NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Evidence Request Tool User Guide

January 2025

RELIABILITY | RESILIENCE | SECURITY

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

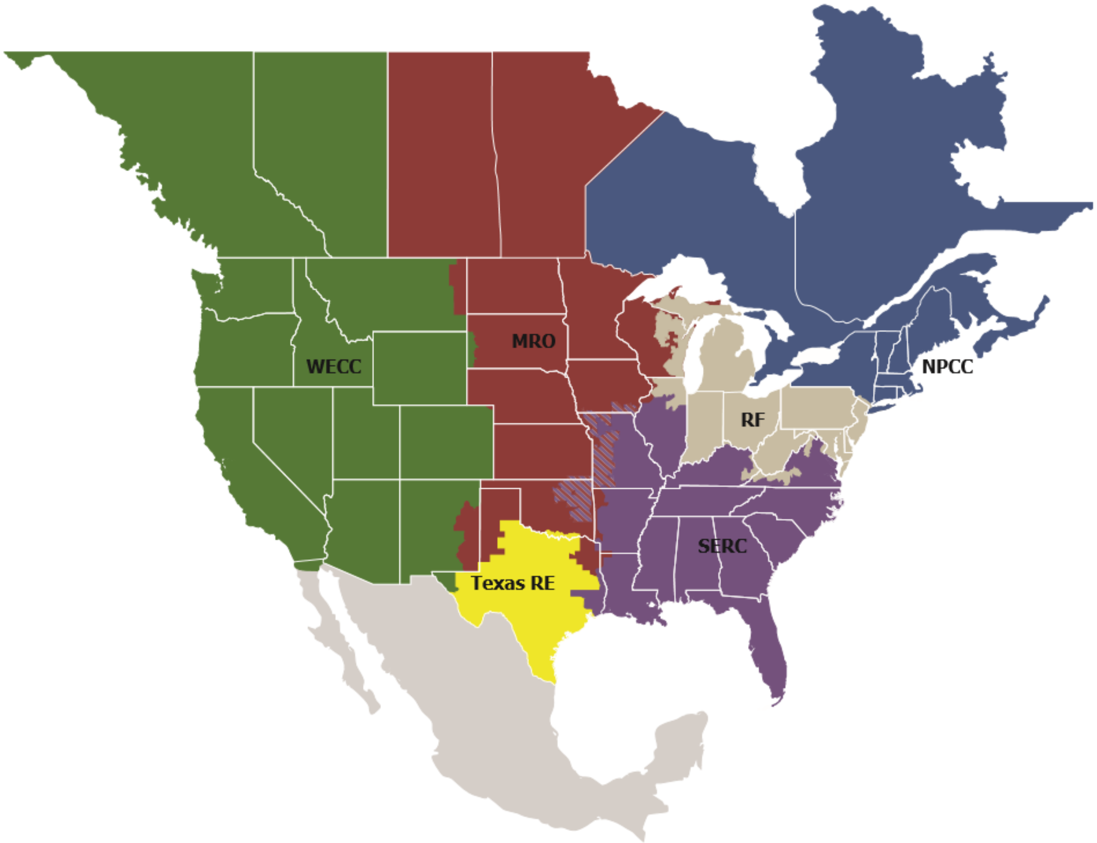
Table of Contents

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 the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable 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 divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region 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	Western Electricity Coordinating Council

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 *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

