Initial Engagement Submissions

Rebekah Barber
Compliance Team Lead

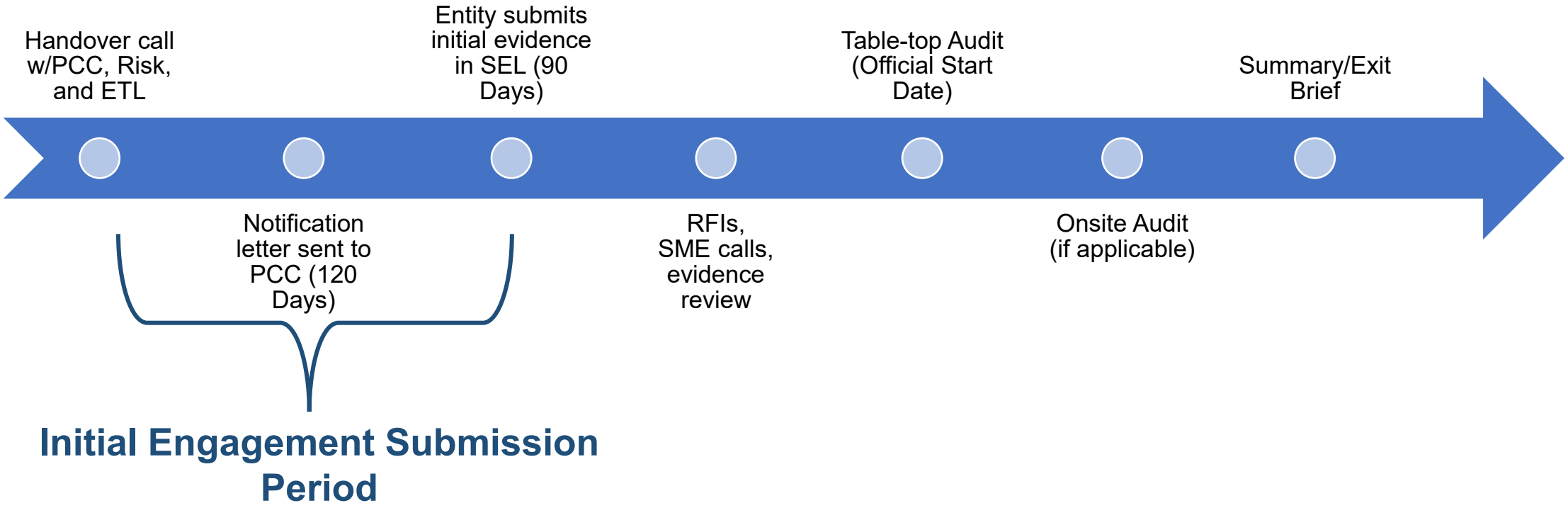
Agenda

- Value of the Initial Submission
- Engagement Timeline
- Initial Submission Expectations

Initial Engagement Submissions

- Fewer Questions
- Reference Point

Audit Process Overview



Audit Notification Package (120 Days)

What's Included:

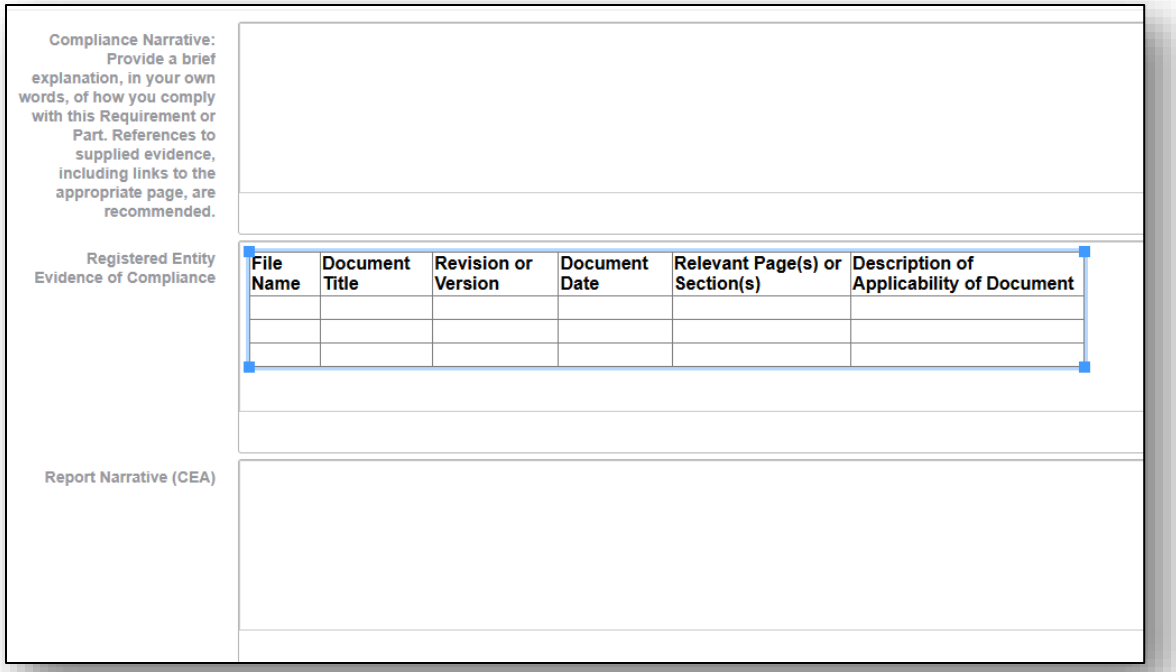
- Audit becomes visible in Align
- Audit Notification Letter (ANL)
- Initial Requests for Information (RFIs)

