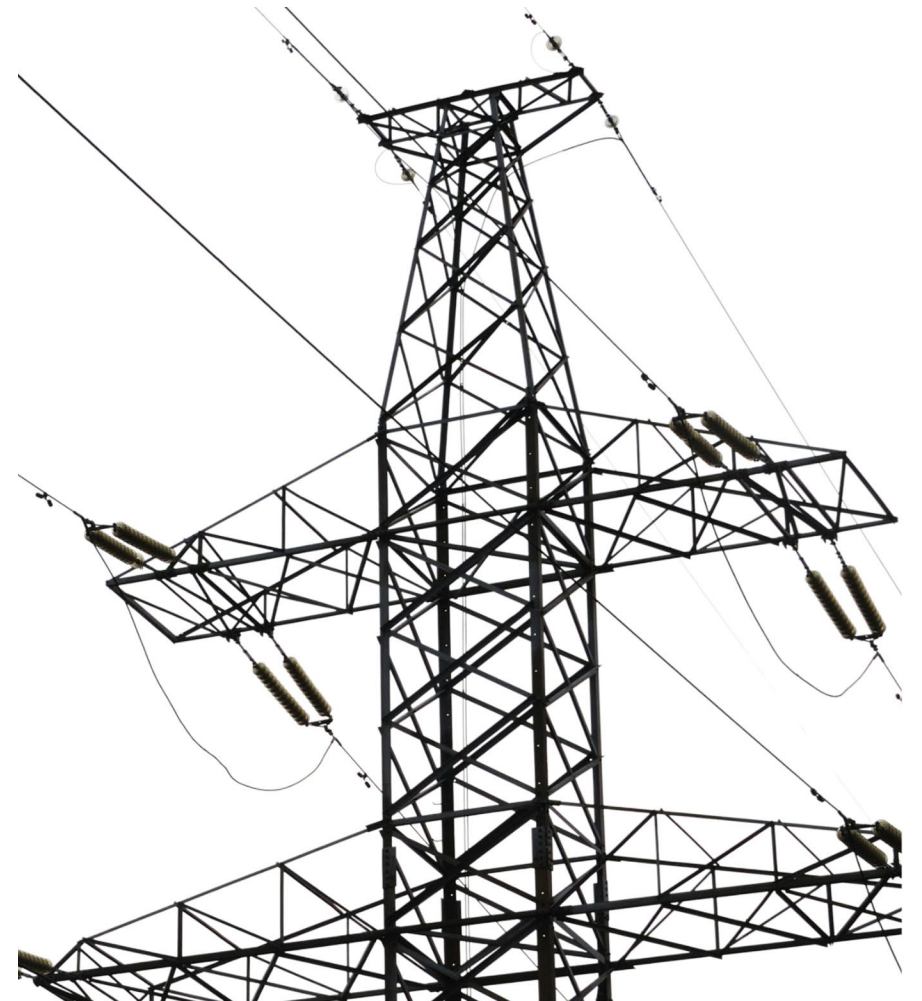


Anti-Trust Statement

It is ReliabilityFirst's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct which violates, or which might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every ReliabilityFirst participant and employee who may in any way affect ReliabilityFirst's compliance with the antitrust laws to carry out this policy.



2026 FALL RELIABILITY & SECURITY SUMMIT

DATA SUBMITTAL TRACK

September 16, 2026



2026 FALL RELIABILITY & SECURITY SUMMIT



Agenda

9:00-9:05

Welcome

Jim Uhrin, Director, Engineering & System Performance, ReliabilityFirst

9:05-9:45

xADS Reporting: Best Practices for Accurate and Effective Submissions

Gerald Esteban, Senior Engineer, Resource Adequacy, ReliabilityFirst

10:00-10:45

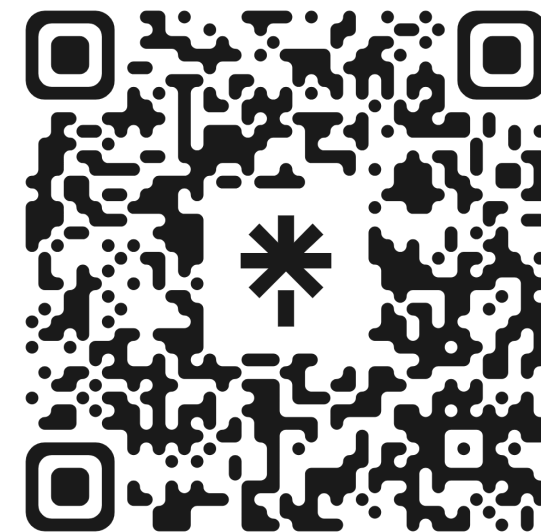
Self-Reports: Expectations and Best Practices

Marian Toney, Counsel, Enforcement, ReliabilityFirst

11:00-11:45

Event Reporting: Best Practices and Expectations

Tony Purgar, Senior Manager, Operational Analysis & Awareness, ReliabilityFirst



xADS REPORTING: BEST PRACTICES FOR ACCURATE AND EFFECTIVE SUBMISSIONS

Gerald Esteban

Senior Engineer, Resource Adequacy, Engineering & System Performance, ReliabilityFirst



RELIABILITY FIRST

PURPOSE

- *Understand what each tool collects, who submits the data, how it is reviewed, and how it becomes reliability insight.*
- *Please share this deck with your TADS, GADS, and MIDAS submittal SMEs.*

WHY IT MATTERS

"Those who cannot remember the past are condemned to repeat it."

George Santayana, *The Life of Reason* (1905)

What is xADS? - Availability Data System

Collection of events, outages, and misoperations used to assess system reliability

- Validates study inputs and assumptions
- Identifies trends before they become reliability risks
- Reveals equipment performance and outage trends
- Provides lessons learned
- Common reporting format makes data comparable across industry

TYPES OF xADS TOOLS

TADS

Focus

Transmission line and transformer outages

*New in 2026

- Load lost caused by outages
- Locational data of facilities

Who submits

Transmission Owners

Example output

Outage frequency and duration metrics

Cause coding

GADS Conventional

Focus

Conventional generating unit availability

Who submits

Generation Owners (nuclear, gas, coal, steam, hydro, etc.)

Example output

Availability and forced outage metrics

Cause coding

GADS Wind

Focus

Wind plant performance and availability

Who submits

Generation Owners (wind)

Example output

Availability and performance metrics

Cause coding

GADS Solar

Focus

Solar plant performance and availability

Who submits

Generation Owners (solar)

Example output

Availability and performance metrics

Cause coding

MIDAS

Focus

Protection system operations and misoperations

Who submits

Transmission Owners
Generation Owners
Distribution Providers

Example output

Protection system operation counts

Misoperation counts and rates

Cause coding

Section 1600 Data Request

Mandatory reporting for all applicable Registered Entities per the NERC Rules of Procedure under Section 1600

TADS: TRANSMISSION AVAILABILITY DATA SYSTEM

Purpose

- Transmission inventory, outage data, and load loss
- Supports frequency, duration, and cause analysis

