NARUC Winter
Policy Summit

Critical Infrastructure Committee

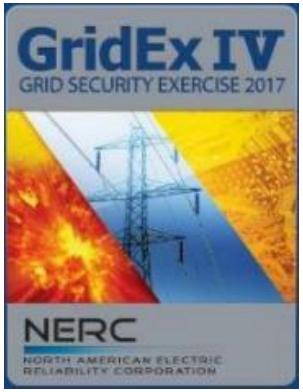
GridEx IV: Lessons Learned

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

GridEx IV Update


GridEx IV
GRID SECURITY EXERCISE 2017
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Bill Lawrence
Director of the Electricity Information Sharing and Analysis Center
NARUC Critical Infrastructure Committee meeting
February 12, 2018

RESILIENCY | RELIABILITY | SECURITY

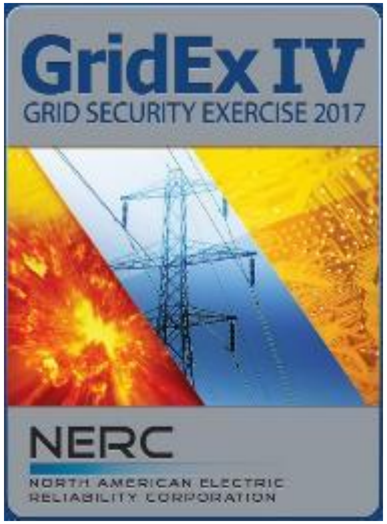
Agenda

- Mission
- Objectives
- Components
- Exercise Components
- Stakeholders
- Participation
- Information sharing
- Preliminary findings – Distributed Play
- Executive tabletop overview and discussion items
- Way forward

Mission statement

GridEx is an unclassified public/private exercise
designed to simulate a coordinated cyber/physical attack
with operational impacts
on electric and other critical infrastructures
across North America
to improve security, resiliency, and reliability

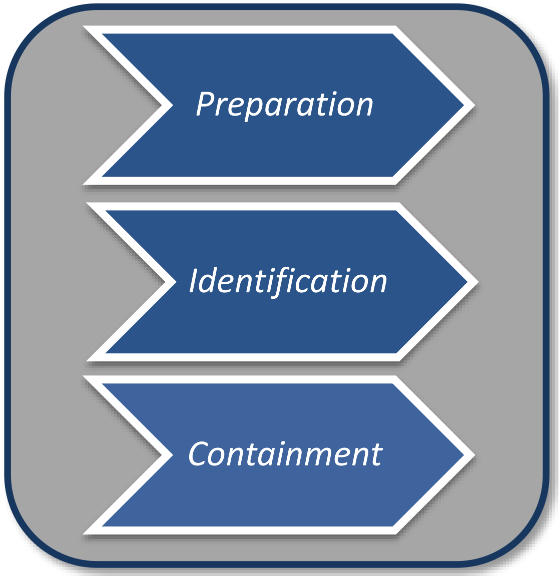
GridEx Objectives



- Exercise incident response plans
- Expand local and regional response
- Engage critical interdependencies
- Improve communication
- Gather lessons learned
- Engage senior leadership

Exercise Components

Move 0 Pre-Exercise



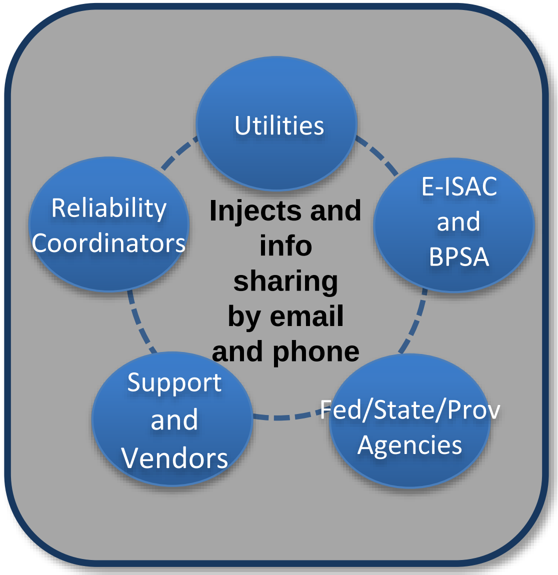
Preparation

Identification

Containment

Operators may participate in Cyber Intrusion detection activities

Distributed Play (2 days)



