Filing Receipt

Received - 2022-04-18 03:04:33 PM
Control Number - 53385
ItemNumber - 398

NERC Reliability Compliance Procedure – GO/GOP

CIP-002-5.1a

Cyber Security - BES Cyber System Categorization

Purpose

This procedure addresses the following requirement(s) of CIP-002-5.1a for the Generator Owner (GO) and Generator Operator (GOP):

R1: GO/GOP must implement a process that considers specified assets

R2: GO/GOP must review and obtain CIP Senior Manager approval of identifications at least once every 15 calendar months

It identifies and categorizes 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 misoperation or instability in the BES.

Procedure

See the References section for a link to the full text of the standard, including non-applicable requirements.

R1: GO/GOP must implement a process that considers specified assets

Th GO/GOP shall implement a process that considers each of the following assets for purposes of parts 1.1, 1.2 and 1.3:

- Control Centers and backup Control Centers
- Transmission stations and substations
- Generation resources
- Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements
- Special Protection Systems that support the reliability operation of the BES and
- For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 of CIP-002-5.1a.

The GO/GOP performs the categorization process as follows:

- Using the Impact Rating Criteria in Appendix A, the GO/GOP identifies the impact rating of each BES Cyber Asset. CIP-002-5.1a Addendum A Impact Categorization Form also describes the GO/GOP's top down BES Cyber System Categorization methodology.
- The GO/GOP's identification of assets as high, medium or low impact to the BES and their associated BES Cyber Systems are documented in CIP-002-5.1a Addendum A Impact Categorization Form.

R2: GO/GOP must review and obtain CIP Senior Manager approval of identifications at least once every 15 calendar months

The GO/GOP reviews the identifications in CIP-002-5.1a Addendum A impact categorization form, and updates them if there are changes identified at least once every 15 calendar months, even if it has no identified items.

The GO/GOP's CIP Senior Manager or delegate approves the identifications in CIP-002-5.1a Addendum A Impact Categorization Form at least once every 15 calendar months, even if it has no identified items.

Acceptable evidence includes, but is not limited to, electronic or physical dated records which reflect the CIP Senior Manager or delegate review and approval.

Review

This procedure must be reviewed for accuracy and compliance with the applicable NERC standard at least annually, not to exceed 15 months between reviews, or when a change is made to the standard. Evidence of the review must be maintained.

Retention of Data

The Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.

Applicable Reliability Functions

See the Applicable Reliability Functions document provided with the compliance program documentation for a list of specific roles relevant to each Facility.

References

Definitions

Glossary of Terms Used in NERC Reliability Standards
https://www.nerc.com/files/glossary_of_terms.pdf

Standard

CIP-002-5.1a Cyber Security - BES Cyber System Categorization
https://www.nerc.com/pa/Stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

Version History

Version	Published	Change Description	By
1.0	9/28/2021	Initial publication of CIP-002-5.1a procedure for GO and GOP.	S. Kerrin

Appendix A: Impact Rating Criteria

The criteria defined in the CIP-002-5.1a Addendum 1 standard do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.
2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.
2.5. Transmission Facilities with these characteristics:
    2.5.1. Operating between 200 kV and 499 kV at a single station or substation,
    2.5.2. The station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below.

    The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation.

For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of CIP-002-5.1a Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the BES.

3.6. For Distribution Providers, Protection Systems specified in Applicability section above.

NERC Reliability Compliance Policy – GO/GOP

CIP-003-8

Addendum A – Cyber Security Policy

Purpose

The purpose of this document is to specify consistent and sustainable security policies that establish responsibility and accountability to protect Akuo Energy's low impact BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Akuo Energy has developed this Cyber Security Policy to outline its commitment to protecting its Low Impact BES Cyber Systems. The intent is to ensure that all personnel are fully aware of their responsibilities and duties with regard to cyber security and protecting the BES.

This Cyber Security Policy addresses the security topics outlined in CIP-003-8 R1.2. It further addresses the specific recommended security topics detailed in the CIP-003-8 Guidelines and Technical Basis section and Attachment 1.

Scope

CIP-003 R1.2 applies to Akuo Energy as an entity with assets identified in CIP-002 containing low impact BES Cyber Systems. Akuo Energy does not have any Medium or High Impact BES Cyber Systems.

Cyber Security Plan

The details of Akuo Energy's Cyber Security Plan can be found in CIP-003-8 R1 Addendum B. It contains the elements listed below.

Cyber Security Awareness

It is the policy of Akuo Energy that all employees, contractors, or vendors, who have a need for physical access to a low impact BES Cyber System, are subject to a Cyber Security Awareness program.

Physical Security Controls

The details of Akuo Energy's physical security controls can be found in the CIP-0038 R1 Addendum B.

Examples of acceptable methods of securing low impact BES Cyber System sites:

- Card Keys
- Biometrics
- Key Pads
- Locks
- Fences and gates that are in good condition

Electronic Access Controls

It is the policy of Akuo Energy that all Low Impact External Routable Connectivity shall pass through an electronic access point that permits only necessary inbound and outbound access.

Dial-up connectivity that provides access to Low Impact BES Cyber Systems at Akuo Energy is prohibited.

Cyber Security Incident Response Plan

The details of Akuo Energy's Cyber Security Incident response plan can be found in CIP-003-8 R1 Addendum C. The Cyber Security Incident response plan includes the following:

- Recognition and Notification of Cyber Security Incidents
- Cyber Incident Reporting Obligation
- Roles and responsibilities for Cyber Security Incident response
- Testing of the Response Plan once every 36 months and updating the plan within 180 days of any change.