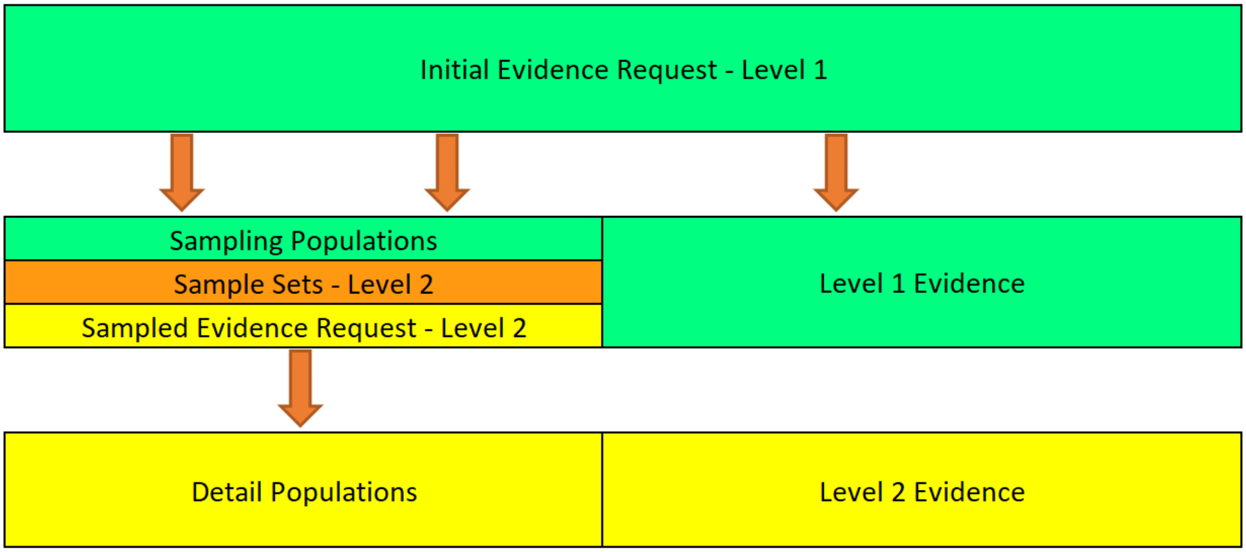


Figure 1

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. They are requests 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 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. 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 asset sampling as part of the monitoring engagement. The registered entity does not need to interact with this tab.

Sample sets include both groups of assets 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 if an evidence request. This value is unique and is the primary key for this table.

Standard

The NERC Reliability Standard that the *Level 2* request is applicable to.

Requirement

The NERC Reliability Standards requirement that the *Level 2* 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.

Sample Set

A reference to the applicable Sample Set for this *Level 2* request. This will match one or more values in the “Sample Set” field from the *Sample Sets L2* worksheet.

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 & Dates

This field is populated by the Regional Entity and returned to the Responsible Entity after the Regional Entity has reviewed the *Level 1* evidence. It contains the index numbers of the associated samples and associated sample set date ranges. The index numbers correlate to the “Index” field in the worksheet denoted by the “Source Tab” label inside the “Sample Set Source & Description” field.

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 Assets) Detail Tab

The *BES Assets* tab requests information about each physical BES asset within the scope of CIP-002, CIP-003, or CIP-012 for which the Responsible Entity has compliance responsibility.

Index

A sequential number for each row in the sheet. This value is unique and is the primary key for this table.

BES Asset ID

A unique identifier or name associated with the asset. If more than one asset bears the same name, modify the name such that the asset being referred to is clear. For example, if both a substation and a generating plant are called “Blue River,” the unique ID could be created as “Blue River Sub” and “Blue River Plant,” respectively.

Asset Type

The type of asset identified. This field contains a pull-down list of acceptable values. These values are the identified asset types within CIP-002, R1:

- Control Center (Control Centers and backup Control Centers)
- Substation (Transmission stations and substations)
- Generation (Generation resources)
- System Restoration (Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements)
- Special Protection System (Special Protection Systems that support the reliable operation of the Bulk Electric System)
- DP Protection System (For Distribution Providers, Protection Systems specified in Applicability section 4.2.1)
- Associated Data Center (for Control Centers, pursuant to the Control Center definition)

Description

A brief description of the asset to aid the audit team in identification.

Commission Date

If the asset was commissioned within the audit period, provide the date of commissioning. Otherwise, leave the field blank.

Decommission Date

If the asset was decommissioned within the audit period, provide the date of decommissioning. Otherwise, leave the field blank.

Location

Provide a brief description of the location of the asset, such as city and/or state name, or floor within a building.

Contains BES Cyber System - High Impact

This column contains a pull-down list. TRUE should be selected if the asset contains a high impact BES Cyber System, or blank if it does not.

