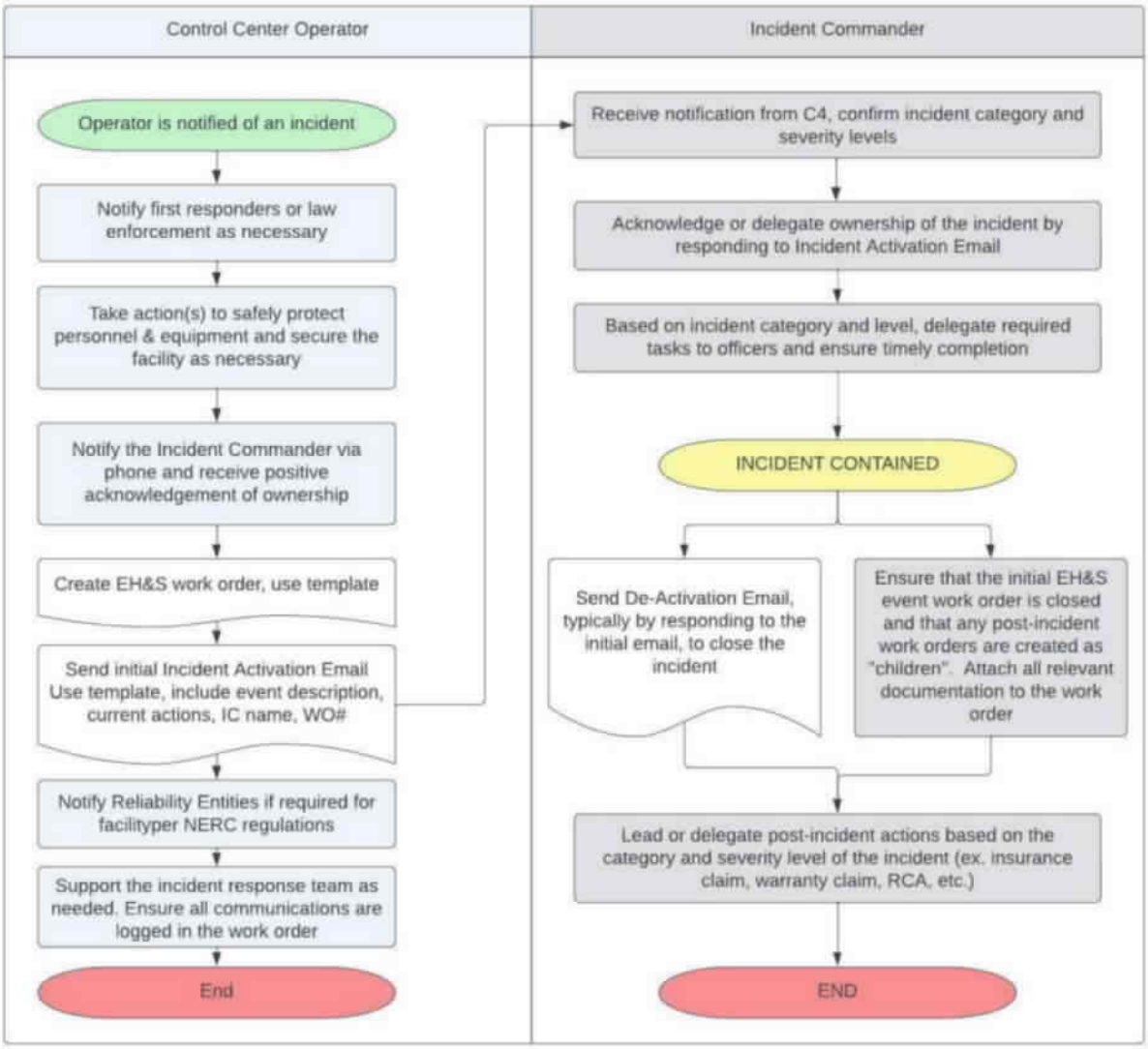
Cyber Security	Malware discovered on company device (OT Network devices not affected) or phishing attempt that has not resulted in compromising company devices	Phishing attempt or another incident that resulted in compromising of multiple company devices (OT Network devices not affected) or Cyber incident that affected operations of individual applications essential for business operations (OT systems not affected)	Cyber incident that resulted in compromising of the entire IT network operations (OT systems not affected) or Suspicious event that results from actual or suspected intentional human action that occurred at a Transmission Site/Distribution Site (that is not registered with NERC) and disrupted or was an attempt to disrupt its functionality; or Cyber event affecting a Transmission Site/Distribution Site (that is not registered with NERC) and impacting, or potentially impacting system vulnerability; or Physical Threat to a site that is not registered with NERC	Cyber event or suspicious event that attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or BES Cyber Systems without necessarily impacting these systems; or Suspicious event that results from actual or suspected intentional human action and was an attempt to disrupt the operations; or Cyber event affecting the Facility or Control Center and potentially impacting system vulnerability; (CSIRP activation required, NERC reporting required)	Cyber event or suspicious event that compromised (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or BES Cyber Systems without necessarily impacting these systems; or Suspicious event that results from actual or suspected intentional human action and disrupted the operations; or Cyber event affecting the Facility or Control Center and impacting system vulnerability; or Physical Threat to a NERC registered entity (C4 or NERC site) (CSIRP activation required, NERC reporting required)

