APPENDIX 15 – CYBER SECURITY PLAN

This CYBER SECURITY PLAN is broken into four sections.

- **Section 1** – Developer Scope of Work: These are the items that shall be required before the site if fully handed over.
- **Section 2** – System Security Plan Template:– Utilized by the Seller. This section provides a starting point on the Buyer's philosophy and overall design. They Seller can modify to their liking.
- **Section 3** – Project **Appendix A(Security Controls) and B (Baseline Testing)**: This is guidance on how the Buyer could audit the sites (regulatory and non-regulatory) once put into operation. The Seller is not strictly held account to these but the purpose is to inform them so they can understand the Buyer's desires.
- **Section 4** –Project Workbook Template: This template provides guidance on how to maintain tracking to the plan, IP configuration of the site, and aids in delivery of inventory.

APPENDIX 15 – CYBER SECURITY PLAN

Section 1 – Developer Scope of Work

This appendix describes the IT and Security deliverables that the Seller will provide to the Buyer. This information will be developed and delivered throughout the execution of the project. This information will be managed the Buyer.

Deliverable	Project Phase	Artifact
Security Plan	Prior to Mechanical Completion	Derived from Entergy Template, submitted, approved and stored by project management
Physical Drawing (Fence, gates, lock locations)	Prior to Mechanical Completion	Autcad, KMZ
Inventory with Attributes (Password, Firmware Rev,Log Locations, Firewall Rules, Backup/Config, Manual etc)	Prior to Substantial Completion	Entergy Provided Project Workbook
Patch Attestation <35 days	Prior to Substantial Completion	Email referencing Entergy Provided Project Workbook
EAC IOT Device Identification and Rationalization Attestation No LTE Modems behind the EAC Firewall Zigbee Wifi Loran Bluetooth	Prior to Substantial Completion	Email stating that the Security Plan section 2.3.3.4 is accurate. If any deviations exist they must be requested and accepted prior to acceptance.
No LTE Behind MSS FW Attestation	Prior to Substantial Completion	Email stating that there is no LTE Behind MSS FW
Equipment Backups/Configs Control Building (located inside Collector Substation Fence) Server Equipment including VMware PPC SCADA Systems Relays Substation RTU Firewall Switches Serial to Ethernet Converters BESS Yard Equipment Batteries Enclosure Inverter Remote Shutdown Panel Miscellaneous	Prior to Substantial Completion	Secure Offsite location reachable by project team for bulk download. Format of each deliverable is variable but based on best practice based on device type. This can include file backups from the source system to a document providing guidance on how to configure the platform. A few examples include: SEL Relay → RDB VM→Snapshot PLC→ company format

APPENDIX 15 – CYBER SECURITY PLAN

Section 2 - System Security Plan TEMPLATE

Site Name Here

City, State

System Security Plan (SSP)

CM Version	1.0
Date Issued	
Author	Robert Lewis
Program Manager	Entergy Program Manager Name Here

APPENDIX 15 – CYBER SECURITY PLAN

Approvals

Name	Position	Signature	Date
	Manager, Security Architecture		
	Sr. Security Solution Architect		
	Power Delivery Program Manager		
	Project Asset Manager		
	ROCC Director		
	Sr. Manager Risk Advisory Services, CSO		
	Director Regulatory Compliance IS		

Revision History

Date	Version	Summary of Changes	Owner
11/6/2022	0.1	Initial Document Template	Robert Lewis
10/15/2024	1	Changed watermark from Draft to Template	Robert Lewis

File Location

This document can be found at the following location:

This document is stored in Share Point under the project documents library.

1. Table of Contents

2. Introduction

2.1. Purpose of this document

The purpose of this document is to describe the System Security Plan (SSP) for the [Project Name] site. Per the scope book *"Seller shall design, build, and deliver a cyber security system and plan for the Project that conforms to applicable NERC CIP rules, regulations, standards, and Laws. Buyer shall provide Security Controls that will be required to be tested prior to site acceptance. Seller shall develop and provide to Buyer a cyber security plan that includes accommodations to test the defined security controls."*

Project sites are very large in size but require very few people to manage. Facilities at Entergy range in size from 500kw to over 100+ MWs in output power connecting from residential primary, 13.8 kv distribution voltages, to transmission interconnect voltages. The size of the physical sites ranges from less than 1 acre to more than 1,000 acres. Facilities are distributed throughout the Entergy service territory in densely populated metro as well as rural areas. Due to these varying configurations the Information Technology (IT), Operational Technology (OT), and security requirements vary.

It is understood that the Lifecycle of a Project Site (Design, Build, Transfer of Ownership, and Operation) are not always the same entity. This SSP defines the agreed to overall cyber architecture for the site in a manner that is necessary and sufficient for readers to understand how the site is to be configured and operated, the key security components of this system, ensuring upon delivery the site can be compliant with the Entergy Security Policies and NERC CIP Requirements.

Seller submits this plan acknowledging the collaborative effort that was required with Buyer with the expectation the Entergy Operational Run Team can meet the Entergy defined controls.

2.2. Scope

This document covers the Project site physical perimeter and electronic systems provided by Seller to Buyer.

3. Audience

The audience of this document is information technology/security professionals and organizational risk acceptors at Entergy who are looking for security-specific information regarding this system and context for how it is designed, deployed, and secured.

4. Requirements

The following sections describe the various requirements that Entergy has identified and that this System Security Plan addresses via direct delivery or by providing the capability to the Entergy Operational Run Team to readily deliver where technically feasible.

4.1. Business Requirements

Below are the general business requirements that shall be present and further defined in the Reference Architecture and Use Cases in Sections 6 and 7. These include:

- Site inventory with required information for site delivery and management by Entergy Operational Run Team
- Location of inventory
- Design that supports 3rd party access from 3rd parties to perform site operations and remote support
- Data exfiltration to defined cloud providers
- Connection back to Entergy systems that may include PI, SCADA, MV-90, Enterprise Ignition, etc

4.2. Risk and Compliance (NERC Designation)

The purpose is to identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.

Seller and Buyer have worked jointly to determine the CIP-002-5.1a -Cyber Security-BES Cyber System Categorization of "CIP Low" and have proceeded with all design and implementation of the site design and implementation with that determination.

4.3. Regulatory Compliance Requirements

Entergy has reviewed this Cyber Security Plan for approval to ensure that the delivery of the site addresses the following Regulatory Compliance Requirements and internal policies and procedures, and they are able to be met when put into production.

- CIP-002-5.1a -Cyber Security-BES Cyber System Categorization.
- Annual Process to the O&M operator
- CIP-007-5
- CIP-003-8
- Cyber Security Awareness Procedures- Entergy's Program
- Physical Security Controls- Entergy's Program
- Electronic Access Controls-Entergy's Program
- Cyber Incident Response – O&M Operator
- Transient Cyber Assets and Removable Media Refer to RASCI
- CIP Exceptional Circumstance Process (e.g. controls have failed and an exception to above procedures)

4.4. Entergy Security Policy and Procedure Requirements

Entergy maintains a series of Policies that shall be implemented for the environments that have Entergy data and or capability to affect its operations. Seller has consulted with Buyer throughout the process to

ensure compliance or future ability to comply with buyer's internal policies upon delivery. The assessment and enforcement of these policies is not the Seller's responsibility. Below are the Entergy items that Buyer has reviewed this plan against:

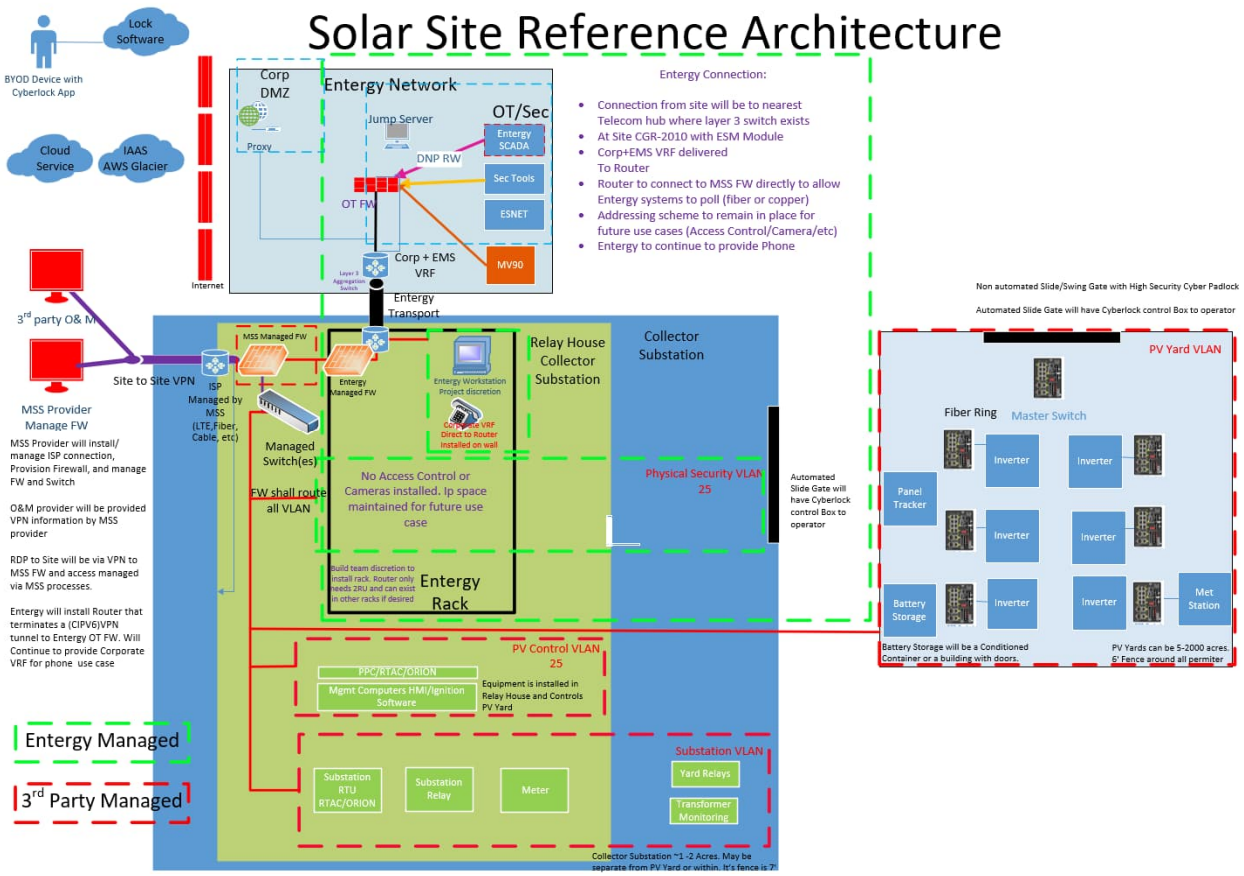
- Protection of Information
- Vulnerability Management
- Asset Management
- User Identify & Access Management Policy
- Network Segmentation
- Patch Management
- Physical Security
- Security Continuous Monitoring
- Cloud Security

