NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Evidence Request Tool User Guide

Version 7.0

January 26, 2023

RELIABILITY | RESILIENCE | SECURITY




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

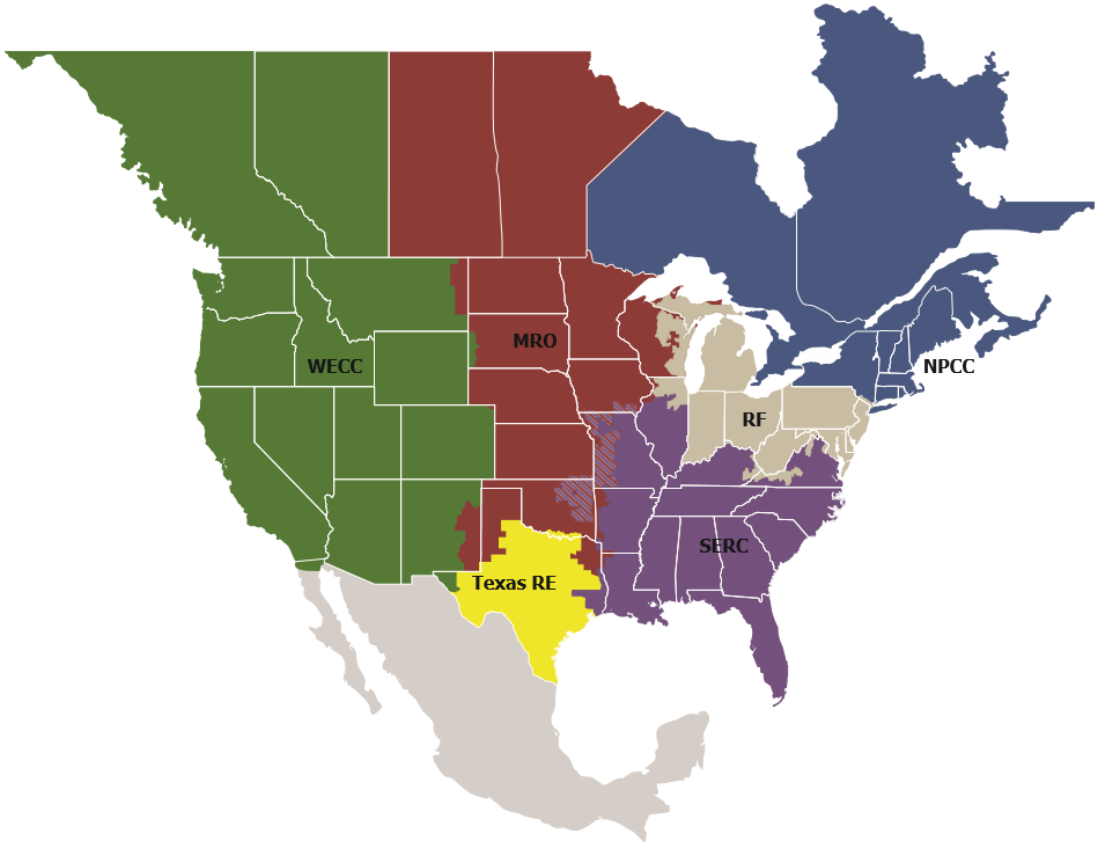
Table of Contents

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 Regions, 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.

While developing the reliability standard audit worksheets (RSAWs), the RSAW Development Team met with industry representatives to develop a better set of RSAWs. Part of that discussion centered on what types of evidence would be requested to demonstrate compliance with the CIP Reliability Standards. Since the RSAWs could not provide that level of detail, the industry representatives sought more transparency in the evidence requests that the Regions send to Responsible Entities as part of the audit process. Additionally, there was a request from the industry representatives to standardize the evidence requests across the ERO – this was especially important to Responsible Entities operating in multiple Regions.