Thermal	Fire that facility personnel have extinguished, Hot spot with imminent failure	Fire that requires fire department support	Active equipment fire	Actions by more than 1st responders or facility personnel are necessary	
Injury	Injury or illness with no first aid measures needed.	Injury or illness requiring minor first aid treatment.	Medical treatment beyond first aid. Employee sought medical attention at a clinic or ER.	Medical attention beyond first aid resulting in the need for ambulance and/or other onsite medical intervention (i.e., AED usage).	Potential fatality or permanent disability
Vehicle	Accidents not requiring first responders, Accidents damaging equipment on site, not involving more than one vehicle.	Accidents involving more than one vehicle with no injuries.	Accident resulting in injury requiring first aid.	Accident resulting in a total loss and/or injury requiring medical attention beyond first aid.	Accident resulting in possible fatality or permanent disability.
SWA	Missed check in from contractor/Tech, Un-safe work practice reported, Equipment failure making the area hazardous, issued due to failure to follow procedure.	SWAs issued due to weather related hazards, inaccessible to emergency personnel, potential to cause minor injury/illness		Potential for serious injury/illness,	SWA issued due to conditions that could result in fatality or serious physical harm, permanent disability.

Near Miss	Minor near miss events not requiring first responders, Missing check out	potential to cause minor injury/illness, potential to cause minimal property damage		potential to result in serious physical injury/illness. could have resulted in property damage over $25k	High potential near miss. Potential to result in a possible fatality or permanent disability. Potential to result in a property damage over $50k.
Environmental	Minor transformer leaks touching the soil, reportable (pin hole slow leaks not touching soil are not reportable) Insect encounters (e.g., ants, bees)	Imminent threat of severe weather posing danger to life/equipment Minor erosion rills confined on-site	Adverse weather conditions that have caused significant damage or created need for additional operational support Large erosion rills formed on-site; sediment loss contained to upland areas inside perimeter fence	Transformer leak of 5 or more gallons touching the soil. Large wildlife encounters (e.g., deer, alligators) or potential adverse impacts to protected species (e.g., turtles, birds) Significant erosion or sediment loss extending beyond perimeter fence or discharged to on-site surface waters (e.g., ditches, streams, wetlands) Severe environmental impact	Transformer leak that reaches a surface water (e.g., ditch, stream, wetland). Bald eagle or large raptor nest

Property Damage	Broken Gates, damaged fence, property damage less than $1k	Minimal damage to equipment (CBs, inverters, transformers, etc.),	Damaged Equipment from External Firearm Discharge, intentional damage caused by theft/vandalism	Property damage over $25k	Property damage over $50k
MEDIA ADDER				If there was a local media inquiry of the incident	National media inquiry of the incident

ATTACHMENT 2: INCIDENT RESPONSE FLOW CHART



ATTACHMENT 3: CONTROL CENTER INCIDENT SCRIPTS

1. If possible, stay on the phone with any local resources until the condition is stabilized or all requisite information is obtained
2. Gather the following information that is pertinent to the event. Use the following as a script for questions.
    a. General
        i. Please provide your name and contact information.
        ii. Please provide the name of the site and/or location.
        iii. Have there been any injuries?
    b. Fire
        i. Are you in a safe location? If not, can you get to a safe location?
        ii. Is the fire contained?
        iii. Can you provide a brief description of the extent of fire/damage?
    c. Injury
        i. Are you in a safe location? If not, can you get to a safe location?
        ii. Do you know the name of the personnel that has been injured?
        iii. Can you provide me with a description and cause of the injuries?
        iv. Is immediate medical attention required?
    d. Security
        i. Are you in a safe location? If not, can you get to a safe location?
        ii. Is the security threat or incident currently posing a threat?
        iii. Provide details of the security incident.
        iv. Who/what/when/where/how, etc.…
    e. Environmental
        i. Are you in a safe location? If not, can you get to a safe location?
        ii. Describe the environmental concern.
        iii. Oil leak, water containment issue, the extent of damage, requiring immediate response, etc.?
        iv. Is oil touching the soil? (If not, field personnel only need to clean and document)
    f. Property Damage
        i. Are you in a safe location? If not, can you get to a safe location?
        ii. Describe property damage.
        iii. Equipment description, the extent of damage, any potential danger due to the damage, etc.?

ATTACHMENT 4: EH&S WORK ORDER TEMPLATE

Note:

To provide as much information as possible to CCR response teams, it is imperative that as much information as can be reasonably be obtained be included in the EH&S work order. This will streamline response and ensure resources are allotted commiserate with severity of the incident. Additionally, this will prevent follow-up communications that may distract from the incident response.

