

# Grid Exercise Working Group Scope

## Statement of Need

NERC's Grid Security Exercise (GridEx) is an opportunity for utilities to demonstrate how they would respond to and recover from simulated coordinated cyber and physical security threats and incidents, strengthen their crisis communications relationships, and provide input for lessons learned. The exercise is conducted every two years. GridEx aims to:

- Exercise incident response plans
- Expand local and regional response
- Engage interdependent sectors
- Increase supply chain participation
- Improve communication
- Gather lessons learned
- Engage senior leadership

## Background

The first NERC GridEx was conducted on November 16-17, 2011. NERC GridEx 2011 engaged 75 participants from industry and government across North America in a sector-wide grid security exercise. GridEx 2011 had a strong cyber focus and in the after-action activities identified key areas as lessons learned for NERC and the industry.

- Entities possess effective cyber incident response plans.
- Effective horizontal communications exist within the industry, however information sharing to NERC was insufficient.
- NERC's E-ISAC teams were effective; however the alert process could be expedited with the Federal Energy Regulatory Commission (FERC).
- Utilities took appropriate steps to secure the Bulk Electric System (BES) throughout the exercise; further focus is needed on a coordinated attack.

As a follow up to GridEx 2011, NERC decided to continue GridEx as a biennial exercise, conducted in November of odd years. The focus is North America wide, with coordinated cyber and physical attack scenarios designed to validate and exercise industrywide maturation and improvements from previous GridEx exercises, and to explore the ramifications of new policy and technological developments, all in a safe space to promote learning.

## GEWG Objectives/Duties

- Refresh the Grid Exercise Working Group (GEWG) at the completion of each exercise cycle, for the upcoming exercise.
- Create exercise scenarios and details to drive the accomplishment of exercise objectives.
- Advise and assist the E-ISAC, on behalf of the Critical Infrastructure Protection Committee (CIPC) and industry, on the technical, operational, and exercise aspects of the GridEx scenario details.
- Serve as ambassadors and champions to increase participation among registered entities, and encourage organizations to coordinate participation with their cross-sector and state/local/tribal/territorial government partner agencies.
- Ensure the GridEx scenario and supporting technologies allow for industry response plans to be exercised in a manner that identifies physical and cyber security gaps in plans, resources, and capabilities.
- Ensure the GridEx scenario and supporting technologies allow NERC, the E-ISAC, and government partner command, control and communication plans to be exercised in a manner that identifies gaps in authorities, resources, and capabilities.
- Provide input and review for after-action reviews and reports, and identifying and communicating lessons learned.
- Other duties as assigned.

## **Members and Structure**

The GEWG will generally follow the organizational structure and voting rights of the CIPC with the following addition:

- Non-voting members who are industry subject matter experts, for the work at hand.
- An E-ISAC staff member will be assigned as the non-voting GEWG Coordinator.
- The GEWG chair and vice chair will be appointed by the CIPC EC for one two-year term.

## **Reporting**

The GEWG will administratively report to the CIPC, and report operationally to the E-ISAC for exercise-specific activities and deliverables.

## **GEWG Deliverables and Work Schedule**

- GridEx takes place every other November, in odd years; GEWG activity is continuous, with the shift from prior exercise to future exercise occurring in the spring of even years.
- Four to six in-person meetings per year, with three or four adjacent to and collocated with CIPC meetings. Conference calls and web-based meetings for targeted sub-groups will vary with the exercise cycle, with as frequent as monthly calls in the 14 months to six months out window from exercise execution.

- Deliverables include liaison to the CIPC and to industry at large, and specific work products (creation, input, and review) as requested by the E-ISAC to include but not limited to exercise goals, high level scenario narrative, detailed scenario injects and supporting material, supporting exercise logistics (e.g., simulated reporting mechanisms and communications channels replicating real-world capabilities unable to be directly used for exercise purposes), lessons learned, and after action reviews.

## References and Resources

- GridEx Public Information -  
<https://www.nerc.com/pa/ci/cipoutreach/pages/gridex.aspx>