Submission tool

- Open Access Technology International, Inc (OATI) - webTADS

Reporting thresholds

- Bulk Electric System (BES) Elements
- Non-BES elements are voluntary

Applicable elements

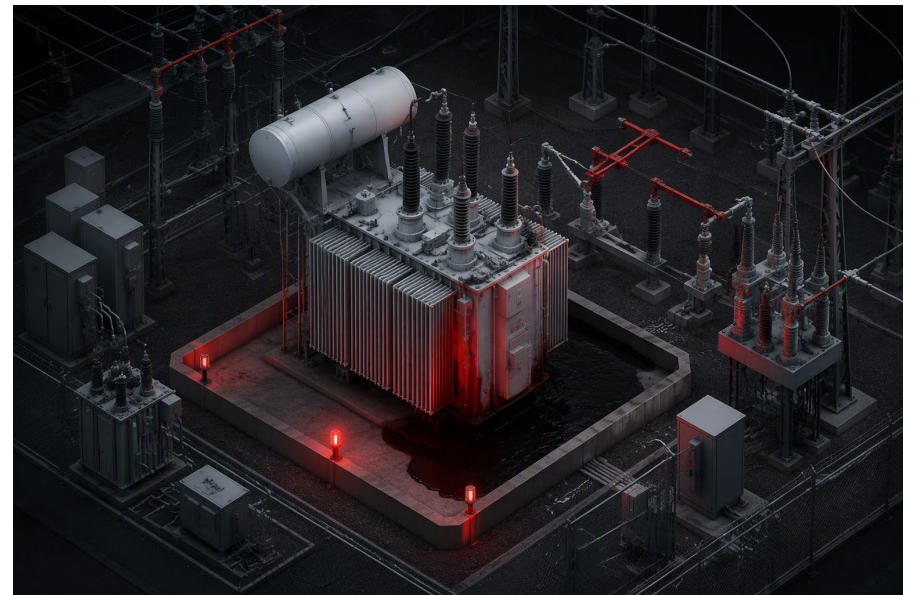
- AC Circuits (overhead and underground)
- Transformers with ≥ 100 kV secondary voltage
- AC/DC Back-to-Back Converters
- DC Circuits (overhead and underground)

Outage types

- Momentary (less than 1 minute)
- Sustained
- Does NOT include planned outages

0-199 kV elements only require Sustained outages

Reference: [TADS Data Reporting Instructions](#)



TADS - DATA SUBMISSION DEADLINES

When a deadline falls on a weekend or holiday, reporting will be extended through the following business day.

Reporting Deadline	Period of Operation to Report
February 15	Any updates for the prior year
May 15	Quarter 1: January - March 31
August 15	Quarter 2: April 1 - June 30
November 15	Quarter 3: July 1 - September 30
February 15	Quarter 4: October 1 - December 31

GADS: GENERATION AVAILABILITY DATA SYSTEM

Purpose

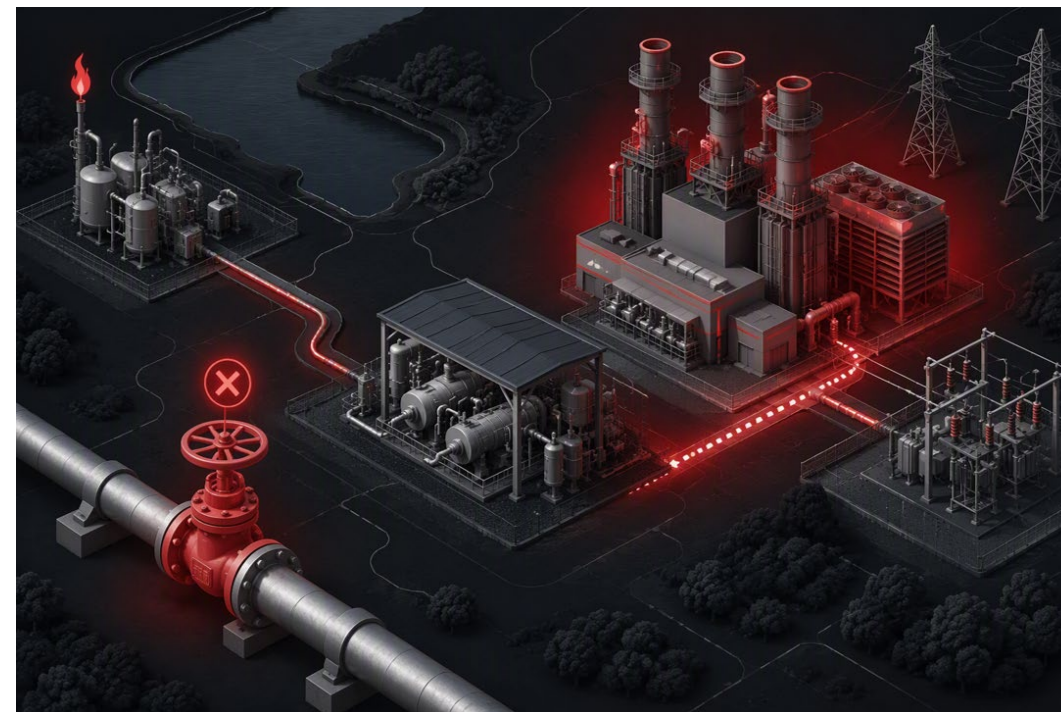
- Availability and outage performance of conventional units
- Supports plant, maintenance, and cause analysis

Submission tool

- Open Access Technology International, Inc. (OATI) - webE-GADS

Table III-1: Event Reporting Requirements vs Unit Type/Size Starting January 1, 2013

Units		Event Classifications			
Types	Size (MW)	Outage	Derates	Reserve Shutdown	Non-Curtailing
Fossil (Steam)	20+	Required	Required	Required	Voluntary
Nuclear	20+	Required	Required	Required	Voluntary
Hydro & Pumped Storage (with automatic data recording equipment)	20+	Required	Required	Required	Voluntary
Hydro & Pumped Storage (without automatic data recording equipment)	20+	Required	Required	Voluntary	Voluntary
Gas Turbines/Jet Engines	20+	Required	Required	Required	Voluntary
Combined Cycle/Co-generators	20+	Required	Required	Required	Voluntary
Internal Combustion/Reciprocating Engines	20+	Required	Required	Required	Voluntary
Fluidized Bed Combustion	20+	Required	Required	Required	Voluntary
Miscellaneous – including multi-boiler/multi-turbine, geothermal, other miscellaneous conventional generating units (such as variable fuel – biomass, landfill gases, etc.) used to generate electric power for the grid and similar in design and operation as the units shown above	20+	Required	Required	Required	Voluntary



CATEGORY 2 RESOURCES

- Inverter-based resources (IBRs): solar, wind, BESS, hybrid
- Addresses growing IBR reliability risk
- ≥ 20 MVA aggregate nameplate
- Connected at ≥ 60 kV
- Not registered as BES generation
- Subject to GO/GOP registration and NERC Reliability Standards



GADS WIND

Purpose

- Performance and availability for qualifying wind plants
- Improves visibility into wind operating patterns

Submission tool

- OATI - GADS Wind

Reporting thresholds

- ≥ 75 MW installed capacity, COD January 1, 2005 or later
- Category 2-only GOs: not required until May 2026



GADS SOLAR

Purpose

- Performance and availability for qualifying solar plants

Submission tool

- OATI - GADS Solar

Reporting thresholds

- ≥ 20 MW installed capacity, COD January 1, 2010 or later
- Category 2-only GOs: not required until May 2026

Event criteria

- 20 MW gap between total and available installed capacity

Reference: [GADS Solar Generation Data Reporting Instructions](#)



GADS - DATA SUBMISSION DEADLINES

Deadlines for Data Submission into GADS Conventional, GADS Wind, and GADS Solar

When a deadline falls on a weekend or holiday, reporting will be extended through the following business day.