Work Order Field	Field Data
Description	**Incident Response – [FACILITY NAME] – [INCIDENT CATEGORY]**
Asset ID	**Use asset ID that best corresponds with the incident**
Account	**Account for affected facility**
Priority	**Emergency**
Status	**Ready to Schedule**
Problem Description/Scope of Work	**Affected Facility(ies):** *[FACILITY NAME]* **Location:** *[FACILITY ADDRESS]* **Owner:** *[FACILITY OWNER]* **Injuries:** *Brief description of injuries, if applicable.* **Description of incident:** *include any description of injury, severity of fire, if incident is contained, stable, or worsening* **First responder status:** *Include when and who was notified. Also include if first responders are on site or en-route*
WO Type	**EH&S Event**
Sub Type	**Either "Site Visit Required" or "Site Visit Not Required"**
Class	**Use incident category**

ATTACHMENT 5: INCIDENT RESPONSE EMAIL TEMPLATE[1]

It is imperative that as much information as can be reasonably be obtained be included in the initial notification. This will streamline response and ensure resources are allotted commensurate with severity of the incident and prevent follow-up communications that may distract from the incident response.

TO: OMIncident@ccrenew.com

CC: [FACILITY RM], [FACILITY OPSENG], [FACILITY AM]

EMAIL SUBJECT LINE:

INCIDENT ACTIVATION – [INCIDENT SEVERITY LEVEL] – [FACILITY NAME] – [INCIDENT CATEGORY]

EMAIL BODY:

Affected Facilities: *[FACILITY NAME]*

Location: *[FACILITY ADDRESS]*

Owner: *[FACILITY OWNER]*

Severity Level: *Initial assessed severity per* ***Error! Reference source not found.***

Injuries: *Brief description of injuries, if applicable.*

Description of incident: *include any description of injury, severity of fire, if incident is contained, stable, or worsening*

First responder status: *Include when and who was notified. Also include if first responders are on site or en-route*

CCR Response: *include description of initial CCR response*

EH&S Work Order:

Incident Commander_*(place name here)* has been notified.

Action Items: List actions to be taken based on incident category and severity level

[1] Pre-made email template: Incident Activation Email Template.emltpl

Status Update Template/Content *(to be completed by Incident Commander or delegate upon acknowledging ownership and at subsequent apparent event milestones):*

Expected time of next update

Confirmation that site is secure and supporting systems have been updated (such as a new lock combination updated in FSM)

Confirmation that the customer or asset manager has been notified

Initial, subsequent, or final assessment of damage or injuries

Status of actions identified in initial OMIncident email based upon type and severity of the event

Identify new owners of follow-on actions for warranty claim, insurance claim, or RCA

CYPRESS CREEK RENEWABLES

Solar Generator Winterization Policy

Version No. 1.0

Effective April 1, 2023

REVISION HISTORY

Version	Effective Date	Author	Description of Changes	Approver Name/Title
1.0	04/01/2023	Burns & McDonald	New Procedure	Julien Glover

TABLE OF CONTENTS

SOLAR GENERATOR WINTERIZATION POLICY

1.0 PURPOSE EOP-011-2

The purpose of this policy is to ensure that each of the Cypress Creek solar farms and any (future BES solar facility) have plans and procedures in place to operate reliably and safely during winter weather conditions by incorporating best industry practices applied to each specific plant configuration.

Due to the impacts across the Bulk Electric System (BES) during the ERCOT event of 1989, the Polar Vortex of 2011, and Winter Storm Uri in 2021 it has become necessary to formalize policy and procedures necessary to ensure continuous, safe, and reliable operation of the power generating station(s) during times of extreme winter weather. Specifically, the requirements of NERC Reliability Standard EOP-011-2, which is effective on 4/1/2023.

2.0 SCOPE

2.1 Applicability

This policy applies to the Cypress Creek Solar farms designated as follows:

1. Bowman
2. Huntley
3. Palmetto Plains
4. Midland sites
5. Wagyu
6. Innovative Solar 46 (NERC)
7. Shakes

This policy will apply to any future Cypress Creek Solar farm.

3.0 ROLES AND RESPONSIBILITIES

3.1 Operational Compliance Team – Establish policy for all Generating Plants to develop procedures to operate during winter weather events safely and reliably.

3.2 Senior Regional O&M Managers or Regional O&M Managers – Develop and update plant-specific winter weather procedures, ensure implementation, assign plan

execution responsibilities, ensure staff training, oversee corrective action plans, and plant procedure updates.

4.0 REVIEWS

4.1 This policy is to be reviewed annually.

5.0 SAFETY

5.1 Working safely is the responsibility of everyone. Winter weather conditions can present exposure to potential safety hazards. Ensure daily and pre-job safety briefings include appropriate winter weather-related topics. Follow OSHA Cold Stress Guide | Occupational Safety and Health Administration (osha.gov).

