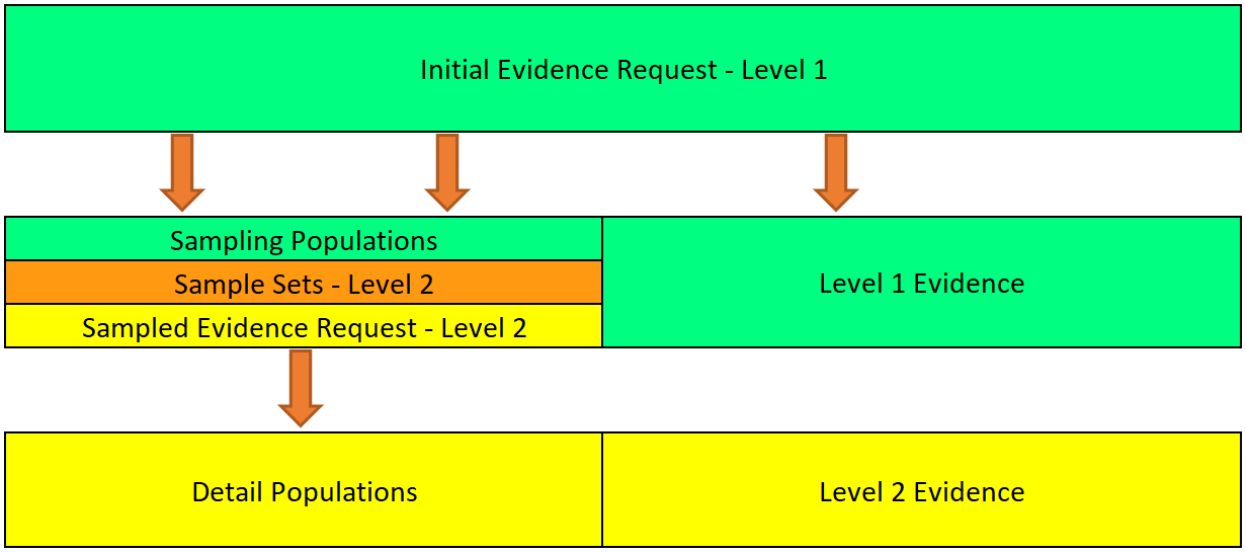


Figure 1: Evidence Request Flow

Figure 1 above shows a summary of the evidence request flow. The ERT contains a *Level 1* tab with the initial evidence needed to begin the evidence submission process. *Level 1*, in general, asks for two different types of evidence: (1) completion of the detail tabs associated with CIP Reliability Standards and used to form populations for sample selection which will feed into *Level 2* requests; (2) general requests for information that an audit team will review to assess compliance, such as the programs, processes, and procedures associated with the applicable Reliability Standards.

Level 2 asks for detailed implementation evidence for specific items sampled by the audit team.

Note: To continue transparency in the evidence requests as part of the audit process, the ERO Enterprise may include requests for CIP Reliability Standards and Requirements subject to future enforcement in *Level 1* and *Level 2* Request IDs.

Sampling

From the detail tabs filled out in response to *Level 1*, and in some cases *Level 2*, audit teams will select a sample size and a set of samples for further review. This sampling is conducted according to the *Compliance Monitoring and Enforcement Manual*.

Note: On the CA, ESP, EAP, PSP, TCA Non-RE, RM, BCSI, Personnel, Reuse_Disposal, CSI, and Procurement tabs, there are “For use by Region” columns with the Sample Set. Regions may either use these columns to place an “x” indicating the chosen sample set for each sample set ID or annotate the sampled index numbers (as identified in column A of each detail tab) for each sample set directly in the *Level 2* tab.

Audit Evidence Submission

Evidence should be submitted in accordance with the schedule and format specified in the audit notification letter (ANL).

Chapter 1: General Instructions

Naming Convention

Each line of the *Level 1* and *Level 2* tabs contains a "Request ID," which uniquely identifies each request. These Request IDs have the following format:

- *CIP-<Standard>-<Version>-<Requirement>-<Level>-<RequestIndex>*

Where:

- **<Standard>** refers to the CIP Reliability Standard number.
- **<Version>** refers to the CIP Reliability Standard version.
- **<Requirement>** is the Requirement within the Standard.
- **<Level>** is the level of the evidence request. Can be either "L1" for *Level 1* or "L2" for *Level 2*.
- **<RequestIndex>** is a two-digit request index for multiple requests of the same Standard, Requirement, and Level.

For example, CIP-002-5.1a-R1-L1-03 is the third *Level 1* evidence request for CIP-002-5.1a, R1.

Quality of Evidence

- Letterhead
- Structure
- Approvals
- Change History

Referenced Documents within a Process or Procedure

Documents that are referenced within a document submitted as evidence may need to be included in the evidence submission as well. If referenced documents are needed to convey the complete compliance picture to an audit team, they should be included. For example, if a CIP-008 Cyber Security Incident response plan references another document that contains specific steps for a system that is within CIP scope, then that referenced document should be included in the evidence submitted.