Reporting Deadline*	Period of Operation to Report
February 15	Any updates for prior year
May 15	Quarter 1: January 1 - March 31
August 15	Quarter 2: April 1 - June 30
November 15	Quarter 3: July 1 - September 30
February 15	Quarter 4: October 1 - December 31

TADS & GADS LESSONS LEARNED

- Complete the checklist in the menu → signals completion
 - Notifies the Regional Coordinator
 - Click Modify/Save – entries are not saved otherwise
- Run validation before you finish
 - Flags potential data errors
 - Submission cannot complete with errors outstanding



Please share the information in this slide deck with the appropriate subject matter experts within your organization.

MIDAS: MISOPERATION INFORMATION & DATA SYSTEM

Purpose

- Protection system operations and misoperations
- Supports root cause analysis

Submission tool

- OATI

Reporting thresholds

- BES Elements

RF review process

- Quarterly peer review with the RF Protection Subcommittee

Resource: *MIDAS Data Reporting Instructions*



MIDAS - DATA SUBMISSION DEADLINES

When a deadline falls on a weekend or a holiday, reporting will be extended through the following business day.

Reporting Deadline	Period of Operation to Report
March 1	Any updates for the prior year
May 30	Quarter 1: January - March 31
August 29	Quarter 2: April 1 - June 30
November 29	Quarter 3: July 1 - September 30
March 1	Quarter 4: October 1 - December 31

Previous quarterly submissions are not required to be updated by the Reporting Deadline

MIDAS tracks Corrective Action Plans that are updated periodically until completion.

MIDAS LESSONS LEARNED

- Avoid accidental overwrites → duplicate work
 - Enter misoperations discretely or batch via spreadsheet
 - Do not overlap batch and discrete entries



Please share the information in this slide deck with the appropriate subject matter experts within your organization.

xADS DATA SUBMITTAL WORKFLOW

1

Entity submission

Data entered into NERC applications or OATI reporting portals.

2

Automated checks

System checks missing or inconsistent information.

3

Regional review

Regional staff support completion and data quality review.

4

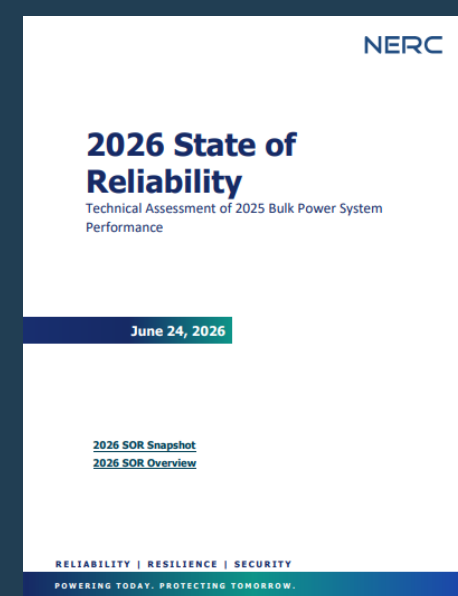
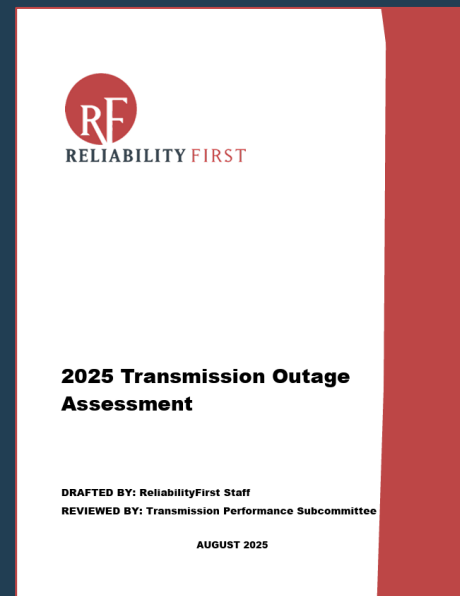
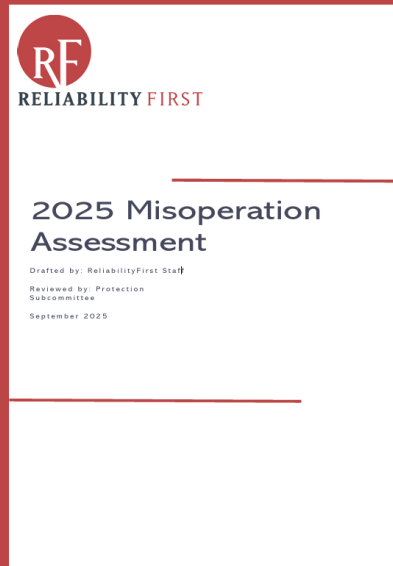
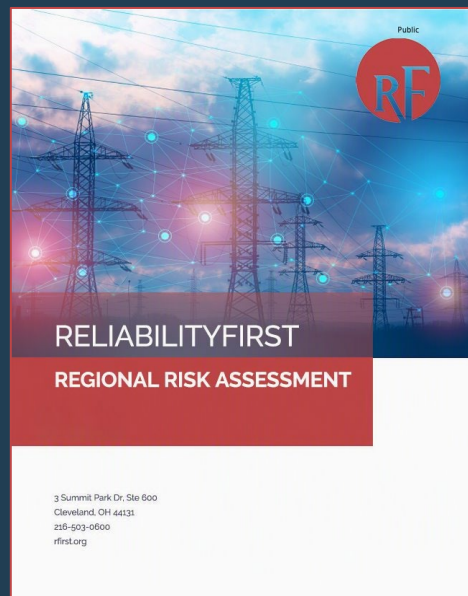
Metric development

NERC and RF aggregate, review, and develop metrics.

5

Reliability insight

Results inform dashboards, reports, outreach, and risk discussions.



RF DATA QUALITY

- Submitted results checked against internal dashboards
- Discrepancies flag calculation, mapping, or data issues
- Corrections improve dashboards, reports, and outreach
- Peer review used where applicable (e.g., MIDAS)



WHERE TO GO FOR HELP

NERC Program Contacts

TADS: tads@nerc.net

GADS Conventional: gads@nerc.net

GADS Wind: gadswind@nerc.net

GADS Solar: gadssolar@nerc.net

MIDAS: MIDAS@nerc.net

User Groups

TADS User Group

GADS User Group

System Protection & Control
Working Group

RF Protection Subcommittee

RF Contacts

TADS: John Idzior
john.idzior@rfirst.org

GADS: Tim Fryfogle
tim.fryfogle@rfirst.org

MIDAS: Thomas Teafatiller
thomas.teafatiller@rfirst.org

Data quality: Gerald Esteban
gerald.esteban@rfirst.org

Training

Available periodically from NERC or Regional Entity staff.
Please reach out if you are interested in having staff participate.