5. Architecture

Text goes here.

6. Entergy Reference Architecture

The Project Site Reference Architecture (an example for Solar below) provides the framework in which a project shall be architected and executed against through the lifecycle of the facility. This includes the design, build, and operation of the facility as it relates to the IT, OT, and Security groups. Overall requirements are driven by various factors requirements as described above.



Seller agrees to review the reference architecture and implement design that meets the reference architecture use cases and underlying security controls where applicable that will be required upon commissioning. The information used and results of the coordination and outcome shall reside in this section.

The Solar Site Reference Architecture represents the high-level overview of the Project site and systems that are typically present at a facility. This drawing is used to facilitate the various discussions around how the site is configured and addresses the requirements as described above.

The drawing represents the primary focus areas, Collector Substation and PV Yard, where both physical and electronic design considerations are made but also addresses how the site connects to the various networks. The decisions in regards to network design and VLAN designation is further elaborated below and memorialized in the inventory artifact.

This site does not contain any Battery Storage devices (BESS) and is an artifact of the reference architecture provided by Entergy.

7. Use Cases to Support

Entergy has requested that the site shall support the various use cases as described below. Entergy has provided this as a way to discuss and solution the various interaction. Seller has reviewed with Entergy the applicable use cases to support in delivery of the site. Of note are:

Interface 3,4, and 5 represent SCADA Interfaces. A SCADA Edit sheet has been agreed to by the parties represented by SCADA Edit Sheet artifact.

Interface 7 MV-90 Use Case: there will be no need for MV-90 to read any meters at the site as that is accomplished with a meter in the adjacent substation.

Interface NOTES

Each Interface is a connection on a specific IP and Port over dedicated fiber path which will require FW rules when Entergy takes over.

Interface #1: O&M Operator utilizes defined VPN approach. Preference is Scenario #3.

Interface #2: These communications will leave via proxy or approved storage connection at Entergy. Proxy connections to cloud will exit via CORP VRF. This will require a FW rule with a static route. HTTPS Required.

Interface #3: Serial Connections over Dark Fiber

Interface #4: PI Data will include specific site data wishing to be stored in historian

Interface #5: MISO connection has 2 potential patterns: 1. MISO→GMS→ Solar site Direct or 2. MISO→GMS→ Interface #3 RTU directly or from EMS SCADA.

Interface #6: Security Tools will be deployed as needed. To date no AD integration or other tools to be deployed.

Interface #7: MV-90 will poll POI metering devices as required.

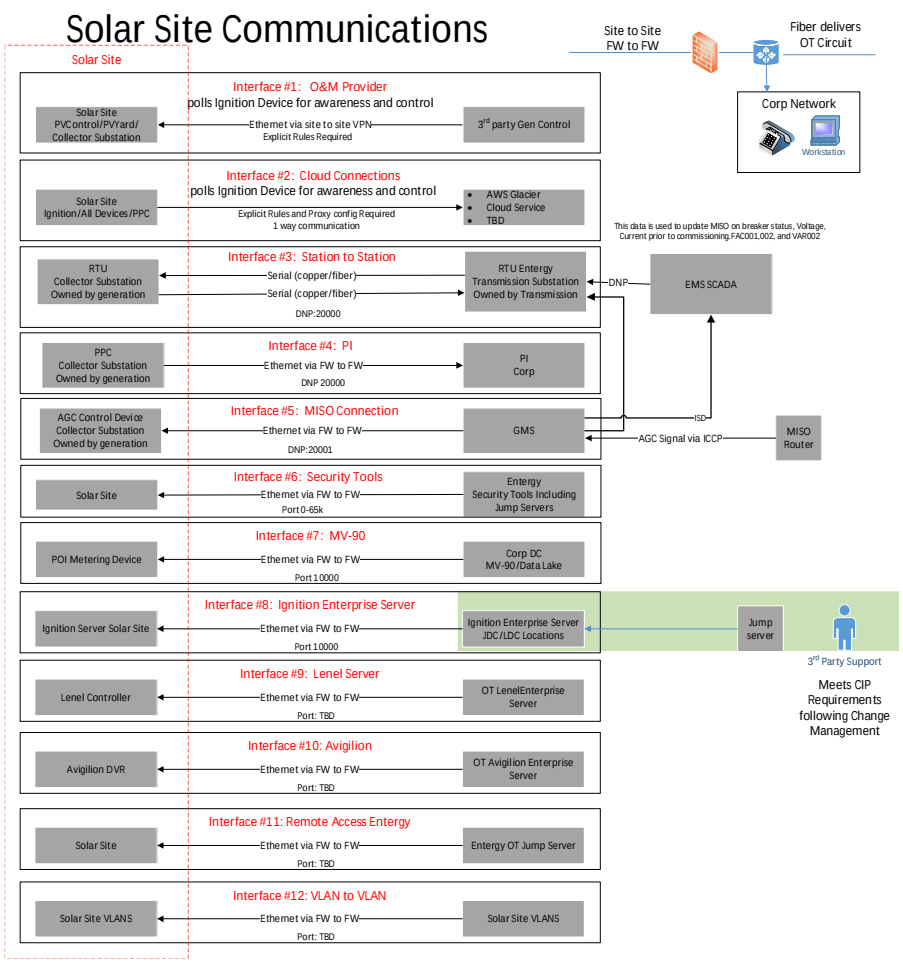
Interface #8: Ignition Enterprise Server will connect to the site and pull information back. Maturity over time will provide more control to Entergy. This includes camera feeds into the tool.

Interface #9: Lenel Server opens and closes doors

Interface #10: Avigilion Enterprise Server allows connection to the local NVR. When requested video recordings are uploaded to the Avigilion Enterprise Server.

Interface #11: RDP/SSH from Entergy OT server to 3rd party managed devices.

Interface #12: VLAN to VLAN. This allows all VLANS at the site to communicate. Explicit FW rules are required to enable this.



8. Design Discussion and Mapping to Requirements:

The below sections will describe the design. Each section will provide a quick reference to the sections of the Security Controls Appendix that they map to. It is understood that all controls in the Security Controls Appendix will not map to a specific deliverable of Seller. These references are typically after the header and may have headers such as PSC or EAC.

8.1. Project Information

The Seller shall provide a general description of the site. This includes the physical location, the applicable project parameters, etc. Other information about the project that may materially affect the SSP and its alignment with the Reference Architecture. In this section the Seller is providing the relevant information as it applies:

1.1	Project Name(s) (Common)
1.2	Project Legal Entity Name (if different)
1.3	Project Type
1.4	Project Legal Address
1.5	Project E911 Address or GPS coordinates
1.6	Does this Facility require NERC registration?
1.7	Project NERC Compliance Registry Number (NCR # - If Applicable) For the avoidance of doubt, Buyer will be responsible for registering site with NERC and obtaining the Compliance Registry Number.
1.8	Are there multiple phases to this project?
1.9	Substantial Completion Date, if applicable
1.10	Commercial Operation Date, if applicable
1.11	MW/MVA
1.12	BESS (Battery Energy Storage System) Substantial Completion Date, if applicable
1.13	BESS (Battery Energy Storage System) Commercial Operation Date, if applicable
1.14	MW/MVA

8.2. Physical Security Design

Seller has provided a physical security design as part of the requirements of the agreed to Scope Book. The site has a regulatory requirement CIP LOW which requires definition of a physical security plan. The combination of permitter fencing and locking of devices is the foundation of the physical security plan. This primarily includes Fencing and Gates as part of the permitter control. The following shows a map of the site. The site is located at the following coordinates AB°CD'EF.7GH"N, AB°CD'EF.GH"W with a physical address of Physical Address. The Fence and Access Control of the physical security solution is further defined below. For the avoidance of doubt, the perimeter fence is provided and installed by the Seller and the gate locks are provided and installed by the Buyer.