Chapter 2: Level 1 Tab

Each row in the *Level 1* worksheet is a request for evidence to support the findings of an audit or other compliance action. A registered entity is required to provide a response to each applicable evidence request in the *Level 1* worksheet. Applicability of each request is as follows:

- Each *Level 1* request where the "Standard" field matches any NERC Reliability Standard in the monitoring engagement scope and is denoted with a brighter green color must be responded to unless otherwise instructed by the Regional Entity.
  - These requests specifically denoted by the different color are not a request for evidence. The request is for specific worksheets (Detail Tabs) within the Evidence Request Tool to be filled in. The applicable worksheet is noted within the "Detail Tab or Request ID" column.
- Each *Level 1* request where the "Standard" and "Requirement" fields match a NERC Reliability Standard and Requirement in the monitoring engagement scope must be responded to unless otherwise instructed by the Regional Entity.
  - Requests where the "Standard" field has the value "All Standards" are always applicable regardless of monitoring engagement scope.

Each section below describes a field on the *Level 1* worksheet. If you are unsure of which requests you must respond to, please work directly with your Regional Entity or Audit Team Lead, and they will assist you. Please refer to Chapter 19 for additional guidance related to some Level 1 requests.

Detail Tab or Request ID

The request ID for a given evidence request or the name of an applicable worksheet. Formatted using the naming convention mentioned previously if the row is an evidence request. This value is unique and is the primary key for this table.

Standard

The NERC Reliability Standard that the *Level 1* request is applicable to. May also contain a value of "All Standards", which means that *Level 1* request is applicable to all NERC Reliability Standards.

Requirement

The NERC Reliability Standards requirement that the *Level 1* request is applicable to. May contain an entire requirement or just a requirement part depending on the request. May also contain more than one requirement or requirement part.

Evidence Request

Outline of the evidence being requested.

SEL Reference ID

The SEL Reference ID for use when uploading evidence to the Secure Evidence Locker. The Regional Entities are responsible for filling out the appropriate information in the "Ref" tab from Align for the SEL Reference ID to be generated properly. See Chapter 18 for further usage information.

Chapter 3: Sample Sets L2

This worksheet contains a list of applicable sample sets that are used for *Level 2* requests. This tab is used by the Regional Entities, and the registered entity does not need to interact with this tab. Each *Level 2* request will only request evidence for assets, personnel, etc., that match specific criteria. Each set of unique criteria is outlined in a separate row in this worksheet. This worksheet contains the name of the sample set, a list of each sample set's applicable Request IDs, a description of the applicable systems, the source tab where the sample set is applied, population filtering instructions, and a brief description of the sample set. This worksheet is used by the Regional Entity when conducting sampling as part of the monitoring engagement. Sample sets include groups as well as specific dates or date ranges.

Chapter 4: Level 2 Tab

Each row in the *Level 2* worksheet is a request for evidence to support the findings of an audit or other compliance action. A registered entity is required to provide a response to each applicable evidence request in the *Level 2* worksheet. Applicability of each request is as follows:

- Each *Level 2* request where the "Standard" and "Requirement" fields match a NERC Reliability Standard and Requirement in the monitoring engagement scope must be responded to unless otherwise instructed by the Regional Entity.

Each section below describes a field on the *Level 2* worksheet. If you are unsure of which requests you must respond to, please work directly with your Regional Entity or Audit Team Lead, and they will assist you.

Request ID
The request ID for a given evidence request. Formatted using the naming convention mentioned previously. This value is unique and is the primary key for this table.

Standard
The NERC Reliability Standard that the request is applicable to.

Requirement
The NERC Reliability Standards requirement that the request is applicable to. May contain an entire requirement or just a requirement part depending on the request. May also contain more than one requirement or requirement part.

Index Sample Set
The applicable sample set population for this request. This will match exactly one value in the "Sample Set" field from the *Sample Sets L2* worksheet.

Date Sample Set
The applicable date/date range sample set for this request. This will match exactly one value in the "Sample Set" field from the *Sample Sets L2* worksheet or be "N/A" if this request does not require evidence to be submitted for specific dates.

Sample Set Source & Description
The source worksheet and a brief description of the sample information being requested.

Sample Set Evidence Request
Outline of the request for evidence.

Sample Set Index Numbers
The index numbers of the associated samples. The index numbers correlate to the "Index" field in the worksheet denoted by the "Source Tab" label inside the "Sample Set Source & Description" field. If this field is blank, no evidence needs to be submitted for this request.

Sampled Dates
A date, list of dates, or date ranges where applicable evidence requested from the "Sample Set Evidence Request" field must be submitted from. If this field is blank, then the "Sample Set Evidence Request" does not have any specific date requirements, and evidence must be submitted to encompass all of the monitoring period.