Contains BES Cyber System - Medium Impact

This column contains a pull-down list. TRUE should be selected if the asset contains a medium impact BES Cyber System, or blank if it does not.

Contains BES Cyber System - Low Impact

This column contains a pull-down list. TRUE should be selected if the asset contains a low impact BES Cyber System, or blank if it does not.

Accessible Via a Routable Protocol – Low Impact

This column contains a pull-down list. TRUE should be selected if the asset contains any low impact BES Cyber System accessible via a routable protocol when entering or leaving the BES asset containing low impact BES Cyber System(s), or blank if it does not.

External Routable Connectivity – High/Medium Impact

This column contains a pull-down list. TRUE should be selected if the asset contains any high and/or medium impact BES Cyber System(s) that has External Routable Connectivity, or blank if it does not.

Is Vendor Remote Access Enabled to this asset?

This column contains a pull-down list. TRUE should be selected if the asset has vendor remote access to the asset, or blank if it does not.

Is Dial-up Connectivity present at this asset?

This column contains a pull-down list. TRUE should be selected if the asset contains any BES Cyber System(s) accessible via Dial-up Connectivity, or blank if it does not.

Region

In this column enter the Region(s) (MRO, NPCC, RF, SERC, Texas RE, WECC) associated with the BES asset (separated by commas).

Function

In this column enter the function(s) (TO, TOP, GO, GOP, etc.) associated with the BES asset (separated by commas).

Chapter 6: Cyber Asset (CA) Detail Tab

The *CA* tab requests information about each CA within the scope of CIP-002 through CIP-013 for which the registered entity has compliance responsibility within the audit period. CAs include virtual machines (VMs) and guest operating systems and should be identified on this tab. Additionally, CAs could include out-of-band management consoles, such as, but not limited to, iDRAC (Integrated Dell Remote Access Controller), iLO (Integrated Lights-Out), Intelligent Platform Management Interface (IPMI), and others. Include identifications of these out-of-band management consoles on this tab.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

Cyber Asset ID

A unique identifier or name associated with the Cyber Asset.

Cyber Asset Classification

This column contains a pull-down list. One of the following should be selected to identify the CIP classification of the Cyber Asset:

- BCA – BES Cyber Asset
- EACMS - Electronic Access Control or Monitoring System
- PACS – Physical Access Control System
- PCA – Protected Cyber Asset (Cyber Asset within an Electronic Security Perimeter but not included in a BES Cyber System)

Impact Rating

This column contains a pull-down list. Select either High or Medium for the impact rating of the BES Cyber System.

BES Cyber System ID(s)

Include the unique identifier for the associated BES Cyber System(s). If the applicable Cyber Asset is associated with more than one BES Cyber System, include them all. For multiple values, list all that apply as comma separated values.

BES Asset ID(s)

Provide the *BES Asset ID* the Cyber Asset is associated with, as referenced on the *BES Assets* tab.

Cyber Asset located at and/or associated with Control Center?

This column contains a pull-down list. TRUE should be selected if the Cyber Asset is located at and/or associated with a Control Center. Otherwise leave it blank.

External Routable Connectivity?

This column contains a pull-down list. TRUE should be selected if the Cyber Asset has External Routable Connectivity, including EACMS, PACS, and PCA associated with a BES Cyber System with External Routable Connectivity. Otherwise leave it blank.

Connected to a Network Via a Routable Protocol?

This column contains a pull-down list. TRUE should be selected if the Cyber Asset is connected to a network via a routable protocol. Otherwise leave it blank.

IP Address

Enter the associated IP address(es) for the Cyber Asset in this column. For multiple values, list all that apply as comma separated values.

NOTE: 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.

Electronic Security Perimeter (ESP) ID [If Any]

If the Cyber Asset is within an ESP, provide the *ESP ID,* as referenced on the *ESP* tab.

Accessible via Dial-up Connectivity

This column contains a pull-down list. TRUE should be selected if the Cyber Asset is accessible via Dial-up Connectivity. Otherwise leave it blank.

Is Interactive Remote Access (IRA) Enabled to this CA?