Seller has agreed per BOT scope book XYX to provide a map in both CAD and KMZ file to Buyer of all fences, gates, equipment locations including locations with electronics with connectivity (ethernet) to Seller prior ot Substantial completion. This artifact is in the list of delivery items that will be provided prior to Substantial Completion.

8.2.1. Fence and Gates:

The site design calls for a fence that will comply with section 3.2.11 of the BOT scope book. The location of the fencing, gates, and operators are shown in the CAD and KMZ files provided.

For the avoidance of doubt, the perimeter fence is provided and installed by the Seller and the gate locks (padlocks) are provided and installed by the Buyer after substantial completion.

8.2.2. Physical Access Control

As a point of reference Entergy has a robust system utilizing a combination of Lenel System for Substations and select gates and Cyber Lock System for locations that are not technically or economically feasible. The following sections will describe the utilization of each. For the avoidance of doubt, the perimeter fence is provided and installed by the Seller and the gate locks are provided and installed by the Buyer at or about Substantial Completion.

Seller has worked with Entergy to understand their desires with regards to Access Control to the physical site and their desire to have a margin of compliance by further locking electronics devices inside the physical permitter on identified devices. This includes inverters, substation, weather stations, etc. This is above and beyond a typical CIP Low Physical security but agree it is a best practice and is able to be document and deliver in compliance with Lock Locations as described in BOT (section 3.9-3.12). Some devices are not technically feasible to lock including the Inverter platform. Seller has worked with Buyer to identify such cases and reflect appropriately on the delivery KMZ and CAD Deliverables.

It was agreed that during the build and up to Substantial Completion the Seller Access Control system will be used at which point a transition to Entergy managed system will be put into place.

8.2.2.1. Lenel System (Connected via Network)

PSC-01, PSC-02, PSC-05

Entergy has a corporate access system that connects to doors and allows use of company provided identification cards to open doors. The system is typically installed in office and high value operational sites such as substations. Entergy has chosen not to use Lenel at the xxxx Site and will connect a lock as described in section 2.3.2.2.2

Per the scope book an electronic door system was to be provide. It has been determine that the Lenel or equivalent is not to be installed and only the conduit to implement automated gate controls and door access solutions to the Relay house will be fitted but nothing installed.

8.2.2.2. Electronic Lock System (Non-Connected)

PSC-01, PSC-02, PSC-05

Entergy has a robust lock program defined for non-digitally connected physical sites. The program is based on a digital lock product with various form factors that support many different lock use cases. It provides an advanced system that allows for electronic controlled access controls with logging versus a brass key program. This includes padlock style, Puck Lock, and classical cylinder-based locks. Entergy has advised that the physical permitter and selected components will be secured using Entergy provided Digital locks after substantial completion Entergy has a pre-existing relationship with reseller who defines, sells and installs the required digital locks at the site.

Seller has reviewed with Entergy the physical security layout drawing that indicates the location where installations will occur and has worked on locations that do not have a drop in lock solution. . This is in

compliance with Lock Locations as described in BOT (section 3.9-3.12). These locations include gates, any device with ethernet, and substation buildings. Seller will provide to Entergy "Artifact name" by "Agreed upon date" so that Entergy may timely procure and schedule installation after substantial completion.

Review of layout drawing will submitted by Seller 2 months prior to Substantial Completion. Buyer will provide timely feedback.

8.2.3. Cyber Asset Management

The below requirements are what the seller will provide prior to SC. Entergy has provided an example Spreadsheet, Appendix A and Appendix B to aide in the delivery of these requirements.

8.2.3.1. Inventory

EAC-01

A full inventory of all physical and cyber assets will be included in the Master Spreadsheet.

Asset management is a foundational item in the execution of the cyber security plan. Seller will provide in separate artifact containing a full inventory of all digital/cyber assets at the site. This has coordinated with Entergy and has decided to include all inventory on a Master Spreadsheet that contains all of the inventory by name, description, firmware/software revision, IP address, and user IDs,Passwords, Logging Configuration, TVM, and location to configuration and for each device type will have at a minimum the OEM manuals. This includes all electronic equipment inside of the Substation permitter including substation and Project Site control equipment. Seller has worked on an agreed upon format that aligns the hardware and software assets with the IP inventory as defined. Specifically in alignment with the Security Controls Entergy will test the O&M provider against the system delivered will comply with the following:

VLAN INFO			SUBNET INFO						
ID	VLAN Name	VLAN Description	Subnet	Mask	Inverse Mask	Subnet	Address Size	Host Range	Broadcast
1450	XYZ-OTNET	OTNET	10.ABC.DEF.0	255.255.255.248		/29	8		
1455	XYZ-OTN-MGMT	OTNET Management	10.ABC.DEF.8	255.255.255.248		/29	8		
1454	XYZ-PROD-NON-ESP	Entergy Substation VLAN	10.ABC.DEF.16	255.255.255.240		/28	16		
1453	XYZ-FAC	Physical Security VLAN	10.ABC.DEF.32	255.255.255.224		/27	32		
1457	XYZ-SOLAR-SUB	3rd Party Substation VLAN	10.ABC.DEF.64	255.255.255.224		/27	32		
1458	XYZ-PV-CONTROL	PV Control VLAN	10.ABC.DEF.96	255.255.255.224		/27	32		
1459	XYZ-PV-YARD	PV Yard VLAN	10.ABC.DEF.128	255.255.255.128		/25	128		
							256		
Entergy Specified									
Seller Specified									

Site Name:	Solar Site XYZ													
IP	Mask	Vlan	VLAN Name	Description	Additional Notes	Physical Location	Firmware Revision	Device Type	ID	Password	Logging	TVM	Config Link	Manual Link
10.ABC.DEF.64	255.255.255.224	1457	XYZ-SOLAR-SUB	Network	3rd Party Substation /27									
10.ABC.DEF.65	255.255.255.224	1457	XYZ-SOLAR-SUB	FW	VRRP									
10.ABC.DEF.66	255.255.255.224	1457	XYZ-SOLAR-SUB	XYZFWAP4001	Firewall									
10.ABC.DEF.67	255.255.255.224	1457	XYZ-SOLAR-SUB	XYZFWAP4002	Firewall									
10.ABC.DEF.68	255.255.255.224	1457	XYZ-SOLAR-SUB											
10.ABC.DEF.69	255.255.255.224	1457	XYZ-SOLAR-SUB											
10.ABC.DEF.70	255.255.255.224	1457	XYZ-SOLAR-SUB											
10.ABC.DEF.71	255.255.255.224	1457	XYZ-SOLAR-SUB											
10.ABC.DEF.72	255.255.255.224	1457	XYZ-SOLAR-SUB	RTU (OrionLX)										
10.ABC.DEF.73	255.255.255.224	1457	XYZ-SOLAR-SUB	COMM 1 (OrionLX)										
10.ABC.DEF.74	255.255.255.224	1457	XYZ-SOLAR-SUB	Meter (SEL-735)										
10.ABC.DEF.75	255.255.255.224	1457	XYZ-SOLAR-SUB	87T1P (SEL-487E)										
10.ABC.DEF.76	255.255.255.224	1457	XYZ-SOLAR-SUB	87T1S (SEL-3311A)										
10.ABC.DEF.77	255.255.255.224	1457	XYZ-SOLAR-SUB	87L1P (SEL 411L)										
10.ABC.DEF.78	255.255.255.224	1457	XYZ-SOLAR-SUB	87L1S (SEL-411L)										
10.ABC.DEF.79	255.255.255.224	1457	XYZ-SOLAR-SUB	50-51/F1 (SEL-751A)										
10.ABC.DEF.80	255.255.255.224	1457	XYZ-SOLAR-SUB	RTU-NTIO1 (Orion I/O)										

8.2.3.2. Authentication

EAC-17, EAC-18, EAC-19, EAC-20, EAC-21, and EAC-22

Seller will provide all username and passwords to digital assets where default passwords have been changed. This information will be included in the Asset Inventory as described in 2.3.3.1.1.

8.2.3.3. Logging

EAC-15 and EAC-16

Seller will Identify the source of logs on all systems and provide as part of the handoff. This includes logs that are created native to the equipment or installation specific. Include location and available methods for extraction (syslog, Database Query, etc). This can be met with a link to documentation that provides this information in the asset list or may be included in operations manual.

8.2.3.4. Patch Management

EAC-10, EAC-11, EAC-12, and EAC-13

Seller shall be responsible for patch management of the devices that they manage until substantial completion. Seller attest via the Device inventory handoff that no published CVEE over 35 days exists. If there are any exceptions seller shall inform Entergy and agree to a mitigation plan.

8.2.3.5. Backup

EAC-22

Seller has provided as part of the Inventory the configuration file, backup file, or configuration guide for identified assets. It is understood there are certain systems where this is not achievable. If so, seller will describe which pieces of equipment and point them to the RISK section to describe. It is understood that this will evolve over time but will be complete prior to SC.