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

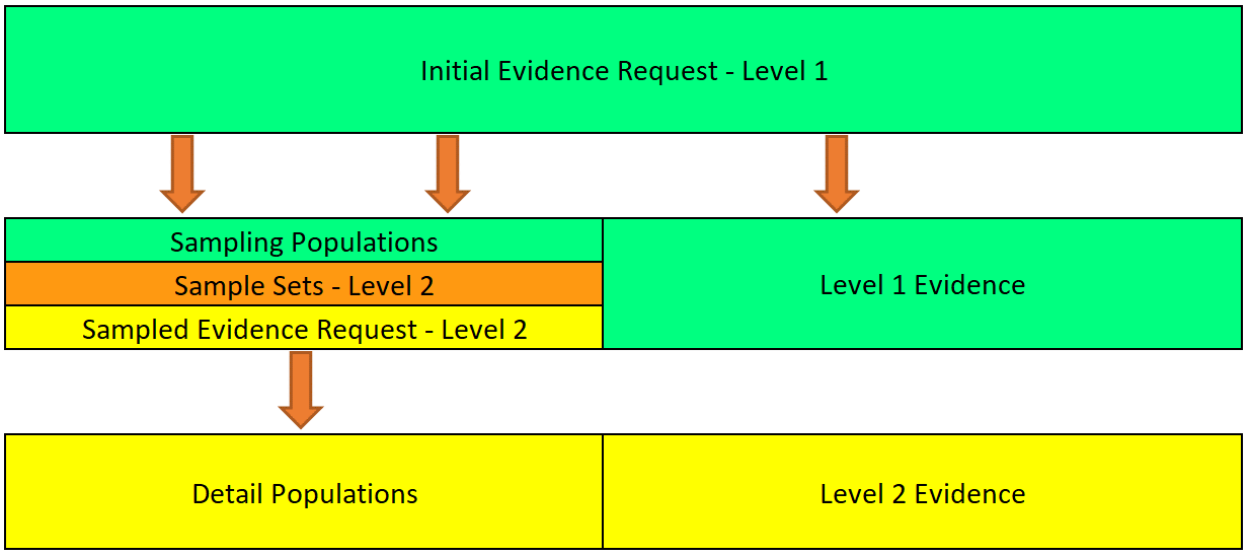


Figure 1

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-sss-Rr-Lm-nn

Where:

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

For example, CIP-002-R1-L1-03 is the third Level 1 evidence request for CIP-002, 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 Instructions

Level 1 Tab

Each row in the *Level 1* tab is a request for evidence to support the findings of an audit or other compliance action.

Detail Tab or Request ID

This column contains the Detail tab or Request ID that must be referenced when the evidence is submitted. This ID correlates the submitted evidence to the specific request for that evidence.

Note: A brighter green color is used for Request IDs that require an associated detail tab to be populated, listed at the top of the Level 1 tab. All associated detail tabs that are associated with enforceable CIP Standards should be populated regardless of scope. The Responsible Entity should work with their Region(s) for clarification or exceptions to associated detail tabs.

The Request ID abbreviations TFE, CEC, SRP, and EOL stand for Technical Feasibility Exception, CIP Exceptional Circumstance, Standards Requirements Parts, and end-of-life. These requests are informative for several Requirements and not scoped to specific Requirements.

- The TFE Request ID requests necessary evidence associated with any active Technical Feasibility Exceptions.
- The CEC Request ID will provide information on CIP Exceptional Circumstances associated with applicable Requirements.
- The SRP Request ID is intended to provide CMEP staff 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).
- The EOL Request ID is intended to inform CMEP staff of an entity's technologies and possible areas of risk associated with security protections.

Standard

The Standard is included in a separate column for sorting and filtering purposes.

Requirement

The Requirement is included in a separate column for sorting and filtering purposes.

Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet

The Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet column contains the text of the request for evidence. This column should be read carefully for each row in the worksheet. Contact the audit team lead or other compliance resource if questions arise about the meaning of any of these requests.

Note: On the Level 1 tab, there is a "For use by Region" column for annotating Response Due Dates. Regions may either use this column to indicate the due date for Request IDs and completion of the Detail tabs or annotate the due dates in alternate methods, such as within the ANL. The Responsible Entity should work with their Region(s) for clarification or exceptions to the use of this column. When submitting Level 1 evidence it is helpful to the audit team if the Responsible Entity submits a supplemental document providing a brief explanation of each of the evidence files included in a Level 1 request.

Chapter 3: Detail Tabs Instructions

Bulk Electric System (BES) Assets

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

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.

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 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).

Cyber Asset (CA)
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. Use Alt+Enter to break lines of text in a single cell.

Asset ID
Provide the *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 blank.

External Routable Connectivity?
This column contains a pull-down list. TRUE should be selected if the Cyber Asset has External Routable Connectivity. Otherwise, leave 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 blank.

IP Address
Enter the associated IP address(es) for the Cyber Asset in this column. Use Alt+Enter to break lines of text in a single cell.

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 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 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 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 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 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 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 blank. Use Alt+Enter to break lines of text in a single cell.

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 blank. Use Alt+Enter to break lines of text in a single cell.

Low CA

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. Use Alt+Enter to break lines of text in a single cell.

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 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 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 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 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).

Electronic Security Perimeter (ESP)

The *ESP* tab 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 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 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 blank.

Electronic Access Point (EAP)
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. Use Alt+Enter to break lines of text in a single cell.

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 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 blank.

Physical Security Perimeter (PSP)
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.). Use Alt+Enter to break lines of text in a single cell for multiple controls.

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 blank.

Transient Cyber Asset (TCA)
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 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 blank.

Removable Media (RM)
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 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 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).

BES Cyber System Information (BCSI)
The *BCSI* tab requests information about each BCSI location managed by the Responsible Entity for which the Responsible Entity has compliance responsibility within the audit period. Enter one row for each identified BCSI storage location.

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.

Designated Storage Location
Name or identifier of the BCSI storage location.

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.

