




TEXAS RE

CIP-008-6 R2 Incident Response

**Jason Georgoulis
CIP Cyber and Physical Security
Analyst II**

November 21, 2025


2025 ERO CMEP IP: Incident Response



2025 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

October 2024

RELIABILITY | RESILIENCE | SECURITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Incident Response

Incident response continues to be a significant risk to the BPS. As attacks such as ransomware increase, industry stakeholders must continue to test and mature our response coordination capabilities throughout the ERO. “Our goal is for the National Cyber Incident Response Plan to provide an agile, actionable framework that can be actively used by every organization involved in cyber incident response to ensure coherent coordination that matches the pace of our adversaries,” said Eric Goldstein, Executive Assistant Director for Cybersecurity. “The success of this effort depends on the involvement of our partners – our output will only be as good as our input. Through our shared efforts, we will build a new NCRIP that helps our nation, and our allies more effectively respond to and recover from cyber incidents in a manner that reduces harm to every possible victim.”¹⁷

Through the Joint Cyber Defense Collaborative ([JCDC](#)), CISA will work to ensure that the updated NCIRP addresses significant changes in policy and cyber operations since the initial NCIRP was released, including:

- Establishment of CISA and ONCD;
- Maturation of private sector incident response and coordination capabilities;
- Increased international collaboration around cyber incident response and coordination;
- Shifts in the threat environment, including the ongoing ransomware threats and advances in adversary capabilities; and
- New authorities, policies, and coordination mechanisms.¹⁸



Risk Element Areas of Focus: Incident Response

Table 5: Incident Response			
Rationale	Standard	Req	Entities for Attention
Mitigate risks to the reliable operation of the BES as the result of a Cyber Security Incident.	CIP-008-6	R1, R2, R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
Ensuring continuous improvement of incident response plans after a rise in low impact events.	CIP-003-8	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner



Cyber Security Incident

- A malicious act or suspicious event that:
 - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
 - Disrupts or attempts to disrupt the operation of a BES Cyber System

Reportable Cyber Security Incident

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



CIP-008-6 R2 Requirement and Parts

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].

R2 Part 2.1 – Test each Cyber Security Incident response plan at least once every 15 calendar months:

- By responding to an actual Reportable Cyber Security Incident
- With a paper drill or tabletop exercise of a Reportable Cyber Security Incident
- With an operational exercise of a Reportable Cyber Security Incident

R2 Part 2.2 – Use the Cyber Security Incident Response Plan under R1 when:

- Responding to a Reportable Cyber Security Incident
- Responding to a Cyber Security Incident that attempted to compromise an applicable system
- Performing an exercise of a Reportable Cyber Security Incident
- Document deviations from the plan

R2 Part 2.3 – Retain Records related to Reportable Cyber Security Incidents and attempts to compromise



Resources: NIST Incident Framework and GridEx



NIST Special Publication 800
NIST SP 800-61r3

Incident Response Recommendations and Considerations for Cybersecurity Risk Management

A CSF 2.0 Community Profile

Alex Nelson
Sanjay Rekhi
Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-61r3>



GridEx VIII New Scenario Options

If the electric grid were ever targeted by a coordinated cyber and physical attack and your organization plays a role in response or recovery, then GridEx VIII is for you! **GridEx is for...**

- | | |
|--|---|
| Electricity asset owners and operators | State/provincial, local, and tribal governments |
| Critical infrastructure partners | Law enforcement agencies |
| Emergency management agencies | And more! |

Held on **November 18-19, 2025**, GridEx VIII will be even easier to tailor to your organization's unique needs and resources. The E-ISAC is excited to introduce three different options for participation in GridEx VIII:

STANDARD SCENARIO	GRIDEx IN A BOX	TABLETOP SCENARIO
<p>This is the default GridEx experience. This scenario will be as big as ever, with both cyber and physical injects that prompt immediate reactions and cause severe damage to the bulk-electric system.</p> <p>Our subject matter experts will make sure the Standard Scenario is feasible and has enough detail for new and experienced Planners to successfully implement GridEx across their organizations while engaging with external partners.</p> <p>The GridEx VIII Standard Scenario is designed as a two-day full-scale exercise with the option to transition into a recovery-focused tabletop on the afternoon of the second day. This option is best for large or experienced planning teams that want to go big.</p>	<p>This year, GridEx will include two abbreviated scenarios specially designed for smaller planning teams that still want to engage in a real-time exercise with fewer resources.</p> <p>One abbreviated scenario will focus on physical injects while the other will focus on cyber injects.</p> <p>Planners can combine the abbreviated scenarios or mix and match specific injects and create a customized scenario, but the abbreviated scenarios will remain a smaller version of GridEx than the Standard Scenario.</p> <p>Both "GridEx in a Box" Scenarios will align with the Standard Scenario and make it possible to coordinate with regional partners that use the Standard Scenario.</p>	<p>For the first time ever, the E-ISAC is offering the option to participate in GridEx VIII as a discussion-based tabletop exercise.</p> <p>This scenario is designed for Planners who simply don't have the bandwidth to develop a full-scale or live exercise but want to participate in GridEx VIII and gather lessons learned from the complex scenario we have developed.</p> <p>This scenario is designed to be "plug and play," taking the form of a pre-populated slide deck that includes scenario updates, injects, and discussion questions.</p> <p>After minimal customization of slide content, Planners can host a tabletop version of GridEx VIII with little assistance beyond the provided Facilitator Guide.</p>

[Join the E-ISAC and register for GridEx here!](#)

For more information, visit the [GridEx Website](#) or email GridEx@eisac.com.

Learn More
@NERC_Official X
Find us on LinkedIn in
GridEx@eisac.com



The background of the slide features a blurred Texas state flag on the left and a target with several darts on the right. The darts are clustered in the center of the target, suggesting a focus on a specific point.

Questions?



TEXAS RE

Ensuring electric reliability for Texans