RELIABILITY FIRST

The following are notes on the NERC CIP Version 5 Evidence Request User Guide that follows this page for use with RF Attachment C

1. **RF is not currently using the Level 3 Evidence**

2. **The following population tabs were eliminated and combined with the CA tab:**
    a. **VM**
    b. **BCS**
    c. **BCS Detail**
    d. **CABCS**

3. **The CSI tab was renamed to Incident Response**

4. **Added CIP-014-2 requests to Level 1**

5. **A Low CA population tab was added. This is purely optional in case someone wishes to provide.**

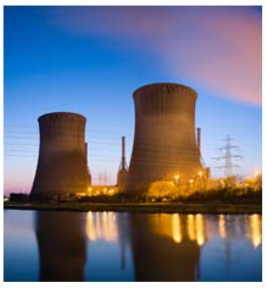
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Version 5 Evidence Request User Guide

Version 1.0

December 15, 2015

RELIABILITY | ACCOUNTABILITY

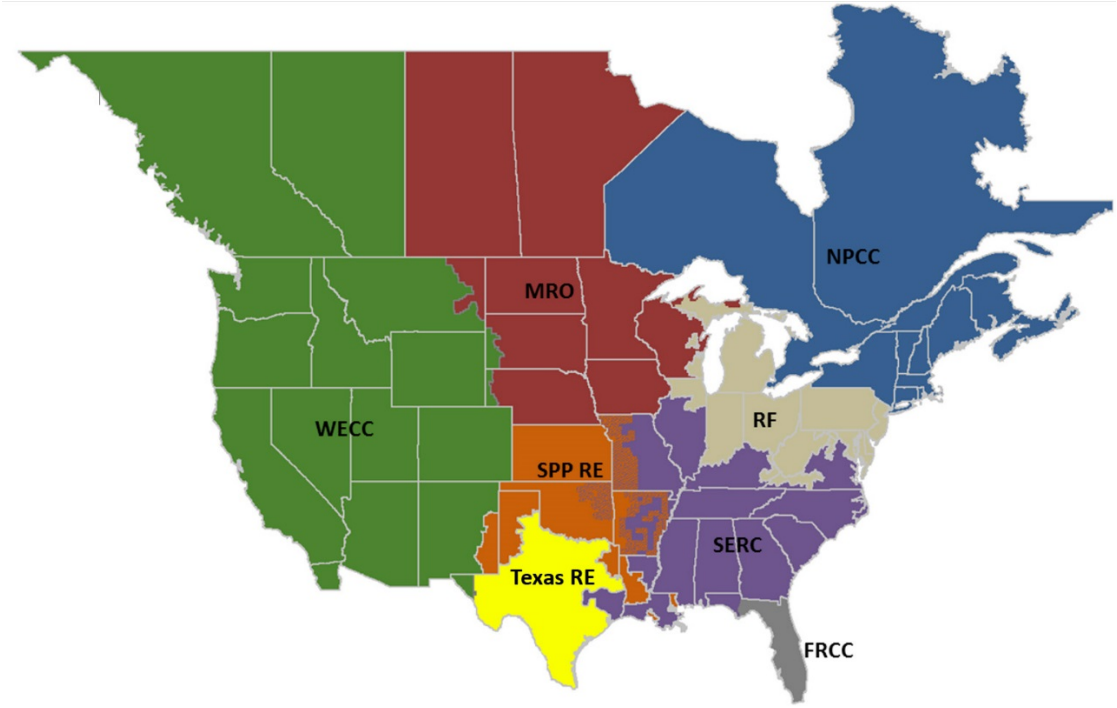
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



The Regional boundaries in this map are approximate. The highlighted area between SPP and SERC 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
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Purpose

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 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