The Cyber Security Incident response plan is intended as a guide to understand how to recognize and respond to a cyber-security incident. The plan shall be used in all situations where there a security incident.

Akuo Energy shall ensure that all events determined to be Reportable Cyber Security Incidents are formally reported to the E-ISAC, unless prohibited by law. A process for this specific obligation shall be developed and included in Akuo Energy's Cyber Security Incident response plan.

Transient Cyber Assets (TCA) and Removable Media (RM) Malicious Code Risk Mitigation

The details of Akuo Energy's TCA and RM malicious code risk mitigation plan can be found in CIP-003-8 R1 Addendum D. The TCA and RM malicious code risk mitigation plan identifies mitigating measures that reduces the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of TCAs or RM. Akuo Energy's Site Manager shall complete the TCA-RM Authorization Form prior to allowing any TCA or RM use on a BES Cyber System.

CIP Exceptional Circumstances Plan

The details of Akuo Energy's CIP Exceptional Circumstances plan can be found in CIP-003-8 R1 Addendum E. Procedures for declaring and responding to CIP Exceptional Circumstances include identification, documentation, and review of the event. Akuo Energy must complete the CIP Exceptional Circumstances Form for each CIP Exceptional Circumstance.

Review

This policy must be reviewed for accuracy and compliance with the applicable NERC standard at least annually, not to exceed 15 months between reviews, or when a change is made to the standard. The review can be documented on the Documentation Review and Sign-off Form provided with the NERC compliance documentation package.

Version History

Version	Published	Change Description	By
1.0	9/28/2021	Initial publication of CIP-003-8 Addendum A for Akuo Energy.	S. Kerrin

NERC Reliability Compliance Plan – GO/GOP

CIP-003-8

Addendum B – Cyber Security Plan

Purpose

This document defines Akuo Energy's Cyber Security Plan for its low impact BES Cyber Systems that includes Cyber Security Awareness and Physical and Electronic Access Controls.

Scope

This plan applies to Akuo Energy's generation Facilities and all operating personnel, employed or contracted.

Cyber Security Awareness

The purpose of Akuo Energy's Cyber Security Awareness program is to ensure that its personnel having a need for physical or electronic access to Low impact BES Cyber Systems receive ongoing reinforcement in sound security practices. Akuo Energy provides this reinforcement at least once every fifteen (15) calendar months.

It is generally understood by the security professional community that people are one of the weakest links in attempts to secure corporate assets. The "people factor" not technology is the key to providing an adequate and appropriate level of security. If people are the key, but also are a weak link, more and better attention must be paid to these resources. A robust security awareness program is of paramount importance in ensuring that people understand their security responsibilities, organizational policies, and how to properly use and protect the assets entrusted to them.

For Akuo Energy to appropriately protect the confidentiality, integrity, and availability of its assets, it must ensure that its personnel:

- Understand their roles and responsibilities related to Akuo Energy's mission and are aware of the security concerns that can affect that mission
- Understand Akuo Energy's security policy, procedures and practices
- Have adequate knowledge of the management, operational, and technical controls required and available to protect Akuo Energy's assets for which they are responsible

To ensure that the above goals are accomplished, the CIP Senior Manager (or delegate) provides periodic awareness information to plant employees and contractors with access to the facility at least once every fifteen (15) calendar months using one of the following methods:

- Emails or bulletins with information on current events and security news.
- Posted informational signs that focus on cyber security. Signs include the use of posters reminding staff of the need for cyber security as they carry out their daily activities.
- Scheduled informal meetings to discuss computer and network security for home and office systems. The topics may include, but are not limited to, the awareness topics such as those listed in Appendix A.

Physical Security Controls

The purpose of Akuo Energy's physical security controls program is to ensure that its Low impact BES Cyber Systems have adequate physical controls. Akuo Energy has implemented physical access controls at the access point into each physical security area and the protected locations housing the physical access control system. The access controls consist of:

- Fences with locks
- Cameras (passive)
- Security Personnel: Plant Managers during normal working hours
- Visitor log in at the substation control room and Operations and Maintenance (O&M) administration building
- Locked doors (e.g. power house buildings)

The following are procedures for the appropriate use of physical access controls, including access management, response to loss, and prohibition of inappropriate use of physical access controls.

Physical access to Low impact BES Cyber Systems is granted to personnel based on need. Examples of roles that need access to Assets include the following:

- Plant Manager ensures proper operation of the facility.
- Systems support personnel ensure that BES Cyber Systems are set up and working correctly.
- Plant management staff including engineers supervise plant employees.
- Technicians ensure proper operation and maintenance of the facility.
- Asset Managers ensure Assets are maintained to the Asset owner's satisfaction and ensure proper operation and management decisions.
- Asset Managers ensure that the plant staff are maintaining the Asset per contract requirements.
- Although Plant Admin Staff do not need access to BES Cyber Systems, they need access to the Plant Facility to ensure plant payroll and other essential paperwork is completed including accounts payable and billing.
- Other positions as dictated by plant needs.

The Plant Manager decides what access is required by Plant personnel, vendors and others.