Initial Engagement Submission (90 Days)

- Completed Compliance Narratives and Supporting Documents
- Responses to RFI's
- Evidence Submitted to the NERC Secure Evidence Locker (SEL)

Compliance Narrative and Supporting Evidence

Compliance Audit



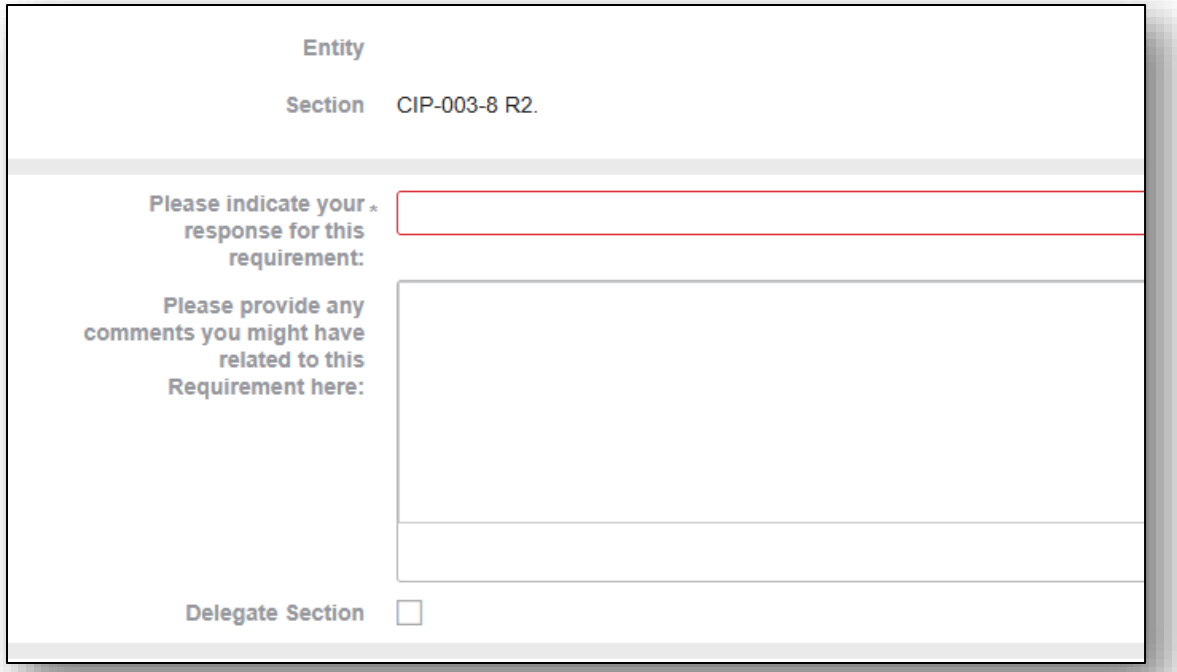
Compliance Narrative: Provide a brief explanation, in your own words, of how you comply with this Requirement or Part. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence of Compliance

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Report Narrative (CEA)

Self Certifications



Entity

Section CIP-003-8 R2.