Utilities

E-ISAC and BPSA

Fed/State/Prov Agencies

Support and Vendors

Reliability Coordinators

Injects and info sharing by email and phone

Players across the stakeholder landscape will participate from their local geographies

Executive Tabletop (1/2 day)

Facilitated discussion engages senior decision makers in reviewing distributed play and exploring policy triggers

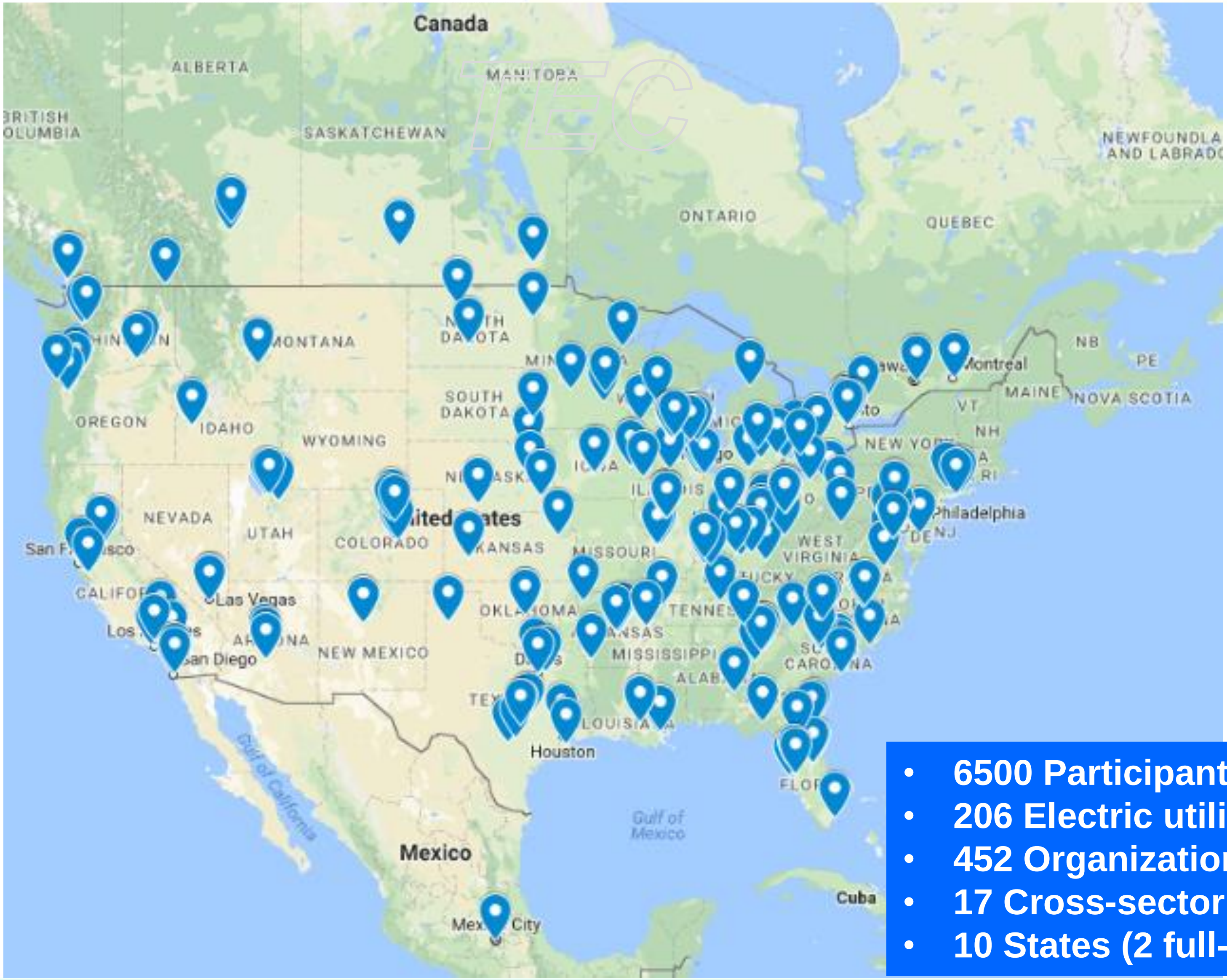
Diverse Stakeholders

Organization	Recommendation	Explanation
Reliability Coordinator	• Active, with multiple entities as Active in the control area	• RC may guide the inject customization in the control area, or entities may customize injects themselves (see slides 9 and 10) • RCs will be involved with utilities in submitting lessons learned per objective #3
Regional Entities, Trade Associations	• Active	• These organizations may have crisis coordination roles and may work with RCs and utilities to determine if an Active role is required. **No compliance-related participation will be permitted.**
US Department of Energy / Natural Resources Canada	• Active	• US DOE, Infrastructure Security and Energy Restoration • Natural Resources Canada, Energy Security Division
Local / State / Provincial Law Enforcement and Emergency Response	• Active, as invited by the utility	• Utilities may invite these organizations to register as Active and participate at the utility location or remotely
Federal Agencies' Headquarters and regional offices (FBI/DHS/RCMP/Public Safety Canada)	• Active (or white cell by ExCon) • Utilities may also invite regional Active participation	• NERC is in coordination with US and Canadian Federal organizations for: ○ Active HQ-level participation (Canadian Cyber Incident Response Centre, CyWatch, NCCIC/ICS-CERT, etc.), and, ○ Active regional participation (e.g. FBI Field Offices, State and Major Urban Area Fusion Centers, etc.)

Diverse Stakeholders (con’t)