This column contains a pull-down list. TRUE should be selected if IRA is permitted to this Cyber Asset. Otherwise leave it blank.

Is Vendor Remote Access Enabled to this CA?

This column contains a pull-down list. TRUE should be selected if vendor remote access (e.g., IRA, system-to-system remote access, authenticated vendor-initiated remote connection) is permitted to this Cyber Asset. Otherwise leave it blank.

Physical Security Perimeter (PSP) ID [If Any]

If the Cyber Asset is within a PSP, provide the *PSP ID,* as referenced on the *PSP* tab.

Date of Activation in a Production Environment, if Activated During the Audit Period

If this Cyber Asset became active in a production environment during the audit period, enter the date the Cyber Asset became active. Otherwise leave it blank.

Date of Deactivation from a Production Environment, if Deactivated During the Audit Period

If this Cyber Asset was deactivated from a production environment during the audit period, enter the date of deactivation. Otherwise leave it blank.

Cyber Asset Function

This column contains a pull-down list. Select the function the Cyber Asset performs. If this Cyber Asset hosts other operating systems as guest/virtual machines, select “Virtual Host” as the Cyber Asset Function. If the function does not appear in the drop-down list, select “Other” and fill in the adjacent column cell.

If Cyber Asset Function is Other, please specify

Enter the Cyber Asset’s function, if “Other” was selected in the previous column.

Cyber Asset Manufacturer

Enter the name of the manufacturer of the Cyber Asset device.

Cyber Asset Model

Enter the model identifier or other descriptor to identify the Cyber Asset device.

Operating System or Firmware Type (specify version)

Enter the operating system or firmware that the Cyber Asset uses. Please include version information as well (e.g., Windows 10, Red Hat 7.1, iOS 14, etc.).

Responsible registered entity and NCR

If this response lists Cyber Asset(s) applicable to more than one registered entity, use this column to identify the registered entity(ies) associated with the Cyber Asset. Otherwise, leave it blank.

Region

In this column enter the Region(s) (MRO, NPCC, RF, SERC, Texas RE, WECC) associated with the Cyber Asset (separated by commas).

Function

In this column enter the function(s) (TO, TOP, GO, GOP, etc.) associated with the Cyber Asset (separated by commas).

Open Enforcement Action (OEA) or self-log ID(s)

If this Cyber Asset is associated with an OEA or self-log, provide the identification number. If the applicable Cyber Asset is associated with more than one ID, include them all. Otherwise leave it blank. For multiple values, list all that apply as comma separated values.

Technical Feasibility Exception (TFE) ID(s)

If this Cyber Asset is associated with a TFE, provide the TFE identification number. If the applicable Cyber Asset is associated with more than one TFE ID, include them all. Otherwise leave it blank. For multiple values, list all that apply as comma separated values.

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

The *Low CA* tab requests information about each low impact BES Cyber Asset within the scope of CIP-002 and CIP-003 for which the Responsible Entity has compliance responsibility. 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.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

BES Cyber Asset ID

A unique identifier or name associated with the BES Cyber Asset.

BES Cyber System ID(s)

Include the unique identifier for the associated BES Cyber System(s). If the applicable BES Cyber Asset is associated with more than one BES Cyber System, include them all. For multiple values, list all that apply as comma separated values.

Asset ID

Provide the *Asset ID* the BES Cyber Asset is associated with, as referenced on the *BES Assets* tab.

Any Routable Protocol Communication?

This column contains a pull-down list. TRUE should be selected if the BES Cyber Asset is using any routable protocol communication when entering or leaving the asset containing the low impact BES Cyber System(s). Otherwise leave it blank.

Accessible via Dial-up Connectivity

This column contains a pull-down list. TRUE should be selected if the BES Cyber Asset is accessible via Dial-up Connectivity. Otherwise leave it blank.

Remote Access Enabled to this CA?

This column contains a pull-down list. TRUE should be selected if remote access is permitted to this BES Cyber Asset. Otherwise leave it blank.

Responsible registered entity and NCR

If this response lists BES Cyber Asset(s) applicable to more than one registered entity, use this column to identify the registered entity(ies) associated with the BES Cyber Asset. Otherwise, leave it blank.