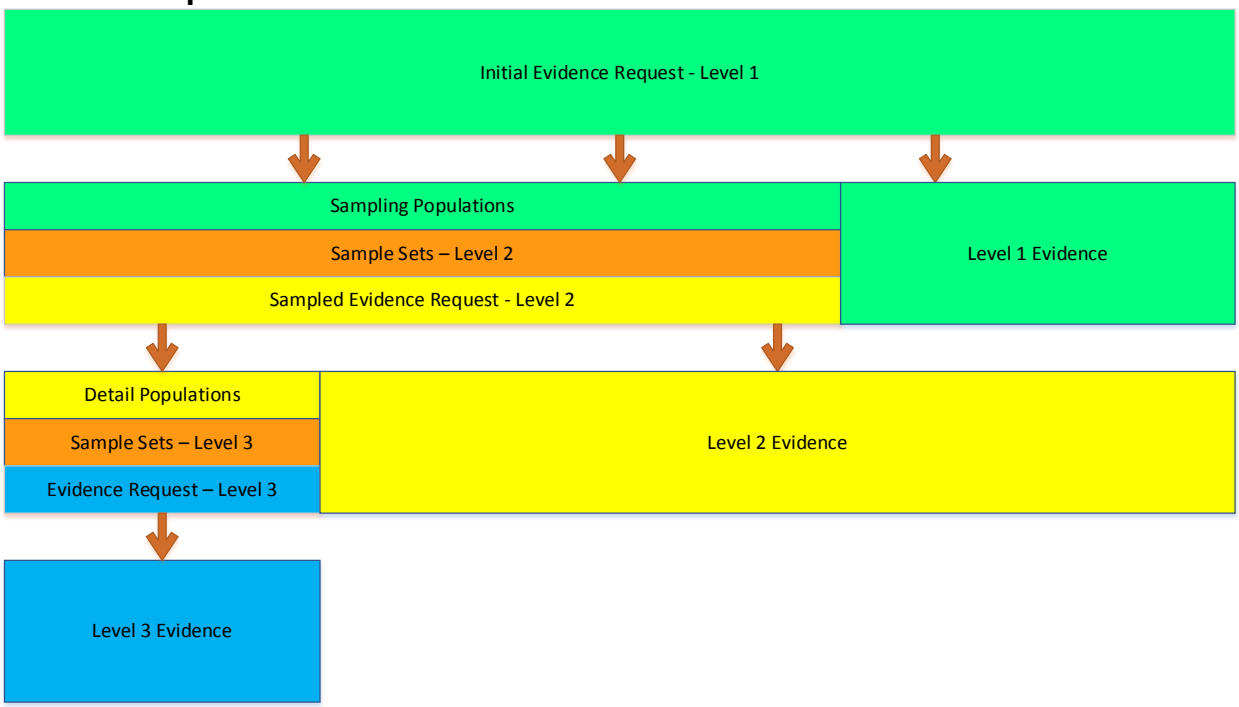


Figure 1: Evidence Request Flow

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. In some cases this will result in a Level 3 request.
Level 3 provides for another layer of sampling in the cases where that is needed.

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*.

Audit Evidence Submission

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

General Instructions

Naming Convention

Each line of the Level 1, Level 2, and Level 3 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, with "1" 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.

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

The Initial 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.

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.

BES Assets

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

Index

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-002-5.1, 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 LERC?
This column contains a pull-down list. TRUE should be selected if the asset contains a low impact BES Cyber System with Low Impact External Routable Connectivity (LERC), 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.

CA

The CA tab is requested by CIP-002-R1-L1-05, and contains information about each Cyber Asset within the scope of CIP-002-5.1 through CIP-011-2 for which the entity has compliance responsibility. As each Cyber Asset must be a "programmable electronic device," list only physical devices in this tab; virtual machines or guest operating systems will be identified later in the "VM" tab.

Index

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

Asset ID
The unique identifier of the BES Asset with which the Cyber Asset is associated. This should match an *Asset ID* entry in the BES Assets tab.

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.

ESP Identifier [If Any]
If the Cyber Asset is within an Electronic Security Perimeter (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.