Akuo Energy authorizes visitors through the main gate by personnel in the control room or Administration Office. After entering Akuo Energy premises, visitors log in on the visitor login sheet located in the control room or Administration office. The visitors log documents each visitor's name, point of contact, time of initial entry and time of last exit of the day.

Electronic Access Controls

Akuo Energy shall implement controls to restrict electronic access for External Routable Connectivity and Dial-up Connectivity, which shall include the following, or other electronic access controls that provide an equal or greater level of protection:

External Routable Connectivity

For any External Routable Connectivity, establish a Low Impact BES Cyber System electronic access point that permits only necessary inbound and outbound electronic access and denies all other access for any communications that are:

- Between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
- Using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and

- 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).; and

Dial-Up Connectivity

Dial-up connectivity that provides access to Low Impact BES Cyber Systems at Akuo Energy is prohibited.

Physical Access to Electronic Access Control Device(s)

All electronic access control devices shall be located within a physical border to protect against unauthorized physical access and compromise. Physical security controls are identified in the Physical Security Controls section.

Access Policy and Access Control List (ACL) Implementation

1. All Cyber Assets used for the purpose of electronic access control must deny access by default for inbound and outbound traffic, meaning that explicit access permissions must be specified (by source & destination IP address and port/service/protocol allowed). Even if an electronic access control device(s) is designed to deny all traffic by default, a specific rule shall be added to the ruleset to explicitly deny all access not explicitly allowed in the ACL.
2. Akuo Energy shall document all inbound and outbound connections for any electronic access control device(s).
3. Whenever Cyber Assets that are permitted to communicate across the electronic access control device(s) boundary are removed from the network or their associated IP addresses are changed, the firewall ACL must be updated to reflect these changes.
4. Akuo Energy permits ERC and has electronic access control device(s).

ERC and Electronic Access Control Device Requirements

It is Akuo Energy's policy to only permit electronic device to device and interactive remote access based upon a business need. This access shall be documented in the configuration file of the electronic access control device(s). Each access control entry (ACE) within the access control device shall be explained in one of these files.

- Prior authorization for the ERC connection to BES Cyber Systems must be obtained from the Akuo Energy Engineer or Control System Administrator.
- Remote user must make arrangements with the Control System Administrator to enable and use interactive remote access.
- The remote access connection shall be physically disconnected or disabled on the device except when in use.
- Akuo Energy shall maintain electronic access control device(s) traffic and access logs to the extent of the device's storage capability or at least 90 calendar days, where possible. This information may aid in Cyber Security Incident investigations.

External Remote Access Procedure

Akuo Energy restricts and tightly controls external interactive remote access to its Low Impact BCS. Only authorized individuals, using two-factor authentication and encrypted VPN connections, are provided with interactive remote access.

Restricting Electronic Access

It is Akuo Energy's policy to permit electronic access to only those personnel and processes with an expressed business need for access. The System Administrator or delegate shall approve all access requests prior to the access being granted/configured.

Electronic Access Documentation Information:

- The company name,
- Department,

- The originating phone number for dial-up,
- The originating public IP address for remote from the Internet access,
- Which BCS system(s) to be accessed,
- User who initiates the connection (if known),
- The purpose of the connection.

The CIP Senior Manager or delegate shall approve all electronic access to LIBCS prior to the access being granted/configured. These access rights shall be documented by the electronic access control device System Administrator. Once authorized, the user must make arrangements with the electronic access control device System Administrator to document and enable the electronic access.

Procedures for Granting and Revoking Electronic Access

Granting Access: Electronic access to Low Impact BES Cyber Systems and Electronic Access Points are granted by the CIP Senior Manager or delegate/System Administrator based on need.

Identified Roles Requiring Access:

- Control room operator - ensure proper operation of the facility.
- Systems support personnel - ensure that BES Cyber Systems are set up and working correctly.
- Plant management staff including engineers - supervise plant employees, including training and performance monitoring.
- Technicians - ensure proper operation and maintenance of the facility.
- Asset Managers (Owner Representatives) - ensure assets are maintained to the asset owner's satisfaction and ensure proper operation and management decisions.
- Project Managers - ensure that the plant staff are maintaining the asset per contract requirements.
- Plant Admin Staff - ensure plant communications and business continuity

Temporary Access

- Other positions as dictated by plant needs may include IT, Testing, or Controls Systems Contractors – Under supervision of an authorized electronic access user, a contractor may be granted electronic access to LIBCS to perform only the work contracted to do.

Revoking Access: Access shall be removed due to any of the following events, as appropriate:

- Employment termination,
- Contract termination,
- Transfer of duties,
- Extended leaves of absence, or
- Change in contract personnel.

Revocation method shall be documented with date of completion revocation action. Documentation of authorization of access shall be attached to revocation documentation to ensure all electronic access has been revoked. All access shall be revoked by exercising one or more of the following actions by the immediate supervisor or security personnel as soon as practical:

- Deactivating personnel within Active Directory,
- Removing electronic access in electronic access control or other firewall devices,

- Changing of user and/or shared account passwords,
- Collecting fobs, physical (brass) keys, updating padlock combinations,
- Collecting and deactivating Plant ID (for key card access and identification as an employee).

Review

These programs are reviewed and updated by the CIP Senior Manager or delegate as needed and upon the approval of any new versions of the CIP Standards.