Region

In this column enter the Region(s) (MRO, NPCC, RF, SERC, Texas RE, WECC) associated with the BES Cyber Asset (separated by commas).

Function

In this column enter the function(s) (TO, TOP, GO, GOP, etc.) associated with the BES Cyber Asset (separated by commas).

Chapter 8: Electronic Security Perimeter (ESP) Detail Tab

The *ESP* worksheet requests information about each ESP within the scope of CIP-005 for which the Responsible Entity has compliance responsibility within the audit period. One row should be completed for each ESP identified.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

ESP ID

A unique identifier or name for the ESP.

ESP Description

Please provide a brief description of the Electronic Security Perimeter.

Network Address

Provide the list of networks in use within the ESP (e.g., 172.16.27.0/24).

Is External Routable Connectivity Permitted into the ESP?

This column contains a pull-down list. TRUE should be selected if this ESP contains a Cyber Asset with External Routable Connectivity. Otherwise leave it blank.

Is Interactive Remote Access Permitted into this ESP?

This column contains a pull-down list. TRUE should be selected if this ESP contains a Cyber Asset which can be accessed via Interactive Remote Access. Otherwise leave it blank.

Were modifications made to ESP during audit period?

This column contains a pull-down list. TRUE should be selected if this ESP experienced modifications during the audit period (e.g., major architectural changes in the network or Cyber Assets included within). Otherwise leave it blank.

Chapter 9: Electronic Access Point (EAP) Detail Tab

The *EAP* tab requests information about each EAP within the scope of CIP-005 for which the Responsible Entity has compliance responsibility within the audit period. Enter one row for each EAP identified.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

EAP ID or Interface Name

Enter an identifier or name of the interface (e.g., 0/01).

IP Address(es)

Provide the IP address(es) of the interface. For multiple values, list all that apply as comma separated values.

Cyber Asset ID of EACMS

Provide the Cyber Asset ID the EAP is associated with, as referenced on the *CA* tab.

ESP ID

Provide the ESP ID the EAP is associated with, as referenced on the *ESP* tab.

Associated with High Impact BCS and/or Medium Impact BCS at Control Centers?

This column contains a pull-down list. TRUE should be selected if the EAP is located at and/or associated with a Control Center. Otherwise leave it blank.

Were modifications made to EAP during audit period?

This column contains a pull-down list. TRUE should be selected if this EAP experienced modifications during the audit period (e.g., changes in the external network connection, added or removed during the audit period). Otherwise leave it blank.

Chapter 10: Physical Security Perimeter (PSP) Detail Tab

The *PSP* tab requests information about each PSP within scope of CIP-006 for which the Responsible Entity has compliance responsibility within the audit period. Enter each PSP and physical access point(s) identified.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

PSP ID

A unique identifier or name for the PSP.

PSP Description

Provide a brief description of the PSP (e.g., building, server room, server rack, control center, telecom room, cabinet, etc.).

Location

Provide the physical location of the PSP (e.g., building name/number, floor, etc.).

Asset ID

Provide the Asset ID the PSP is associated with, as referenced on the *BES Assets* tab.

Physical Access Point(s) ID

Provide a unique identifier or name for the physical access point associated with the PSP ID, multiple rows will be required.

Physical Access Control Type(s)

Provide a brief summary of the types of physical access control(s) used at the PSP (e.g., electronic key, physical hard key, badge reader, fingerprint sensor, iris scanner, etc.). For multiple values, list all that apply as comma separated values.

Physical Access Point(s) Description

Provide a brief description of the physical access points identified (e.g., primary door, secondary door, emergency exit only, etc.).

Impact Rating

This column contains a pull-down list. Select either High or Medium with ERC for the impact rating of the BES Cyber System(s) this PSP protects.

Were changes made to PSP during audit period?

This column contains a pull-down list. TRUE should be selected if any changes were made to the PSP during the audit period (e.g., newly commissioned, change in physical access points). Otherwise leave it blank.