RF xADS BEST PRACTICES

- Contact RF when data submitter responsibility changes
- Avoid shift in data submitter responsibilities near submission deadlines
- Data submitters should be familiar with appropriate Data Reporting Instructions (DRIs)
- Contact RF for latest training opportunities

WHEN IN DOUBT: PLEASE REACH OUT

Reach out to appropriate RF contact with questions or concerns

RF should be your first contact prior to NERC

QUICK REFERENCES

NERC Sources

TADS: <https://www.nerc.com/programs/reliability-assessment--performance-analysis/transmission-availability-data-system>

GADS Conventional: <https://www.nerc.com/programs/reliability-assessment--performance-analysis/generating-availability-data-system/gads-conventional>

GADS Wind: <https://www.nerc.com/programs/reliability-assessment--performance-analysis/generating-availability-data-system/gads-wind>

GADS Solar: <https://www.nerc.com/programs/reliability-assessment--performance-analysis/generating-availability-data-system/gads-solar>

NERC State of Reliability Reports: <https://www.nerc.com/our-work/reports/state-of-reliability>

RF Sources

Section 1600 Data Requests: <https://www.rfirst.org/events-data-requests/section-1600-data-requests/>

Misoperation Assessment: <https://www.rfirst.org/wp-content/uploads/2025/10/2025-RF-Misoperation-Assessment.pdf>

Transmission Outage Assessment: <https://www.rfirst.org/wp-content/uploads/2025/10/2025-RF-Transmission-Outage-Assessment.pdf>



QUESTIONS & ANSWERS

Gerald Esteban

gerald.esteban@rfirst.org

BREAK TIME



SELF-REPORTS: EXPECTATIONS AND BEST PRACTICES

Marian Koussaie Toney

Counsel, Enforcement,
ReliabilityFirst



RELIABILITY FIRST

OVERVIEW

- SELF-REPORTS & MITIGATING ACTIVITIES
 - Audience
 - Lifecycle
 - Components
 - Forum

SELF-REPORTS: THE AUDIENCE

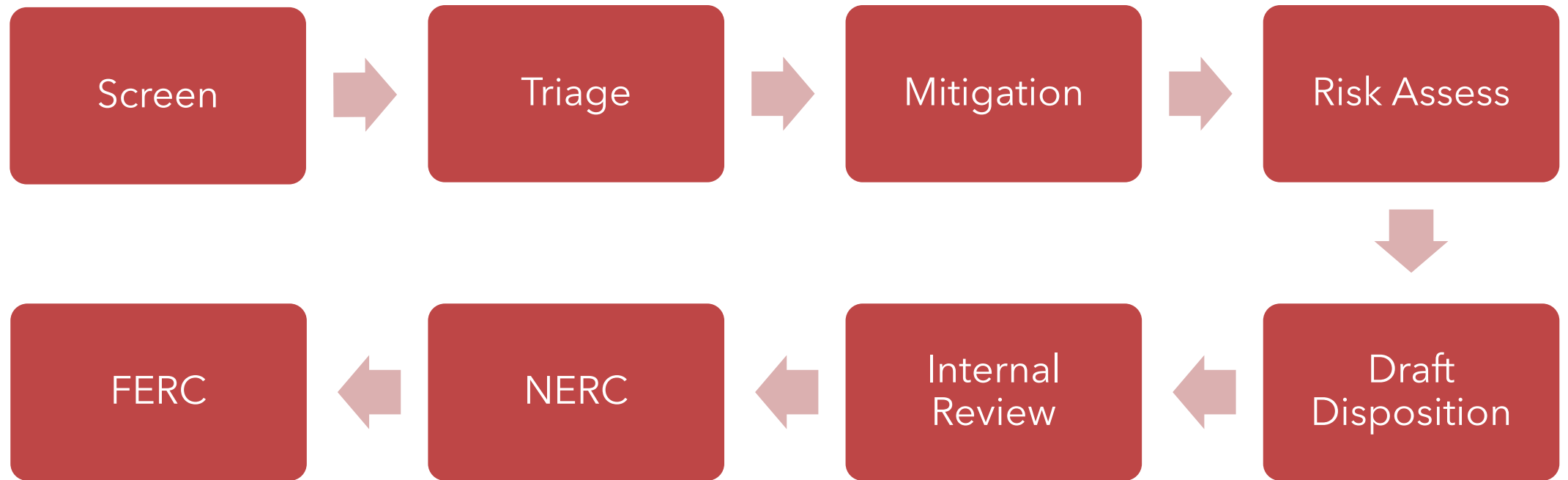
Enforcement Team

- Case Managers
- Composes disposition
- Acts as point of contact

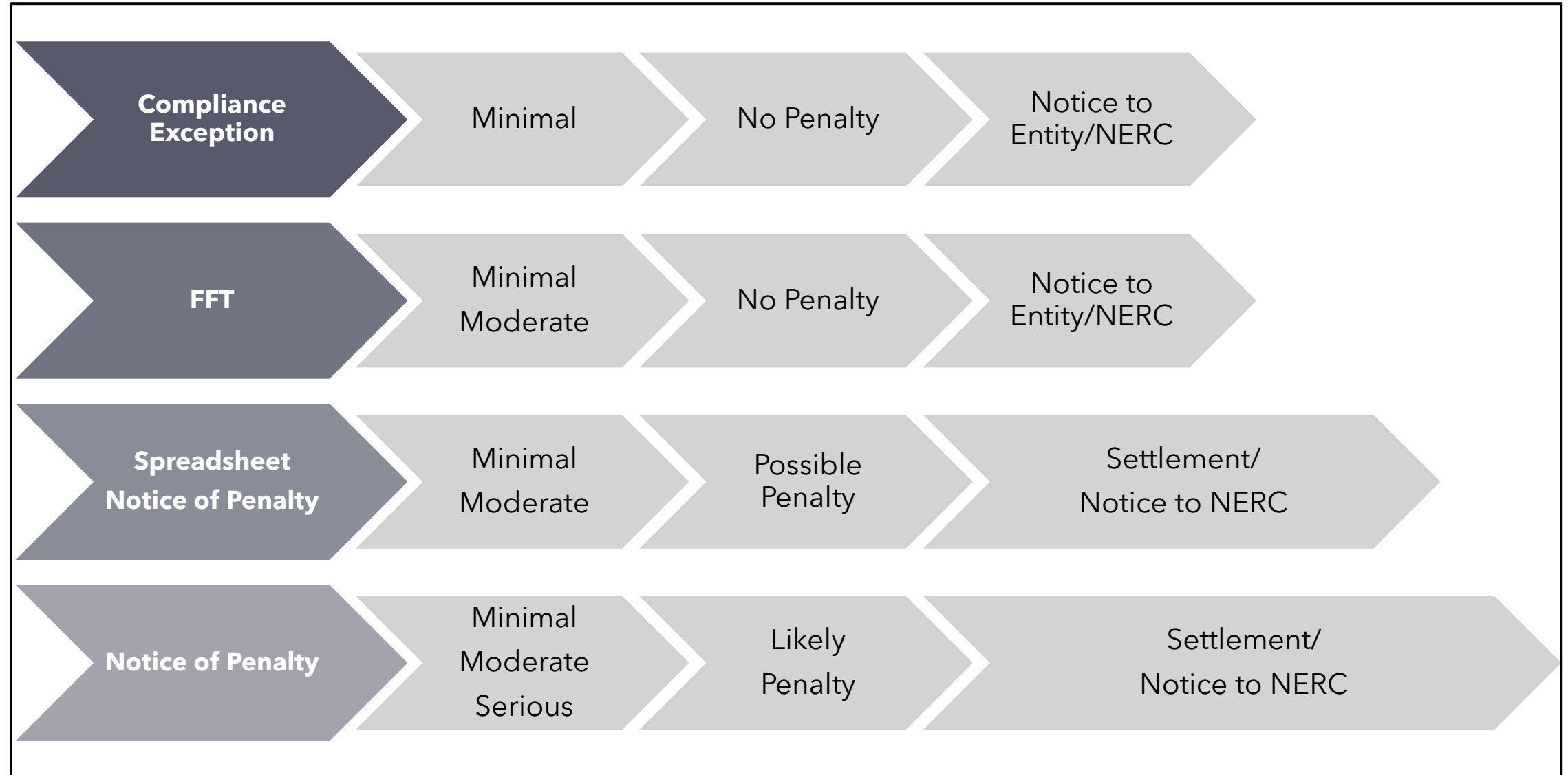
Risk Analysis and Mitigation Team

- Subject Matter Experts (SME)
- Identifies and assesses risk
- Reviews proposed mitigating activities