6.0 POLICY

6.1 Overview (EOP-011-2 7.1 and 7.2)

The subject solar farms currently do not have elements that utilize liquid or pressure systems, other than the main power transformers, that require specific winterization tasks. The solar field designs consider high winds and freezing temperatures, and these are not a concern. Therefore, normally monthly, semi-annual, and annual maintenance activities ensure the winterization preparedness is being performed.

6.2 Plant Procedures

Each Solar farm facility shall provide Generating unit(s) cold weather data, to include: (EOP-011-2, R7.3)

a. Generating unit(s) operating limitations in cold weather to include:

1. Capability and availability
2. Fuel supply and inventory concerns
3. Fuel-switching capabilities
4 Environmental constraints

NOTE: For the Solar Farms within scope there are no fuel supply and inventory concerns, no issues with fuel switching capabilities, and environmental constraints during a cold winter event. Therefore, each procedure within the scope of this policy will provide the Capability and the minimum design temperature.

b. Generating unit(s) minimum:

1. Design temperature; or
2. Historical operating temperature; or
3. Current cold weather performance temperature determined by engineering analysis.

7.0 WORK MANAGEMENT SYSTEM

7.1 Review the Work Management system (Sales Force) to ensure necessary preventive work orders (PMs) exist for cold weather events.

7.1.1 N/A

7.1.2 Verify Inverter cabinet seals are in good working order and prevent any leaks.

7.1.3 Verify GSU liquid and gas levels are normal. Check for leaks and ensure proper function of low-pressure relays.

7.1.4 Verify heating elements within GSU control panels are operating per design.

7.1.5 Verify heating within the control house/ battery storage building is working properly.

7.1.6 Verify the Automatic Transfer Switch is working properly.

7.1.7 If there are Backup Generators at the site verify testing is being performed.

7.1.8 Verify fuel storage and availability for BU Generators.

7.1.9 Verify any required heat tracing or winterization required activities associated with starting up the BU Generators.

8.0 EVALUATION OF POTENTIAL PROBLEM AREAS WITH CRITICAL COMPONENTS

8.1 Identify and prioritize critical components, systems, and other areas of vulnerability which may experience freezing problems or other cold weather operational issues. Schedule any routine cold weather readiness inspections, repairs, and winterization work to be completed annually by October 31st.

Potential vulnerabilities associated with emergency generators should be evaluated when developing the plant-specific winter weather preparation procedure, as they may provide critical system(s) backup.

Some additional checks and winterization activities might be needed before forecasted winter events. This includes critical instrumentation or equipment that has the potential to:

1. Initiate an automatic unit trip.
2. Impact unit start-up
3. Cause damage to the solar farm
4. Adversely affect the environmental controls that could cause full or partial outages.
5. Cause operational problems such as slowed or impaired field devices, or
6. Create a weather-related safety hazard.

8.2 In the event of a plant trip, derate, or failure to start due to severe winter weather, Plant Management, as appropriate, should conduct an analysis, develop lessons learned, and incorporate good industry practices.

This process shall include a feedback loop to enhance current winter weather readiness programs, processes, procedures, checklists, and training. Use the Corrective Action Plan (CAP) template contained in Attachment 1 for this process.

9.0 TRAINING (EOP-011-2 R8)

All plant personnel requiring training shall be identified in each plant(s) procedure.

Training shall be conducted annually for all personnel that are required to have such training. Records of this training and attendance logs shall be kept for documentation. Identify all required personnel within the Roles and Responsibility section.

Coordinate annual training, before October 31st, in winter-specific and plant-specific awareness and maintenance training. This may include response to freeze protection panel alarms, troubleshooting, and repair of freeze protection circuitry, identification of plant areas most affected by winter conditions, review of special inspections or rounds implemented during severe weather, knowledge of the ambient temperatures for which the freeze protection was designed, and lessons learned from previous experiences or the NERC Lessons Learned program.

For any new or transferring personnel ensure the Winterization procedure is included within the onboard training curriculum.

Ensure appropriate NERC Generation Availability Data Systems (GADS) coding for unit derates or trips that were the result of severe winter weather events to promote lessons learned, knowledge retention, and consistency. Examples may include NERC GADS code 9036 “Storms (ice, snow, etc.)” or code 9040 “Other Catastrophe”.

10.0 REFERENCES

10.1 EOP-011-2 Emergency Preparedness and Operations.

10.2 Reliability Guideline Generating Unit Winter Weather Readiness – Current Industry Practices – Version 4 dated October 2022

10.3 Cold weather-related Lessons Learned see link below.
https://www.nerc.com/pa/rrm/ea/ColdWeatherTrainingMaterials/Info_on_cold_weather_prep_and_bps_impacts.pdf

ATTACHMENT 1

Corrective Action Plan (CAP)Template

(Use this form to assist in developing corrective actions needed in the event of a cold weather-related event which has caused a Solar Farm to trip offline, derate, or fail to start, OR for required new freeze protection measures or modification of existing freeze protection measures.)

1) Description of Event (including weather conditions):

2) Identify the Cause of the Event (what equipment was affected):

3) Identify what actions are needed to prevent the occurrence of this event in the future:

4) What is the time required to implement the corrective actions needed?