8.2.3.6. Segmentation Strategy

EAC-17, EAC-18

Entergy provided Seller a high-level reference architecture. The architecture described a segmentation strategy that shows various sections of the plant to be logically segmented and routed via a local firewall with defined rules for enforcement. Seller has gained agreement with Entergy on the segmentation strategy for site and Buyer has provided the network vlan definition for ease of integration into Entergy network. Seller will configure and route the segments via the MSS Firewall (Seller provided) for distribution onto the managed switches. Make a reference to Spreadsheet?

8.2.3.7. Firewall

EAC-04, EAC-17, EAC-18,

The Solar Reference Architecture has two firewalls installed back-to-back. There is an Entergy Corporate Managed Firewall and a Managed Security Service (MSS) Firewall. The Entergy Corporate Firewall will be installed prior to substantial completion to ensure all end to end acceptance testing is able to be performed. The MSS Firewall make, model, and features was mutually agreed to by Entergy and Seller and was installed as part of the build process. As part of the engagement Seller configured the MSS firewall to communicate via a public telecom circuit of their choosing. This was set as the default gateway and is where all primary traffic for the site is to be routed. This allowed Seller to configure the MSS firewall to readily communicate with the site during the build process and allows Entergy MSS provider to perform on boarding with nominal changes to configuration to quickly facilitate transition from Seller to Buyer.

The MSS Firewall will be additionally configured to allow communications to and from the Entergy Firewall. Entergy will provide a firewall ruleset that was mutually agreeable by both parties that would allow systems such as Entergy's PI Historian, various RDP Servers, Security tools, and Ignition Enterprise System to communicate with the site.

The firewall will be configured to only allow defined firewall rules utilizing the segmentation as described in the Segmentation section below. Between each segment Explicit firewall rules were written where interactions between each segment where required. Those rules are shown below.

Interface Name	Source	IP	Destination	IP	Port	udp/tcp	Service	Description

Table ABC: Example Firewall Rules

8.2.3.8. Wireless IOT Protocols

The use of IOT protocols are typically defined as non-wifi protocols and offer an ability for the devices to be deployed and managed at a low cost. Each can be deployed securely if configured correctly. IOT protocols create an opportunity for an EAC and potential violation if not configured correctly. The following sections provide the context in which they are used at these sites.

8.2.3.8.1. Zigbee Wireless

EAC-04

The use of Zigbee at the Project sites is fairly typical for control of Arrays.

Explanation of Zigbee at the site is required including use case and the technical security configuration. If no Zigbee is present at the site the following is adequate: Seller confirms this site contains no Zigbee as all controllers are… .

8.2.3.8.2. LoRa

EAC-04

The use of LoRa is becoming more popular at Project sites by some manufactures of trackers and is the method used to communicate between controllers in the PV Yard.

Explanation of LoRa at the site is required including use case and the technical security configuration. If no LoRa is present at the site the following is adequate: Seller confirms this site contains no LoRa as all controllers are… .

8.2.3.8.3. Bluetooth

EAC-04

The use of Bluetooth is becoming more popular at Project sites. Specifically connecting to inverters and tracker control units in the PV Yard. Blue tooth introduces a TCA risk as many of the use cases involve the techs connecting from Ipads or phone devices creating a TCA risk.

Explanation of Bluetooth at the site is required including use case and the technical security configuration. If no Bluetooth is present at the site the following is adequate: Seller confirms this site contains no Bluetooth as all controllers are… .

8.2.3.9. Cellular/LTE At Site

EAC-04

The use of a cell modem as a WAN link (connected to the WAN interface on the MSS firewall) for either primary and/or back up WAN connectivity is expected and acceptable.

Project sites have a history for equipment manufacturers installing/embedded cell(LTE) modems within equipment in the PV Array that create an Electronic Access Point Concern. Seller guarantees that no Cellular/LTE modems or equivalent will present at the site beyond the one connected to the MSS firewall. If any other LTE modems are found Entergy will be notified and they will be physically removed from the devices prior to Substantial Completion.

8.2.3.10. VLAN Segmentation

EAC-03, EAC-04, EAC-05

The overall segmentation strategy has been normalized by Entergy. All Project sites will be segmented in the same convention as described by Entergy. Seller has coordinate with Entergy Data Network Team to identify the VLAN, VLAN Segment and Addressing that is acceptable to Buyer. Seller received the Segment in Table 1 and has deployed the XYZ-Project-SUB, XYZ PV-CONTROL, AND XYZ PV-YARD segments (Green) back to Buyer.

VLAN INFO			SUBNET INFO		
ID	VLAN Name	VLAN Description	Subnet	Mask	Invers
1450	XYZ-OTNET	OTNET	10.ABC.DEF.0	255.255.255.248	
1455	XYZ-OTN-MGMT	OTNET Management	10.ABC.DEF.8	255.255.255.248	
1454	XYZ-PROD-NON-ESP	Entergy Substation VLAN	10.ABC.DEF.16	255.255.255.240	
1453	XYZ-FAC	Physical Security VLAN	10.ABC.DEF.32	255.255.255.224	
1457	XYZ-SOLAR-SUB	3rd Party Substation VLAN	10.ABC.DEF.64	255.255.255.224	
1458	XYZ-PV-CONTROL	PV Control VLAN	10.ABC.DEF.96	255.255.255.224	
1459	XYZ-PV-YARD	PV Yard VLAN	10.ABC.DEF.128	255.255.255.128	
Entergy Specified					
Seller Specified					

Table 1: VLAN Definition and Address space Default VLAN configuration

8.2.3.11. Managed Switches

EAC-03, EAC-23

The Project site consists of many switches. The VLANs that consist as part of the segmentation policy will be delivered by the firewall and assigned physical ports on the managed switches. This may consist of 1 or many ports that connects to downstream switches. The switch shall follow the normal configuration that no VLAN to VLAN communications occur on the switch but are routed via the Firewall and if allowed via ruleset are then routed back to the managed switch.

8.2.3.12. Remote Access

EAC-04, EAC-05,EAC-08, EAC-09

Interactive remote access is a key element to performing the O&M function of the site. There is a need to connect to the site and manage the devices. The design supports various patterns to accomplish this task either from a 3rd party separate to Entergy or from within Entergy. The MSS firewall has been configured with a site to site VPN with defined source and destination addresses during the build process. Upon competition Entergy will be able to configure the firewall to allow connections from trusted parties in a similar manner as well as configure the MSS firewall to allow further connections from the Entergy managed firewall.

9. Security Controls and Testing

The security control baseline is based upon the guidance in *CIP-003-8 – Cyber Security – Security Management Controls*

As this is more closely aligned to a Low Impact asset there are minimum controls. However, in line with best practices the site design and delivery has more restrictive controls capabilities that allow alignment with best practice and Medium CIP site and applicable Entergy controls, where financially and operationally feasible.

Buyer by acceptance of this document acknowledges Seller has provided a security Plan/Design that allows/enables the identified Security Controls in Appendix A and Test in Appendix B to to be met by Buyer or its assigned provider at COD.

10. Controls

Appendix A has been provided by Entergy as a requirement to be met by the responsible party (Entergy Operational Run Team) and list each of the discrete security controls in each of the following sections that shall be tested by the Entergy Operational Run Team.

1. Cyber Security Awareness
2. Physical Security Controls
3. Electronic Access Controls
4. Cyber Security Incident Response
5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation

11. Testing

Appendix B has been provided by Entergy as a document to help document the Controls identified in Appendix A Security Controls. Seller has reviewed and submits this template with confidence that the design and deliverables can be readily met by the Entergy Operational Run Team.

Entergy description of Testing:

The test plan is designed to take each security significant requirement and to demonstrate due diligence in testing to ensure the control is adequately implemented. Se Each test will capture the following information:

- Requirement # (from ID)
- Expected Setting(s) and Test Plan - expected security outcome
- Test Evidence – steps taken to test, screenshots, and logs
- Test Result –Pass, Fail, Partial Pass, N/A
- Tested By – person who tested
- Date Tested – Date the person tested

For each test, documentation should be attached as evidence to include log files, screen shots, or other information relevant to providing assurance to risk acceptance officials that the system is adequately secured or configured as documented. The appendixes provide the test plan for the security baselines. It is expected that before the site is turned over via Generation Operation Ready Assessment (ORA) that these artifacts be completed.

12. Risk Assessment

Entergy has provided this section. Seller has included it to help normalize any risk identified through the design that the Entergy Operational Run Team may have meeting.