SEL Reference ID

The SEL Reference ID for use when uploading evidence to the Secure Evidence Locker. The Regional Entities are responsible for filling out the appropriate information in the “Ref” tab from Align for the SEL Reference ID to be generated properly. See Chapter 18 for further usage information.

Chapter 5: Bulk Electric System Assets (BES) Detail Tab

The *BES Assets* tab requests information about each physical BES asset as defined by CIP-002 R1 for which the Responsible Entity has compliance responsibility. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 1: BES Assets Tab

Field Name	Description	Data Type	Constraints	Example
BES Asset ID	A unique identifier or name associated with the asset.	String	Must be unique	North Control Center
Asset Type	The category type associated with this asset (values are the identified asset types within CIP-002 R1).	List	▪ `Control Center` ▪ `Substation` ▪ `Generation` ▪ `System Restoration` ▪ `SPS/RAS` ▪ `DP Protection System` ▪ `Associated Data Center`	`Control Center`
Description	A description of the BES asset.	String		Primary control center
Commission Date	The date the asset was commissioned if the BES asset was provisioned within the audit period. Otherwise, leave this field blank.	String	ISO 8601 date string	2020-04-15
Decommission Date	The date the asset was decommissioned if the BES asset was decommissioned within the audit period. Otherwise, leave this field blank.	String	ISO 8601 date string	2020-04-15
Location	A brief description of the location of the asset, such as city and/or state name, or floor within a building.	String		Western Idaho
High Impact	The BES asset contains a high impact BES Cyber System.	Boolean		`TRUE`
Medium Impact	The BES asset contains a medium impact BES Cyber System.	Boolean		`TRUE`
Low Impact	The BES asset contains a low impact BES Cyber System.	Boolean		`TRUE`

Table 1: BES Assets Tab				
Field Name	**Description**	**Data Type**	**Constraints**	**Example**
Low Routable	The BES asset contains a low impact BES Cyber System accessible via a routable protocol when entering or leaving this BES asset. Required only when *Low Impact* is TRUE.	Boolean		TRUE
External Routable Connectivity	The BES asset contains any high and/or medium impact BES Cyber Systems that have External Routable Connectivity. Required only for high and medium impact BES Assets	Boolean		TRUE
Vendor Remote Access	The BES asset is electronically and remotely accessible by vendors.	Boolean		TRUE
Dial-up Connectivity	The BES asset contains any BES Cyber Systems accessible via a Dial-up connection.	Boolean		TRUE
Regional Entities	The Regional Entities associated with the BES asset.	String	Comma Separated Values	RF, WECC
Registered Functions	The functions associated with the BES asset.	String	Comma Separated Values	TOP, GO

Chapter 6: Cyber Asset (CA) Detail Tab

The *CA* tab requests information about each BES Cyber Asset, Protected Cyber Asset, Electronic Access Control and Monitoring System, Physical Access Control System, and Shared Cyber Infrastructure as defined in the Glossary of Terms for which the registered entity has compliance responsibility within the audit period. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 2: Cyber Asset Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	A unique identifier or name associated with the Cyber Asset or Shared Cyber Infrastructure.	String	Must be unique	Pcc-dac1
Classification	Indicate the type of Cyber Asset, or indicate this asset is Shared Cyber infrastructure (SCI). Please note, SCI Host is added specifically for Reliability Standards from Standard Drafting Project 2016-02 pending FERC approval at time of ERTv10 publication.	List	• BCA • EACMS • PACS • PCA • SCI Host (future use)	PCA
Virtual (future use)	This Cyber Asset or Shared Cyber Infrastructure is a virtual asset (VM). FALSE indicates a physical Cyber Asset or Shared Cyber Infrastructure. This column is for future use only. It was added specifically for Reliability Standards from Standard Drafting Project 2016-02 pending FERC approval at time of ERTv10 publication.	Boolean		TRUE
Impact Rating	The impact rating of the BES Cyber System this Cyber Asset (or Shared Cyber Infrastructure, if applicable) belongs to.	List	• High • Medium	High
BES Cyber System IDs	The unique identifier for the associated BES Cyber Systems. If the applicable Cyber Asset (or Shared Cyber Infrastructure, if applicable) is associated with more than one BES Cyber System, include them all.	String	Comma Separated Values	BCC, North Backup
BES Asset ID	The BES asset this Cyber Asset (or Shared Cyber Infrastructure, if applicable) is associated with.	String	Must map to a value in the *BES Asset ID* field from the "BES Assets" tab	West Control Center