5) Are there any temporary operating limitations that apply to the generating unit until the corrective actions are completed?

6) Are revisions to the generating unit's winterization preparedness plan, or further corrective actions to be taken required?

7) If the answer to 6. above is NO; Document any technical, commercial, or operational constraints to support the declaration.

GO/GOP CIP-003-8 / CIP-008-6 PLAN: Cyber Security Incident Response Plan

Version No. 4.1

Effective May 19, 2023

TABLE OF CONTENTS

1 REVISION HISTORY

VERSION NO.	EFFECTIVE DATE*	REVIEWED BY	SUMMARY OF CHANGES
1.0	7/1/2018	GridSME	New Plan
2.0	10/14/2019	Sean McCormick	Annual review. Content updates to reflect current practices.
2.1	12/27/19	Courtney Lai	Updated standard references to reflect CIP-003-8. No content changes.
2.2	6/29/20	Sean McCormick	Annual Review. Minor edits.
2.3	4/21/21	Courtney Wall	Minor update to references for renamed NERC Incident Evaluation Form.
3.0	8/25/21	Khrystsina Navumenka; Sean McCormick; Dan DeRosa	Annual review. Revisions based on incident response plan test conducted May 7, 2021. Added instructions for communication during incident. Added DOE-417 reporting criteria.
3.1	8/12/22	Khrystsina Navumenka	Annual review. Minor edits in the language. Updated TexasRE contact information for reporting.
4.0	5/19/23	Derrick Bethea	Created a single Cyber Security Incident response plan for both GO and GOP obligations. Updated plan to incorporate CIP-008-6 in preparation for a medium impact BES assets. Added reference and notification to ERCOT for Cybersecurity Incidents.
4.1	9/12/23	Derrick Bethea	Minor update to the title and header.

*Effective Date is the date of approval by the CIP Senior Manager or delegate.

2 PURPOSE

Cypress Creek Renewables uses this plan to mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

This document serves as the Cyber Security Incident Response Plan (CSIRP) in accordance with CIP-003-8 (for low impact) and CIP-008-6 (for medium or high impact) to support security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperations or instability in the Bulk Electric System (BES).

3 SCOPE

This plan applies to persons with responsibilities with a role in this Cyber Security Incident Response Plan.

Direct questions to the CIP Senior Manager or the Operational Compliance Team with any questions regarding the applicability of this document.

4 DEFINITIONS

4.1 Internal Definitions

No internal definitions are used within this plan.

4.2 External Definitions

Unless otherwise noted, capitalized terms used in this document are found in the Reliability Standard, NERC Glossary of Terms, or other FERC or NERC approved documents.

5 ACRONYMS

Acronym	Term
BCA	BES Cyber Asset
BES	Bulk Electric System
EACMS	Electronic Access Control Monitoring System
EAP	Electronic Access Point
ERC	External Routable Connectivity
ESP	Electronic Security Perimeter
MSSP	Managed Security Service Provider
PACS	Physical Access Control System
PCA	Protected Cyber Asset
PSP	Physical Security Perimeter

6 ROLES AND RESPONSIBILITIES

Role	Responsibility
CIP Senior Manager / Delegate	• Provide input during the evaluation of an actual or suspected incident, its impact(s) on the BES, and proposed actions in response to an incident, ensuring input from appropriate team members is considered. • Participate in post-incident reviews, as well as the identification and incorporation of lessons learned into appropriate documentation and processes.
Incident Commander (IC)	• Direct incident response activities of all the involved personnel in the CSIRP process. • Facilitate incident communications between appropriate personnel and ensure information is disseminated for internal and external reporting as required. • Submit evidence to OC Team upon completion and upon request.
Initial Discoverer	• The Initial Discoverer of any potential or suspected incidents. • May participate as a CSIRT member, to the extent necessary.
Operating Personnel	• If Initial Discoverer, fulfill role as described. • Notify the Incident Commander of any potential incidents as per standard operating protocols. • Provide feedback on potential impact(s) to Operations of the incident and proposed containment actions. • Submit evidence to OC Team upon completion and upon request.
GridSEC Managed Security Services Team (Grid Security Team)	• If Initial Discoverer, fulfill role as described. • Analyze potential and suspected Cyber Security Incidents and provide technical, containment, and remediation guidance. • Provide evidence related to Cyber Security Incidents.
Nor-Cal Controls SCADA Team (SCADA Engineer)	• If Initial Discoverer, fulfill role as described. • Analyze potential and suspected Cyber Security Incidents and provide technical, containment, and remediation guidance. • Provide evidence related to Cyber Security Incidents.
Cypress Creek Renewables, LLC Information	• Provide support to identify and mitigate potential threats. • Assist in developing lessons learned and corrective actions.