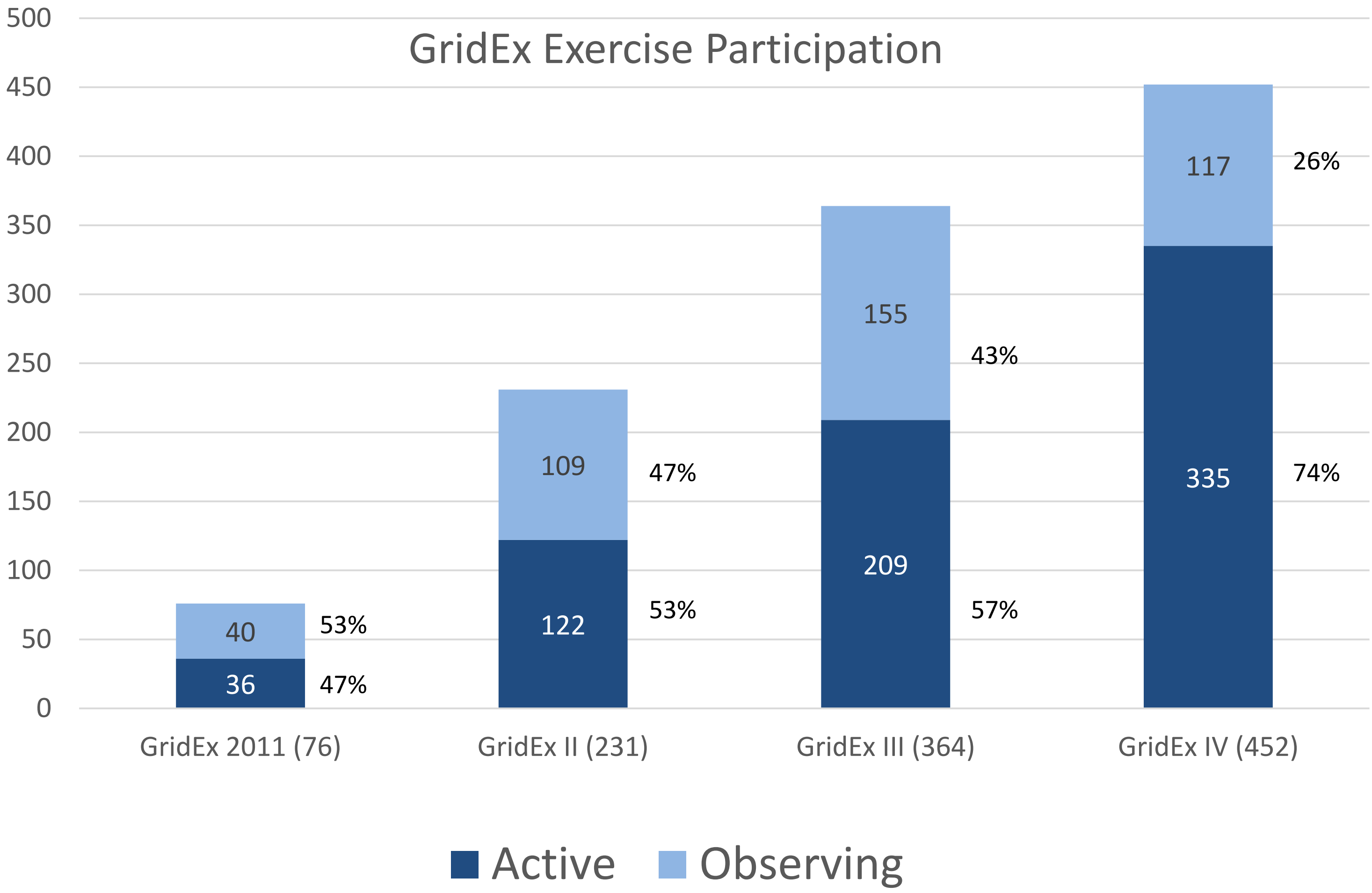
Organization	Recommendation	Explanation
Cross-sector ISACs / ISAOs and other organizations	• Observing	• E-ISAC will invite specific interdependent sectors (e.g. Nuclear, Down-stream Natural Gas, Communications, Financial, Water, etc.) • Cross-sector organizations may be invited by electric utilities to participate as Active or Observing
Support Vendors / Consultants	• Active (**only** by invitation from participating utility or by E-ISAC)	• Utilities are encouraged to involve 3rd party support in planning and during the exercise ○ Organizations will be listed in Exercise Directory as “Acme Utility – Somebody’s Internet Co.,” using their own organizational email addresses
Public Utility Commissions / Public Service Commissions	• Observing	• Crisis response roles vary by organization; some may coordinate with RCs to determine if an Active role is required. **No regulatory-related participation.**
Defense and Intelligence	• Observing	• Utilities may invite Active or Observing regional participation (e.g. National Guard, etc.) • E-ISAC will share information with key stakeholders (e.g. Canadian Security Intelligence Service, National Security Agency, etc.)
Federally Funded Research and Development Centers / Academia	• Observing	• E-ISAC will invite

