Improving Self-Reporting

William Sanders
Cybersecurity Principal

Jodi Ernst
Operations & Planning Principal

Antitrust Admonition

Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Sli.do

slido

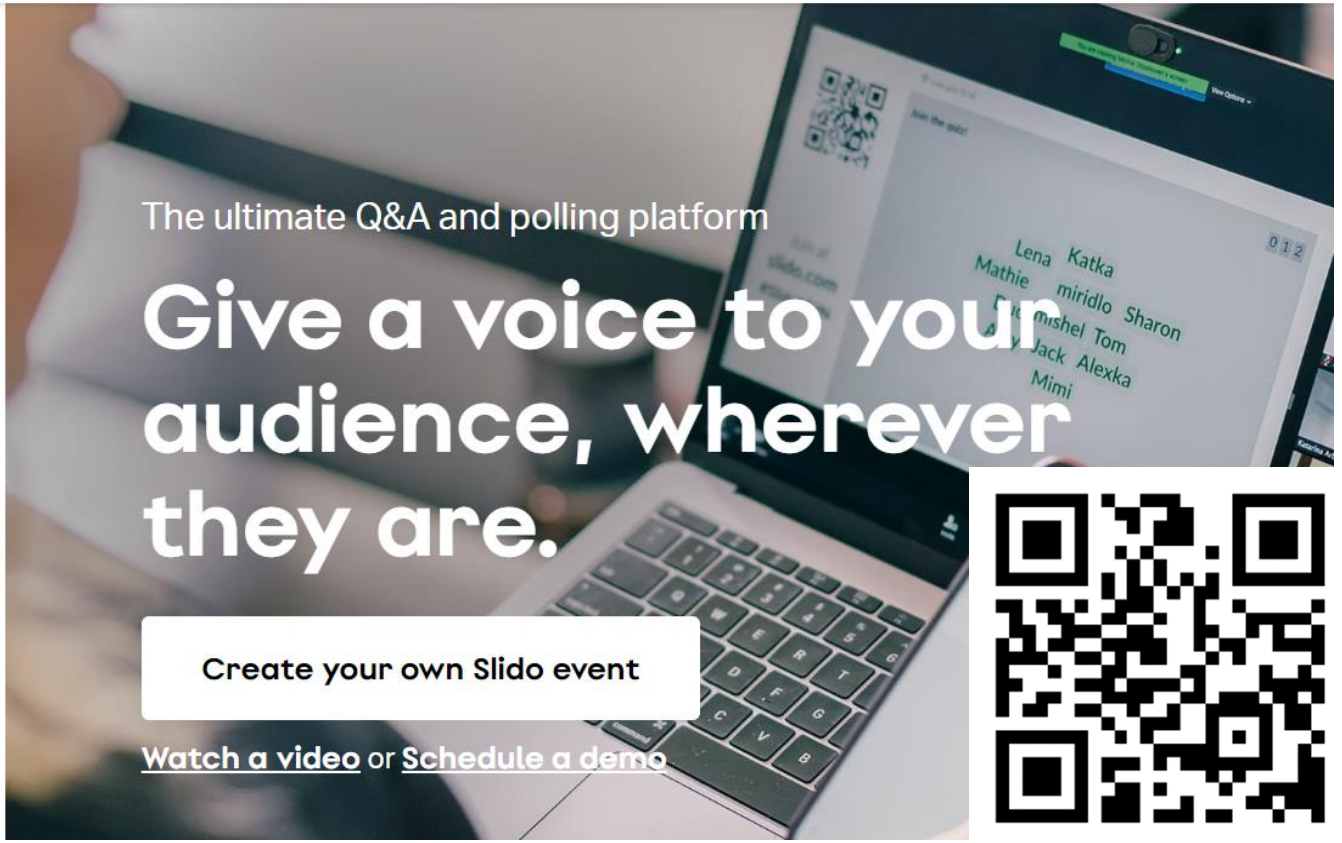
Product Solutions Pricing Resources Enterprise Log In **Sign Up**

#TXRE

Joining as a participant?

Enter event code

Join an existing event



Agenda

A review of what information NERC expects Texas RE to provide with each submitted case

Common issues Texas RE sees with Self-Reports

How to improve self-reporting

- Expedite issue processing
- Reduce or eliminate the need for RFIs

Note: The topics discussed today are also applicable to the submission of self-logs

ERO Expectations for a Self-Report

- Standard and Requirement
- Discovery date
- Discovery/root cause
- Scope of violation
- How the root cause was addressed
- How the violation ended
- If an extent of condition review was performed
- If no extent of condition review was performed, why not?
- If an extent of condition review was performed, what were the results?
- Verification of evidence

Standard and Requirement

Was the Standard enforceable on the start date of the violation?

Is the Standard applicable to the functional registration?

Align will only allow entities to submit Self-Reports for Standards and Requirements that are currently enforceable.

Discovery Date

What was the date that the entity initially discovered there was a violation?

Depending on discovery date and Self-Report submission date NERC may ask why there was a delay in reporting.