Entergy description of Risk Assessment:

The risk assessment evaluates possible negative events and/or threats that could occur, the possibility of occurring (likelihood), and the impacts of them occurring (consequence). Mitigations are then applied based on the controls, architecture, and baselines documented in the security plan to calculate the residual risk if the prescribed controls in Appendix A are not fully met. The residual

risk allows Entergy decision makers to make an informed decision to authorize a new system or major change to an existing system based on the cyber and information security risks that it presents. An explanation of the risk evaluation methodology is provided below:

- Risks – Identify the new risks introduced by this technology and any known threats that would be able to exploit this risk
- Consequence – Identify the "so-what" of this risk occurring
    - Low – minor or insignificant damage
    - Medium – measurable impact but recoverable
    - High – significant impact and/or unrecoverable
- Likelihood – Identify the likelihood of the risk actually occurring
    - Low – unlikely to happen in the immediate future
    - Moderate – reasonable possibility of happening in the immediate future
    - High – near certainty of happening in the immediate future
- **Mitigations** – Identify the mitigations already in place or being put in place to minimize or eliminate this risk
- Residual Risk/Risk Score – Identify the residual risk score after the mitigations are in place
    - Low – risk is acceptable low after mitigation
    - Medium – risk level is not acceptable long-term but should not impact short-term operations; additional mitigations should be funded over time
    - High – risk level is not acceptable short-term and the system should not be authorized to operate

The following risks were evaluated as applicable to this system:

This should be a list of each controls the Seller feels will not be able to be met due to technical feasibility. This could include a Zigbee reference, LTE, or say a clasp on an inverter where Entergy would have to add a clasp o accomplish locking.

An O&M PROVIDER responds with their implementation, this table should be populated

Risk/Threat	Consequence	Likelihood	Mitigations	Residual Risk
Risk/Threat 1	Medium	Low	Mitigation 1 Mitigation 2	Low
Risk/Threat 2	Medium	Low	Mitigation 1 Mitigation 2	Low

Section 3 - Project Appendix A(Security Controls) and B (Baseline Testing)

12.1. Cyber Security Awareness / Personnel and Training

Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

CSA-01

- **Description**: Ensure all users receive cyber security awareness training at least once every 15 calendar months
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-003-8 – Appendix 1
    - CIP-004-6 R2

CSA-02

- **Description**: Ensure all users are identified and meet Entergy's requirements for accessing data/systems
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-003-8 – Appendix 1
    - CIP-004-6 R3
    - IT-PR-007 "IT Vendor Resource On-Boarding Procedure"

CSA-03

- **Description**: Ensure all users with electronic and unescorted physical access are documented
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-003-8 – Appendix 1
    - CIP-004-6 R4
    - IT-PR-518 "Access Management"

CSA-04

- **Description**: Ensure access is revoked when users/contractors are terminated
- **Implementation**:

- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-003-8 – Appendix 1
    - CIP-004-6 R5
    - IT-PR-007 “IT Vendor Resource On-Boarding Procedure”

12.2. Physical Security Controls

Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented in the *Electronic Access Controls* section, if any.

PSC-01

- **Description**: Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-006-6 1.2

PSC-02

- **Description**: Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-006-6 1.8

PSC-03

- **Description**: Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:
    - encryption of data that transits such cabling and components;
    - monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication

failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or
    - an equally effective logical protection.
- **Implementation:**
- **Implementation Status:**
- Responsible Party:
- References:
    - CIP-006-6 1.10

PSC-04

- **Description**: Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-006-6 R1, 2.1

PSC-05

- **Description**: Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-006-6 R1, 2.2

12.3. Electronic Access Controls

For each asset that is a Cyber System(s), the Responsible Entity shall implement electronic access controls to:

1. Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:
    a. between a Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
    b. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
    c. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR- 61850-90-5 R-GOOSE).

12.3.1. Asset Management

EAC-01

- **Description**: Identify each Cyber Asset and update inventory list whenever changes are made and review/update it at least every 15 months.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-002-5.1a R1, R2

EAC-02

- **Description**: When replacing/retiring a system validate sensitive information is destroyed according to NIST data destruction guidance
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - NIST Special Publication 800-88

EAC-22

- **Description**: System configuration shall be backed up/stored and readily accessible for restoration.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - NIST Special Publication 800-88

12.3.2. Electronic Security Perimeter and Electronic Access Points

EAC-03

- **Description**: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-005-5 1.1

EAC-04

- **Description**: All External Routable Connectivity must be through an identified Electronic Access Point (EAP).

- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-005-5 1.2

EAC-05

- **Description**: EAPs Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-005-5 1.3

EAC-06

- **Description**: EAPs must have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-005-5 1.5

EAC-07

- **Description**: Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-005-5 2.1

EAC-08

- **Description**: For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-005-5 2.2

EAC-09

- **Description**: Require multi-factor authentication for all Interactive Remote Access sessions.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-005-5 2.3

12.3.3. Patch Management

EAC-10

- **Description**: A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-007-6 2.1
    - IT-PR-506 "Security Patch Management"
    - IT-PR-513 "Threat and Vulnerability Management"

EAC-11

- **Description**: At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in EAC-10.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-007-6 2.2
    - IT-PR-506 "Security Patch Management"
    - IT-PR-513 "Threat and Vulnerability Management"

EAC-12

- **Description**: For applicable patches identified in EAC-11, within 35 calendar days of the evaluation completion, take one of the following actions:
    - Apply the applicable patches; or
    - Create a dated mitigation plan; or
    - Revise an existing mitigation plan.

  Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.
- **Implementation:**
- **Implementation Status:**
- Responsible Party
- References:

  - CIP-007-6 2.3
  - IT-PR-506 "Security Patch Management"
  - IT-PR-513 "Threat and Vulnerability Management"

EAC-13

- **Description**: For each mitigation plan created or revised in EAC-12, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in EAC-11 is approved by Entergy Security Compliance.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
  - CIP-007-6 2.4
  - IT-PR-506 "Security Patch Management"
  - IT-PR-513 "Threat and Vulnerability Management"

12.3.4. Malicious Code

EAC-14

- **Description**: Where technically feasible, deploy method(s) to deter, detect, or prevent malicious code
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
  - CIP-007-6 R3

12.3.5. Logging

EAC-15

- **Description**: All applicable systems within the scope of this procedure shall be configured to generate system access logs, audit trails, and security status alerts for the identification of Cyber Security Incidents per Cyber Asset or Cyber System capability. At a minimum, this includes the following types of events: 1) Detected successful login attempts; 2) Detected failed access attempts and failed login attempts; 3) Detected malicious code
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
  - CIP-007-6 R4

EAC-16

- **Description**: A Centralized Monitoring, Logging, and Alerting Platform (CMLAP) should perform the logging and monitoring of devices, where technically feasible

- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-007-6 R4

12.3.6. Authentication and System Access Controls

EAC-17

- **Description**: Have a method(s) to enforce authentication of interactive user access, where technically feasible.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP 007-6 5.1

EAC-18

- **Description**: Identify individuals who have authorized access to shared accounts.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP 007-6 5.3

EAC-19

- **Description**: Change known default passwords, per Cyber Asset capability
- **Implementation**:
- **Implementation Status**:
- Entergy:
- DEPCOM:
- Responsible Party:
- References:
    - CIP 007-6 5.4

EAC-20

- **Description**: For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 1) Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 2) Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non- alphanumeric) or the maximum complexity supported by the Cyber Asset.
- **Implementation**:
- **Implementation Status**:

- Responsible Party:
- References:
    - CIP 007-6 5.5

EAC-21

- **Description**: Where technically feasible, either: 1) Limit the number of unsuccessful authentication attempts; or 2) Generate alerts after a threshold of unsuccessful authentication attempts.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP 007-6 5.6

EAC-22

- **Description**: Where technically feasible, include a warning banner for notifying those logging into a system that they are logging into a sensitive system and access is restricted/monitored.
- **Implementation**:
    - Entergy: "Warning! Legal Notice. This system is the property of Entergy and is for the use of authorized users only. Personal use should only be occasional, incidental, and infrequent. Individuals using this system or otherwise accessing the Entergy network waive any expectation of privacy. Use of this system is express consent to monitoring, and users are advised that if unauthorized activities, including but not limited to theft, tampering, misuse, creation, or dissemination of malicious software (e.g., computer viruses), destruction, or loss have occurred, appropriate action will be taken, such as disciplinary action up to and including termination. Entergy retains the right, exercisable in its sole discretion, at any time and from time to time, to monitor, intercept, search, and record any and all activities on this system, and undertaken through any pc or other device connected to the Entergy network, and disclose information, as Entergy deems appropriate, to others such as the U.S. Government to help ensure information security and protect the Entergy network. Entergy further reserves the right, without the consent of or liability to any user or third party, to record, screen, edit, curtail, or remove any content on this system at any time and for any reason, including because it believes such content to be harmful, harassing, abusive, offensive, or in violation of this notice or any other terms, conditions, and policies applicable to this system. Entergy shall have no liability to any user or third party for the performance or non-performance of monitoring or other actions taken to protect the Entergy network. Additionally, the unauthorized activity may be reported to government authorities including law enforcement. Clicking I ACCEPT or LOG ON, or continuing to use this computer or accessing the Entergy network constitutes an acknowledgement and acceptance of the terms of this notice, and Entergy's Communications Systems policy and the Electronic Information Security policy."
    - Third Party: Similar language as above
- **Implementation Status:**
- Responsible Party:
- References:

12.4. Cyber Security Incident Response

Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

1. Identification, classification, and response to Cyber Security Incidents;
2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;
3. Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;
4. Incident handling for Cyber Security Incidents;
5. Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and
6. Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

CIR-01

- **Description**: Have a documented Cyber Security Incident response plan, which includes identification, classification, and response to Cyber Security Incidents
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-003-8 Attachment 1
    - CIP-008-5 1.1
    - *IT-PR-502 "Security Incident Response Procedure"*