Technology Team (CCR IT)	

Operational Compliance (OC) Team	• Assess the Cyber Security Incident, with assistance from other roles, to determine if it is a Reportable Cyber Security Incident.
	• If required, report the Reportable Cyber Security Incident to E-ISAC without delay.
	• Facilitate additional communication with appropriate industry reporting agencies, as necessary.
	• Ensure the Cyber Security Incident Response Plan (CSIRP) is tested at least once every 15 calendar months for medium or high impact applicable cyber systems.
	  ○ If no medium or high impact applicable cyber systems are identified, then the plan may be tested every 36 calendar months per CIP-003-8.
	• Ensure the CSIRP is updated, based on lessons learned, within 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, along with notification of updates to anyone with a role in the CSIRP.
	  ○ If no medium or high impact applicable cyber systems are identified, then updates to the plan and subsequent updates may be made within 180 calendar days per CIP-003-8 of executing the plan.

7 CYBER SECURITY INCIDENT RESPONSE PLAN SPECIFICATIONS

Cypress Creek Renewables (CCR) uses the following procedural steps for this plan and to adhere to CIP-003-8 and CIP-008-6 for Cyber Security Incident reporting and response. Note that if the CIP-002-5.1 results do not yield any BES assets with medium or high impact BES Cyber Systems, then this plan will comply only with the Cyber Security Incident response plans in CIP-003-8 R2, Section 4.

7.1 Cyber Security Incident Response Plan Specifications (R1)

The following steps are taken to identify, classify, and respond to Cyber Security Incidents.

7.1.1 Identifying Cyber Security Incidents

The primary activities in the incident identification phase are:

- Review events and alarms;
  - Cyber indicators such as:

- Unexplained changes in the availability or unavailability of a service;
- GSoftware performance, increased command latency;
- Software crashes and data-base corruptions;
- Changes in software behavior, (such as reset commands performing an alarm test);
- Line, bus, or transformer relay actions with no indicated fault targets or unusual combinations of fault targets;
- Social engineering efforts directed at Personnel;
- Unexplained use of privileged accounts;
- Suspicious, unusual, or excessive unsuccessful login attempts;
- Unexplained new user accounts;
- Unstable systems or system crashes;
- Poor or inconsistent system response time.

- Physical indicators such as:
  - Physical security alarms or obvious signs of intrusion (e.g. cut fencing, broken locks, pry marks, etc.);
  - Unescorted, unauthorized visitors within a BES Cyber Systems perimeter;
  - Any suspicious packaging, unknown equipment, unexplainable changes to wiring;
  - USB drives or other foreign devices found connected to BES Cyber Systems

- Gather evidence; and
- Analyze logs, artifacts, and indicators of compromise to determine if an incident has occurred.

Information included in the analysis is intended to provide the CSIRT with enough guidance to determine if a potential Cyber Security Incident has occurred and whether to notify Operating Personnel and Incident Commander. Items identified may indicate a potential Cyber Security Incident or may be caused by approved work or benign software issues. It is important to be aware that seemingly unrelated cyber and physical events may be related; be cautious to not draw conclusions before analysis and communications have been conducted. Initial Discovers and Operating Personnel are not expected to make the determination of a potential Cyber Security Incidents, only to be aware of the signs and make the appropriate notifications so the CSIRT can begin investigating any potential Cyber Security Incidents.

7.1.2 Classifying Cyber Security Incidents

A Cyber Security Incident is assessed to determine if it meets the NERC definition of a Cyber Security Incident as follows:

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or

- Disrupts or attempts to disrupt the operation of a BES Cyber System

Additionally, a Cyber Security Incident is considered reportable if it meets the NERC definition of a Reportable Cyber Security Incident as follows:

A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BES Cyber System; or
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System.

The analysis is performed cooperatively by OC Team and the Incident Commander. The **CCR Cyber Security Incident Evaluation Form** is used during the assessment and classification. This process assists in responding to the incident and determining whether a Cyber Security Incident is a Reportable Cyber Security Incident.

7.1.2.1 Assessment of Affected System(s)

The following steps are taken to determine potential Cyber Assets or system are affected:

1. Determine which Cyber Assets or systems are, or could be, affected by the incident;
2. Observe/analyze for any decreased performance, loss of control, latency, etc.;
3. Gather applicable reference documentation for the affected system(s);
4. Determine if the incident is a physical threat or an electronic threat, or both;
5. Attempt to determine if the damage originated internally or from an external source(s);
6. Determine if the threat can be blocked or isolated;
7. Determine extent of damage and if it can be repaired;

8. Determine time to repair or update security at access point; and
9. Conduct analysis to understand the effects of the event on Cyber Assets and the related BES Cyber Systems.

7.1.2.2 Determination of BES Cyber Systems Impacted

If a determination is made that applicable BES Cyber Systems or EACMS are affected, the IC leads the determination of the severity the threat presents to BES Cyber System or EACMS, and the impact(s) to the continued reliable operation of the BES by using the **CCR Cyber Security Incident Evaluation Form**.

If the impacted BES Cyber System or EACMS has a manual work-around process, the IC leads the evaluation to determine if it is prudent to isolate and cease use of the impacted BES Cyber System and implement the manual process.