Please indicate your response for this requirement: *

Please provide any comments you might have related to this Requirement here:

Delegate Section

Questions and Narrative

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Compliance Assessment Approach

Compliance Assessment Approach Specific to CIP-005-7 R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more process(es) which require all applicable Cyber Assets connected to a network via a routable protocol to reside within a defined ESP.
	Verify each Cyber Asset of an Applicable System that is connected to a network via a routable protocol resides within a defined ESP.
	For each defined ESP, verify the identification of any associated PCA.

Notes to Auditor:

1. This Part is applicable to all high and medium impact BES Cyber Systems and their associated PCA regardless of External Routable Connectivity.
2. Those Cyber Assets that are part of a high or medium impact BES Cyber System that are not connected to a network via a routable protocol need not reside within a defined ESP.
3. For Cyber Assets that are part of a high or medium impact BES Cyber System that do not reside within a defined ESP, the absence of a connection to a network via a routable protocol will be verified.
4. The reason to identify an ESP without External Routable Connectivity is to identify the PCA associated with the ESP.
5. In order to verify that each Cyber Asset residing within a defined ESP has been identified as either a BES Cyber Asset or as a PCA, it may be necessary to examine the ESP and conduct an inventory of network connections within the ESP.
6. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same defined ESP.

Requests For Information (RFIs)

Compliance Audit and Self Certifications

Request for Information

Parent Source

Applicable Standard/Requirement: FAC-003-4 R1.

Related Registration: NCR9999999 - TXRE - Training Energy Corp. TXRE in TXRE

Requestor

Requestor Comments: New Comment : Please provide missing evidence

Requestor Attachments

Request Sent On: August 17, 2021

Response Due By: September 16, 2021

Respondent Comments*: Paragraph | Example

Note: You cannot proceed in the workflow until the Respondent Comments are filled in. If evidence is submitted to the SEL, please check the box for Upload to SEL.

Upload to SEL

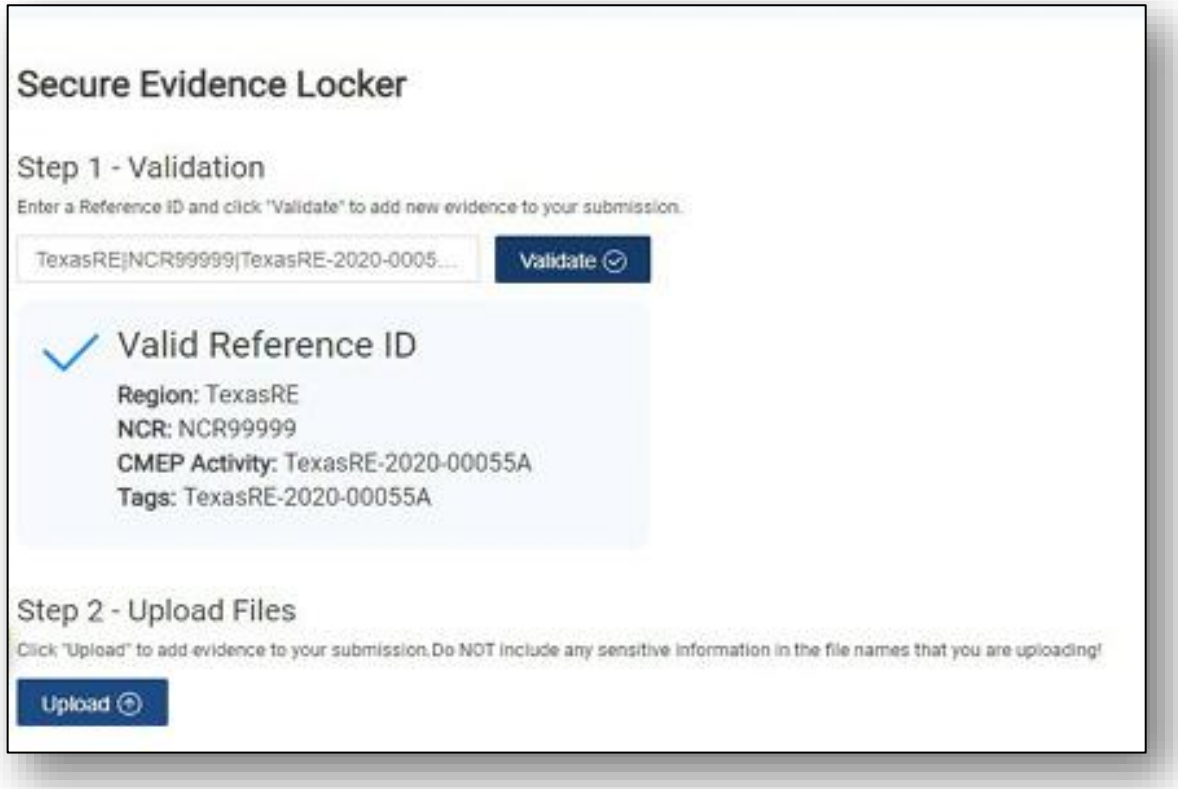
Evidence

Secure Evidence Locker Instructions: Submit Evidence or Attachments related to this item via ERO Secure Evidence Locker (SEL) located at **https://eusstg.eroenterprise.com/nerc-infrastructure** with the following reference number:

For evidence related to FAC-003-4 R1. use: TXRE|NCR9999999 - TXRE|Engagement ID| Engagement ID, RFI ID |FAC-003-4|R1.|

If you are hosting your own SEL, please provide a hyperlink to your locker in the comment section above.

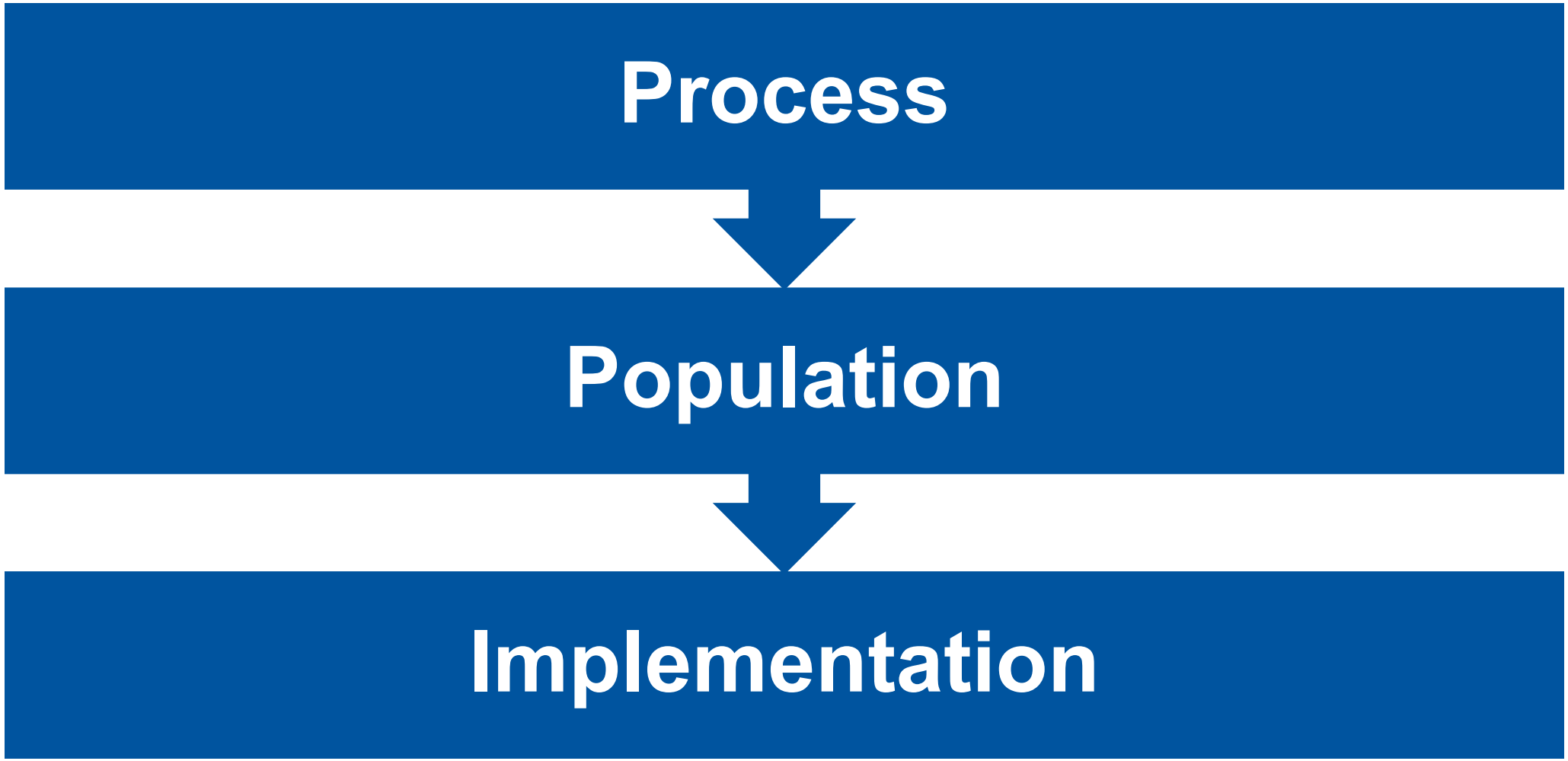
Submitting to the SEL



File Limitations:

- Individual file uploads are limited to 100 MB in size
- Do not use the '%' character in the filenames
- No compression or executable files
  - .zip
  - .7z
  - .exe

Initial Submission Guidance



Initial Submission Guidance

Process

- Provide and reference documented processes
- Explain completion of task
- Identify systems and tools used

Initial Submission Guidance

Population

- Identify applicable facilities/events/personnel/assets
- Explain how population was identified

Population Example

	Cyber Assets								El
Index	Cyber Asset	Cyber Asset Classification	Impact Rating	BES Cyber System ID(s)	BES Asset ID(s	Cyber Asset located at and/or associated with Control Center	External Routable Connectivity	Connected to a Network Via a Routable Protocol?	IP Address
1	Workstation 1	BCA	High	PCC	CC1	TRUE	TRUE	TRUE	xxx.xxx.xxx.xxx
2	Firewall	EACMS	High	PCC	CC2	TRUE	TRUE	TRUE	xxx.xxx.xxx.xxx
3	Workstation 2	BCA	Medium	Substation	SS1		TRUE	TRUE	xxx.xxx.xxx.xxx
4	Server	BCA	High	PCC	CC3	TRUE	TRUE	TRUE	xxx.xxx.xxx.xxx
5	Switch	PCA	Medium	Substation	SS2		TRUE	TRUE	xxx.xxx.xxx.xxx

Request ID	Standard	Requirement	Sample Set	Sample Set Source & Description	Sample Set Evidence Request	Sample Set Index Numbers & Dates
CIP-005-7-R1-L2-01	CIP-005-7	R1 Part 1.1	ESP-L2-01	Source Tab: ESP Description: Sample of ESPs	For each ESP in the Sample Set ESP-L2-01, provide a network diagram that includes any paths used by Interactive Remote Access and/or any paths used by dial-up connectivity.	N/A
CIP-005-7-R1-L2-02	CIP-005-7	R1 Part 1.1	CA-L2-01	Source Tab: CA Description: Sample of applicable Cyber Assets connected to a network via a routable protocol	For each Cyber Asset in Sample Set CA-L2-01, provide evidence that the Cyber Asset resides in a defined ESP.	N/A
CIP-005-7-R1-L2-03	CIP-005-7	R1 Part 1.1	CA-L2-02	Source Tab: CA Description: Sample of BES Cyber Assets and/or Protected Cyber Assets not connected via a routable protocol	For each Cyber Asset in Sample Set CA-L2-02, that are identified as not being connected to a network via a routable protocol, provide one of the following: 1. Documentation that the Cyber Asset is not capable of connecting to a network via a routable protocol; 2. Documentation that the Cyber Asset is capable of connecting to a network via a routable protocol but that the Cyber Asset is not so connected.	N/A
CIP-005-7-R1-L2-04	CIP-005-7	R1 Part 1.3	EAP-L2-01	Source Tab: EAP Description: Sample of EAPs	For each EAP in Sample Set EAP-L2-01, provide evidence of inbound and outbound access permissions (most recent version available), including the reason for granting access for each permission.	N/A
CIP-005-7-R1-L2-05	CIP-005-7	R1 Part 1.4	CA-L2-03	Source Tab: CA Description: Sample of Cyber Assets with Dial-up Capability	For each Cyber Asset in Sample Set CA-L2-03, with Dial-up Connectivity, provide evidence that authentication is required for access, or that a TFE is applicable for this device.	N/A

Initial Submission Guidance

Implementation

- Evidence creation and retrieval
- Annotate and highlight as necessary
- Examples may be appropriate based on population size

Evidence

Sufficient

- 8.99 Sufficiency is a measure of the quantity of evidence used to support the findings and conclusions related to the audit objectives*
- Sampled from the ERO Sampling Handbook

Appropriate

- 8.102 Appropriateness is the measure of the quality of evidence that encompasses the relevance, validity, and reliability of evidence used for addressing the audit objectives and supporting findings and conclusions*

**Government Auditing Standards (Yellow Book)*

What to Avoid

Data Dumping

Missing Evidence

Uncorrelated Evidence

Key Points

Tell the Story (Process)

What is Applicable? (Population)

How Did You Do It? (Implementation)