Subject to CIP-005-5 R1.4
This column is calculated by a formula. Do not modify this column.

Is IRA Enabled to this CA?
This column contains a pull-down list. TRUE should be selected if Interactive Remote Access (IRA) is permitted to this Cyber Asset.

PSP Identifier [If Any]
If the Cyber Asset is within a Physical Security Perimeter (ESP), provide the *PSP ID* as referenced on the PSP tab.

Is logging performed at the CA or BCS Level?

- This column contains a pull-down list. One of the following should be selected to indicate how logging for this Cyber Asset (if any) (see CIP-007-6, R4, Part 4.1) is organized:
- CA – Logging is performed at the Cyber Asset level
- BCS – Logging is performed at the BES Cyber System level
- None – Logging is not performed

If logging is performed at the BCS level, identify the BCS that this CA is a member of where logging occurs
If logging is performed at the BES Cyber System level, enter the BES Cyber System that is being logged. This should match a *BES Cyber System ID* from either the BCS tab or the BCSdetail tab, as appropriate.

Identify the log collector for the CA or BCS
Provide the *Cyber Asset ID* (from this CA tab) of the Cyber Asset that collects the logs generated by this Cyber Asset.

Date of Activation in a Production Environment, if Activated During the Audit Period
If this Cyber Asset became active in a production environment subject to CIP-010-2, R3, Part 3.3 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 and enter the guest/virtual machines on the “VM” tab. 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 Vendor
Enter the name of the manufacturer or vendor 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
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.

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

System logging capable?
This column contains a pull-down list. TRUE should be selected if this Cyber Asset is capable of generating logs. Otherwise leave blank.

Alerting capable?
This column contains a pull-down list. TRUE should be selected if this Cyber Asset is capable of generating alerts. Otherwise leave blank.

VM

Fill out the VM tab if virtual machines are in use by any Cyber Asset in CIP scope. Each row consists of three sections, each with its own columns. Fill out one row for each virtual machine/physical host combination. For example, if one virtual machine is capable of running on three different physical hosts, then three rows should be created for that virtual machine, one for each physical host the virtual machine is capable of running on. The physical host should also appear on the "CA" tab; the virtual machine should not appear on the "CA" tab.

Index

Virtual Machine

The following columns contain information about the virtual machine (aka guest, aka client). The columns for Hypervisor and Host will be the same for each virtual machine that is capable of running on that hardware.

Name

Name or other unique identifier for the virtual machine.

Operating System

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

If Operating System is Other, please specify

Enter the virtual machine's operating system type, if "Other" was selected in the previous column.

Function

This column contains a pull-down list. Select the function the virtual machine performs. If the function does not appear in the drop-down list, select "Other" and fill in the following column.

If Function is Other, please specify

Enter the virtual machine's function, if "Other" was selected in the previous column.

Hypervisor, if other than the host operating system

If the virtual machine functionality is not provided directly by the core operating system running on the physical hardware, please identify the software providing this functionality. If the core operating system does provide this functionality (e.g., VMware vCenter Server), please leave these columns blank.

Vendor

Enter the name of the manufacturer or vendor of the hypervisor.

Product

Enter the name of the hypervisor manufacturer or vendor's product.

Host (Physical Cyber Asset/Hardware)

The host is the physical hardware platform that the virtual machines run on. This host should be identified here, and detailed information about the host should appear on the "CA" tab.

Cyber Asset ID

A unique identifier or name associated with the Cyber Asset. This should be the same ID that appears for this Cyber Asset on the "CA" tab.

BCS

The “BCS” and “BCSdetail” tabs record information about each high or medium impact BES Cyber System identified.

If all BES Cyber Systems are used to meet the obligations of all CIP Standards, Requirements, Parts, and Attachment Sections, then the “BCS” tab should be used.