Version History

Version	Published	Change Description	By
1.0	9/28/2021	Initial publication of CIP-003-8 Addendum B for Akuo Energy.	S. Kerrin

Appendix A – Cyber Security Awareness Topics

- Basic NERC CIP familiarity
- Internet Safety and Security Risks (e.g., Unknown e-mail/attachments)
- Protection of personal information and social engineering
- Personal use and gain issues on systems at work and home
- Software license restriction issues—when copies are allowed and not allowed
- Personally owned systems and software at work—Network Connection Not Allowed
- Supported/allowed software on organization systems, part of configuration management
- Data backup and storage—centralized or decentralized approach
- Desktop security—use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems
- Timely application of system patches—part of configuration management
- Use of acknowledgement statements—passwords, access to systems and data, personal use and gain
- Inventory and property transfer—responsible organization and user responsibilities (e.g., media sanitization)
- Web usage—allowed versus prohibited; monitoring of user activity
- Spam
- Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions
- E-mail list etiquette—attached files and other rules
- Visitor control and physical access to spaces—applicable physical security policy and procedures, e.g., challenging strangers, tailgating, reporting unusual activity
- Workplace violence prevention and response
- Handheld device security issues—both physical and wireless security issues
- Laptop security while on travel—both physical and information security issues

NERC Reliability Compliance Plan – GO/GOP

CIP-003-8

Addendum C – Cyber Security Incident Response Plan

Purpose

This document defines Akuo Energy's Cyber Security Incident Response plan. The plan addresses the actions and reporting procedures to be followed in the event of a Cyber Security Incident.

Scope

This plan applies to Akuo Energy Facilities and all operating personnel, employed or contracted.

Identification of Cyber Security Incident

A Cyber Security Incident is any adverse event that threatens the confidentiality, integrity or availability of Akuo Energy's information resources or disrupts or attempts to disrupt the operation of the BES Cyber System.

Symptoms of a Cyber Security Incident can include the following:

- Abnormal response time or non-responsiveness
- Unexplained account lockouts
- Passwords not working
- Programs not running properly
- Running unexpected programs
- Lack of disk space or memory
- Bounced-back emails
- Inability to connect to the network
- Constant or increasing crashes
- Abnormal hard drive activity
- Connecting to unfamiliar sites
- Browser settings changed
- Extra toolbars that cannot be deleted

This list is not comprehensive, but is intended to raise the awareness level of potential signs. If unsure about a possible incident, treat the signs as a security incident and notify the plant's On Shift Operator who will contact the Shift Supervisor, who will work with the organization's technical support staff or vendor to determine if there is a Cyber Security Incident or other issue effecting the system.

Classification of Cyber Security Incidents

A Reportable Cyber Security Incident includes any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. Akuo Energy defines reporting requirements which may include the U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability (pursuant to Form OE- 417), NERC, FERC, E-ISAC, and any report to the Federal Bureau of Investigation (FBI) or a local law enforcement agency based on the following criteria:

Reportable Cyber Security Incidents include compromises or attempts to compromise the low impact electronic security zone or low impact physical security zone and disruptions or attempts to disrupt the operation of a BES Cyber System.

Event Classifications

- Physical Event – An attack on any part of Akuo Energy's Facilities causing damage or destruction that results from actual or suspected intentional human action. Additionally, any threat that has the potential to degrade normal operation of the facility or the manifestation of a suspicious device or activity at the facility. Physical events may include defeating security barriers or physical monitoring devices to obtain unauthorized access.

- Cyber Event – Disruption, degradation or destruction of a Cyber Asset resulting from actual or suspected intentional human actions with or without a complementary physical event. Cyber events may include malware, unauthorized access and denial of service attacks.
- Vandalism – Action involving deliberate destruction of or damage to public or private property.

Incident Handling General Guidance

Evidence Collection and Documentation

As soon as a Cyber Security Incident is suspected to have occurred or is occurring, immediately start recording all facts regarding the incident. A log notebook is an effective and simple medium for this, but email, smart phones, laptops, audio recorders, meeting notes, post incident review notes, security logs and digital cameras can also serve this purpose. Documenting system events, telephone conversations, and observed changes in files can lead to a more efficient, more systematic and less error-prone handling of the problem. Every step taken from the time the incident was detected to its final resolution should be documented. If log entries are used, the documented incident should be dated, time-stamped, and signed by the author. Whenever possible, incident responders should work in teams of at least two: one person to record and log events, while the other person performs the necessary tasks.

Incident Response Process

The incident response process is initiated when there is a reasonable basis to conclude that an incident with potential to disrupt one or more reliability tasks of the facility has occurred. The CIP Senior Manager, delegate or assigned Incident Coordinator assembles the CSIRT to confirm that a malicious incident has occurred, takes measures to contain the incident, implements measures to eradicate the threat and determines whether the incident is resolved or implements the recovery plan. Reporting of the incident is conducted via communication with third parties including:

- Law Enforcement – CIP Senior Manager or delegate determines the necessity and timing of contact with local law enforcement in the event of an immediate threat to life or property.
- E-ISAC – CIP Senior Manager or delegate pre-registers with E-ISAC to facilitate reporting, when necessary, a reportable Cyber Security Incident to the E-ISAC. Registration is available at https://www.esisac.com. Submission of a report to the E-ISAC adheres to the time reporting guidelines. Initial reporting of a Reportable Cyber Security Incident is to occur within one hour of identification as a Reportable Cyber Security Incident.