Storage Type
This column contains a pull-down list. Select the type of storage location ("Physical" or "Electronic").

Personnel
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 designated storage locations, whether physical or electronic, for BES Cyber System Information.

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 the individual.

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 designated storage locations, whether physical or electronic, for BES Cyber System Information. Otherwise, leave blank.

Was 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 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 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 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 blank.

Terminated Individual had access to storage locations for 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 designated storage locations, whether physical or electronic, for BES Cyber System Information. Otherwise, leave 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 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 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 blank.

Authorized Access to storage locations for BES Cyber System Information

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

Was Access Authorized During the Audit Period?

This column contains a pull-down list. TRUE should be selected if any of the following access(es) were authorized for this individual during the audit period (e.g., initial access, newly acquired additional access):

- electronic access to a high impact, or medium impact with ERC, BES Cyber System or associated EACMS or PACS;
- unescorted physical access to a high impact, or medium impact with ERC, BES Cyber System or associated EACMS or PACS; or
- access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

If the individual did not have any applicable access authorized during the audit period (e.g., access was authorized prior to the audit period), leave this column blank.

Reuse_Disposal

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.

Cyber Security Incident (CSI)
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 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 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 blank.

Procurement

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**: (i) procuring and installing vendor equipment and software; and (ii) 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, use Alt+Enter to break lines of text in a single cell.

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 blank.

Procurement for Vendor Services?

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

Identification & Assessment Start Date

Specify the planning start date associated with this procurement. Otherwise, leave blank if the date is unknown.

Identification & Assessment End Date

Specify the planning end date associated with this procurement. Otherwise, leave blank if the date is unknown.

Procurement Start Date

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

Procurement End Date

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

Cyber Asset Classification (future use)

Specify the appropriate Cyber Asset classification(s) (BCA, EACMS, or PACS) associated with the procurement.

Chapter 4: Sample Sets L2

After the audit team receives the completed detail tabs from the Level 1 requests, the audit team will perform the sampling for the Level 2 Request IDs. Once the sampling is completed, the sample sets and the Level 2 requests for detailed implementation evidence, based on those samples, will be provided to the Responsible Entity.

Using the *Sample Sets L2* tab information and population filtering instructions, the audit team will identify the applicable populations for each sample set. The audit team will also select range or ranges of dates throughout the audit period as part of the samples. For example, if the audit period were January 1, 2018 through December 31, 2020 the range of dates could be:

- January 1, 2018 - April 1, 2018
- April 1, 2019 - July 1, 2019
- September 1, 2020 - December 1, 2020

Chapter 5: Level 2 Instructions

Level 2 Tab
Each row in the *Level 2* tab is a request for evidence to support the findings of an audit or other compliance action. Contact the audit team lead or other compliance resource if questions arise about the meaning of any of these requests. Note: Level 2 Request IDs may include CIP Reliability Standards and/or Requirements subject to future enforcement.

Request ID
This column contains the Request ID that must be referenced when the evidence is submitted. This ID correlates the submitted evidence to the specific request for that evidence.

Standard
The Standard is included in a separate column for sorting and filtering purposes.

Requirement
The Requirement is included in a separate column for sorting and filtering purposes.

Sample Set
The Sample Set ID used to narrow the evidence requested. Refer to the *Sample Sets L2* tab for more information regarding a specific sample set ID.

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

Sample Set Evidence Request
The Sample Set Evidence Request column contains the text of the request for evidence. This column should be read carefully for each row in the worksheet. Contact the audit team lead or other compliance resource if questions arise about the meaning of any of these requests.

Sample Set Index Numbers & Dates
The Sample Set Index Numbers column, if used by the Region, contains the index numbers of the associated samples for this Request ID and associated sample set date ranges, where applicable to the Request ID. The index numbers should be carefully correlated to the source tab's Index column for each Request ID. Contact the audit team lead or other compliance resource if questions arise about sampled index numbers. Note: The Index Number on each source tab is a sequential number for each row in the source tab and is used for referencing a specific row in the completed tab.

Entity Response
Insert the response to the Level 2 requests in this column and include references to supporting evidence. Make sure the supporting evidence clearly maps to the selected sample set (Cyber Assets, PSPs, ESPs, EAPs, etc.). It may be helpful to provide a spreadsheet or chart that lists each sample set (Cyber Assets, PSPs, ESPs, EAPs, etc.) mapped to each applicable evidence document name with the corresponding section and/or page numbers.

Note: For any system-generated evidence, the Responsible Entity should generate evidence in a manner that does not impact Real-Time operations. When submitting Level 2 evidence, provide a summary overview of the various pieces of evidence, how/why they were collected and how they fit together to demonstrate compliance. Samples/Examples using the tools and features in the PDF such as comment blocks/bubbles lassos, highlighter,

arrows, etc. are always helpful. A recommendation is to give the same evidence to someone within your organization who is less familiar with it to determine if you have provided sufficient context or explanation.