Table 2: Cyber Asset Detail Tab				
Field Name	**Description**	**Data Type**	**Constraints**	**Example**
Associated with Control Center	The Cyber Asset (or Shared Cyber Infrastructure, if applicable) is located at and/or associated with a Control Center.	Boolean		TRUE
SCI ID (future use)	The ID of the Shared Cyber Infrastructure in which this Virtual Cyber Asset resides. Required only for Cyber Assets where *Virtual* is TRUE and the Cyber Asset resides on Shared Cyber Infrastructure. This column is for future use only. It was added specifically for Reliability Standards from Standard Drafting Project 2016-02 pending FERC approval at time of ERTv10 publication.	String	Must map to a value in the *ID* field of this tab where the *Classification* is "SCI Host"	Vsphere-cluster1
VCA Classifications (future use)	The classifications of the Virtual Cyber Assets being hosted by Shared Cyber Infrastructure. Required only for Shared Cyber Infrastructure where *Classification* is "SCI Host". This column is for future use only. It was added specifically for Reliability Standards from Standard Drafting Project 2016-02 pending FERC approval at time of ERTv10 publication.	List	• BCA • PCA • EACMS • PACS • BCA, PCA • BCA, EACMS • BCA, PACS • PCA, EACMS • PCA, PACS • EACMS, PACS • BCA, PCA, EACMS • BCA, PCA, PACS • BCA, EACMS, PACS • PCA, EACMS, PACS • BCA, PCA, EACMS, PACS	BCA, EACMS

Table 2: Cyber Asset Detail Tab				
Field Name	**Description**	**Data Type**	**Constraints**	**Example**
Routable	The Cyber Asset (or Shared Cyber Infrastructure, if applicable) is connected to a network via a routable protocol.	Boolean		TRUE
External Routable Connectivity	The Cyber Asset (or Shared Cyber Infrastructure, if applicable) has External Routable Connectivity. For Cyber Assets outside of an Electronic Security Perimeter, set this value to FALSE.	Boolean		TRUE
IP Addresses[1]	The IP addresses for this Cyber Asset (or Shared Cyber Infrastructure, if applicable).	String	RFC 791 addresses, separated by commas	10.0.25.69
ESP ID	The ESP ID the Cyber Asset (or Shared Cyber Infrastructure, if applicable) resides within. If it does not reside inside an ESP, leave this field blank.	String	Must map to a value in the *ESP ID* field in the "ESP" tab.	BCC1
EACMS Controls ESP (future use)	The Cyber Asset or Shared Cyber Infrastructure controls access to an ESP. Required only for assets where *Classification* is EACMS, or SCI Host where *VCA Classifications* contains EACMS. This column is for future use only. It was added specifically for Reliability Standards from Standard Drafting Project 2016-02 pending FERC approval at time of ERTv10 publication.	Boolean		TRUE
Dial-up Connectivity	The Cyber Asset (or Shared Cyber Infrastructure, if applicable) is accessible via a Dial-up connection.	Boolean		TRUE
Interactive Remote Access	Interactive Remote Access is permitted to this Cyber Asset (or Shared Cyber Infrastructure, if applicable).	Boolean		TRUE
Vendor Remote Access	The Cyber Asset (or Shared Cyber Infrastructure, if applicable) is electronically and remotely accessible by vendors.	Boolean		TRUE

[1] The ERO Enterprise understands that IP address information is extremely sensitive and should be handled with the utmost protection and care. However, the ERO Enterprise does require this information for use during CMEP engagements. Security of this information is handled by using the ERO Enterprise Secure Evidence Locker, an approved entity owned Secure Evidence Locker, or the BES Artifact Exception Process. Please work directly with your Regional Entity on providing this information using the aforementioned methods.

Table 2: Cyber Asset Detail Tab				
Field Name	**Description**	**Data Type**	**Constraints**	**Example**
PSP ID	The PSP ID that this Cyber Asset (or Shared Cyber Infrastructure, if applicable) resides within. If it does not reside inside a PSP, leave this field blank.	String	Must map to a value in the *ID* field on the "PSP" tab	Back Room PSP
Intermediate System	This Cyber Asset (or Shared Cyber Infrastructure, if applicable) is an Intermediate System.	Boolean		`TRUE`
Activation Date	The date that the Cyber Asset (or Shared Cyber Infrastructure, if applicable) becomes CIP applicable within a production environment during the monitoring period for an audit engagement. If it was CIP applicable before the monitoring period, this field should be blank.	String	ISO 8601 date string	2020-04-15
Deactivation Date	The date that the Cyber Asset (or Shared Cyber Infrastructure, if applicable) is no longer CIP applicable within a production environment. If it is still in production, then this field should be blank.	String	ISO 8601 date string	2020-04-15
Device Function	The function that this Cyber Asset (or Shared Cyber Infrastructure, if applicable) performs.	List	See the applicable device functions below table	`Application Server`
If Function is Other, please specify	The function that this Cyber Asset (or Shared Cyber Infrastructure, if applicable) performs. Required only if field *Device Function* is set to "Other (please specify)".	String		Data Acquisition Server
Manufacturer	The name of the manufacturer of the Cyber Asset (or Shared Cyber Infrastructure, if applicable).	String		Arbiter
Model	The model identifier or other descriptor to identify the Cyber Asset (or Shared Cyber Infrastructure, if applicable).	String		1202C
Operating System/Firmware Type	The operating system or firmware that the Cyber Asset (or Shared Cyber Infrastructure, if applicable) uses. Please include versioning information as well.	String		Windows 11