CIR-02

- **Description**: Have a documented Cyber Security Incident response plan, which includes determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-003-8 Attachment 1
    - CIP-008-5 1.2
    - *IT-PR-502 "Security Incident Response Procedure"*

CIR-03

- **Description**: Have a documented Cyber Security Incident response plan, which includes identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-003-8 Attachment 1
    - CIP-008-5 1.3
    - *IT-PR-502 "Security Incident Response Procedure"*

CIR-04

- **Description**: Have a documented Cyber Security Incident response plan, which includes incident handling for Cyber Security Incidents
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-003-8 Attachment 1
    - CIP-008-5 1.4
    - *IT-PR-502 "Security Incident Response Procedure"*

CIR-05

- **Description**: Have a documented Cyber Security Incident response plan, which includes testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
    - CIP-003-8 Attachment 1
    - CIP-008-5 2.1
    - *IT-PR-502 "Security Incident Response Procedure"*

CIR-06

    - **Description**: Have a documented Cyber Security Incident response plan, which includes updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident
    - **Implementation**:
    - **Implementation Status**:
    - Responsible Party:
    - References:

- CIP-003-8 Attachment 1
- CIP-008-5 R3
- *IT-PR-502 "Security Incident Response Procedure"*

CIR-07

- **Description**: Third parties which operate, maintain, or have ongoing electronic access to the site must appoint an Incident Response contact. Additionally, require immediate (within 12 hours of discovery) notification to Entergy for any suspected or actual cyber events on the third party's computer systems. This should be required through contractual language of the third party's O&M agreement with Entergy.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
  - CIP-003-8 Attachment 1
  - CIP-008-5 1.3

12.5. Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation

Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets or Removable Media. The plan(s) shall include:

1. For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability):
   a. Antivirus software, including manual or managed updates of signatures or patterns;
   b. Application whitelisting; or
   c. Other method(s) to mitigate the introduction of malicious code.
2. For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any:
   a. Use one or a combination of the following prior to connecting the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset capability):
      i. Review of antivirus update level;
      ii. Review of antivirus update process used by the party;
      iii. Review of application whitelisting used by the party;
      iv. Review use of live operating system and software executable only from read-only media;
      v. Review of system hardening used by the party; or
      vi. Other method(s) to mitigate the introduction of malicious code.
   b. For any method used pursuant to above, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.
3. For Removable Media, the use of each of the following:

a. Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System; and
b. Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BES Cyber System.

TCA-01

- **Description**: For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability): 1) Antivirus software, including manual or managed updates of signatures or patterns; 2) Application whitelisting; or 3) Other method(s) to mitigate the introduction of malicious code.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
  - CIP-003-8 Attachment 1
  - *IT-PR-517 "Transient Cyber Asset and Removable Media Security Plan"*

TCA-02

- **Description**: For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, use one or a combination of the following prior to connecting the Transient Cyber Asset to a Cyber System (per Transient Cyber Asset capability): 1) Review of antivirus update level; 2) Review of antivirus update process used by the party; 3) Review of application whitelisting used by the party; 4) Review use of live operating system and software executable only from read-only media; 5) Review of system hardening used by the party; or 6) Other method(s) to mitigate the introduction of malicious code. For any method used pursuant to above, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
  - CIP-003-8 Attachment 1
  - *IT-PR-517 "Transient Cyber Asset and Removable Media Security Plan"*

TCA-03

- **Description**: For Removable Media, the use of each of the following: 1) Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a Cyber System; and 2) Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a BES Cyber System.
- **Implementation**:
- **Implementation Status**:
- Responsible Party:
- References:
  - CIP-003-8 Attachment 1

- *IT-PR-517 "Transient Cyber Asset and Removable Media Security Plan"*

13. Appendix B – Baseline Testing

Text goes here.

14. Cyber Security Awareness Testing

CSA-01 – Ensure all users receive cyber security awareness training at least once every 15 calendar months	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate each of the site users has received cyber security awareness training in the last 15 months. Evidence can be a sign-in sheet, training log, or electronic records.	
Testing Evidence	
Testing Result	Pass / Fail

CSA-02 – Ensure all users are identified and meet Entergy's requirements for accessing data/systems	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate each of the SITE users is identified and meet Entergy's requirements. Evidence can be electronic records or manual validation.	
Testing Evidence	
Testing Result	Pass / Fail

CSA-03 – Ensure all users with electronic and unescorted physical access are documented	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate each of the users that have electronic or physical access are documented. Evidence can be a log on a central repository or electronic records.	
Testing Evidence	
Testing Result	Pass / Fail

CSA-04 – Ensure access is revoked when users/contractors are terminated	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure all users are still valid and have not been terminated. Evidence can be a full or random audit.	
Testing Evidence	
Testing Result	Pass / Fail

15. Physical Security Testing

PSC-01 – Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate at least one physical access control mechanism is in use at the Physical Security Perimeter. Evidence can be a picture showing this.	
Testing Evidence	
Testing Result	Pass / Fail

PSC-02 – Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure a log exists for access to the site. Evidence should be a picture of a paper log or attachment of electronic records	
Testing Evidence	
Testing Result	Pass / Fail

PSC-03 – Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure all cabling that is outside of the Electronic Security Perimeter is encrypted. Evidence should be a screen capture of configuration settings or a packet capture showing these are encrypted. Additionally, if physical access restrictions are in use, evidence should be a picture showing this.	
Testing Evidence	
Testing Result	Pass / Fail

PSC-04 – Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure signage and training are present for those escorting visitors. Evidence can be pictures of signs and/or training logs	
Testing Evidence	
Testing Result	Pass / Fail

PSC-05 – Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	
Tested By	

PSC-05 – Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure a log exists for visitor access to the site. Evidence should be a picture of a paper log or attachment of electronic records	
Testing Evidence	
Testing Result	Pass / Fail

16. Electronic Access Testing

EAC-01 – Identify each Cyber Asset and update inventory list whenever changes are made and review/update it at least every 15 months.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate the Cyber Asset list is up to date. Evidence can include an inventory list compared to actual assets at the site. This assessment can be a full or random sampling of devices.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-02 – When replacing/retiring a system validate sensitive information is destroyed according to NIST data destruction guidance	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Look for evidence of destruction process. If possible, randomly sample a device that was supposed to be sanitized. If not possible, interview SMEs to see if this is being done.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-03 – All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Compare the inventory list to the network diagram; ensure all networked assets are within the ESP. If any are not, they should be documented as an exception.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-04 – All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure there are no out of band internet/external network connections to the site assets. All connectivity should utilize the connections detailed above. This will require a site visit or interview to attest that there are no other connections.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-05 – EAPs Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Get a list of firewall rules. Ensure there is a Deny All at the end of the Access Control List. Ensure there are no Allow Any/Any rules unless explicitly documented. Ensure rules/exceptions are documented as part of Entergy's existing processes. Evidence should be a screenshot or list of rules.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-06 – EAPs must have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	
Tested By	

EAC-06 – EAPs must have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure the SITE firewall has Intrusion Detection enabled and logging. Evidence should be a screenshot or firewall configuration settings.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-07 – Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure that all interactive access to the site is through the Jump Servers or the RTAC. Evidence could be firewall rules.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-08 – For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Verify encryption is turned on for both the Jump Server/Citrix as well as the VPN tunnel. Evidence could be screenshots or configuration settings.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-09 – Require multi-factor authentication for all Interactive Remote Access sessions.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Test the interactive login to the Jump Server and ensure it requires MFA. Evidence can be a screenshot.	

EAC-09 – Require multi-factor authentication for all Interactive Remote Access sessions.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-10 – A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure a patch management process exists for the assets. Evidence should be the process.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-11 – At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in EAC-10.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
View the last patch evaluation and a current scan. Ensure all patches > 35 days old are installed or evaluated.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-12 – For applicable patches identified in EAC-11, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
View the last patch evaluation and a current scan. Ensure all patches > 35 days old are installed or evaluated.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-13 – For each mitigation plan created or revised in EAC-12, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in EAC-12 is approved by Entergy Security Compliance.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
View all mitigation plans and ensure all are up to date and have been implemented within the timeframe specified or that an extension is in place. If the number of mitigation plans is more than 10, randomly sample 10 plans.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-14 – Where technically feasible, deploy method(s) to deter, detect, or prevent malicious code	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure endpoint protection is installed, updated, and functioning for all systems that technically support it. Evidence can be a screenshot.	
Testing Evidence	

EAC-14 – Where technically feasible, deploy method(s) to deter, detect, or prevent malicious code	
Testing Result	Pass / Fail

EAC-15 – All applicable systems within the scope of this procedure shall be configured to generate system access logs, audit trails, and security status alerts for the identification of Cyber Security Incidents per Cyber Asset or Cyber System capability. At a minimum, this includes the following types of events: 1) Detected successful login attempts; 2) Detected failed access attempts and failed login attempts; 3) Detected malicious code	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure all systems are generating logs that meet the events specified. Ideally this should be centrally logged, but if not, ensure the logs at least exist locally. Testing should include a screenshot of the logs or the actual logs, including testing for the three types of logs mentioned.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-16 – A Centralized Monitoring, Logging, and Alerting Platform (CMLAP) should perform the logging and monitoring of devices, where technically feasible	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure all systems are generating logs that meet the events specified. This should be centrally logged. Testing should include a screenshot of the logs or the actual logs in the CMLAP, including testing for the three types of logs mentioned.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-17 – Have a method(s) to enforce authentication of interactive user access, where technically feasible.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure all devices require authentication for interactive user access. This could be a random sampling of at least one of each type of device, showing a screenshot of the required authentication.	