In the event an entity has logically grouped a BES Cyber Asset into more than one BES Cyber System for purposes of meeting the obligations of a Standard, Requirement, Part, or Attachment Section, then the “BCSdetail” tab is used. An example of this could include a BES Cyber Asset that is logically grouped in a BES Cyber System for purposes of a specific requirement, such as CIP-007-6 R3, and is logically grouped in a different BES Cyber System for all other Requirements. In this example, the BES Cyber System used for CIP-007-6 R3 would receive an X in each column pertaining to CIP-007-6 R3, and blanks in all other columns. The BES Cyber System used for all other Requirements would receive a blank each column pertaining to CIP-007-6 R3, and an X in all other columns.

Do not fill out both the “BCS” and “BCSdetail” tabs; one should be left blank.

Index

BES Cyber System ID
Unique identifier for the 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.

Description
Please provide a brief description of the BES Cyber System.

BES Cyber System has External Routable Connectivity
This column contains a pull-down list. TRUE should be selected if this BES Cyber System has External Routable Connectivity. Otherwise leave blank.

BES Cyber System is Located at a Control Center
This column contains a pull-down list. TRUE should be selected if this BES Cyber System is located at a Control Center. Otherwise leave blank.

Applicable Physical Security Plan Identifier(s)
Please identify any physical security plans that are applicable to this BES Cyber System.

BCS Detail

The “BCS” and “BCSdetail” tabs record information about each high or medium impact BES Cyber System identified.

If all BES Cyber Systems are used to meet the obligations of all CIP Standards, Requirements, Parts, and Attachment Sections, then the “BCS” tab should be used.

In the event an entity has logically grouped a BES Cyber Asset into more than one BES Cyber System for purposes of meeting the obligations of a Standard, Requirement, Part, or Attachment Section, then the “BCSdetail” tab is used. An example of this could include a BES Cyber Asset that is logically grouped in a BES Cyber System for purposes of a specific requirement, such as CIP-007-6 R3, and is logically grouped in a different BES Cyber System for all other Requirements. In this example, the BES Cyber System used for CIP-007-6 R3 would receive an X in each column pertaining to CIP-007-6 R3, and blanks in all other columns. The BES Cyber System used for all other Requirements would receive a blank each column pertaining to CIP-007-6 R3, and an X in all other columns.

Do not fill out both the “BCS” and “BCSdetail” tabs; one should be left blank.

Index

BES Cyber System ID
Unique identifier for the 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.

Description
Please provide a brief description of the BES Cyber System.

BES Cyber System has External Routable Connectivity
This column contains a pull-down list. TRUE should be selected if this BES Cyber System has External Routable Connectivity. Otherwise leave blank.

BES Cyber System is Located at a Control Center
This column contains a pull-down list. TRUE should be selected if this BES Cyber System is located at a Control Center. Otherwise leave blank.

Applicable Physical Security Plan Identifier(s)
Please identify any physical security plans that are applicable to this BES Cyber System.

Applicability of Standards, Requirements, Parts, or Attachment Sections to BES Cyber Systems
For each BES Cyber System, place an X in each column for which a Standard, Requirement, Part, or Attachment Section is applicable.

CABCS

The “CABCS” tab is used to logically group Cyber Assets into one or more BES Cyber Systems, and to associate supporting Cyber Assets with BES Cyber Systems. For each Cyber Asset, specify the BES Cyber System into which it has been logically grouped or with which it is associated. Provide one row for each Cyber Asset/BES Cyber System grouping or association. Indicate the type of the association (“Member of BCS” or “Associated with BCS”).

Index

Cyber Asset ID
A unique identifier or name associated with the Cyber Asset. This should be the same ID that appears for this Cyber Asset on the “CA” tab.

BCS Association
This is a pull-down field. Select “Member of BCS” or indicate the Cyber Asset is logically grouped into the identified BCS. Select “Associated with BCS” to indicate the Cyber Asset is associated with the identified BCS.

BES Cyber System ID
A unique identifier for the BES Cyber System. This should be the same ID that appears for this BES Cyber System on the “BCS” tab or the “BCSdetail” tab.