Table 2: Cyber Asset Detail Tab				
Field Name	**Description**	**Data Type**	**Constraints**	**Example**
Responsible Registered Entity and NCR	The registered entity this Cyber Asset (or Shared Cyber Infrastructure, if applicable) is associated with. Required only if listing Cyber Assets (or Shared Cyber Infrastructure) that are applicable to more than one Registered entity.	String	Comma Separated Values	NCR12345 – Big Electric, NCR67890 – Small Electric
Regional Entities	The Regional Entity associated with this Cyber Asset (or Shared Cyber Infrastructure, if applicable).	String	Comma Separated Values	Texas RE, WECC
Registered Functions	The function associated with this Cyber Asset (or Shared Cyber Infrastructure, if applicable).	String	Comma Separated Values	TO, TOP
OEA/self-log IDs	The identification number of any Open Enforcement Actions (OEA) or Self Logs associated with this Cyber Asset (or Shared Cyber Infrastructure, if applicable).	String	Comma Separated Values	2025-87231-P
TFE IDs	The identification number of any Technical Feasibility Exception associated with this Cyber Asset.	String	Comma Separated Values	2024-MRO-TFE-000655-7

Applicable device functions are as follows:

- Application Server
- Data Server
- Dial-up Modem
- Domain Controller (DC)
- Firewall
- HMI Workstation
- Industrial Control System (ICS)
- Infrastructure Support
- Intelligent Electronic Device (IED)
- Intermediate System
- Intrusion Detection (IDS/IPS)
- Management Console
- Out of Band Management (iDRAC/iLO)
- Protective Relay
- Remote Terminal Unit (RTU)

- Router
- Security Information and Event Management (SIEM)
- Serial/IP Converter
- Switch
- Virtual Host
- Virtual Server
- Other (please specify)

Chapter 7: Low Cyber Asset (Low CA) Detail Tab

The *Low CA* tab requests information about each Cyber Asset associated with a low impact BES Cyber System as defined in CIP-002, Attachment 1, section 3 for which the registered entity has compliance responsibility within the audit period. This tab is not mandatory and is only optional for the registered entity that has chosen to have a list of low impact BES Cyber Systems.

This tab requests information that is already requested by the *CA* tab and documented in Chapter 6. Please reference Chapter 6 for the specification on providing the following information in the *Low CA* tab:

- ID
- BES Cyber System IDs
- BES Asset ID
- Routable
- Dial-up Connectivity
- Interactive Remote Access
- Responsible Registered Entity and NCR
- Responsible Regional Entities
- Registered Functions

Chapter 8: Electronic Security Perimeter (ESP) Detail Tab

The *ESP* worksheet requests information about each Electronic Security Perimeter as defined by the Glossary of terms for which the Responsible Entity has compliance responsibility within the audit period. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 3: Electronic Security Perimeter Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	A unique identifier or name associated with the ESP.	String	Must be unique	PCC1
Description	A brief description of the ESP.	String		The primary control center
Address Spaces	A list of Classless Inter-Domain Routing (CIDR) addresses in use within the ESP.	String	RFC 4632 address, separated by commas	10.241.0.0/16
External Routable Connectivity	The ESP has External Routable Connectivity.	Boolean		TRUE
Interactive Remote Access	Interactive Remote Access is permitted to this ESP.	Boolean		TRUE
Modified	The ESP experienced modifications during the audit period. Events like, but not limited to, the address space changing, most of the contained Cyber Assets changing, or routing technology changes would be considered a modification in this context.	Boolean		TRUE

Chapter 9: Electronic Access Point (EAP) Detail Tab

The *EAP* tab requests information about each Electronic Access Point as defined by the Glossary of Terms for which the Responsible Entity has compliance responsibility within the audit period. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 4: Electronic Access Point Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	A unique identifier or name associated with the EAP. This can be a device ID or a network interface ID.	String	Must be unique	Gi0/1
IP Addresses[1]	The IP addresses for this Cyber Asset (or Shared Cyber Infrastructure, if applicable).	String	RFC 791 addresses, separated by commas	10.0.25.69
EACMS ID	The EACMS Cyber Asset ID the EAP is associated with.	String	Must map to a value in the *ID* field from the "CA" tab where *Classification* is "EACMS", or where *Classification* is "SCI Host" and *VCA Classifications* contains "EACMS"	Bcc-fw1
ESP ID	The ESP ID the EAP is associated with.	String	Must map to a value in the *ID* field from the "ESP" tab	BCC1
Associated with Control Center	The EAP is located at and/or associated with a Control Center.	Boolean		TRUE
Modified	The EAP experienced modifications during the audit period. Events like, but not limited to, the address space changing, architectural changes, or routing technology changes would be considered a modification in this context.	Boolean		TRUE