If the impacted BES Cyber System or EACMS has a redundant system that has not been impacted, the IC leads the evaluation to determine if it is prudent to isolate and cease use of the impacted system and failover to the redundant system.

7.1.2.3 Determination of Reportable Cyber Security Incident

The OC Team assesses whether the Cyber Security Incident is considered a Reportable Cyber Security Incident by using information provided by the IC and other members of the CSIRT.

If it is determined by the OC Team that the Cyber Security Incident has compromised or disrupted one or more reliability task, a Reportable Cyber Security Incident has occurred or is occurring and is reported as required.

The OC Team sends an email to the Operational Compliance Program (OCP) Executive, OCP Compliance Officer, CIP Senior Manager, and appropriate Generator Owner representatives immediately upon determination of a Reportable Cyber Security Incident. There is no action required from the recipients to approve reporting. The OC Team reports the incident without delay.

7.1.3 Responding to Cyber Security Incidents

Upon discovery of any potential indicators, the Initial Discover reports the potential incident to C4 via phone. C4 operators will notify the Incident Commander of the potential Cyber Security Incident per the CCR OM Emergency Incident Response Plan.

The IC directs initial response to the incident with Operating Personnel. If a Cyber Security Incident is suspected, the IC activates the CSIRT as follows:

- The OC Team to ensure they are aware and can help in classifying the event;
- GridSEC Managed Security Services Team, as the 3rd party managed security provider;
- CCR IT for incident handling to resolve any issues created by the Cyber Security Incident;
- Operating Personnel and Field Personnel who may be affected or have a role in responding to the incident; and
- The CIP Senior Manager, for awareness and to assist in directing response if needed.

Activation of the CSIRT may include, as needed, some of the following approaches:

- An email to OMIncident@ccrenew.com per the CCR OM Emergency Incident Response Plan
- Creation of an emergency channel in the company messaging application (Slack or similar technology). GridSEC personnel on the CSIRT are available via the messaging application for inclusion into the emergency channel.
- Establishing a conference call bridge (via Zoom or similar technology) recurring meeting. This conference bridge may be utilized as needed by CSIRT members to coordinate response.

The role of Incident Commander may be delegated to another person on the CSIRT at the discretion of the on-duty Incident Commander at the time of the potential cybersecurity incident.

7.1.3.1 Containment

The following steps are taken, to the extent possible, to contain the Cyber Security Incident:

- Determine which systems are, or could be, affected by the incident;
- Observe/analyze for any decreased performance, loss of control, latency, etc.;
- Gather applicable reference documentation for the affected system(s);
- Determine if the incident is a physical threat or an electronic threat, or both;
- Attempt to determine if the damage originated internally or from an external source(s);
- Determine if the threat can be blocked or isolated;
- Determine extent of damage and if it can be repaired;
- Determine time to repair or update security at access point; and
- Conduct analysis to understand the effects of the event on Cyber Assets and the related BES Cyber Systems.

Short-Term Containment: Immediate actions performed or directed by CCR IT, Grid Security Team and the Nor-Cal Controls SCADA Team to prevent further impact of the attack. These actions may cause a disruption of some business services and, as such, should only be implemented for a short period. Due to the potentially disruptive nature of certain containment actions, notification to Operating Personnel is imperative.

Short-term containment actions may include the following:

- Network isolation
- Disconnection of a machine, device, or user account from the network
- Removal of electronic/suspend access
- Implementation of firewall rules or other security control applications

System Back-Up: For evidentiary and forensics purposes, a back-up of the system image should be created if possible and if supported by the affected system(s).
Back-up should be accomplished as soon as practical and, if the conditions allow, prior to any further investigation/analysis taking place.

Long-term Containment: Preventative actions taken to mitigate the opportunities for machines or data from being exploited in any ongoing or future attacks.
Long-term containment actions may include the following:

- Security patching of machines
- Changing of passwords or account privileges
- Application of firewall rules or filters
- Redesign of network architecture or communication flow
- Altering of trust relationships between domains or sites
- Disabling of unused ports and services on network devices and servers
- Implementation of security tools, applications, or controls

7.1.3.2 Eradication

The purpose for the eradication phase is to remove all remnants and artifacts used as part of the attack (files, folders, programs, executables, malware, accounts, etc.).

The eradication phase normally should not begin until the CSIRT is confident that the incident is fully identified and contained. If, during eradication, it is discovered the incident is not contained, the team should re-evaluate the incident and perform necessary containment actions. If these containment actions are not performed, the team risks exposing "clean" or uncompromised devices to the threat/vulnerabilities again, or for the first time.

7.1.3.3 Recovery / Incident Resolution

Restoration from backups or replacement of primary equipment (as necessary) should begin as soon as practicable. Important items to consider in the recovery phase include the following:

- Preservation of evidence, if not already preserved, to the extent practicable;
- Performing additional analysis as needed to complete the investigation;
- Removal of the components of the incident impacting the affected systems, such as deleting the malicious code or disabling a compromised user account;
- Mitigating the attack vector so a similar incident does not occur (for example, patch the vulnerability used to compromise the system, apply standard system hardening procedures, adjust firewall rulesets, etc.); and
- Restoration of systems to normal operation.