Identification and Detection

Once an event has been identified or detected, the CSIRT performs an investigation to verify if the event is considered a security incident and determines the type of threat it imposes. Sources of detection can be personnel, Intrusion Detection Systems, firewalls, anti-virus software or other detection methods. Once a security incident is identified and classified, the CSIRT immediately moves to the containment step while documenting the results of the incident detection and evaluation phase.

Preservation of Evidence

Conduct collection of information from the target system in accordance with appropriate forensic practices. Collect other relevant data that may correlate with the evidence of unauthorized access, including intrusion detection alerts and firewall logs. If a physical security breach occurs during the incident, collect physical security system logs, security camera videos and eyewitness accounts. Securely store collected evidence.

Containment

Perform containment at the earliest possible stage to avoid cascading incidents. If the threat is internal from a compromised system or device, isolate the device from the network to reduce the threat to unaffected systems. If the threat is external (e.g., attempt to access the low impact physical security area or electronic security area), take steps to sever or block the external accessibility to the extent possible.

Extensive analysis may be required to determine exactly what has happened. In the case of an active attack, the state of things may change rapidly. In most cases, it is advisable to perform an initial analysis of the incident, prioritize the incident, implement initial containment measures and then perform further analysis to determine whether the containment measures were sufficient.

Eradication, Recovery and Resolution

Successful attackers frequently install root kits, which modify or replace system binaries and other files. Root kits hide much of what they do, making it tricky to identify what was changed. If an attacker appears to have gained root access to a system, the best solution is to restore the system from a known good backup or reinstall the operating system and applications from scratch, and then secure the system properly. Changing all passwords on the system, and possibly on all systems that have trust relationships with the victim system, is also recommended. Some unauthorized access incidents involve the exploitation of multiple vulnerabilities, so it is important for the CSIRT to identify all vulnerabilities that were used and to determine strategies for correcting or mitigating each vulnerability.

If an attacker only gains a lesser level of access than administrator-level, base eradication and recovery actions on the extent to which the attacker gained access. Mitigate appropriately any vulnerabilities used to gain access.

Incident Handling – Unauthorized Physical Access

Unauthorized physical access occurs when a person gains access or attempts to obtain access to the physical security area that the person was not intended to have. Examples of unauthorized access incidents or their precursors and indications include:

- Unauthorized access attempt
- Breached border security
- Damage to the physical security system

If the event is occurring in real time:

1. Do not attempt to physically engage the violator.
2. Notify the Plant Manager, CIP Senior Manager or other plant staff
3. Observe areas accessed and methods of access
4. Report findings to the CSIRT

If the event is identified after the fact:

1. Notify the Plant Manager or CIP Senior Manager
2. Attempt to identify the point or method of access
3. Do not disturb any disturbed or damaged equipment until documented

The CSIRT should evaluate the extent and severity of the event and implement immediate methods to secure the breach or supplement monitoring at the access point. Once the immediate threat has been addressed, the CSIRT develops appropriate steps to fully repair the defeated security measures and identify methods to prevent future occurrences.

Incident Handling – Unauthorized Electronic Access

Unauthorized electronic access can occur both internally if access to the low impact physical security zone has already been achieved or externally by attempting to gain access from outside the facility. Unauthorized access is typically gained through the exploitation of the operating system or application vulnerabilities allowing access through a firewall or social engineering. Attackers may acquire limited access through one vulnerability and use that access to take advantage of additional vulnerabilities, eventually gaining higher levels of access.

1. Immediately notify the Plant Manager or CIP Senior Manager of the real or attempted access event
2. The CSIRT evaluates the extent of the unauthorized access, the source of the access (internal or external) as well as whether the offender used an employee account or alternate method of access (i.e., administrator account or malware breach)
3. Change the affected account passwords.
4. Where possible, isolate the access point from the network to prevent further access to the network.
5. For external attacks, implement additional security measures to prevent further access or temporarily remove external access capabilities (where feasible).
6. Once the immediate threat has been addressed, the CSIRT fully analyzes the nature and extent of access as well as any corrupted or appropriated information and executes measures to resolve the event or eradicate the potential for a future attack of the same nature.
7. Identify methods to prevent future occurrences.

Incident Handling – Malware, Virus and Malicious Code

Malicious code can manifest in different forms and can be delivered through many vectors either intentionally or unintentionally. Anti-Virus and malware scanning software provides an effective first line of defense, but evolution of malicious code and masking techniques may allow unidentified signatures to avoid detection.

1. Immediately notify the Plant Manager or CIP Senior Manager when evidence of malware or malware related indicators are detected.
2. The CSIRT identifies and documents a list of affected systems
3. Isolate the affected systems from the network to minimize the risk to additional systems.
4. Evaluate all data available to identify the source and extent of the malicious code and preserve as much evidence as possible for further investigation.
5. Manually update Anti-Virus signatures and initiate full system scans to remove the infected files. If the Anti-Virus software fails to disinfect the system, contact the vendor for a resolution.
6. Following successful removal of the infected files and successful full scan, restart the quarantined systems to determine if any rootkit elements exist that can potentially re-infect the system.
7. Evaluate the systems to verify that the appropriate operating system and software security patches have been applied.
8. When the system is determined to be secure and properly updated it can be restored to the network
9. Once the immediate threat has been addressed, the CSIRT will fully analyze effect and origin of the event and execute measures to eradicate the potential for a future occurrence.

