GridEx IV Summary

Scott Heffentrager

Sr. Director Physical Security, BCP and Facility Services

MC Webinar

November 27, 2017

2017 GridEx IV

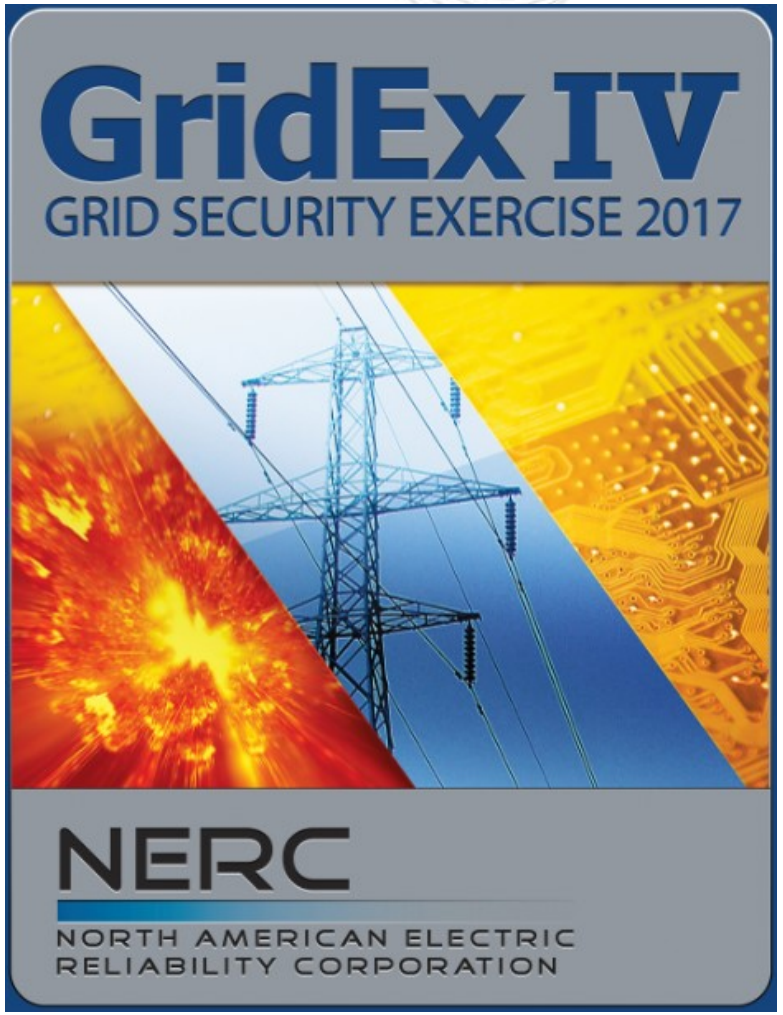
What: NERC Sponsored, North American grid resilience exercise conducted every 2 years.

When: November 15 – 16, 2017.

Purpose: Strengthen Industry capabilities to respond to and recover from severe physical, cyber and operational events affecting the bulk power system.

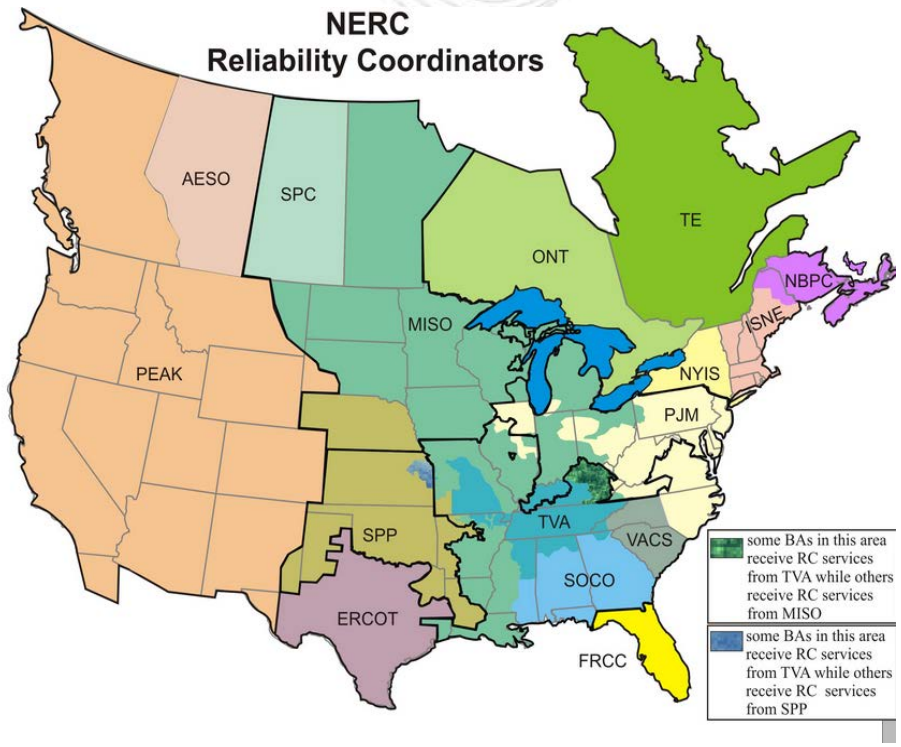
Who: NERC-registered entities, law enforcement, local government, suppliers. Voluntary participation

