NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 (Revised) Evidence Request User Guide

Version 2.0

August 22, 2018

RELIABILITY | ACCOUNTABILITY




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

Table of Contents

Preface iv

Introduction v

Sampling vi

Audit Evidence Submission vi

Chapter 1 : General Instructions 1

Naming Convention 1

Quality of Evidence 1

Referenced Documents within a Process or Procedure 1

Chapter 2 : Level 1 Instructions 2

Level 1 Tab 2

Request ID 2

Standard 2

Requirement 2

Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet 2

Note: CIP-014-2 2

Chapter 3 : Detail Tabs Instructions 3

Bulk Electric System (BES) Assets 3

Cyber Asset (CA) 4

Low CA 6

Electronic Security Perimeter (ESP) 7

Electronic Access Point (ESP) 8

Physical Security Perimeter (PSP) 8

Transient Cyber Asset (TCA) 9

TCA Non-RE 9

Removable Media (RM) 9

BES Cyber System Information (BCSI) 10

Personnel 10

Terminations 11

Type of Access Authorized 11

Reuse_Disposal 11

Cyber Security Incident (CSI) 12

Chapter 4 : Sample Sets L2 13

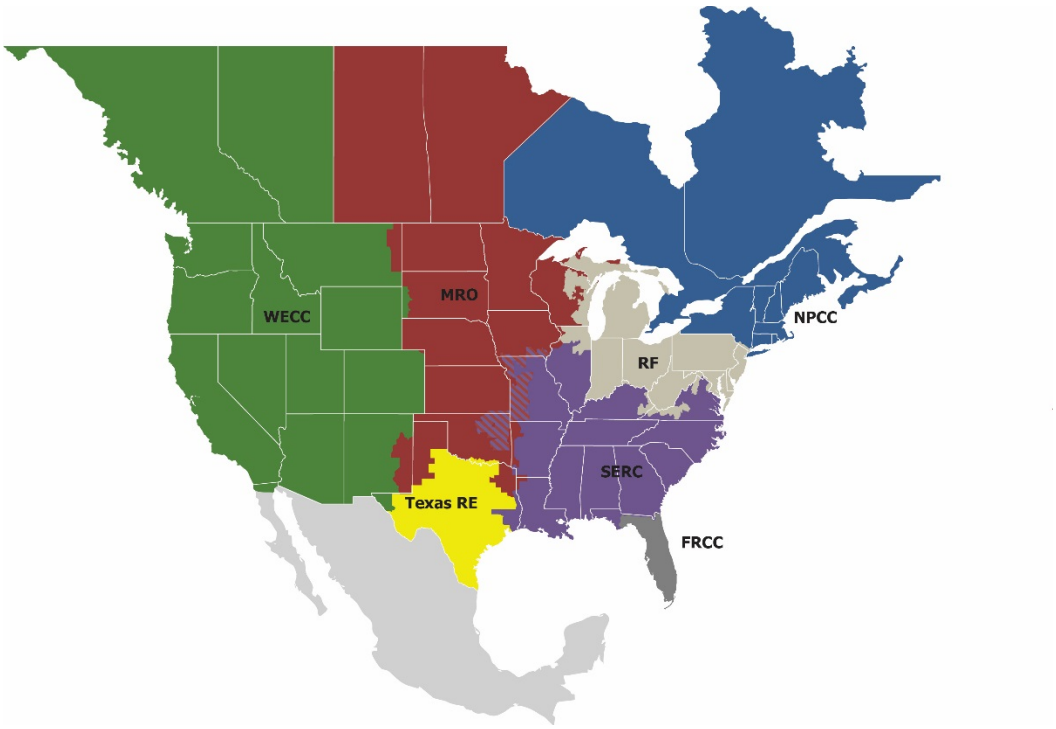
Chapter 5 : Level 2 Instructions 14

Level 2 Tab....14
Request ID....14
Standard....14
Requirement....14
Sample Set....14
Sample Set Description....14
Sample Set Evidence Request....14
Entity Response....14

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven 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.

The North American BPS is divided into seven 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.



FRCC	Florida Reliability Coordinating Council
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.