Chapter 11: Transient Cyber Asset (TCA) Detail Tab

The *TCA* tab requests information about each TCA managed or not managed by the Responsible Entity within the scope of CIP-003 and CIP-010 for which the Responsible Entity has compliance responsibility within the audit period. Provide one row for each TCA managed during the audit period by the Responsible Entity or a party other than the Responsible Entity.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

TCA ID

A unique identifier or name associated with the Transient Cyber Asset.

TCA Management Type

This column contains a pull-down list. Select the management type used for this Transient Cyber Asset (Ongoing, On-demand, or Ongoing/On-demand).

Description of Use

Provide a brief description of the Transient Cyber Asset. Additionally, provide information if the TCA was used for high, medium, and/or low impact BES Cyber System(s), associated ESP(s), or PCA(s).

Managed by

This column contains a pull-down list. Select the managed by for this Transient Cyber Asset (Entity or Other Party).

Asset ID Where Used

Provide the Asset ID(s) the Transient Cyber Asset use is associated with, as referenced on the *BES Assets* tab.

Connected at Asset with High/Medium Impact BCS

This column contains a pull-down list. TRUE should be selected if this TCA connected at BES assets with high and/or medium impact BES Cyber Systems. Otherwise leave it blank.

Connected at Asset with Low Impact BCS

This column contains a pull-down list. TRUE should be selected if this TCA connected at BES assets with low BES Cyber Systems. Otherwise leave it blank.

Were changes made during the audit period?

This column contains a pull-down list. TRUE should be selected if any changes were made to Transient Cyber Assets during the audit period (i.e., changes in vulnerability management, malicious code detection, or other TCA management processes, etc.). Otherwise leave it blank.

Chapter 12: Removable Media (RM) Detail Tab

The *RM* tab requests information about RM within the scope of CIP-003 and CIP-010 for which the Responsible Entity has compliance responsibility within the audit period. Provide one row for each RM used and/or authorized during the audit period by the Responsible Entity.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

Removable Media ID

A unique identifier or name associated with the Removable Media.

Asset ID Where Used

Provide the Asset ID(s) the Removable Media is used at and/or authorized for use, as referenced on the *BES Assets* tab.

Connected at Asset with High/Medium impact BCS

This column contains a pull-down list. TRUE should be selected if this RM connected at BES assets with high and/or medium impact BES Cyber Systems. Otherwise leave it blank.

Connected at Asset with Low Impact BCS

This column contains a pull-down list. TRUE should be selected if this RM connected at BES assets with low BES Cyber Systems. Otherwise leave it blank.

Description of Use

Provide a brief description of the Removable Media. Additionally, provide information if the RM was used for high, medium, and/or low impact BES Cyber System(s), associated ESP(s), or PCA(s).

Were changes made during the audit period?

This column contains a pull-down list. TRUE should be selected if any changes were made to Removable Media during the audit period (i.e., changes in vulnerability management, malicious code detection, or other RM management processes, etc.). Otherwise leave it blank.

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

The *BCSI* tab requests information about each BCSI grouping managed by the Responsible Entity for which the Responsible Entity has compliance responsibility within the audit period. Enter one row for each logical grouping of BCSI that is being protected.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

BCSI Groupings and Description

Name or identifier of the logical grouping of BCSI.

Description of Protection Method

Description of how the BCSI is being protected. See the CIP-011-3 measures for R1 for examples of how evidence may be protected.

BCSI Type

Specify the type of BCSI. The options are as follows:

- Physical: BCSI is physical information such as printed documents
- Electronic – On Premises: BCSI is electronic and is stored onsite.
- Electronic – Off Premises: BCSI is electronic and stored offsite.

Impact Rating

This column contains a pull-down list. Select the appropriate impact rating associated with the BCSI of either ‘High,’ ‘Medium with ERC,’ or ‘Medium without ERC.’ If the BCSI location is associated with varying impact ratings of BES Cyber Systems, identify the highest impact rating.

Were changes made during the audit period?

This column contains a pull-down list. TRUE should be selected if any changes were made to the BCSI grouping during the audit period (e.g., new BCSI groupings were created or retired during the audit period, etc.). Otherwise leave it blank.