EAC-17 – Have a method(s) to enforce authentication of interactive user access, where technically feasible.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-18 – Identify individuals who have authorized access to shared accounts.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Ensure a list exists of all users that have access to shared accounts. For testing, view the accounts on devices, identify shared accounts, and ensure the match the documentation provided.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-19 – Change known default passwords, per Cyber Asset capability	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Provide evidence that default passwords have been changed. Testing should also include research and trial of the default password on each type of device to ensure it has truly been changed.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-20 – For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 1) Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 2) Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non- alphanumeric) or the maximum complexity supported by the Cyber Asset.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Provide a configuration setting or screenshot showing this policy is enabled. If that is not possible, try to set a password without meeting the requirements and validate if the system will let you. If this is strictly an	

EAC-20 – For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 1) Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 2) Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non- alphanumeric) or the maximum complexity supported by the Cyber Asset.	
administrative control, show evidence where the user is made aware of this requirement (user agreement, training, warning banner, etc)	
Testing Evidence	
Testing Result	Pass / Fail

EAC-21 – Where technically feasible, either: 1) Limit the number of unsuccessful authentication attempts; or 2) Generate alerts after a threshold of unsuccessful authentication attempts.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Provide a configuration setting or screenshot showing this policy enabled, if technically feasible. Testing should also include testing this by providing bad credentials to verify the user is either locked out or alerts are generated. If not technically feasible for a system, this should be documented.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-22 – Where technically feasible, include a warning banner for notifying those logging into a system that they are logging into a sensitive system and access is restricted/monitored.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Provide a configuration setting or screenshot showing the warning banner or where this policy enabled, if technically feasible.	
Testing Evidence	
Testing Result	Pass / Fail

EAC-23 – System configuration shall be backed up/stored and readily accessible for restoration.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Provide a mapping to each inventory Item of configuration or backup file location.	
Testing Evidence	
Testing Result	Pass / Fail

17. Cyber Security Incident Response Testing

CIR-01 – Have a documented Cyber Security Incident Response Plan, which includes identification, classification, and response to Cyber Security Incidents	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate the Cyber Security Incident Response Plan exists and is current. Provide a screenshot of the front of Incident Response Plan.	
Testing Evidence	
Testing Result	Pass / Fail

CIR-02 – Have a documented Cyber Security Incident response plan, which includes determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate the Cyber Security Incident Response Plan exists and is current. Provide a screenshot of the page that shows the process for Reportable Cyber Security Incidents.	
Testing Evidence	
Testing Result	Pass / Fail

CIR-03 – Have a documented Cyber Security Incident response plan, which includes identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate the Cyber Security Incident Response Plan exists and is current. Provide a screenshot of the page that shows the roles and responsibilities.	
Testing Evidence	
Testing Result	Pass / Fail

CIR-04 – Have a documented Cyber Security Incident response plan, which includes incident handling for Cyber Security Incidents	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate the Cyber Security Incident Response Plan exists and is current. Provide a screenshot of the page that shows the incident handling details.	
Testing Evidence	
Testing Result	Pass / Fail

CIR-05 – Have a documented Cyber Security Incident response plan, which includes testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate the Cyber Security Incident Response Plan exists and is current. Provide a screenshot or other evidence that shows when it was last tested.	
Testing Evidence	
Testing Result	Pass / Fail

CIR-06 – Have a documented Cyber Security Incident response plan, which includes updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate the Cyber Security Incident Response Plan exists and is current. Provide a screenshot or other evidence that shows it was updated within 180 days of the last incident or test. Additionally, if the plan was updated less than 180 days prior to the evaluation of this control, that is considered a pass.	
Testing Evidence	
Testing Result	Pass / Fail

CIR-07 – Third parties which operate, maintain, or have ongoing electronic access to the site must appoint an Incident Response contact. Additionally, require immediate notification to Entergy for any suspected or actual cyber events on the third party's computer systems. This should be required through contractual language of the third party's O&M agreement with Entergy.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Provide evidence that DEPCOM has provided an Incident Response contact in either this plan or another document. Additionally, provide evidence that there are the above requirements in the third party's contract with Entergy.	
Testing Evidence	
Testing Result	Pass / Fail

18. Transient Cyber Asset & Removable Media Malicious Code Risk Mitigation Testing

TCA-01 – For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability): 1) Antivirus software, including manual or managed updates of signatures or patterns; 2) Application whitelisting; or 3) Other method(s) to mitigate the introduction of malicious code.	
Tested By	
Date Tested	

TCA-01 – For Transient Cyber Asset(s) managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per Transient Cyber Asset capability): 1) Antivirus software, including manual or managed updates of signatures or patterns; 2) Application whitelisting; or 3) Other method(s) to mitigate the introduction of malicious code.	
Expected Setting(s) and Test Plan	
Validate that one of the above methods is in use on any transient cyber assets. As these are transient, in nature, take credit for assessments of this control whenever they take place.	
Testing Evidence	
Testing Result	Pass / Fail

TCA-02 – For Transient Cyber Asset(s) managed by a party other than the Responsible Entity, if any, use one or a combination of the following prior to connecting the Transient Cyber Asset to a Cyber System (per Transient Cyber Asset capability): 1) Review of antivirus update level; 2) Review of antivirus update process used by the party; 3) Review of application whitelisting used by the party; 4) Review use of live operating system and software executable only from read-only media; 5) Review of system hardening used by the party; or 6) Other method(s) to mitigate the introduction of malicious code. For any method used pursuant to above, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	
Validate that one of the above methods is in use on any third party transient cyber assets. As these are transient, in nature, take credit for assessments of this control whenever they take place.	
Testing Evidence	
Testing Result	Pass / Fail

TCA-03 – For Removable Media, the use of each of the following: 1) Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a Cyber System; and 2) Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a BES Cyber System.	
Tested By	
Date Tested	
Expected Setting(s) and Test Plan	

TCA-03 – For Removable Media, the use of each of the following: 1) Method(s) to detect malicious code on Removable Media using a Cyber Asset other than a Cyber System; and 2) Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a BES Cyber System.	
Validate that one of the above methods is in use on any third party transient cyber assets. As these are transient, in nature, take credit for assessments of this control whenever they take place.	
Testing Evidence	
Testing Result	Pass / Fail

Section 4 - Project Workbook Template

MASTER IP LIST

VLAN INFO				SUBNET INFO					
ID	VLAN Name	VLAN Description	Subnet	Mask	Inverse Mask	Subnet	Address Size	Host Range	Broadcast
1450	XYZ-OTNET	OTNET	10.ABC.DEF.0	255.255.255.248		/29	8		
1455	XYZ-OTN-MGMT	OTNET Management	10.ABC.DEF.8	255.255.255.248		/29	8		
1454	XYZ-PROD-NON-ESP	Entergy Substation VLAN	10.ABC.DEF.16	255.255.255.240		/28	16		
1453	XYZ-FAC	Physical Security VLAN	10.ABC.DEF.32	255.255.255.224		/27	32		
1457	XYZ-SOLAR-SUB	3rd Party Substation VLAN	10.ABC.DEF.64	255.255.255.224		/27	32		
1458	XYZ-BESS-CONTROL	BESS Control VLAN	10.ABC.DEF.96	255.255.255.224		/27	32		
1459	XYZ-BESS-YARD	BESS Yard VLAN	10.ABC.DEF.128	255.255.255.128		/25	128		
1460	XYZ-BESS-YARD	BESS Yard VLAN extension	10.ABC.XYZ.0	255.255.255.224			223		
1461	XYZ-MSS-Security	MSS Security VLAN	10.ABC.XYZ.224	255.255.255.224			27		
Entergy Specified							506		
Seller Specified									