How: Simulated cyber and physical attacks that degrade bulk power system operations.



ISO & RTO Participation in 2017 GridEx IV

Code	Name
ERCOT	ERCOT ISO
FRCC	Florida Reliability Coordinating Council
HQT	HydroQuebec TransEnergie
ISNE	ISO New England Inc.
MISO	Midcontinent Independent System Operator
NBPC	New Brunswick Power Corporation
NYIS	New York Independent System Operator
ONT	Ontario - Independent Electricity System Operator
PJM	PJM Interconnection
SPC	SaskPower
SOCO	Southern Company Services, Inc.
SPP	Southwest Power Pool
TVA	Tennessee Valley Authority
VACS	VACAR-South
PEAK	Peak Reliability
AESO	Alberta Electric System Operator



Over 4500 participants

2017 GridEx IV

GridEx IV is a biennial unclassified public/private exercise designed to simulate a cyber/physical attack on electric and other critical infrastructures across North America to improve security, resilience and reliability.

15 Transmission Operators

- American Electric Power (AEP)
- Atlantic City Electric (ACE)
- Baltimore Gas & Electric (BGE)
- Commonwealth Edison (ComEd)
- Dayton Power & Light (DPL)
- DelMarva Power
- Dominion
- Duquesne
- East Kentucky Power (EKPC)
- First Energy
- PECO
- Pepco
- PPL
- PSE&G
- RECO

3 Generation Operators

- East Kentucky Power (EKPC)
- PSE&G
- American Electric Power (AEP)

Key Observers

- Department of Homeland Security (DHS)
- FEMA
- U.S. Army Cyber Command
- Defense Advanced Research Projects Agency (DARPA)
- Utility Commissions (PA, NJ, MD)

Key Objectives

- Exercise Incident response plans
- Exercise Crisis Communications
- Exercise Incident Response Capabilities with PJM members, adjacent Reliability Coordinators, and external agencies
- Engage Interdependent Sectors
- Engage Senior Leadership

PJM Participants

- Corporate Incident Response Team (IRT)
- Operational Emergency Response Team (OERT)
- Cyber Security Response Team (CSIRT)
- Physical Security Incident Response Team (PSIRT)
- Crisis Communication Response Team (CCRT)
- System Operations Training
- Business Continuity Planning
- State and Member Training
- State and Government Policy
- Enterprise Information Security
- Corporate Applications
- Applied Solutions

Exercise Results

Due to the decisive actions taken by PJM and TO/GO operators, the PJM footprint stood resilient against operational, physical and cyber injects.

Exercised

- Loss of extra high voltage assets
- Realistic communications
- Incorporated lessons learned from 2016 Annual Security Exercise
- Promoted awareness of cyber events with dispatchers
- Provided 13 Continuing Education Hours for dispatchers
- Provided CIP compliance evidence

Next Steps

- Conduct Lessons Learned with PJM internal / external participants
- Compile and Report Lessons Learned to NERC
- Review Executive Tabletop Summary for Lessons Learned
- NERC Report Issued out in February
- Incorporate Lessons Learned from GridEx IV into Annual Security Exercise
- Incorporate Lessons Learned updates into emergency procedures
- Conduct Annual Security Exercise in 2018