In the course of 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 V5 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 Version 5 (Revised) Evidence Request* (V5R Evidence request) 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

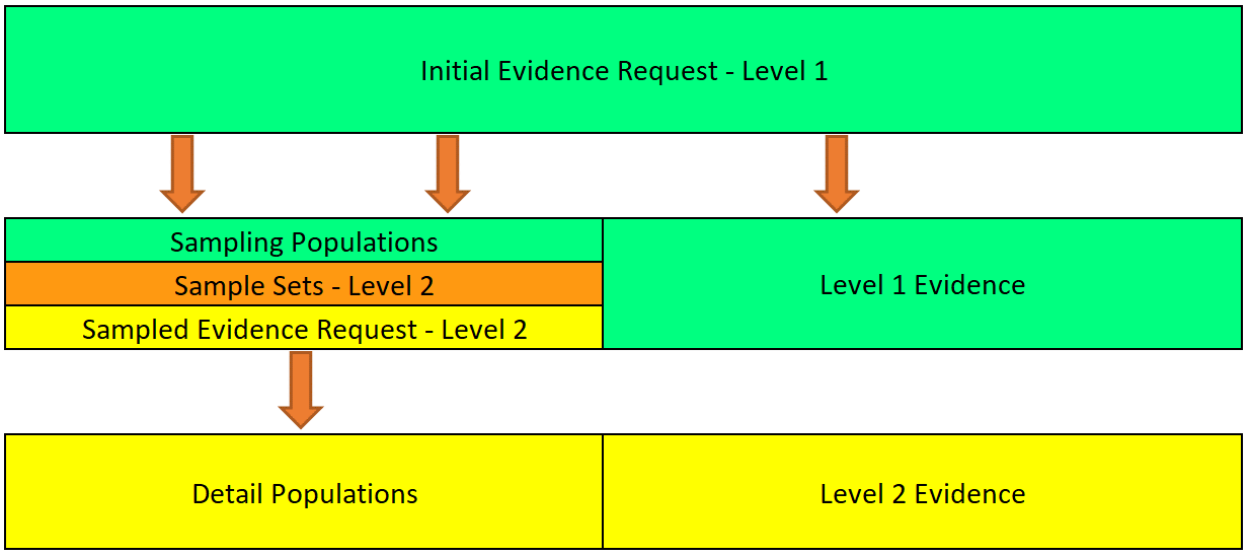


Figure 1

Figure 1 above shows a summary of the evidence request flow. The V5R Evidence Request 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. The first type is the programs, processes, and procedures that an audit team will need to review to determine compliance. The second type is the detail tabs used to form populations for sample selection which will feed into Level 2.

Level 2 asks for detailed information about individual items selected by the audit team.

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, and CSI tabs, there are "For use by Region" columns with the Sample Set. Regions may use these columns to place an "x" indicating the chosen sample set.

Audit Evidence Submission

Evidence should be submitted on the schedule and in the format specified in the audit notification.

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

For example, CIP-003-R3-L1-03 is the third Level 1 evidence request for CIP-003-6, R3.

Quality of Evidence

- Letterhead
- Structure
- Approvals
- Change History

Referenced Documents within a Process or Procedure

Documents that are referenced within a document being 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-008-5 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.

Request ID
This column contains the Request ID that must be referenced when the evidence is submitted. This ID ties 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.

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: CIP-014-2

Do not send evidence ahead of time for the following requests. The audit team will review on-site:

- CIP-014-R1-L1-01
- CIP-014-R1-L1-02
- CIP-014-R2-L1-01
- CIP-014-R3-L1-01
- CIP-014-R4-L1-01
- CIP-014-R5-L1-01
- CIP-014-R5-L1-02
- CIP-014-R6-L1-01

Note: When submitting Level 1 evidence it is helpful to the audit team if you submit a document with a brief explanation of each of the evidence files included in a Level 1 request.

Chapter 3: Detail Tabs Instructions

Each detail tab contains an *Index* as its first column. 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.

Bulk Electric System (BES) Assets

The *BES Assets* tab is requested by CIP-002-R1-L1-02, and contains information about each physical BES asset within the scope of CIP-002-5.1a for which the Responsible Entity has compliance responsibility.

Index (see Detail Tabs Instructions)

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 six identified asset types within CIP-002-5.1a, 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)

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 name, latitude/longitude, 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.

Does any BES Cyber System have routable protocol communication?
This column contains a pull-down list. TRUE should be selected if the asset contains a BES Cyber System with routable protocol communication, 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 is accessible via Dial-up Connectivity, or blank if it does not.

Region
In this column enter the region(s) (Texas RE, NPCC, MRO, FRCC, SERC, WECC, RF) of the Responsible Entity associated with the BES asset.

Function
In this column enter the function(s) (TO, TOP, GO, GOP, etc.) of the Responsible Entity associated with the BES asset.

Cyber Asset (CA)
The *CA* tab is requested by CIP-002-R1-L1-05, and contains information about each CA within the scope of CIP-002-5.1a through CIP-011-2 for which the registered entity has compliance responsibility. CAs include virtual machines (VMs) and guest operating systems. Include VMs on this tab.