Incident Handling – Denial of Service Attack

Denial of service can render cyber resources unavailable for its intended users or functions. While the attack may initially be external to a network, there are wide variations of attack types that can originate from within a network. While there are cases where the denial of service is the sole attempt, it has also been used as a secondary attack method or a diversion tactic allowing time for a more insidious attack to run its course.

1. Immediately notify the Plant Manager or CIP Senior Manager when evidence of denial of service attack detected or suspected.
2. The CSIRT identifies and documents a list of affected systems.
3. Isolate the system or network that is under attack.
4. Examine the evidence available through logs and events to determine the method and source of the attack.
5. Evaluate firewalls and routers to determine if they are configured appropriately and not a manipulated precursor to the attack.
6. Reconfigure firewalls and routers to block the source address or addresses and/or limit allowable destination addresses.
7. Reconnect the network and test for functionality and performance.
8. Examine the data logs to determine whether the origin of the attack was internal or external.
9. If the attack is determined to have originated from an internal source, evaluate the source system in a method similar to the one applied for Malware, Virus and Malicious Code identified above.
10. If the attack is determined to have originated from an external source, evaluate the systems with external connections in a method similar to the Unauthorized Access via Cyber Event as identified above.

Cyber Security Incident Response Team

Detection by direct observation and internal reporting of a Cyber Security Incident are the responsibilities of each Akuo Energy employee and vendor who is entrusted with the responsibility of safeguarding the physical or cyber security of CIP-related assets.

Role	Responsibility
Akuo Energy CIP Senior Manager or Delegate(s)	• This role functions as the onsite incident responder that provides overall direction and authority during a Cyber Security Incident, leads the classification and response to the incident, and coordinates other communication as may become necessary. • Shares in the decision-making process concerning the reporting of a Cyber Security Incident to law enforcement and E-ISAC. • Maintains a copy of the current version of this Cyber Security Incident Response plan and coordinates plan testing, approving changes to the plan and ensuring that it meets the requirements of the NERC CIP Reliability Standards. • Ensures testing of the Incident Response Plan 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 as required at least once every 36 calendar months. • Activates the Cyber Security Incident Response plan.
On Shift Operator	• Maintains communication with other parties in the interchange • Supports the BES Cyber Systems required for operation of the low impact facility • Maintains vendor support and contact information • Provides information on normal and abnormal equipment functions and functional cycles, and • Assesses the potential impacts when a component in the network is removed from service.
Shift Supervisor	• Assists in identifying and confirming an incident involving unauthorized access or unauthorized attempted access to a physical security area and communicating details of the incident to the CIP Senior Manager or delegate.

Role	Responsibility
Plant Administrator	• Taking notes and documenting the Cyber Security Incident. If needed, the Plant Administrator updates the Cyber Security Incident response plan within 180 calendar days after an actual Reportable Cyber Security Incident.
Information Technology Specialist	• Collects any available activity logs from network switches, routers, firewalls, and other relevant network components and access points before, during and after a Cyber Security Incident.
Corporate Compliance	• Assists the CIP Senior Manager in determining whether a Cyber Security Incident is reportable and reporting it to the E-ISAC, if necessary. • Archives all relevant Cyber Security Incident logs, communications, and other records pertaining to reportable Cyber Security Incidents.
Vendors	• May have an essential role in ensuring the CSIRT understands how to resolve or work around equipment failures and how to resume operations when necessary. • May be called upon for the supply of replacement software and hardware.

Communication Plan

CSIRT Contacts – The Akuo Energy cyber security roles and contact information documentation contains important contact information, including but not limited to members of the CSIRT, Akuo Energy staff and or vendor(s), and CIP-related asset vendors.

Initial Identification Notification – Direct the initial incident notification to the CIP Senior Manager or delegate. Notifications may originate from any of the personnel listed in the CISRT roles that receive alerts from applicable sources including any employee or vendor who is entrusted with the responsibility of safeguarding the physical and/or cyber security of Akuo Energy CIP-related Cyber Assets.

Vendor Support – If required, the CSIRT is responsible for initiating vendor support services.

Review and Approval

This program is reviewed and updated by the CIP Senior Manager or delegate as needed and upon the approval of any new versions of the CIP Standards.

Version History

Version	Published	Change Description	By
1.0	9/28/2021	Initial publication of CIP-003-8 Addendum C for Akuo Energy.	S. Kerrin

AFFIDAVIT

STATE OF ILLINOIS §
§
COUNTY OF COOK §

Before me, the undersigned notary public, on this day personally appeared Thomas Coté, to me known to be the person whose name is subscribed to the foregoing instrument, who being duly sworn according to law, deposes and says:

"1. My name is Thomas Coté. I am over the age of eighteen and am a resident of the State of Michigan. I am competent to testify to all the facts stated in this Affidavit, and I have the authority to make this Affidavit on behalf of TG East Wind Project LLC ("TG East").

2 I swear or affirm that in my capacity as President of TG East, I have personal knowledge of the facts stated in the Emergency Operations Plan ("EOP") submitted to ERCOT and filed into Project No. 53385.

3. I further swear or affirm that I have personal knowledge of the facts stated below:

- Relevant operating personnel are familiar with and have received training on the applicable contents and execution of the EOP, and such personnel are instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency;
- The EOP has been reviewed and approved by the appropriate executives;
- Drills have been conducted to the extent required by subsection (f) of PUC Subst. R. § 25.53 and limited by paragraph 4 below;
- The EOP or an appropriate summary has been distributed to local jurisdictions as needed;
- TG East maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident; and
- TG East's emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events will receive the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management Systems training by December 2022.