Participation

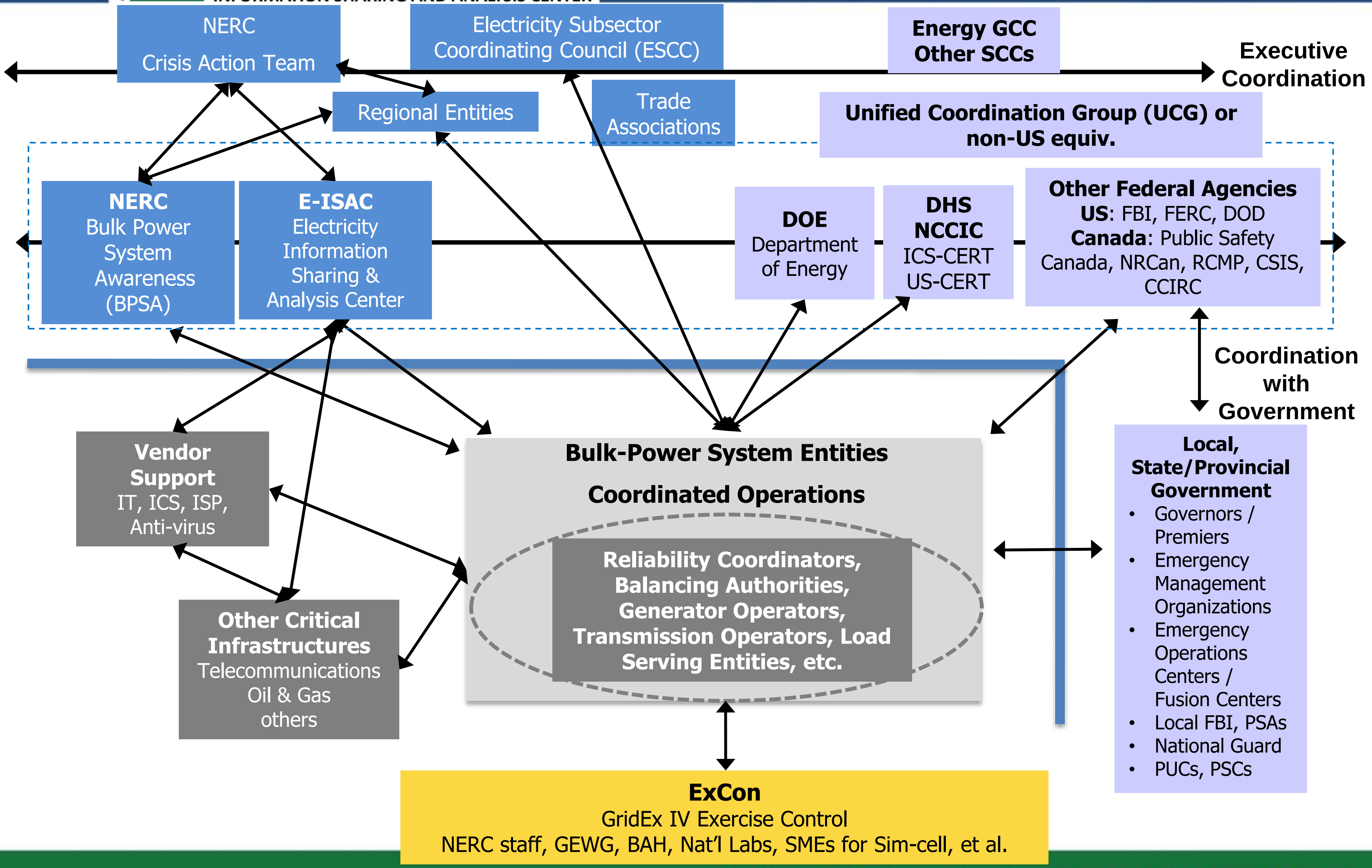


- 6500 Participants
- 206 Electric utilities
- 452 Organizations
- 17 Cross-sector partners
- 10 States (2 full-scale)

Active and Observing



GridEx IV Communications



NERC

Crisis Action Team

Electricity Subsector Coordinating Council (ESCC)

Energy GCC Other SCCs

Executive Coordination

Regional Entities

Trade Associations

Unified Coordination Group (UCG) or non-US equiv.

NERC Bulk Power System Awareness (BPSA)

E-ISAC Electricity Information Sharing & Analysis Center

DOE Department of Energy

DHS NCCIC ICS-CERT US-CERT

Other Federal Agencies
US: FBI, FERC, DOD
Canada: Public Safety Canada, NRCan, RCMP, CSIS, CCIRC

Coordination with Government

Vendor Support IT, ICS, ISP, Anti-virus

Bulk-Power System Entities

Coordinated Operations

Reliability Coordinators, Balancing Authorities, Generator Operators, Transmission Operators, Load Serving Entities, etc.