Index (see Detail Tabs Instructions)

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)
- CA in BCS – Cyber Asset that is not a BES Cyber Asset but is 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* with which the Cyber Asset is associated as referenced on the *BES Assets* tab.

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.

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.

Physical Security Perimeter (PSP) Identifier [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 following column.

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
This column contains a pull-down list. Select the operating system type or firmware type the Cyber Asset uses. If the operating system or firmware type does not appear in the drop-down list, select "Other" and fill in the following column.

If Operating System or Firmware Type is Other, please specify
Enter the Cyber Asset's operating system type or firmware type, if "Other" was selected in the previous column.

Responsible registered entity and NCR
If this response covers more than one registered entity, identify the registered entity with compliance responsibility for this Cyber Asset. If this response is applicable to only one registered entity, leave blank.

Region
In this column enter the region(s) (Texas RE, NPCC, MRO, FRCC, SERC, WECC, RF) of the registered entity associated with the Cyber Asset. Use Alt+Enter to break lines of text in a single cell.

Function
In this column enter the function(s) (TO, TOP, GO, GOP, etc.) of the registered entity associated with the Cyber Asset. Use Alt+Enter to break lines of text in a single cell.

Included in an active Open Enforcement Action (OEA) or self-log?
This column contains a pull-down list. TRUE should be selected if this Cyber Asset is associated with an OEA or self-log. Otherwise leave blank.

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 is requested by CIP-002-R1-L1-06, and contains information about each low impact BES Cyber Asset within the scope of CIP-002-5.1a and CIP-003-6 for which the Responsible Entity has compliance responsibility. This tab is not mandatory and is only optional.

Index (see Detail Tabs Instructions)

Cyber Asset ID
A unique identifier or name associated with the 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* with which the Cyber Asset is associated 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 covers more than one registered entity, identify the registered entity with compliance responsibility for this BES Cyber Asset. If this response is applicable to only one registered entity, leave blank.

Region
In this column enter the region(s) (Texas RE, NPCC, MRO, FRCC, SERC, WECC, RF) of the registered entity associated with the BES Cyber Asset.

Function
In this column enter the function(s) (TO, TOP, GO, GOP, etc.) of the registered entity associated with the BES Cyber Asset.

Electronic Security Perimeter (ESP)
The *ESP* tab is requested by CIP-005-R1-L1-02, and contains information about each ESP within the scope of CIP-005-6 for which the Responsible Entity has compliance responsibility. One row should be completed for each ESP identified.

Index (see Detail Tabs Instructions)

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.

Electronic Access Point (ESP)
The *EAP* tab is requested by CIP-005-R1-L1-04, and contains information about each EAP within the scope of CIP-005-6 for which the Responsible Entity has compliance responsibility. Enter one row for each EAP identified.

Index (see Detail Tabs Instructions)

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 with which the EAP is associated as referenced on the *CA* tab.

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

Physical Security Perimeter (PSP)
Per request CIP-006-R1-L1-02, enter each PSP identified.

Index (see Detail Tabs Instructions)

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, etc.).

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

Asset ID
Provide the Asset ID with which the PSP is associated 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 Point(s) Description
Provide a brief description of the physical access points identified (e.g. badge reader, fingerprint sensor, iris scanner, etc.).

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

Transient Cyber Asset (TCA)

The *TCA* tab is requested by CIP-010-R4-L1-02, and contains information about each TCA managed by the Responsible Entity within the scope of CIP-010-2 for which the Responsible Entity has compliance responsibility. Provide one row for each TCA managed by the Responsible Entity during the audit period.

Index (see Detail Tabs Instructions)

Transient Cyber Asset 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 or On-demand).

TCA Description

Provide a brief description of the Transient Cyber Asset.

TCA Non-RE

The *TCA Non-RE* tab is requested by CIP-010-R4-L1-03, and contains information about each TCA not managed by the Responsible Entity within the scope of CIP-010-2 for which the Responsible Entity has compliance responsibility. Provide one row for each Transient Cyber Asset managed by a party other than the Responsible Entity.

Index (see Detail Tabs Instructions)

TCA ID

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

Managed by

Responsible Entity responsible for management of the Transient Cyber Asset.

Asset ID Where Used

Provide the Asset ID with which the Cyber Asset being accessed by the Transient Cyber Asset is associated as referenced on the *BES Assets* tab.