4. TG East intends to conduct a drill consistent with subsection (f) of PUC Subst. R. § 25.53 by December, 2022 and will provide notice to the Commission at least 30 days before that drill is conducted. Once that drill is conducted, TG East will notify the Commission.

5. I further swear or affirm the information, statements and/or representations contained in the Emergency Operations Plan are true, complete, and correct to the best of my knowledge and belief."

Further affiant sayeth not.

Thomas Coté
President
TG East Wind Project LLC

SWORN TO AND SUBSCRIBED TO BEFORE ME on the ____ day of April 2022.

Notary Public in and for the
State of Illinois

My Commission Expires:

AFFIDAVIT

STATE OF ILLINOIS §
§
COUNTY OF COOK §

Before me, the undersigned notary public, on this day personally appeared Thomas Coté, to me known to be the person whose name is subscribed to the foregoing instrument, who being duly sworn according to law, deposes and says:

"1. My name is Thomas Coté. I am over the age of eighteen and am a resident of the State of Michigan. I am competent to testify to all the facts stated in this Affidavit, and I have the authority to make this Affidavit on behalf of Rocksprings Val Verde Wind LLC ("Rocksprings").

2 I swear or affirm that in my capacity as President of Rocksprings, I have personal knowledge of the facts stated in the Emergency Operations Plan ("EOP") submitted to ERCOT and filed into Project No. 53385.

3. I further swear or affirm that I have personal knowledge of the facts stated below:

- Relevant operating personnel are familiar with and have received training on the applicable contents and execution of the EOP, and such personnel are instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency;
- The EOP has been reviewed and approved by the appropriate executives;
- Drills have been conducted to the extent required by subsection (f) of PUC Subst. R. § 25.53 and limited by paragraph 4 below;
- The EOP or an appropriate summary has been distributed to local jurisdictions as needed;
- Rocksprings maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident; and
- Rocksprings' emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events will receive the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management Systems training by December 2022.

4. Rocksprings intends to conduct a drill consistent with subsection (f) of PUC Subst. R. § 25.53 by December, 2022 and will provide notice to the Commission at least 30 days before that drill is conducted. Once that drill is conducted, Rocksprings will notify the Commission.

5. I further swear or affirm the information, statements and/or representations contained in the Emergency Operations Plan are true, complete, and correct to the best of my knowledge and belief."

Further affiant sayeth not.

Thomas Coté
Manager
Rocksprings Val Verde Wind LLC

SWORN TO AND SUBSCRIBED TO BEFORE ME on the ____ day of April 2022.

Notary Public in and for the
State of Illinois

My Commission Expires:

NERC Reliability Compliance Procedure – GO/GOP

EOP-004-4

Addendum A – Event Reporting Operating Plan

Purpose

This addendum addresses the following requirement(s) of EOP-004-4 for Akuo Energy:

R1: Event reporting Operating Plan

R2: Report specified events within the required timeframe

It improves the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

Procedure

See the References section for a link to the full text of the standard, including non-applicable requirements.

R1: Event reporting Operating Plan

A site's response to unusual events or activities follows a path of recognition, evaluation, action, and communication. Overall, BES reliability is enhanced when unusual events and electrical incidents are reported and analyzed by the proper authorities so that identified risks can be mitigated.

- The site employees or contractors shall promptly inform the Site Manager of any unusual occurrences or events that are recognized on company facilities.
- The following table gives examples of the kinds of unusual events/activities that shall be escalated to the Site Manager without intentional time delay. The list is not exhaustive, and employees shall err on the side of caution and over-communicate suspicious incidents to their superiors.

Unusual Events/Activities To Be Escalated To Facility Management	
Unauthorized access/entry to facility premises	Unauthorized attempt to gain access to a facility computer system
Vandalism, damage, or destruction discovered at a facility	Suspicion of (or actual) cyber intrusion on any computer network or system
Unauthorized physical surveillance or photography	Unexpected or unusual response of equipment to control inputs
Verbal or written threats to security, software, operations, or facility(ies)	Unexplained loss of communication systems or generating capability
Unidentified packages or deliveries discovered	Unexplained operation or failure of operation of facility systems
Unauthorized intelligence gathering, such as requests regarding operational data, software, telecommunications, schedules, etc.	Multiple suspicious events occurring within a short period

Employees who make the initial discovery shall attempt to gather as much detail about the unusual events/activities as possible including:

- Type of activity observed or discovered
- Time of discovery
- Time that incident potentially occurred
- Location of the incident
- Complete description of persons and or vehicles involved, if known. For persons: please note height, build, complexion and clothing. For vehicles: please give make, model, and color.

R2: Report specified events within the required timeframe

Evaluate and Act: The Site Manager shall then promptly evaluate unusual events/activities and initiate any emergency response actions based on the urgency of the situation to secure the safety of the facility and its personnel.

Communicate: Once the unusual event/activity has been identified and any immediate threat of danger has been addressed, the Site Manager shall begin notifying the appropriate contacts without intentional delay:

- Director of Asset Management
- Local law enforcement and first responders (call 911 if necessary)

If evaluation indicates a potential Cyber Security or DOE/NERC Reportable Incident:

- The Site Manager emails Incident Report Form to the Director of Asset Management and files the completed form onsite.
- The Site Manager contacts GE ROC via phone to report the incident.