Other Critical Infrastructures Telecommunications Oil & Gas others

Local, State/Provincial Government

- Governors / Premiers
- Emergency Management Organizations
- Emergency Operations Centers / Fusion Centers
- Local FBI, PSAs
- National Guard
- PUCs, PSCs

ExCon
GridEx IV Exercise Control
NERC staff, GEWG, BAH, Nat'l Labs, SMEs for Sim-cell, et al.

E-ISAC
A DIVISION OF NERC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Information Sharing with the E-ISAC

- Cyber shares
  - 204
- Physical Security shares
  - 364
- OE-417s submitted
  - 244
- EOP-004s submitted
  - 132
- Utilities participating in Cyber Mutual Assistance
  - 43

YOUR COMPUTER AND FILES ARE ENCRYPTED

YOU MUST PAY 0.2 BITCOINS TO UNLOCK YOUR COMPUTER

YOUR FILES HAVE BEEN MOVED TO A HIDDEN PARTITION AND CRYPTED. ESSENTIAL PROGRAMS IN YOUR COMPUTER HAVE BEEN LOCKED AND YOUR COMPUTER WILL NOT FUNCTION PROPERLY.

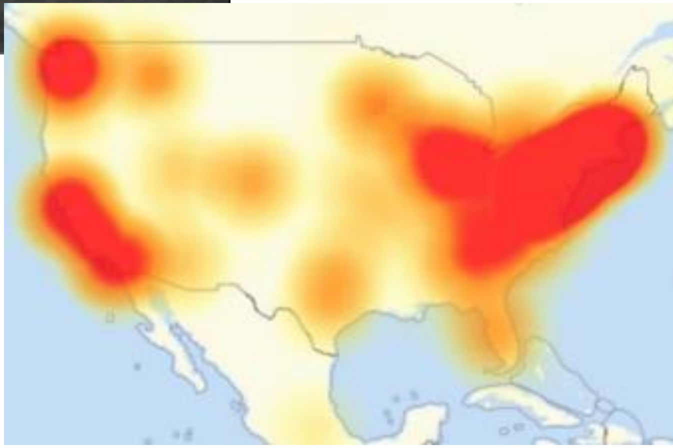
ONCE YOUR BITCOIN PAYMENT IS RECEIVED YOUR COMPUTER AND FILES WILL BE RETURNED TO NORMAL INSTANTLY.

YOUR BITCOIN PAYMENT ADDRESS IS:

18m8Q5L1T3LhZavz5bqIIu2aFXgU5T9fu4

PAY 0.2 BTC

[illegible]



Preliminary Findings – GridEx IV Distributed Play

- Where's the Cavalry?
  - Relationship building with partners (e.g. cross-sector, law enforcement, emergency managers, etc.)
  - What is the State/Federal Government's role during a Grid Emergency?
- E-ISAC Portal improvements
- Greater cross-sector participation
- Public Affairs and Corporate Communications vs. Incorrect or Misleading information
- Communication resiliency (e.g. WPS, GETS, HF Radio, etc.)
- Electric Utility – RC emergency communications
- Cyber Mutual Assistance
- On-keyboard cyber training
- Active Lead Planners