Site Name:	Solar Site XYZ														
IP	Mask	Vlan	VLAN Name	Description	Additional Notes	Physical Location	Firmware Revision	Device Type	ID	Password	Logging	TVM	Config Link	Manual Link
10.ABC.DEF.0	255.255.255.248	1450	XYZ-OTNET	Network		OTNET /29								
10.ABC.DEF.1	255.255.255.248	1450	XYZ-OTNET	Router	VRRP									
10.ABC.DEF.2	255.255.255.248	1450	XYZ-OTNET	XYZRTRP4001	CGR-2010									
10.ABC.DEF.3	255.255.255.248	1450	XYZ-OTNET											
10.ABC.DEF.4	255.255.255.248	1450	XYZ-OTNET	FW	VRRP									
10.ABC.DEF.5	255.255.255.248	1450	XYZ-OTNET	XYZFWAP4001	Firewall									
10.ABC.DEF.6	255.255.255.248	1450	XYZ-OTNET	XYZFWAP4002	Firewall									
10.ABC.DEF.7	255.255.255.248	1450	XYZ-OTNET	Broadcast										
10.ABC.DEF.8	255.255.255.248	1455	XYZ-OTN-MGMT	Network		OT Mgmt /29								
10.ABC.DEF.9	255.255.255.248	1455	XYZ-OTN-MGMT	Router	VRRP									
10.ABC.DEF.10	255.255.255.248	1455	XYZ-OTN-MGMT	XYZRTRP4001	CGR-2010									
10.ABC.DEF.11	255.255.255.248	1455	XYZ-OTN-MGMT											
10.ABC.DEF.12	255.255.255.248	1455	XYZ-OTN-MGMT	XYZSW2P4003 (ESM)	RWIC-D-ES-2S-8PC									
10.ABC.DEF.13	255.255.255.248	1455	XYZ-OTN-MGMT											
10.ABC.DEF.14	255.255.255.248	1455	XYZ-OTN-MGMT	unassigned										
10.ABC.DEF.15	255.255.255.248	1455	XYZ-OTN-MGMT	Broadcast										
10.ABC.DEF.16	255.255.255.240	1454	XYZ-PROD-NON-ESP	Network		Prod NON-ESP /28								
10.ABC.DEF.17	255.255.255.240	1454	XYZ-PROD-NON-ESP	FW	VRRP									
10.ABC.DEF.18	255.255.255.240	1454	XYZ-PROD-NON-ESP	XYZFWAP4001	Firewall									
10.ABC.DEF.19	255.255.255.240	1454	XYZ-PROD-NON-ESP	XYZFWAP4002	Firewall									
10.ABC.DEF.20	255.255.255.240	1454	XYZ-PROD-NON-ESP	XYZSW2P4001	Non-ESP Switch									
10.ABC.DEF.21	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.22	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.23	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.24	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.25	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.26	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.27	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.28	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.29	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.30	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.31	255.255.255.240	1454	XYZ-PROD-NON-ESP											
10.ABC.DEF.32	255.255.255.224	1453	XYZ-FAC	Network		Facility / Phys Sec /27								
10.ABC.DEF.33	255.255.255.224	1453	XYZ-FAC	FW	VRRP									
10.ABC.DEF.34	255.255.255.224	1453	XYZ-FAC	XYZFWAP4001	Firewall									
10.ABC.DEF.35	255.255.255.224	1453	XYZ-FAC	XYZFWAP4002	Firewall									
10.ABC.DEF.36	255.255.255.224	1453	XYZ-FAC											
10.ABC.DEF.37	255.255.255.224	1453	XYZ-FAC											
10.ABC.DEF.38	255.255.255.224	1453	XYZ-FAC	XYZCACP4001	rd Access Controller									
10.ABC.DEF.39	255.255.255.224	1453	XYZ-FAC											
10.ABC.DEF.40	255.255.255.224	1453	XYZ-FAC	XYZCACP4002	rd Access Controller									
10.ABC.DEF.41	255.255.255.224	1453	XYZ-FAC	XYZBESSOITP4001	-3355 VMS Video Svr									
10.ABC.DEF.42	255.255.255.224	1453	XYZ-FAC	XYZBESSOITP4002	-3355 VMS Video Svr									
10.ABC.DEF.43	255.255.255.224	1453	XYZ-FAC	Cluster (OS) Client Access	-3355 VMS Video Svr									
10.ABC.DEF.44	255.255.255.224	1453	XYZ-FAC	Cluster (App)	-3355 VMS Video Svr									
10.ABC.DEF.45	255.255.255.224	1453	XYZ-FAC											
10.ABC.DEF.46	255.255.255.224	1453	XYZ-FAC											
10.ABC.DEF.47	255.255.255.224	1453	XYZ-FAC	XYZENCP4001	Encoder									
10.ABC.DEF.48	255.255.255.224	1453	XYZ-FAC	XYZENCP4002	Encoder									
10.ABC.DEF.49	255.255.255.224	1453	XYZ-FAC	XYZENCP4003	Encoder									
10.ABC.DEF.50	255.255.255.224	1453	XYZ-FAC	XYZENCP4004	Encoder									
10.ABC.DEF.51	255.255.255.224	1453	XYZ-FAC											
10.ABC.DEF.52	255.255.255.224	1453	XYZ-FAC											

10.ABC.DEF.64	255.255.255.224	1457	XYZ-SOLAR-SUB	Network		3rd Party Substatio
10.ABC.DEF.65	255.255.255.224	1457	XYZ-SOLAR-SUB	FW	VRRP	
10.ABC.DEF.66	255.255.255.224	1457	XYZ-SOLAR-SUB	XYZFWAP4001	Firewall	
10.ABC.DEF.67	255.255.255.224	1457	XYZ-SOLAR-SUB	XYZFWAP4002	Firewall	
10.ABC.DEF.68	255.255.255.224	1457	XYZ-SOLAR-SUB			
10.ABC.DEF.69	255.255.255.224	1457	XYZ-SOLAR-SUB			
10.ABC.DEF.70	255.255.255.224	1457	XYZ-SOLAR-SUB			
10.ABC.DEF.71	255.255.255.224	1457	XYZ-SOLAR-SUB			
10.ABC.DEF.72	255.255.255.224	1457	XYZ-SOLAR-SUB	RTU (OrionLX)		
10.ABC.DEF.73	255.255.255.224	1457	XYZ-SOLAR-SUB	COMM 1 (OrionLX)		
10.ABC.DEF.74	255.255.255.224	1457	XYZ-SOLAR-SUB	Meter (SEL-735)		
10.ABC.DEF.75	255.255.255.224	1457	XYZ-SOLAR-SUB	87T1P (SEL-487E)		
10.ABC.DEF.76	255.255.255.224	1457	XYZ-SOLAR-SUB	87T1S (SEL-3311A)		
10.ABC.DEF.77	255.255.255.224	1457	XYZ-SOLAR-SUB	87L1P (SEL 411L)		
10.ABC.DEF.78	255.255.255.224	1457	XYZ-SOLAR-SUB	87L1S (SEL-411L)		
10.ABC.DEF.79	255.255.255.224	1457	XYZ-SOLAR-SUB	50-51/F1 (SEL-751A)		
10.ABC.DEF.80	255.255.255.224	1457	XYZ-SOLAR-SUB	RTU-NTIO1 (Orion I/O)		
10.ABC.DEF.81	255.255.255.224	1457	XYZ-SOLAR-SUB	50BF/T1 (SEL-352-2)		
10.ABC.DEF.82	255.255.255.224	1457	XYZ-SOLAR-SUB			
10.ABC.DEF.83	255.255.255.224	1457	XYZ-SOLAR-SUB			

10.ABC.DEF.96	255.255.255.224	1458	XYZ-BESS-CONTROL	Network		Vendor BESS Contr
10.ABC.DEF.97	255.255.255.224	1458	XYZ-BESS-CONTROL	FW	VRRP	
10.ABC.DEF.98	255.255.255.224	1458	XYZ-BESS-CONTROL	XYZFWAP4001	Firewall	
10.ABC.DEF.99	255.255.255.224	1458	XYZ-BESS-CONTROL	XYZFWAP4002	Firewall	
10.ABC.DEF.100	255.255.255.224	1458	XYZ-BESS-CONTROL			
10.ABC.DEF.101	255.255.255.224	1458	XYZ-BESS-CONTROL			
10.ABC.DEF.102	255.255.255.224	1458	XYZ-BESS-CONTROL	Development for Ignition		
10.ABC.DEF.103	255.255.255.224	1458	XYZ-BESS-CONTROL	Top Server		
10.ABC.DEF.104	255.255.255.224	1458	XYZ-BESS-CONTROL	Ignition SCADA Server		
10.ABC.DEF.105	255.255.255.224	1458	XYZ-BESS-CONTROL	Ignition Historian		
10.ABC.DEF.106	255.255.255.224	1458	XYZ-BESS-CONTROL	M340 PLC CPU		
10.ABC.DEF.107	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.108	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.109	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.110	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.111	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.112	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.113	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.114	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.115	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.116	255.255.255.224	1458	XYZ-BESS-CONTROL	Dell VM Admin IP		
10.ABC.DEF.117	255.255.255.224	1458	XYZ-BESS-CONTROL			
10.ABC.DEF.118	255.255.255.224	1458	XYZ-BESS-CONTROL			

10.ABC.DEF.128	255.255.255.128	1459	XYZ-BESS-YARD	Network		BESS Yard /25
10.ABC.DEF.129	255.255.255.128	1459	XYZ-BESS-YARD	FW	VRRP	
10.ABC.DEF.130	255.255.255.128	1459	XYZ-BESS-YARD	XYZFWAP4001	Firewall	
10.ABC.DEF.131	255.255.255.128	1459	XYZ-BESS-YARD	XYZFWAP4002	Firewall	
10.ABC.DEF.132	255.255.255.128	1459	XYZ-BESS-YARD			
10.ABC.DEF.133	255.255.255.128	1459	XYZ-BESS-YARD			

APPENDIX 15 – CYBER SECURITY PLAN

SOFTWARE

Software Name	Present at Site (Y/N)	License Transfer
VMWARE		
Windows		
Ignition		
ModBus SCADA		
Software Toolbox		
TOPS Server		

FIREWALL RULES

Rule Name	Source	IP	Destination	IP	Port	udp/tcp	Service	Description (provide interface to interface description and reason why)