GE ROC serves as intermediary for the majority of external communications:

- Transmission Operator, Transmission Owner, Transmission Planner
- Balancing Authority, Planning Authority, Reliability Coordinator, Transmission Service Provider
- Regional Entity, Regional Reliability Organization

GE ROC contacts internal departments as needed.

Validate Contact Information: Annually, site personnel or the GE ROC Team validate the contact information contained within this procedure and related work instruction for accuracy and retain evidence of that validation. The site requests GE ROC Team validation via phone or via email.

Version History

Version	Published	Change Description	By
1.0	9/28/2021	Initial publication of EOP-004-4 Addendum A Event Reporting Operating Plans for Akuo Energy.	S. Kerrin

Appendix A: Guidelines for NERC and DOE Reporting

Event Type	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of its Facility	TO, TOP, GO, GOP, DP	Damage or destruction of its Facility that results from actual or suspected intentional human action. It is not necessary to report theft unless it degrades normal operation of its Facility.
Physical threats to its Facility	TO, TOP, GO, GOP, DP	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at its Facility.

NERC Notification

- Items 1 - 3 above must be communicated to NERC, ERO, RC, TOP and Regional Entity within 24 hours of meeting an event type threshold listed above (or by the end of the next business day if the event occurs on a weekend).
- Entity shall submit NERC EOP-004 Attachment 2: NERC Event Reporting Form (see Appendix B or refer to the EOP-004 standard) via email to NERC at systemawareness@nerc.net.
- IF entity is required to submit a DOE Form OE-417 then simply copy NERC on the DOE submission (see DOE section below)
    - If email is unavailable then fax Event Reporting Form to NERC at 404-446-9770.
    - If email and fax are unavailable, call NERC at 404-446-9780 to verbally provide a preliminarily report.

Applicable DOE Reportable Incidents and Disturbances

1. Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations
2. Cyber event that causes interruptions of electrical system operations
3. Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems
4. Cyber event that could potentially impact electric power system adequacy or reliability

DOE Notification

- Items 1 and 2 above must be communicated to DOE within 1 hour of incident.
- Items 3 and 4 above must be communicated to DOE within 6 hours of incident.
- Submit updates as needed and a final report (all of Schedules 1 and 2) within 72 hours of the incident.
- Entity shall submit DOE Form OE-417 via email to DOE at doehqeoc@hq.doe.gov. Copy NERC at systemawareness@nerc.net. The form and instructions for completing it are available at https://www.oe.netl.doe.gov/oe417.aspx
- If Email is unavailable then fax Form OE-417 to DOE at 202-586-8485 and NERC at 404-446-9770.
- If Email and fax are unavailable, call DOE at 202-586-8100 and NERC at 404-446-9780 to verbally provide a preliminary report.

Appendix B: EOP-004 Attachment 2: Event Reporting Form

EOP-004 Attachment 2: Event Reporting Form Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net, Facsimile 404-446-9770 or voice: 404-446-9780, Option 1. Also submit to other applicable organizations per Requirement R1 "... (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or Applicable Governmental Authority)."		
Task		**Comments**
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes ☐ No ☐ Unknown ☐
4.	Event Identification and Description:	
	(Check applicable box) ☐ Damage or destruction of a Facility ☐ Physical threat to its Facility ☐ Physical threat to its BES control center ☐ BES Emergency: ☐ Firm load shedding ☐ Public appeal for load reduction ☐ System-wide voltage reduction ☐ Voltage deviation on a Facility ☐ Uncontrolled loss of firm load ☐ System separation (islanding) ☐ Generation loss ☐ Complete loss of off-site power to a nuclear Generating plant (grid supply) ☐ Transmission loss ☐ Unplanned evacuation of its BES control center ☐ Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability at its staffed BES control center ☐ Complete loss of monitoring or control capability at its staffed BES control center	Written description (optional):

NERC Reliability Compliance Procedure – GO/GOP

EOP-004-4

Event Reporting

Purpose

This procedure addresses the following requirement(s) of EOP-004-4 for the Generator Owner (GO) and the Generator Operator (GOP):

R1: Event reporting Operating Plan

R2: Report specified events within the required timeframe

It improves the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

Procedure

See the References section for a link to the full text of the standard, including non-applicable requirements.

R1: Event reporting Operating Plan

Each GO and GOP shall have a plan for reporting events to the Electric Reliability Organization (ERO) and other organizations (Regional Entity, company personnel, Reliability Coordinator, law enforcement, or governmental authority). Refer to EOP-004-4 Addendum A Event Reporting Operating Plan for plan details.

R2: Report specified events within the required timeframe

The GO and GOP must report events to the specified entities within either 24 hours of recognition of the event or by the end of the next business day (considered to be 4:00 p.m. local time).

Retention of Data

The GO must retain evidence since its last compliance audit.

Applicable Reliability Functions

See the Applicable Reliability Functions document provided with the compliance program documentation for a list of specific roles relevant to each Facility.

References

Definitions

Glossary of Terms Used in NERC Reliability Standards

https://www.nerc.com/files/glossary_of_terms.pdf

Standard

BAL-001-TRE-2 Primary Frequency Response in the ERCOT Region

https://www.nerc.com/pa/Stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

Version History

Version	Published	Change Description	By
1.0	9/28/2021	Initial publication of EOP-004-4 Event Reporting Procedure for GO/GOP.	S. Kerrin