Cyber Asset ID of BCA/PCA Accessed

Provide the Cyber Asset ID of the Cyber Asset being accessed by the Transient Cyber Asset as referenced on the *CA* tab.

Date and Time of Access

Date and time the Transient Cyber Asset accessed the Cyber Asset indicated in the "Cyber Asset ID of BCA/PCA Accessed" column.

Removable Media (RM)

The *RM* tab is requested by CIP-010-R4-L1-04, and contains information about RM within the scope of CIP-010-2 for which the Responsible Entity has compliance responsibility. Provide one row for each location where RM is authorized for use.

Index (see Detail Tabs Instructions)

Removable Media ID
A unique identifier or name associated with the Removable Media.

Asset ID Where Removable Media is Authorized for Use
Provide the Asset ID with which the Removable Media is authorized for use as referenced on the *BES Assets* tab.

Description of Use
Provide a brief description of the Removable Media.

BES Cyber System Information (BCSI)
The *BCSI* tab is requested by CIP-004-R4-L1-02, and contains information about each BCSI location managed by the Responsible Entity within the scope of CIP-004-6 for which the Responsible Entity has compliance responsibility. Enter one row for each identified BCSI storage location.

Index (see Detail Tabs Instructions)

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

Impact Rating
This column contains a pull-down list. Select either High or Medium for the impact rating of the BCSI.

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

Personnel
The *Personnel* tab is requested by CIP-004-R2-L1-01, and contains information about each individual within the scope of CIP-004-6 for which the Responsible Entity has compliance responsibility. Provide one row for each person who has or has had electronic access to a high impact, or medium impact with External Routable Connectivity, BES Cyber System or associated EACMS or PACS, unescorted physical access to a high impact, or medium impact with External Routable Connectivity, BES Cyber System or associated EACMS or PACS, or access to designated storage locations, whether physical or electronic, for BES Cyber System Information, during the audit period.

Index (see Detail Tabs Instructions)

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, 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, were modified during the audit period. 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. Otherwise leave blank.

Terminations

If Individual Was Terminated During the Audit Period, Date of Termination Action
For termination actions, enter the date of termination. Otherwise leave blank.

Terminated Individual had 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 access to high impact BES Cyber Systems or associated EACMS. Otherwise leave blank.

Type of Access Authorized

Date Electronic Access Authorized
If this individual had authorized electronic access to a high impact, or medium impact with External Routable Connectivity, BES Cyber System or associated EACMS or PACS at any time during the audit period, include all date(s) when electronic access was authorized. Otherwise leave blank. Use Alt+Enter to break lines of text in a single cell.

Date Unescorted Physical Access Authorized
If this individual had authorized unescorted physical access to a high impact, or medium impact with External Routable Connectivity, BES Cyber System or associated EACMS or PACS at any time during the audit period, include all date(s) when unescorted physical access was authorized. Otherwise leave blank. Use Alt+Enter to break lines of text in a single cell.

Date Access to storage locations for BES Cyber System Information Authorized
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, include all date(s) when access to storage locations for BES Cyber System Information was authorized. Otherwise leave blank. Use Alt+Enter to break lines of text in a single cell.

Reuse_Disposal
The *Reuse_Disposal* tab is requested by CIP-011-R2-L1-02, and contains information about each CA released for reuse or disposal within the scope of CIP-011-2 for which the Responsible Entity has compliance responsibility. Provide one row for each Cyber Asset released for reuse or disposed of during the audit period.

Index (see Detail Tabs Instructions)

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 (Release for Reuse or Disposal)
Provide the applicable status: 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 is requested by CIP-008-R2-L1-02, and contains information about each Cyber Security Incident Response Plan activation within the scope of CIP-008-6 for which the Responsible Entity has compliance responsibility. Provide one row for each activation of a CSI response plan.

Index (see Detail Tabs Instructions)

Cyber Security Incident Response Plan (CSIRP) Designator
Provide the document number or other designator for the CSIRP activated.

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 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.

Chapter 4: Sample Sets L2

After the audit team receives the filled-out detail tabs from the Level 1 requests, the audit team will perform the samples to be used in the Level 2 response. The Level 2 samples will be returned to the Responsible Entity and additional evidence requested, based on those samples, in the *Level 2* tab.

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.

Request ID
This column contains the Request ID that must be referenced when the evidence is submitted. This ID ties 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. See the *Sample Sets L2* tab for more information regarding the sample.

Sample Set Description
Provides a brief description of the 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.

Entity Response
Insert your 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: When submitting Level 2 evidence it is helpful to the audit team if you submit a document with a brief explanation of each of the evidence files included in a Level 2 request.