SELF-REPORTS: THE LIFECYCLE



DISPOSITIONS



SELF-REPORTS: THE COMPONENTS

- Discovery & Description
 - Explain when and how the noncompliance was initially identified
 - Describe what happened in each instance of noncompliance
- Start & End Dates
 - Provide when the noncompliance began and ended with context
- Root Cause
 - Identify why and how the noncompliance occurred
 - Include the primary cause and any contributing causes
- Extent of Condition Review
 - Provide detailed results – description, duration, root cause, etc.
- Risk Assessment
 - Minimal, moderate, or serious
 - Potential magnitude and probability of harm

DISCOVERY & DESCRIPTION

- Discovery
 - Internal control or periodic review?
 - Happenstance?
 - Internal discovery or third party?
- Description
 - Timelines
 - Avoid conclusory statements
 - Provide definitions as appropriate, including acronyms
 - Include pertinent details - what type of systems or assets impacted; how many
 - Does the noncompliance implicate other Reliability Standards and Requirements?

ROOT CAUSE

- Underlying factors and fundamental reasons for an occurrence
- All noncompliances must have an identified root cause
 - Consistent with facts
 - Assists in identification and implementation of effective mitigation efforts
- NERC Enforcement and Mitigation Resources
 - ERO Enterprise Enforcement Cause Code User Guide
 - Enforcement Cause Code Training Video

NERC

Who We Are ▾ Our Work ▾ Standards ▾ Programs ▾ Initiatives ▾ Applications

Home > Programs > Enforcement > Enforcement Resource...

Enforcement Resources

Enforcement Resources

Enforcement Dispositions

CMEP and ORCP and
Vegetation Reports

Resource Documents

	CEII Justification Document	Modified: 01/17/2021
	Consolidated Hearing Process	Modified: 09/02/2025
	Drafting Templates for CEs, FFTs, and SNOs	Modified: 07/24/2023
	ERO Enterprise Enforcement Cause Coding User Guide	Modified: 12/16/2024

Resource Videos

Enforcement Cause Code Training Video

Violations Themes - CIP Violations Webinar

RISK ASSESSMENT

- Minimal, moderate, or serious
- Focus on potential magnitude of harm and probability of harm
 - What could have happened and the likelihood of that harm occurring
 - Utilize the harm the applicable Standard and Requirement seek to prevent
 - Disclose actual harm
- FERC Directive (138 FERC ¶ 61, 193)
 - “A possible violation does not pose a minimal risk simply because there was no adverse impact to the [BPS]. . . . [R]isk assessment should not be based on a ‘no harm, no foul’ theory.”
 - “[R]isk assessment . . . must be based on facts, rather than assumptions.”
- Risk Factors
 - Does this factor increase or decrease the probability of harm?
 - Does this factor increase or decrease the potential magnitude of harm?

SELF-REPORTS: MITIGATION

- Remediate the noncompliance and prevent similar instances of noncompliance from occurring in the future
- Milestones
 - Remediating: terminates the noncompliance
 - Extent of Condition review: reviews similar systems and/or conditions to determine if the noncompliance extends beyond the initially identified instance
 - Controls: implementation of an internal preventative, detective, or validation control to prevent recurrence

SELF-REPORTS: THE FORUM

- “Align has positioned the core CMEP business processes of NERC and the Regional Entities on a single, secure platform that includes functionality related to **Enforcement and Mitigation**, Periodic Data Submittals, Technical Feasibility Exceptions, Self-Certifications, Audits and Spot Checks, Inherent Risk Assessment, and Compliance Oversight Plans.”
- [Align Enforcement and Mitigation User Guide](#)

The screenshot displays the NERC website interface. At the top, the NERC logo is on the left, and a navigation menu includes 'Who We Are', 'Our Work', 'Standards', 'Programs', 'Initiatives', 'Applications', and 'Events'. Below the navigation, a dark blue banner features the text 'Align and Secure Evidence Locker'. To the right of the banner, a sidebar lists 'ERO Portal' and 'Align and Secure Evidence Locker'. The main content area is titled 'Align and SEL Entity User Guides' and contains a table of user guides. The table has two rows: 'Registered Entity Align Attestations User Guide' (modified 07/12/2025) and 'Registered Entity Align Enforcement and Mitigation User Guide' (modified 06/27/2026). The second row is circled in red.

User Guide	Modified
Registered Entity Align Attestations User Guide	07/12/2025
Registered Entity Align Enforcement and Mitigation User Guide	06/27/2026

EXAMPLE: CIP-004-7 (CYBER SECURITY - PERSONNEL & TRAINING) R4

Discovery and Description

Entity personnel granted one individual unescorted physical access into a Physical Security Perimeter without authorization.

On July 1, 2026, during a routine quarterly access review, entity personnel discovered unauthorized physical access for one employee within the entity's Physical Access Control System. On June 23, 2026, entity personnel granted the employee unauthorized physical access rights to High Impact Physical Security Perimeter A without authorization instead of granting unescorted physical access to High Impact Perimeter B for which the employee had authorization. Upon discovery, on July 1, 2026, entity personnel immediately revoked the employee's authorized unescorted physical access rights to High Impact Physical Security Perimeter A.

EXAMPLE: CIP-004-7 R4

Root Cause

The root cause of this noncompliance was human error. Entity personnel inadvertently selected Physical Security Perimeter A instead of Physical Security Perimeter B.

The root cause of this noncompliance was internal process deficiencies. The documented access management process checklist lacked validation tasks to compare authorization records to provisioned accesses both before and after provisioning.

EXAMPLE: CIP-004-7 R4

Risk Assessment

This noncompliance posed minimal risk.

This noncompliance posed a minimal risk to the Bulk Power System for the following reasons. First, the employee was unaware she had unescorted physical access to Physical Security Perimeter A, minimizing the likelihood the employee would utilize the unauthorized access. Second, the noncompliance was limited to one employee for approximately one week and the entity successfully identified the noncompliance through execution of an internal control.

ADDITIONAL RESOURCES

- [NERC Enforcement and Mitigation Resources](#)

NERC

[Who We Are](#) ▾[Our Work](#) ▾[Standards](#) ▾[Programs](#) ▾[Initiatives](#) ▾[Applications](#) ▾[Events](#)

[Home](#) > [Programs](#) > [Enforcement](#) > [Enforcement Resource...](#)

Enforcement Resources

[Enforcement Resources](#)

[Enforcement Dispositions](#)

[CMEP and ORCP and Vegetation Reports](#)

Resource Documents

	CEI Justification Document	Modified: 01/17/2021
	Consolidated Hearing Process	Modified: 09/02/2025
	Drafting Templates for CEs, FFTs, and SNOPs	Modified: 07/24/2023
	ERO Enterprise Enforcement Cause Coding User Guide	Modified: 12/16/2024
	Penalty Inflation Adjustment Notice	Modified: 07/02/2026
	Registered Entity Self-Report and Mitigation Plan User Guide	Modified: 10/21/2025