ESP

One row should be completed for each Electronic Security Perimeter (ESP) identified.

Index

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. For example, 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.

EAP

Enter one row for each Electronic Access Point (EAP) identified.

Index

EAP ID or Interface Name
Enter an identifier or name of the interface (or IP address of the interface, if an identifier or name does not exist).

Cyber Asset ID of EACMS
A unique identifier or name associated with the Cyber Asset containing the EAP. This should be the same ID that appears for this Cyber Asset on the “CA” tab.

ESP ID
A unique identifier or name associated with the ESP to which the EAP is connected. This should be the same ID that appears for this ESP on the “ESP” tab.

TCA

Provide one row for each Transient Cyber Asset managed by the Responsible Entity during the audit period.

Index

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

Provide one row for each Transient Cyber Asset managed by a party other than the Responsible Entity.

Index

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

Managed by
Entity responsible for management of the Transient Cyber Asset.

BES Asset ID Where Used
The unique identifier of the BES Asset with which the Cyber Asset being accessed by the Transient Cyber Asset is associated. This should match an *Asset ID* entry in the BES Assets tab.

Cyber Asset ID of BCA/PCA Accessed
The unique identifier or name associated with the Cyber Asset being accessed by the Transient Cyber Asset. This should be the same ID that appears for this Cyber Asset on the "CA" tab.

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

RM

Provide one row for each location where Removable Media is authorized for use.

Index

BES Asset ID Where Removable Media is Authorized for Use

The unique identifier of the BES Asset where Removable Media is authorized for use. This should match an *Asset ID* entry in the BES Assets tab.

BCSI

Enter one row for each identified BES Cyber System Information (BCSI) storage location.

Index

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

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

Personnel

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

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

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 External Routable Connectivity, BES Cyber System or associated EACMS or PACS at any time during the audit period. Otherwise leave blank.

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 External Routable Connectivity, BES Cyber System or associated EACMS or PACS at any time during the audit period. Otherwise leave blank.

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.

Reuse

Provide one row for each Cyber Asset released for reuse during the audit period.

Index

Cyber Asset ID
The unique identifier or name associated with the Cyber Asset being released for reuse. This should be the same ID that appears for this Cyber Asset on the “CA” tab.

Date of Release for Reuse
Specify the date the Cyber Asset was released for reuse.

Date of Prevention of Unauthorized BCSI Retrieval
Date of completion of the actions taken to prevent unauthorized BES Cyber System Information retrieval.

Disposal

Provide one row for each Cyber Asset disposed of during the audit period.

Index

Cyber Asset ID
The unique identifier or name associated with the Cyber Asset being disposed of. This should be the same ID that appears for this Cyber Asset on the “CA” tab.

Date of Disposal
Specify the date the Cyber Asset was disposed of.

Date of Prevention of Unauthorized BCSI Retrieval
Date of completion of the actions taken to prevent unauthorized BES Cyber System Information retrieval.

CSI

Provide one row for each activation of a Cyber Security Incident response plan.

Index

CSIRP Designator
Provide the document number or other designator for the Cyber Security Incident response plan activated.

Date of Activation
Provide the date of activation of the Cyber Security Incident response plan.

Was the Incident a Test?
This column contains a pull-down list. TRUE should be selected if this activation of the Cyber Security Incident response plan 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 Cyber Security Incident response plan was due to an actual Reportable Cyber Security Incident. Otherwise leave blank.

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 entity and additional evidence requested, based on those samples, in the Level 2 tab.

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.

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 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 Sets L3

In response to the submission of Level 2 evidence, the audit team will perform additional sampling in a limited number of instances. These additional samples are to be used in the Level 3 response. The Level 3 samples will be returned to the entity and additional evidence requested, based on those samples, in the Level 3 tab.

Level 3 Tab

Each row in the Level 3 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

Sample Set

The Sample Set ID used to narrow the evidence requested. See the Sample Sets L3 tab for more information regarding the sample.

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.