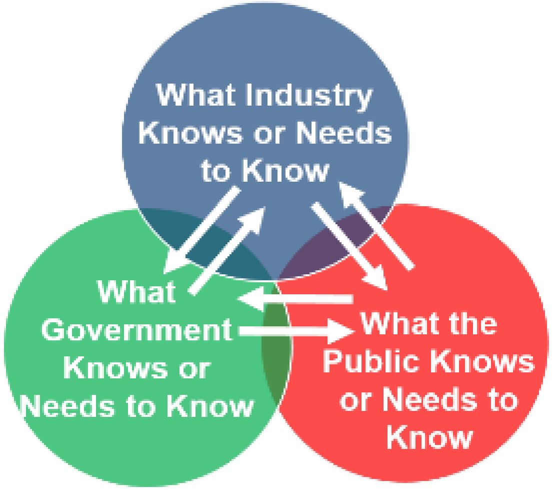
Executive Tabletop Overview

- Five-hour Executive Tabletop held on November 16, 2017, the second day of the large-scale GridEx IV security and emergency response exercise. Parallel, separate tabletops were held in Canada and Australia
- Objective:

Engage senior industry and government leadership in a robust discussion of the policy issues, decisions, and actions needed to respond to protect and restore the reliable operation of the grid

Executive Tabletop Themes

Messaging

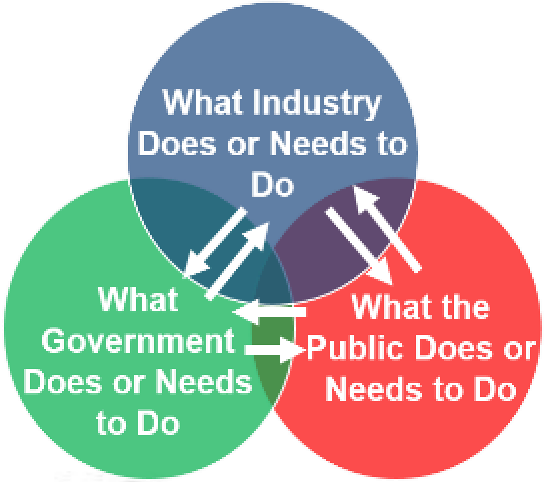


What Industry Knows or Needs to Know

What Government Knows or Needs to Know

What the Public Knows or Needs to Know

Effort

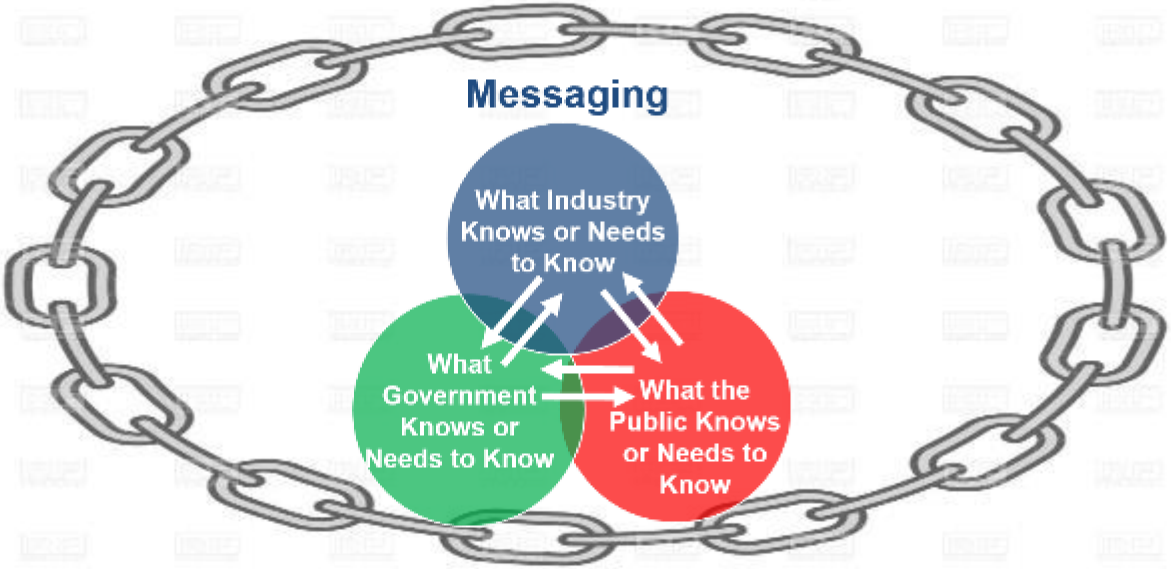


What Industry Does or Needs to Do

What Government Does or Needs to Do

What the Public Does or Needs to Do

Extraordinary Measures



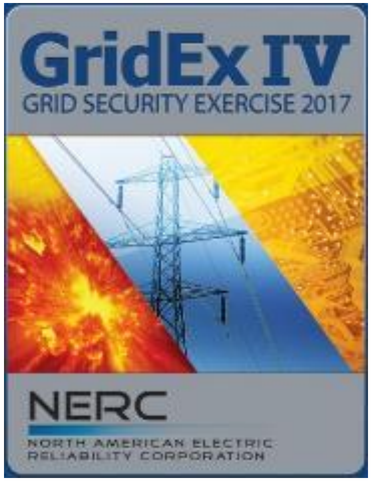
Messaging

What Industry Knows or Needs to Know

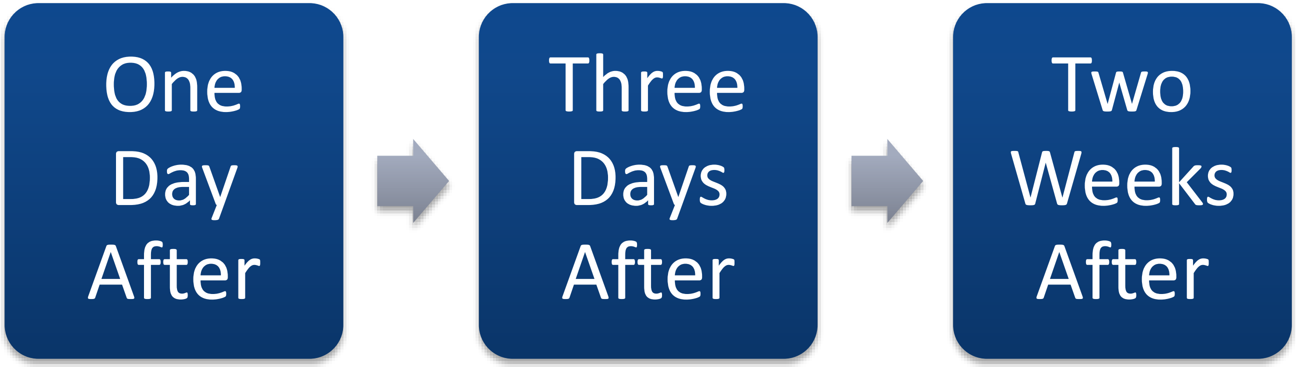
What Government Knows or Needs to Know

What the Public Knows or Needs to Know

Phased Scenario Discussion


GridEx IV
GRID SECURITY EXERCISE 2017
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attacks Begin



One Day After → Three Days After → Two Weeks After

For each phase after attacks begin:

- Participants role-play actions and the decisions needed to respond to the situation, restore power, and secure the grid
- Identify any gaps

Tabletop Discussion

- Situation assessment and initial response by industry and government
- Communications between utilities and with local, state, and federal government
  - Utility liaison with state emergency operations centers
- Immediate government priority: **Stop the Attacks**
  - Utility liaison with National Guard
- Grid Emergency Operations
  - Utilities have the authority to implement emergency actions (e.g., shed load) to maintain grid operation
  - Utilities coordinate with local and state government to identify high-priority customers

Tabletop Discussion

- Share sensitive information
  - Need to distribute information quickly and declassify if necessary
- Decide national-level priorities
  - When resources are limited, balance local, state, and national interests
- Critical infrastructure interdependencies
  - Communications, financial services, natural gas, and critical manufacturing sectors as “life-line” sectors
- Utility finances to fund recovery and restoration

Way Forward

- GridEx IV Reports will be complete by end of March, 2018
- GridEx V Initial Planning Meeting will be held November 2018

Questions and Answers

Critical Infrastructure Committee