Chapter 14: Personnel (Personnel) Detail Tab

The *Personnel* tab requests information about each individual within the scope of CIP-004 for which the Responsible Entity has compliance responsibility within the audit period. If an individual had any of the following applicable access(es) during the audit period, provide one row for that individual:

- Electronic access to a
  - High impact BES Cyber System and/or associated EACMS or PACS, or
  - 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, or
  - Medium impact BES Cyber Systems with External Routable Connectivity and/or associated EACMS or PACS; or
- Access to BES Cyber System Information, whether physical or electronic.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

Unique Identifier (Employee Number, Badge Number, etc.)

An identifier that will uniquely identify the individual. If names are used, ensure no duplicate names exist. Do not use a social security number or other personally identifiable information.

Individual's Full Name

Enter the individual's full name in upper case. Enter the individual's last name, followed by a comma and a space, followed by the first name, optionally followed by a space and the middle name or initial. For example, “SMITH, JOHN H” matches this format.

Personnel Type

This column contains a pull-down list. Select the personnel type (Employee, Contractor, or Service Vendor) from this list. Optionally, the Contractor type may be used to designate any non-employee including service vendors.

Individual's Company

Company employing individuals.

Position/Job Title

Position name or job title of the individual.

Did Access Permissions Change During the Audit Period?

This column contains a pull-down list. TRUE should be selected if any of this 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. Otherwise leave it blank.

Was an Individual Transferred or Reassigned During the Audit Period?

This column contains a pull-down list. TRUE should be selected if this individual was transferred or reassigned during the audit period. Otherwise leave it blank.

If Individual was Transferred or Reassigned During the Audit Period, Date of Reassignment/Transfer Action

For transfer or reassignment actions during the audit period, enter the date of reassignment or transfer action. Otherwise leave it blank.

If Individual Was Terminated During the Audit Period, Date of Termination Action

For termination actions during the audit period, enter the date of termination. Otherwise leave it blank.

Terminated Individual had Electronic Access to High Impact BES Cyber Systems or Associated EACMS?

This column contains a pull-down list. TRUE should be selected if this individual was terminated during the audit period and had authorized electronic access to high impact BES Cyber Systems or associated EACMS. Otherwise leave it blank.

Terminated Individual had access BES Cyber System Information?

This column contains a pull-down list. TRUE should be selected if this individual was terminated during the audit period and had authorized access to BES Cyber System Information, whether physical or electronic. Otherwise leave it blank.

Revoked Individual had access to shared user accounts to High Impact BES Cyber Systems and associated EACMS?

This column contains a pull-down list. TRUE should be selected if this individual’s access was revoked during the audit period and had authorized electronic access to shared user accounts for high impact BES Cyber Systems and/or associated EACMS. Otherwise leave it blank.

Authorized Electronic Access

This column contains a pull-down list. TRUE should be selected if this 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. Otherwise leave it blank.

Authorized Unescorted Physical Access

This column contains a pull-down list. TRUE should be selected if this 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. Otherwise leave it blank.

Authorized Access to BES Cyber System Information

This column contains a pull-down list. TRUE should be selected if this individual had authorized access to BES Cyber System Information, whether physical or electronic, at any time during the audit period. Otherwise leave it blank.

Was Access Authorized During the Audit Period?

If newly applicable access was authorized during the audit period, select an option from the list of available options that applies to the access authorized for the applicable personnel. The available options are:

- **Electronic:** Personnel was authorized electronic access applicable BCS
- **Physical:** Personnel was authorized unescorted physical access to BCS

- **BCSI:** Personnel was authorized and provisioned access, either electronic or unescorted physical access, to applicable BCSI

Along with these options, any combination of the three options is available. For example, “Electronic, Physical” means that the personnel were newly authorized electronic access and unescorted physical access to applicable BCS during the audit period. If the individual did not have any newly applicable access authorized during the audit period (e.g., access was authorized prior to the audit period), leave this column blank.