<u>Self-Reports</u> are expected to be submitted within three months of discovery.

Note: It is better to submit a Self-Report without all of the information Texas RE needs over waiting an extended period of time to submit the Self-Report.

Discovery/Root Cause

What series of events led to the discovery of the violation?

If applicable, describe in detail the internal controls that led to discovery.

Be verbose

Scope of Violation

- What types of BES Assets (Control Center, substation, generation resource, etc.) are involved?
- How many devices are involved?
- What are the impact ratings, or associated impact ratings, of the devices involved?
- What are the categorizations (BCA, EACMS, etc.) of the devices involved?

How the Violation Ended

What series of events led to the violation ending?

How does the provided evidence support that conclusion?

Does the evidence support the violation end date?

Actions to Prevent Reoccurrence

What actions have been taken (or will be taken in the future) to ensure that the events described in the root cause do not occur again?

Does the evidence support that conclusion?

Does the evidence support the implementation date?

Extent of Condition Review

Whether or not an Extent of Condition review was performed.

What were the results of the Extent of Condition review?

If no Extent of Condition review was performed, why not?

Verification of Evidence

Evidence should demonstrate what actions were taken.

Evidence should demonstrate when the actions were taken.

In some situations (such as training) evidence will need to demonstrate who took the actions.

Critical Infrastructure Protection

Examples – CIP-003 R1

Original

- **Scenario:** Entity did not document CIP Senior Manager approval of documented cyber security policies at least once every 15 calendar months.
- **Root Cause:** No calendar reminders to ensure that personnel were made aware of upcoming deadlines.
- **Prevention of Reoccurrence:** Provided reinforcement training to personnel to remind them of the importance of meeting deadlines.

Improved

- **Issue:** Root cause and prevention of reoccurrence actions do not align.
- **Root Cause:** No calendar reminders to ensure that personnel were made aware of upcoming deadlines.
- **Prevention of Reoccurrence:** Will acquire and implement a new compliance tool to generate calendar reminders and escalation notices as due dates approach. Current timeline is for tool to be implemented by end of Q4 2023.

Examples – CIP-004 R2 Part 2.3

Original

- **Scenario:** Entity discovered an individual's training expired six months prior.
- **Actions Taken:** Entity revoked user's access until training was completed. No Extent of Condition review performed.

Improved

- **Issue:** Without performing an Extent of Condition review there may be other individuals with lapsed training.
- **Actions Taken:** Entity revoked user's access until training was completed.
- Entity performed Extent of Condition review and determined that seven additional users were not current on CIP training.

Examples – CIP-004 R3 Part 3.5

Original

- **Scenario:** Entity discovered that numerous personnel did not have personnel risk assessments performed prior to granting electronic access and unescorted physical access.
- **Actions Taken:** None. Revoking access from affected personnel would reduce reliability.

Improved

- **Issue:** After reporting a violation of a NERC Requirement, entities need to either take actions to address the violation or plan actions to take in the future to address the violation.
- **Actions Taken:** Access left in place while personnel risk assessments performed. Attestation of dates personnel risk assessments were performed uploaded to the SEL.

Examples – CIP-005 R1 Part 1.3

Original

- **Scenario:** Entity has discovered noncompliant firewall rules.
- **Description:** Firewall rules were overly permissive on numerous firewalls.

Improved

- **Questions:**
  - How many firewalls?
  - How many noncompliant access permissions?
  - In what way were the access permissions overly permissive?
    - *Example: Was a single excess port being permitted or was this an any/any/any rule?*
  - What are the impact ratings of the BCS the firewalls were protecting?
  - How many BCS were put at risk?
- **Description:** For two firewalls located at one substation with medium impact BCS the firewall rules were overly permissive. Each firewall protects a medium impact BCS. Firewall #1 protects the RTU BCS and Firewall #2 protects the Protective Relay BCS. A detailed description of the firewall rules will be uploaded to the SEL.

Examples – CIP-007 R2 Part 2.3

Original

- **Scenario:** Entity did not install applicable patches within 35 calendar days, did not create a dated mitigation plan, and did not revise an existing mitigation plan.
- **Actions Taken:** Self-Report states that entity ended violation by installing the patches, but no evidence is provided.

Improved

- **Issue:** Texas RE needs to perform some type of verification in order to ensure that violations have ended.
- **Examples of Evidence:**
  - Change management tickets.
  - Baseline documentation showing the patch is installed.
  - Screenshots of command output showing application version.

Examples – CIP-008 R2 Part 2.1

Original

- **Scenario:** Entity tested their Cyber Security Incident response plan but did not use a Reportable Cyber Security Incident.
- **Evidence Submission:** Calendar invites showing when new test was conducted and updated Cyber Security Incident response plan to show documentation of lessons learned.

Improved

- **Issue:** The violation was for not using a Reportable Cyber Security Incident in the test scenario. Texas RE will need to review the new scenario that was used.
- **Evidence Submission:** Calendar invites showing when new test was conducted. Test document showing what actions occurred during the test scenario and what actions were taken in response. Cyber Security Incident response plan uploaded to show documentation of lessons learned.