QUESTIONS & ANSWERS

BREAK TIME



EVENT REPORTING: BEST PRACTICES AND EXPECTATIONS OF EFFECTIVE EVENT DATA

Tony Purgar

Senior Manager, Operational
Analysis & Awareness,
ReliabilityFirst



RELIABILITY FIRST

WHAT YOU WILL LEAVE WITH



Understand expectations for **timely event submittals**



Know what makes a **complete and review-ready submission**



Learn the structure of a **strong brief report**



Recognize **common errors** and how to avoid them

WHY REPORTING QUALITY MATTERS

- Supports reliable event analysis and awareness (OAA visibility)
- Reduces review cycles and clarification delays
- Improves accuracy of event records and trends
- Strengthens internal and external reporting confidence

EVENT REPORTING LIFECYCLE

Detect / identify event

Gather initial data

Submit event data (EOP-004 or OE-417 form)

Prepare (interim) brief report and submit

Review and refine

Finalize, **submit** (final) brief report, and retain

WHO DOES WHAT



OPERATIONS

- Facts
- Records / Logs
- System actions
- Timing



EVENT ANALYSIS

- Structure
- Validation
- Synthesis



REVIEWERS

- Completeness
- Clarity
- Procedural alignment

TIMELY SUBMITTALS

- Meet required deadlines (*per ERO EA Process: Appendix A - Targeted Timeframes*)
- Submit **initial information early**
- Clearly identify:
 - Known facts
 - Unknowns
 - Pending updates
- Use consistent timestamps

PRACTICAL TIMELINESS STANDARD



Initial submittal = **early + structured**



Updates = **incremental additions & improvements**



Unknowns are:

Explicitly stated

Not guessed



Deadlines are met without sacrificing clarity

WHAT MUST BE INCLUDED

Event description
and summary

Date/time
(consistent
format)

Location/affected
elements

Chronology

Impacts

Actions taken

Cause status

Supporting
evidence

FOUR QUALITY PILLARS



- **Complete** - all required elements
- **Accurate** - aligns with records, logs, data
- **Consistent** - naming, timestamps
- **Useful** - understandable without follow-up

COMMON SUBMITTAL GAPS

Missing or inconsistent timestamps

Vague descriptions ("issue occurred")

No clear timeline / incomplete Sequence of Events

Unsupported cause statements

Missing information / attachments

No restoration details

MOVING FROM DATA TO STORY



DATA = INPUTS



BRIEF REPORT =
STRUCTURED
NARRATIVE



GOAL: MAKE THE EVENT
UNDERSTANDABLE
QUICKLY

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Appendix C Brief Report Template

Registered entities are requested to use the Brief Report template as a guideline for submitting event information to their applicable RE and NERC in accordance with **Appendix A** (Target Time Frames for Completion of Brief Reports, Event Analysis Reports, and Lessons Learned). The template may also be used for less significant events.

APPENDIX C BRIEF REPORT TEMPLATE

Concise Checklist

Purpose



Use as a guideline to submit event information to the applicable RE and NERC, aligned to Appendix A target timeframes. May also be used for less significant events.

1 Report Basics

- Reported event title, including event date and location/entity details
- Initial submittal date and any subsequent update date
- Interim or final report status

2 Entity & Contact

- Entity name and NCR number
- Entity contact information and contact person
- Local event date, time, and time zone

3 Event Identification

- Brief description: what happened, when, and where
- Proposed event categorization, such as 1a or 2b
- Leave Items 6–12 blank if not applicable to the event

4 Operational Impacts

- Generation MW loss and frequency information
- Load/customers impacted and forced outages
- Emergency actions and inverter momentary cessation/tripping

5 Event Analysis

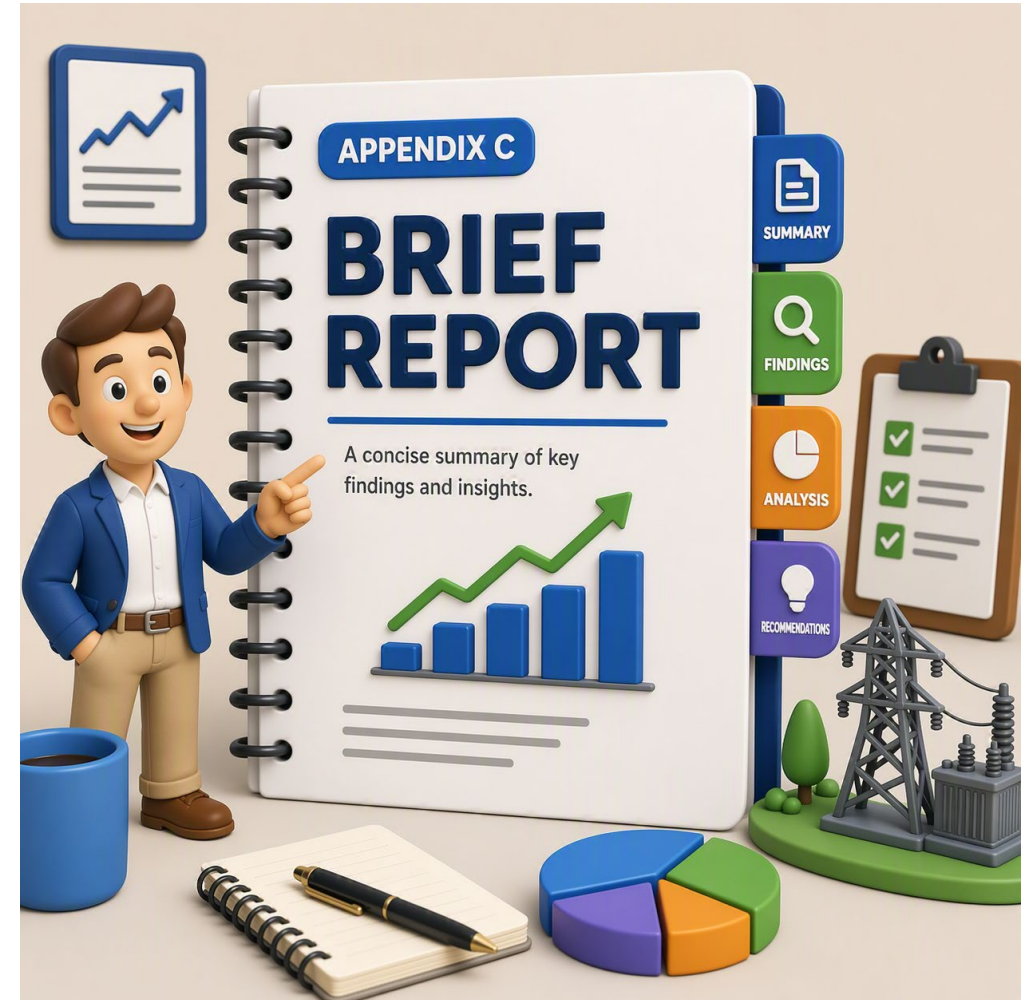
- Chronological sequence of events
- Contributing causes and protection system misoperations
- GADS, DADS, TADS, or misoperation reports to be submitted

6 Narrative & Follow-Up

- Detailed narrative with what, when, how, where, impact, and assumptions
- One-line diagram explanation and monitoring/control event significance
- Corrective actions to prevent similar events

STANDARD REPORT STRUCTURE

1. Event summary
2. Pre-event conditions
3. Chronology
4. Impacts
5. Cause discussion
6. Actions taken
7. Current status
8. Evidence