Chapter 15: Reuse and Disposal (Reuse_Disposal) Detail Tab

The *Reuse_Disposal* tab requests information about each Cyber Asset released for reuse or disposal within the scope of CIP-011 for which the Responsible Entity has compliance responsibility within the audit period. Provide one row for each Cyber Asset released for reuse or disposed of during the audit period.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

Cyber Asset ID

Provide the Cyber Asset ID with which the Cyber Asset being released for reuse or disposal is associated as referenced on the *CA* tab.

Date of Prevention of Unauthorized BCSI Retrieval

Date of completion of the actions taken to prevent unauthorized BES Cyber System Information retrieval.

Status

This column contains a pull-down list. Select the status of the Cyber Asset (Release for Reuse or Disposal).

Date of Status

Specify the date the Cyber Asset was released for reuse or disposed of.

Chapter 16: Cyber Security Incident (CSI) Detail Tab

The *CSI* tab requests information about each Cyber Security Incident response plan activation within the scope of CIP-003 and CIP-008 for which the Responsible Entity has compliance responsibility within the audit period. Provide one row for each activation of a CSI response plan.

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

Cyber Security Incident Response Plan (CSIRP) Designator

Provide the document number or other designator for the CSIRP activated.

BCS Impact Rating

This column contains a pull-down list. Select the appropriate BES Cyber System impact rating associated with the activated CSIRP of either 'High/Medium' or 'Low.' If the Cyber Security Incident response plan activation is associated with varying impact ratings of BES Cyber Systems, identify the highest impact rating.

Brief Description of Incident

Provide a description of the CSI or the incident test.

Date of Activation

Provide the date of activation of the CSIRP.

Was the Incident a Test?

This column contains a pull-down list. TRUE should be selected if this activation of the CSIRP was a test. Otherwise leave it blank.

Was the Incident responding to a Cyber Security Incident that attempted to compromise a system?

This column contains a pull-down list. TRUE should be selected if this activation of the CSIRP was due to responding to a Cyber Security Incident that attempted to compromise a system. Otherwise leave it blank.

Was the Incident Reportable?

This column contains a pull-down list. TRUE should be selected if this activation of the CSIRP was due to an actual Reportable CSI. Otherwise leave it blank.

Chapter 17: Procurement (Procurement) Detail Tab

The *Procurement* tab requests information about each procurement within the scope of CIP-013 for which the Responsible Entity has compliance responsibility within the audit period. Provide one row for each procurement of vendor products or services resulting from:

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

Index

This is a sequential number for each row in the sheet, and is used for referencing a specific row in the completed tab. This numbering should be kept intact across work with the various Levels.

Unique ID

A unique identifier or name associated with the procurement. For example, a change request ticket identification number, project plan identification number, request for proposal identification number, or “EMS upgrade” could be used.

Vendor

Identify the vendor(s) associated with this procurement. If multiple vendors are associated with the procurement, list all that apply as comma separated values.

BES Cyber System Impact Level

This column contains a pull-down list. Select either High, Medium, or High and Medium for the impact rating(s) of the BES Cyber System(s) associated with this procurement.

Description of Products or Services by Vendor or Vendor Transition(s)

Provide a brief description of the products or services or vendor transition(s) associated with this procurement.

Procurement for Vendor Products?

This column contains a pull-down list. TRUE should be selected if this procurement included vendor products. Otherwise leave it blank.

Procurement for Vendor Services?

This column contains a pull-down list. TRUE should be selected if this procurement included vendor services. Otherwise leave it blank.

Procurement resulting in Vendor Transition?

This column contains a pull-down list. TRUE should be selected if this procurement included vendor transitions. Otherwise leave it blank.

Procurement Start Date

Specify the procuring start date associated with this procurement. Otherwise leave it blank if the date is unknown.

Procurement End Date

Specify the procuring end date associated with this procurement. Otherwise leave it blank if the date is unknown.

Cyber Asset Classification

Specify the appropriate Cyber Asset classification(s) (BCA, EACMS, or PACS) associated with the procurement. If listing a software or service, provide the Cyber Asset classification that is associated with the Cyber Assets receiving the service or software. If multiple Cyber Asset are associated with the procurement with different classifications, list all that apply as comma separated values.

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.[1] 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.

[1] 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, the 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.