Chapter 10: Physical Security Perimeter (PSP) Detail Tab

The *PSP* tab requests information about each Physical Security Perimeter as defined by the Glossary of Terms, and its associated physical access points for which the Responsible Entity has compliance responsibility within the audit period. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 5: Physical Security Perimeter Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	A unique identifier or name associated with the PSP.	String	Must be unique	Main Office
Description	A brief description of the PSP.	String		The Primary Office
Location	The physical location of the PSP.	String		Building 4A
BES Asset ID	The BES asset this PSP is associated with.	String	Must map to a value in the *BES Asset ID* field from the "BES Assets" tab	West Control Center
Physical Access Points	A list of physical access points associated with this PSP.	String	Each value must be unique, separated by commas	East door, west door, south door
Physical Access Points Description	A description of the physical access points identified.	String	Comma Separated Values	Door on east side of building
Control Types	The types of physical access controls used at the PSP.	String	Comma Separated Values	Badge reader, iris scanner, key
Impact Rating	The impact rating of the BES Cyber Systems this PSP protects.	List	• `High` • `Medium with ERC`	`High`
Modified	The PSP experienced modifications during the audit period. Events like, but not limited to, the physical access points changing, or the control types changing would be considered a modification in this context.	Boolean		`TRUE`

Chapter 11: Transient Cyber Asset (TCA) Detail Tab

The *TCA* tab requests information about each Transient Cyber Asset managed or not managed by the Responsible Entity as defined by the Glossary of Terms for which the Responsible Entity has compliance responsibility within the audit period. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 6: Transient Cyber Asset

Field Name	Description	Data Type	Constraints	Example
ID	A unique identifier or name associated with the TCA.	String	Must be unique	Bcc-laptop1
Management Type	The management type used for this TCA.	List	• `Ongoing` • `On-demand` • `Ongoing/On-demand`	`On-demand`
Description	A brief description of the TCA. Provide information if the TCA was associated with ESP(s) or PCA(s).	String		Laptop used within ESP for firmware updates
Managed By	Who manages this TCA.	List	• `Entity` • `Other Party`	`Entity`
BES Asset ID	The BES Asset ID(s) where the TCA is used at.	String	Must map to a value in the *BES Asset ID* field from the "BES Assets" tab	BCC1
Connected to High/Medium Impact BCS	Indicates the TCA is connected at a BES asset(s) with high and/or medium impact BES Cyber Systems.	Boolean		`TRUE`
Connected to Low Impact BCS	Indicates the TCA is connected at a BES asset(s) with low impact BES Cyber Systems.	Boolean		`TRUE`
Modified	The TCA experienced modifications during the audit period. Events like, but not limited to, changes in vulnerability management, malicious code detection, or other TCA management processes would be considered a modification in this context.	Boolean		`TRUE`

Chapter 12: Removable Media (RM) Detail Tab

The *RM* tab requests information about Removable Media as defined by the Glossary of Terms for which the Responsible Entity has compliance responsibility within the audit period. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 7: Removable Media Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	A unique identifier or name associated with the RM.	String	Must be unique	Pcc-flash1
Description	A brief description of the RM. Provide information if the RM was associated with ESP(s) or PCA(s).	String		Flash drive used within ESP for firmware updates
BES Asset ID	The BES Asset ID(s) where the RM is used at.	String	Must map to a value in the *BES Asset ID* field from the "BES Assets" tab	BCC1
Connected to High/Medium Impact BCS	Indicates the RM is connected at a BES asset(s) with high and/or medium impact BES Cyber Systems.	Boolean		TRUE
Connected to Low Impact BCS	Indicates the RM is connected at a BES asset(s) with low impact BES Cyber Systems.	Boolean		TRUE
Modified	The RM experienced modifications during the audit period. Events like, but not limited to, changes in vulnerability management, malicious code detection, or other RM management processes would be considered a modification in this context.	Boolean		TRUE

Chapter 13: BES Cyber System Information (BCSI) Detail Tab

The *BCSI* tab requests information about each BES Cyber System Information grouping managed by the Responsible Entity for which the Responsible Entity has compliance responsibility within the audit period. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 8: BES Cyber System Information (BCSI) Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	A unique identifier or name associated with the BCSI grouping.	String	Must be unique	SharePoint1
Description	A brief description of the BCSI, including how the BCSI is protected. See CIP-011-3 measures for R1 for examples of how evidence may be protected.	String		Protected via ACLs, and physical keys
Type	The type of BCSI. Types for Electronic refer to the BCSI storage location. "On premises" means the BCSI is stored electronically at a facility owned by the registered entity.	List	• `Physical` • `Electronic – On Premises` • `Electronic – Off Premises`	`Physical`
Impact Rating	The impact rating of the BCSI. If the BCSI is associated with varying impact ratings of BES Cyber Systems, select the highest impact rating.	List	• `High` • `Medium with ERC` • `Medium without ERC`	`High`
Modified	The BCSI experienced modifications during the audit period. Events like, but not limited to, BCSI groupings were created or retired during the audit period would be considered a modification in this context.	Boolean		`TRUE`

Chapter 14: Personnel (Personnel) Detail Tab

The *Personnel* tab requests information about each individual for which the Responsible Entity has compliance responsibility within the audit period. Applicable Personnel include those who had access to one or more of the following:

- Electronic access to a high impact BES Cyber System and/or associated EACMS or PACS
- Electronic access to a medium impact BES Cyber System with External Routable Connectivity and/or associated EACMS or PACS
- Unescorted physical access to a high impact BES Cyber System and/or associated EACMS or PACS
- Unescorted physical access to a medium impact BES Cyber Systems with External Routable Connectivity and/or associated EACMS or PACS
- BES Cyber System Information, whether physical or electronic.