CLEAR EVENT SUMMARY



Be thorough, concise, and meaningful



What happened, when, where



Why it mattered

BUILDING A CLEAR TIMELINE



Time-ordered
sequence



Exact timestamps



Key system changes
and operator actions

CAUSE: BE PRECISE AND QUALIFIED



Confirmed vs.
Suspected vs.
Unknown



Supported by
evidence



Avoid speculation

ACTIONS TAKEN

Operator actions

System restoration

Notifications

Conclusions

Follow-up actions

SUPPORTING EVIDENCE



Records / Logs



SCADA / Alarms data



Relay targets



Screenshots



One-line diagrams

WEAK VS STRONG REPORTING

Weak

- Vague description
- No timestamps
- No clear actions
- Assumed cause

Strong

- Specific time-based sequence
- Clear actions and results
- Cause properly qualified
- Evidence referenced

WEAK VS STRONG BRIEF REPORT

Element	Weak Brief Report	Strong Brief Report
Event Description	"The relay operated unexpectedly and caused an outage."	"At 14:32 EDT, Line 322 was removed from service following an unexpected operation of Protection Relay R301 at Substation A, resulting in the loss of approximately 125 MW of load for 18 minutes."
Chronology	"The relay tripped and operators responded."	"14:32 – Relay R322 operated. 14:33 – Control center received alarm. 14:35 – Operators verified system conditions. 14:41 – Field personnel dispatched. 14:50 – Relay settings reviewed. 14:50–14:59 – Equipment restored. 15:00 – Line returned to service."
Cause Description	"The cause is under investigation."	"Initial review indicates a failed current transformer secondary connection produced erroneous relay inputs, resulting in an unnecessary protection operation. Final root cause investigation remains in progress."
Impact Statement	"There was some impact to customers."	"Approximately 12,400 customers experienced interruptions ranging from 5–18 minutes. No BES reliability impacts or personnel injuries were identified."
Actions Taken	"Operations restored the equipment."	"Operators isolated the affected protection scheme, verified system stability, coordinated with field personnel, and restored Line 322 after confirming relay inputs were stable."
Supporting Evidence	None provided.	"Relay event records, SCADA alarm logs, operator logs, and field inspection findings support the preliminary cause determination."
Corrective Actions	"Corrective actions will be determined later."	"Current actions include replacement of the failed connection, verification testing of associated CT circuits, and review of preventive maintenance procedures for similar installations."
Clarity	Uses vague language such as "issue," "problem," or "equipment malfunction."	Uses specific equipment names, locations, timestamps, impacts, and actions.
Completeness	Missing key facts, timelines, impacts, and evidence.	Provides a complete picture of what happened, why it happened, what was affected, and what is being done.
Value to Reviewers	Generates follow-up questions and delays analysis.	Allows reviewers to quickly understand the event and assess significance.

EXAMPLE NARRATIVE COMPARISON

Weak Brief Report

A relay problem caused an outage. Operations responded and restored the equipment. The cause is still being investigated. Corrective actions will be determined later.

Why It Is Weak

- No event timing
- No equipment identification
- No impact information
- No cause details
- No evidence cited
- No description of operator actions
- Requires multiple follow-up questions

Strong Brief Report

At 14:32 EDT on June 12, 2026, Protection Relay R322 at Substation A unexpectedly operated and removed Line 322 from service. The operation resulted in the interruption of approximately 125 MW of load affecting roughly 12,400 customers. Operators immediately reviewed SCADA indications, confirmed system stability, and dispatched field personnel. Preliminary investigation determined a failed current transformer secondary connection provided erroneous inputs to the relay, causing the unnecessary operation. The line was restored to service at 15:00 EDT after verification of stable relay inputs. Supporting evidence includes relay event records, alarm logs, operator logs, and field inspection results. Corrective actions include replacement of the failed connection, testing of associated CT circuits, and review of maintenance practices for similar installations.

Why It Is Strong

- Clearly explains **what happened**
- Provides a logical **timeline**
- Quantifies the **impact**
- Identifies the **preliminary cause**
- Documents **actions taken**
- References **supporting evidence**
- Describes **corrective actions**
- Enables efficient event analysis

TAKEAWAYS

Brief Report expectations for practical event analysis

1

Right-size the analysis

Match the depth of the review to the event's severity, impact, and risk. Patterns or recurring issues deserve a deeper dive.

2

Focus on cause and prevention

Identify what happened, why it happened, and what corrective actions will reduce the chance of recurrence.

3

Share what others can learn

When an event offers broader value, consider an ERO Enterprise Lessons Learned so others can benefit before the next event.



Right-sized • Cause-focused • Shared

Bottom line: The goal is not paperwork — it is learning, prevention, and reliability improvement.

QUICK SELF-CHECK BEFORE SUBMISSION

Checklist

- Is the event clearly described?
- Are all key times included and in the proper order?
- Does the chronology align with logs and records?
- Are equipment names and locations correct?
- Are facts separated from assumptions?
- Is the cause statement properly qualified?
- Are operator actions and restoration actions described?
- Are attachments included and referenced?
- Are open questions or pending validations identified?
- Is any required limited-disclosure handling applied?

Common Weaknesses

- "Cause appears to be..." with no support
- Missing post-event status
- No explanation of significance
- Inconsistent equipment names between text and attachments
- Long narrative with no chronology
- Overuse of acronyms with no explanation
- Copying logs directly without analysis

WHAT GOOD LOOKS LIKE



Be timely



Be complete



Be
chronological



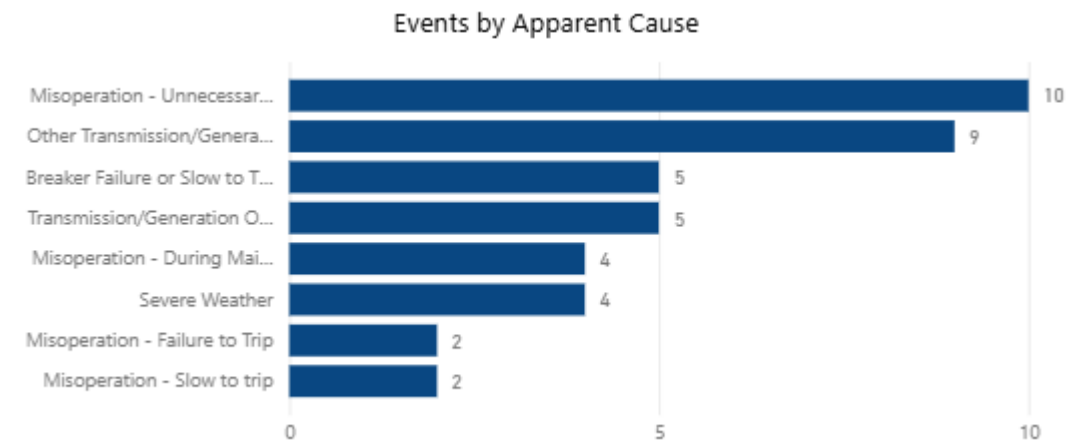
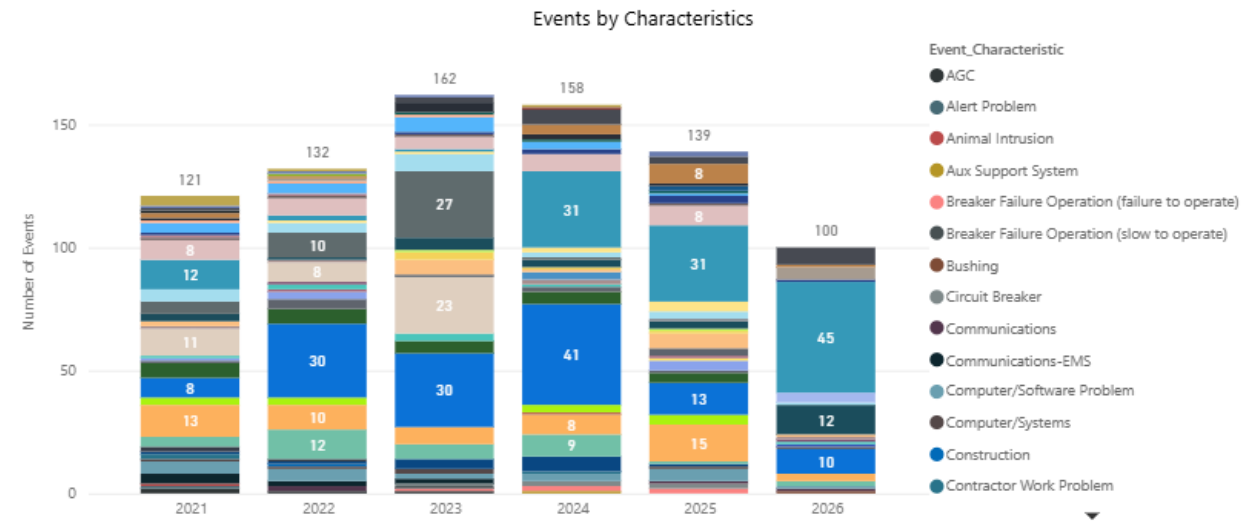
Be fact-based