7.2 Cyber Security Incident Response Plan Implementation and Testing (R2)

7.2.1 Plan Testing

This Cyber Security Incident Response Plan is tested at least once every 36-calendar months if the CIP-002-5.1a process does not yield any BES assets with medium or high impact BES Cyber Systems. Otherwise, this plan is tested every 15-calendar months in accordance with CIP-008-6.

Testing may be accomplished by any of the following:

- Responding to an actual Reportable Cyber Security Incident;
- With a paper drill or table top exercise of a Reportable Cyber Security Incident; or
- With an operational exercise of a Reportable Cyber Security Incident.

Cyber Security Incident tests or drills follow this plan. Any variations to the implementation of the plan during testing should be noted and utilized for plan updates as deemed necessary.

7.2.1.1 Evidence of the Plan Testing

Evidence for testing this plan via either a response to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident is retained and may include, but is not limited to, dated evidence of:

- Exercise test plan and participant lists;
- Exercise notes, completed **CCR Cyber Security Incident Response Team Post-Incident Review Form**, and evidence of communications made (e.g. emails, phone logs); and

- Post-exercise review notes and lessons learned.

7.2.1.2 Evidence of a Reportable Cyber Security Incident

Evidence related to a Reportable Cyber Security Incident is retained and may include, but is not limited to, dated evidence of:

- Incident notes, completed **CCR Cyber Security Incident Evaluation Forms**, and evidence of communications made (e.g. emails, phone logs);
- Forensic analysis;
- Security logs; and
- Post-incident review notes and lessons learned

7.3 Cyber Security Incident Response Plan Review, Update, and Communication (R3)

The following actions are taken within 90 calendar days after completion of a Cyber Security Incident Response Plan test or actual Reportable Cyber Security Incident response. If no BES assets with medium or high impact BES Cyber Systems are identified in the CIP-002-5.1a process, these actions may be completed in 180 calendar days.

7.3.1 Actions Following the Use of the Cyber Security Incident Response Plan

The following actions are taken after the use of the plan from either testing or an actual response to a Reportable Cyber Security Incident:

1. Any lessons learned, or absence of them, are documented from the use of the plan.
2. Lessons learned are then considered for potential updates to the plan. If the OC Team determines that an update of the plan is not needed, it documents that determination.
3. If any changes are made to the plan, notification to each person or group with a defined role in the Cyber Security Incident response plan is made with the updates to the Cyber Security Incident response plan.

8 EVIDENCE

8.1 Evidence Format

The associated form(s) with this document are one manner for capturing evidence. Other formats may be used, such as electronic systems, as long as they collect the equivalent information.

8.2 Evidence Retention

All documentation created by this procedure shall be stored in C4's compliance evidence repository for three (3) calendar years, unless directed by the Regional Entity or NERC to retain specific evidence for a longer period of time as part of an investigation.

9 ASSOCIATED DOCUMENTS

Listed below are additional documents that may be referenced.

- **OCP Applicable Entities List**
- **CCR BES Cyber Security Policies**
- **GO-GOP Cyber Security Incident Response Team Contact List**
- **CCR Cyber Security Incident Evaluation Form** (equivalent documentation may be used)
- **CCR Cyber Security Incident Response Team Post-Incident Review Form**
- **Generator Owner Cyber Security Incident Response Plan**

10 REFERENCES

Listed below are additional external resources, policies, and procedures that are relevant to this policy. The list may be amended, revised, or supplemented over time.

- NERC Standard CIP-003-8 https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-8.pdf
- NERC Standard CIP-008-6 https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf
- Department of Energy (DOE)
  - DOE OE-417 Reporting Form and Instructions:
  - Form: https://www.oe.netl.doe.gov/docs/OE417_Form_05312024.pdf
  - Instructions: https://www.oe.netl.doe.gov/docs/OE417_Form_Instructions_05312024.pdf
  - Online Reporting: https://www.oe.netl.doe.gov/OE417/Form/Home.aspx (allows you to include to NERC System Awareness and E-ISAC in the submittal)
- United States National Cybersecurity and Communications Integration Center (NCCIC)

- Incident Reporting Form:
- Form: https://www.cisa.gov/report

- Office of Cybersecurity, Energy Security & Emergency Response: https://www.oe.netl.doe.gov/oe417.aspx

- Texas Reliability Entity
  - Regional criteria - https://www.texasre.org/reliabilityservices

- SERC
  - SERC Regional Criteria - Disturbance Reporting: https://www.serc1.org/docs/default-source/program-areas/standards-regional- criteria/regional-criteria/serc-regional-criteria-disturbance-reporting-rev4.pdf4
- ERCOT
  - Nodal Protocol 16.18 -https://www.ercot.com/files/docs/2022/12/01/16-020123_Nodal.docx