The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 9: Personnel (Personnel) Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	A unique identifier or name associated with the individual. Do not use any personally identifying information.	String	Must be unique	0596812
Full Name	The full name of the individual.	String	Format as "<SURNAME>, <FIRSTNAME> <MIDDLE INITIAL>". Middle initial is optional	SMITH, JOHN H
Type	The type of Personnel. Optionally, the Contractor type may be used to designate any non-employee including service vendors.	List	• `Employee` • `Contractor` • `Service Vendor`	
Company	The company employing the individual.	String		Super Big Power Company
Position/Job Title	The position name or job title of the individual.	String		Plant Manager

Table 9: Personnel (Personnel) Detail Tab				
Field Name	**Description**	**Data Type**	**Constraints**	**Example**
Access Permission Changed	The individual's access permissions were modified during the audit period, whether electronic access to a BES Cyber System or associated EACMS or PACS; unescorted physical access into a Physical Security Perimeter; or access to BES Cyber System Information, whether physical or electronic.	Boolean		TRUE
Transferred/Reassigned	The individual was transferred or reassigned during the audit period.	Boolean		TRUE
Transfer/Reassignment Date	The date that the individual was transferred or reassigned. Required only if *Transferred/Reassigned* is TRUE.	String	ISO 8601 date string	2020-04-15
Termination Date	The date of termination if an individual was terminated during the audit period. If terminated outside the audit period, leave blank.	String	ISO 8601 date string	2020-04-15
Had Electronic BCS Access	The individual had authorized electronic access to high impact BES Cyber Systems or associated EACMS. Required only when *Termination Date* is not blank.	Boolean		TRUE
Had BCSI Access	The individual had authorized electronic access to high impact BES Cyber Systems or associated EACMS. Required only when *Termination Date* is not blank.	Boolean		TRUE
Had Shared Account Access	The individual's access was revoked and had authorized electronic access to shared user accounts for high impact BES Cyber Systems and/or associated EACMS. Required only when *Termination Date* is not blank.	Boolean		TRUE

Table 9: Personnel (Personnel) Detail Tab				
Field Name	**Description**	**Data Type**	**Constraints**	**Example**
Authorized Electronic Access	The individual had authorized electronic access to a high impact, or medium impact with ERC, BES Cyber System or associated EACMS or PACS at any time during the audit period.	Boolean		`TRUE`
Authorized Unescorted Physical Access	The individual had authorized unescorted physical access to a high impact, or medium impact with ERC, BES Cyber System or associated EACMS or PACS at any time during the audit period.	Boolean		`TRUE`
Authorized BCSI Access	The individual had authorized access to BES Cyber System Information, whether physical or electronic, at any time during the audit period.	Boolean		`TRUE`
New Access Authorized	The individual had newly applicable access (Electronic, Unescorted Physical, or BCSI) that was authorized at any time during the audit period. Leave Blank if no new applicable access was authorized.	List	• `Electronic` • `Physical` • `BCSI` • `Electronic, Physical` • `Electronic, BCSI` • `Physical, BCSI` • `Electronic, Physical, BCSI`	`Electronic, BCSI`

Chapter 15: Reuse and Disposal (Reuse_Disposal) Detail Tab

The *Reuse_Disposal* tab requests information about each Cyber Asset or Shared Cyber Infrastructure released for reuse or disposal for which the Responsible Entity has compliance responsibility within the audit period. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 10: Reuse and Disposal (Reuse_Disposal) Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	The Cyber Asset (or Shared Cyber Infrastructure, if applicable) ID being released for reuse or disposal.	String	Must map to a value in the *ID* field from the "CA" tab	Pcc-his1
Prevention Date	The date of completion of the actions taken to prevent unauthorized BES Cyber System Information retrieval.	String	ISO 8601 date string	2020-04-15
Status	Status of the Cyber Asset (or Shared Cyber Infrastructure, if applicable).	List	`- Release for Reuse` `- Disposal`	`Disposal`
Status Date	The date the Cyber Asset (or Shared Cyber Infrastructure, if applicable) was released for reuse or disposed of.	String	ISO 8601 date string	2020-04-15

Chapter 16: Cyber Security Incident (CSI) Detail Tab

The *CSI* tab requests information about each Cyber Security Incident Response Plan activation for which the Responsible Entity has compliance responsibility within the audit period. The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to TRUE or FALSE.