Be evidence-
supported

REPORTING AN EVENT TO RF

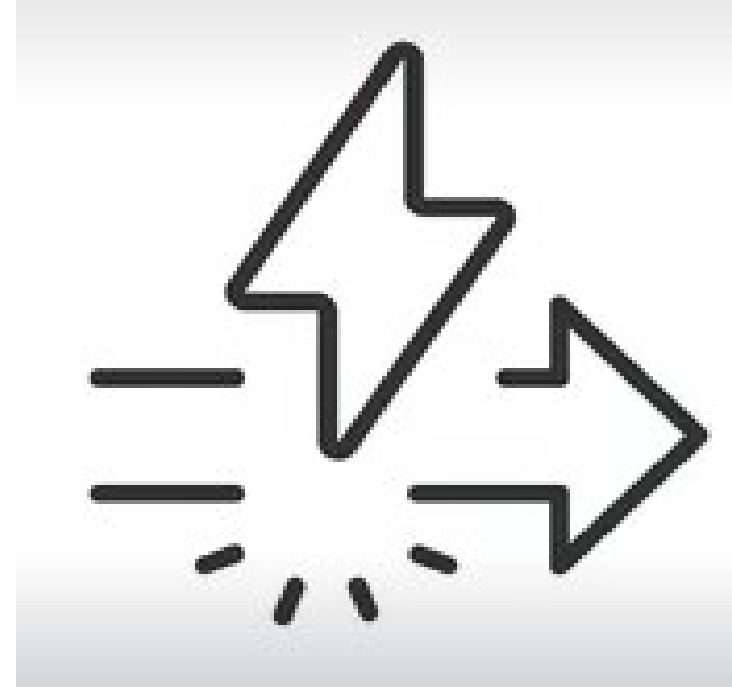
- Reporting is highly encouraged and critical for overall industry awareness, learning, and sharing.
- Why is Event Reporting Important?
 - Trends
 - Helps to create RF trends
 - Supports ERO trending for
 - Event Characteristics
 - Apparent Causes
 - Identifying vendor issues
 - Awareness, Learning, and Sharing
 - Why is the data important?
 - How do we use the data?
 - What does the data tell us ("What story")?
 - MIDAS Reporting
 - Lessons Learned



REPORTING AN EVENT TO RF



DRONES



MISOPERATIONS

- Please report these types of events and any other system disturbances you encounter.
- If you're not sure, please reach out to OAA contacts to discuss it and determine next steps.

REPORTING AN EVENT TO RF



Disturbance mailbox

disturbance@rfirst.org



Unable to email -

Business hours - 216.503.0600

After hours - 216.503.0646

- Instructions are available at: [ReliabilityFirst Public Website under Data Requests > Event Reporting](#)
- The after hours number is routed to one of the OAA team members that will be available to discuss your event information with you.

RF OPERATIONAL ANALYSIS & AWARENESS CONTACTS

- Tony Purgar - Sr. Manager
 - tony.purgar@rfirst.org
- Dwayne Fewless - Principal Analyst
 - dwayne.fewless@rfirst.org
- Kellen Phillips - Principal Analyst
 - Kellen.phillips@rfirst.org
- Darren Schue - Senior Analyst
 - darren.schue@rfirst.org
- Danielle Daugherty - Analyst
 - danielle.daugherty@rfirst.org

EVENT ANALYSIS RESOURCES

- NERC EA Program
 - ERO Event Analysis Process Documents
 - Reference Materials
 - Event Analysis Lessons Learned
 - Event Analysis Webinars
- RF EA Guidance Page:
 - <https://www.rfirst.org/events-data-requests/event-reporting/>

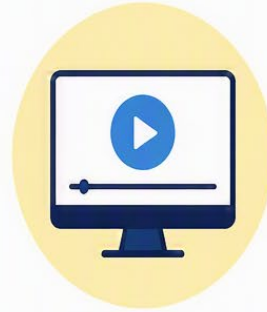
TRAINING AIDS



JOB AIDS



PRESENTATIONS



VIDEOS



CHECKLISTS



ACTIVITIES

WHAT GOOD LOOKS LIKE - CHECKLIST

Event data submittal checklist

- ☐ Submitted on time
- ☐ Required fields complete
- ☐ Accurate timestamps
- ☐ Event clearly described
- ☐ Chronology included
- ☐ Impacts identified
- ☐ Actions taken documented
- ☐ Cause status appropriately stated
- ☐ Evidence attached
- ☐ Open items identified

WHAT GOOD LOOKS LIKE - CHECKLIST

Brief Report checklist

- ☐ Clear summary
- ☐ Good pre-event context
- ☐ Clean chronology
- ☐ Specific impacts
- ☐ Cause discussion is supportable
- ☐ Actions and restoration documented
- ☐ Evidence cited
- ☐ Plain, concise writing

WHAT GOOD LOOKS LIKE - STRONG BRIEF REPORT TEST

A strong brief should answer these questions:

- ✓ What happened?
- ✓ When did it happen?
- ✓ What equipment or facilities were involved?
- ✓ What was the operational or reliability impact?
- ✓ What is the known or suspected cause?
- ✓ What actions were taken immediately?
- ✓ What evidence supports the conclusions?
- ✓ What corrective actions are planned or completed?
- ✓ Could a reviewer understand the event without asking follow-up questions?

Training takeaway: A weak report tells reviewers that an event occurred. A strong report tells reviewers **what happened, why it happened, what was affected, and what is being done about it.** The goal is to minimize assumptions and maximize understanding.

QUESTIONS & DISCUSSION

- Where do you struggle most today?
- What delays submissions?
- What would improve first-pass quality?



WRAP UP

- Please share this material internally within your organization, where applicable.
- If you have questions about any material covered, please reach out to the Operational Analysis & Awareness (OAA) team directly, or through our [Contact Us](#) page.





CONTACT INFORMATION

Tony Purgar

tony.purgar@rfirst.org

Thank You for Attending

Please complete the Survey in Linktree