Operations & Planning

VAR-002-4.1 R1 Background

R1. The Generator Operator shall operate each generator connected to the interconnected transmission system in the automatic voltage control mode (with its automatic voltage regulator (AVR) in service and controlling voltage) or in a different control mode as instructed by the Transmission Operator unless: 1) the generator is exempted by the Transmission Operator, or 2) the Generator Operator has notified the Transmission Operator of one of the following:

That the generator is being operated in start-up, shutdown or testing mode pursuant to a Real-time communication or a procedure that was previously provided to the Transmission Operator.

That the generator is not being operated in automatic voltage control mode or in the control mode that was instructed by the Transmission Operator for a reason other than start-up, shutdown, or testing.

Example – VAR-002-4.1 R1

Original

- **Scenario:** Generator Operator discovered that a generation resource that started up and came online over 4 hours ago, had never turned on the automatic voltage regulator (AVR).
- **Actions Taken:** Generator Operator notified the generation resource to place it's AVR in service immediately, ending the noncompliance.

Improved

- **Issue:** The Self-Report stated the noncompliance had ended. However, there was no description on how it ended along with no evidence uploaded to the SEL to verify.
- **Actions Taken:**
  - Verification of actual generation volts against the Transmission Operator voltage schedule OK.
  - Direction to the generation resource with an operating instruction to place the unit's AVR in service.
  - Verification of the AVR status change, indicating ON via SCADA.
  - Re-verification of the actual generator volts against the Transmission Operator voltage schedule OK.
  - Notification was made to the Transmission Operator with generation resource name, unit online time, and all AVR status change times since synchronizing on that operating day.

VAR-002-4.1 R2 Part 2.2 Background

R2. Unless exempted by the Transmission Operator, each Generator Operator shall maintain the generator voltage or Reactive Power schedule (within each generating Facility's capabilities) provided by the Transmission Operator, or otherwise shall meet the conditions of notification for deviations from the voltage or Reactive Power schedule provided by the Transmission Operator.

R2.2. When instructed to modify voltage, the Generator Operator shall comply or provide an explanation of why the schedule cannot be met.

Example – VAR-002-4.1 R2 Part 2.2

Original

- **Scenario:** Transmission Operator instructs the Generation Operator to decrease voltage by 1kV until further notice.
- **Action Taken:** Entity checks generation resource and determines that it will not be able to decrease the voltage. The generation resource is already at minimum voltage capability with all 34.5kV shunt capacitors out of service, and all 34.5kV shunt reactors in service.

Improved

- **Issue:** Self-Report and submitted evidence in the SEL do not state whether the Transmission Operator was notified by the Generation Operator of being unable to comply with the voltage schedule change instruction.
- **Examples of Evidence:**
  - Generator Operator log entries of actions taken to mitigate the noncompliance.
  - Generation Operator voice recordings of communications with the Transmission Operator.

VAR-002-4.1 R3 Background

R3. Each Generator Operator shall notify its associated Transmission Operator of a status change on the AVR, power system stabilizer, or alternative voltage controlling device within 30 minutes of the change. If the status has been restored within 30 minutes of such change, then the Generator Operator is not required to notify the Transmission Operator of the status change.

Example – VAR-002-4.1 R3

Original

- **Scenario:**
  - Just after taking shift, Generation Operator receives an alarm that a generation resource AVR has just turned OFF.
  - The Generation Operator noted the time and acknowledged the alarm, stopping the audible sound and flashing on the energy management system (EMS) alarm display
  - Generator Operator monitored the AVR status for a few minutes checking for the return to normal ON indication
  - Generator Operator was distracted with other operator actions and lost track of time, with the alarm acknowledged and silenced 36 minutes ago and the AVR continuing to indicate OFF

Improved

- **Issue:**
  - Generation Operator was made aware of generation resource AVR indicating OFF and failed to notify the Transmission Operator of AVR status change within 30 minutes of the change
  - No statement or evidence uploaded to the SEL of the Transmission Operator being notified
- **Examples of Evidence:**
  - Generator Operator log entries of actions taken to mitigate the noncompliance
  - Generation Operator log entries or voice recordings of communications with the Transmission Operator

Contact

William Sanders
Cybersecurity Principal
William.Sanders@texasre.org
512-583-4979

Jodi Ernst
Operations & Planning Principal
Jodi.Ernst@texasre.org
512-583-4954

Upcoming Sessions

- ~~June 5 – Intro to Align~~
- ~~June 6 – Standards Development~~
- ~~June 8 – Compliance Monitoring~~
- ~~June 13 – CIP 201~~
- ~~June 14 – Foundations of O&P~~
- ~~June 15 – O&P 201~~
- ~~June 20 – Risk-Based Approach to Reliability~~
- ~~June 21 – Improving Self-Reporting 201~~
- June 22 – NERC Data Submission, Events Analysis, and Guidelines
- June 27 – Initial Engagement Submissions
- June 29 – Reliability Services

TEXAS RE
Ensuring electric reliability for Texans