Table 11: Cyber Security Incident (CSI) Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	The document number or other designator for the Cyber Security Incident Response Plan activated.	String		TestIncident03
Impact Rating	The BES Cyber System impact rating associated with the activated Cyber Security Incident Response Plan. If the Cyber Security Incident Response Plan activation is associated with varying impact ratings of BES Cyber Systems, identify the highest impact rating.	List	• `High/Medium` • `Low`	`Low`
Description	A description of the CSI or the incident test.	String		Quarterly tabletop exercise
Activation Date	The date of activation of the Cyber Security Incident Response Plan.	String	ISO 8601 date string	2020-04-15
Test	Indicates the activation of the Cyber Security Incident Response Plan was a test.	Boolean		`TRUE`
Response to Attempted Compromise	Indicates the activation of the Cyber Security Incident Response Plan was due to responding to a Cyber Security Incident that attempted to compromise a system.	Boolean		`TRUE`
Reportable	Indicates the activation of the Cyber Security Incident Response Plan was due to an actual Reportable Cyber Security Incident.	Boolean		`TRUE`

Chapter 17: Procurement (Procurement) Detail Tab

The *Procurement* tab requests information about each procurement for which the Responsible Entity has compliance responsibility within the audit period. Applicable procurements include each procurement of vendor products or services resulting from:

- procuring and installing vendor equipment and software; and
- transitions from one vendor(s) to other vendor(s) during the audit period.

The table below is the data specification for data that needs to be entered into this tab. Any row with the *Data Type* of "Boolean" must be explicitly set to `TRUE` or `FALSE`.

Table 12: Procurement (Procurement) Detail Tab

Field Name	Description	Data Type	Constraints	Example
ID	A unique identifier or name associated with the procurement.	String		EMS Upgrade 2020
Vendor	The vendor(s) associated with this procurement. If multiple vendors are associated with the procurement, list all that apply.	String	Comma Separated Values	Dell, SEL
Impact Rating	The impact rating of the BES Cyber System(s) associated with this procurement.	List	• `High` • `Medium` • `High and Medium`	`Medium`
Description	A brief description of the product(s), service(s) or vendor transition(s) associated with this procurement.	String		Updated all hardware in EMS system
Procured Products	Indicates the procurement included vendor products.	Boolean		`TRUE`
Procured Services	Indicates the procurement included vendor services.	Boolean		`TRUE`
Changed Vendor	Indicates the procurement included vendor transitions.	Boolean		`TRUE`
Start Date	The start date associated with this procurement. If unknown, leave blank.	String	ISO 8601 date string	2020-04-15
End Date	The end date associated with this procurement. If unknown, leave blank.	String	ISO 8601 date string	2020-04-15

Table 12: Procurement (Procurement) Detail Tab				
Field Name	**Description**	**Data Type**	**Constraints**	**Example**
Asset Classifications	The appropriate Cyber Asset classifications (or Shared Cyber Infrastructure, if applicable) associated with the procurement. If listing a software or service, provide the classification that is associated with the Cyber Asset (or Shared Cyber Infrastructure) receiving the service or software	**List**	• BCA • EACMS • PACS • SCI • BCA, EACMS • BCA, PACS • BCA, SCI • EACMS, PACS • EACMS, SCI • PACS, SCI • BCA, EACMS, PACS • BCA, EACMS, SCI • BCA, PACS, SCI • EACMS, PACS, SCI • BCA, EACMS, PACS, SCI	

Chapter 18: Using SEL Reference IDs

When uploading evidence to the ERO Secure Evidence Locker (SEL), a valid Reference ID must be used. The CIP ERT provides an SEL Reference ID that should be used when uploading evidence for the associated Request ID. The CIP ERT generated SEL Reference ID follows the "Required Reference ID Information" section of the ERO SEL Portal Guide[2]. Please work with your Regional Entity or Audit Team Lead if you have any questions or want to make modifications to the SEL Reference IDs used for evidence upload.

[2] https://www.nerc.com/ResourceCenter/Align%20Documents/RE_ERO_SEL_Portal_UserGuide.pdf

Chapter 19: Request Specific Instructions

This section is to provide additional information on specific Request IDs as noted in the Evidence Request Tool. See the specific Request IDs below for additional information

CIP-002-R1-L1-07

This request is for the Regional Entity to review any devices that were considered during the CIP-002 process but not identified as an applicable Cyber Asset. The evidence provided may be an explanation of the reasoning used while reviewing specific assets. Based on the response to this request, Regional Entities may request additional information regarding specific assets.

CIP-TFE-L1-01

Requests necessary evidence associated with any active Technical Feasibility Exceptions.

CIP-CEC-L1-01

Requests information on CIP Exceptional Circumstances associated with applicable Requirements.

CIP-SRP-L1-01

Request an overview of tools and technology used in support of CIP compliance (e.g., tabulated list of tools associated with Standards and Requirements in scope).

CIP-EOL-L1-01

Requests an entity's technologies and possible areas of risk associated with security protection.