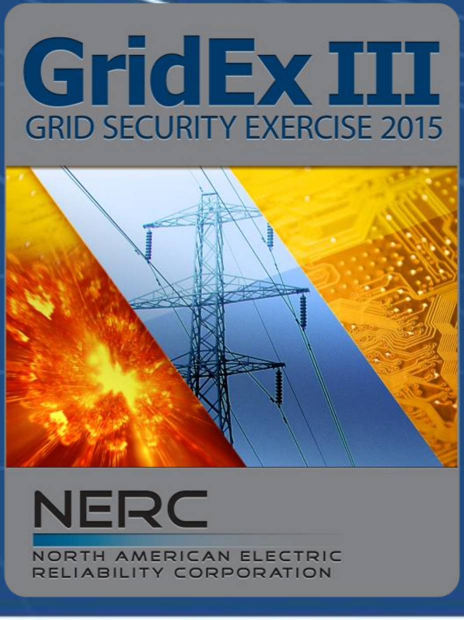
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

GridEx 2015 – Nov 18/19

ERCOT Reliability & Operations Subcommittee (ROS) Meeting

July 9, 2015

Presented by: Jim Brenton, Regional Security Coordinator, ERCOT



RELIABILITY | ACCOUNTABILITY

The GridEx Program

What: North American-wide exercise conducted every 2 years

Purpose: Strengthen the industry's capability to respond to and recover from **simulated** severe security events affecting the bulk power system

Who: NERC-registered entities and others as determined by individual entities (e.g., law enforcement, local government, suppliers). Voluntary, not mandatory.

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

GridEx III Objectives

1. Exercise crisis response and recovery
2. Improve communication
3. Identify lessons learned
4. Engage senior leadership*

*New Objective for GridEx III related to enhanced Electric Sector Coordinating Council.

GridEx II Review--History

- NERC conducted GridEx II in November 2013.
- GridEx II brought together NERC, industry, and government agencies, as well as participants from Canada and Mexico
- GridEx II was the largest, most comprehensive effort, to address security of the Bulk Power System by the industry to date

- The GridEx Program serves as an example of the commitment of industry and government partnership to continuously improve cyber and physical security of the North American Bulk Power System*

* Note: Bulk Power Systems include Generation and Transmission system assets but does not reach into Distribution system or Customer level assets..

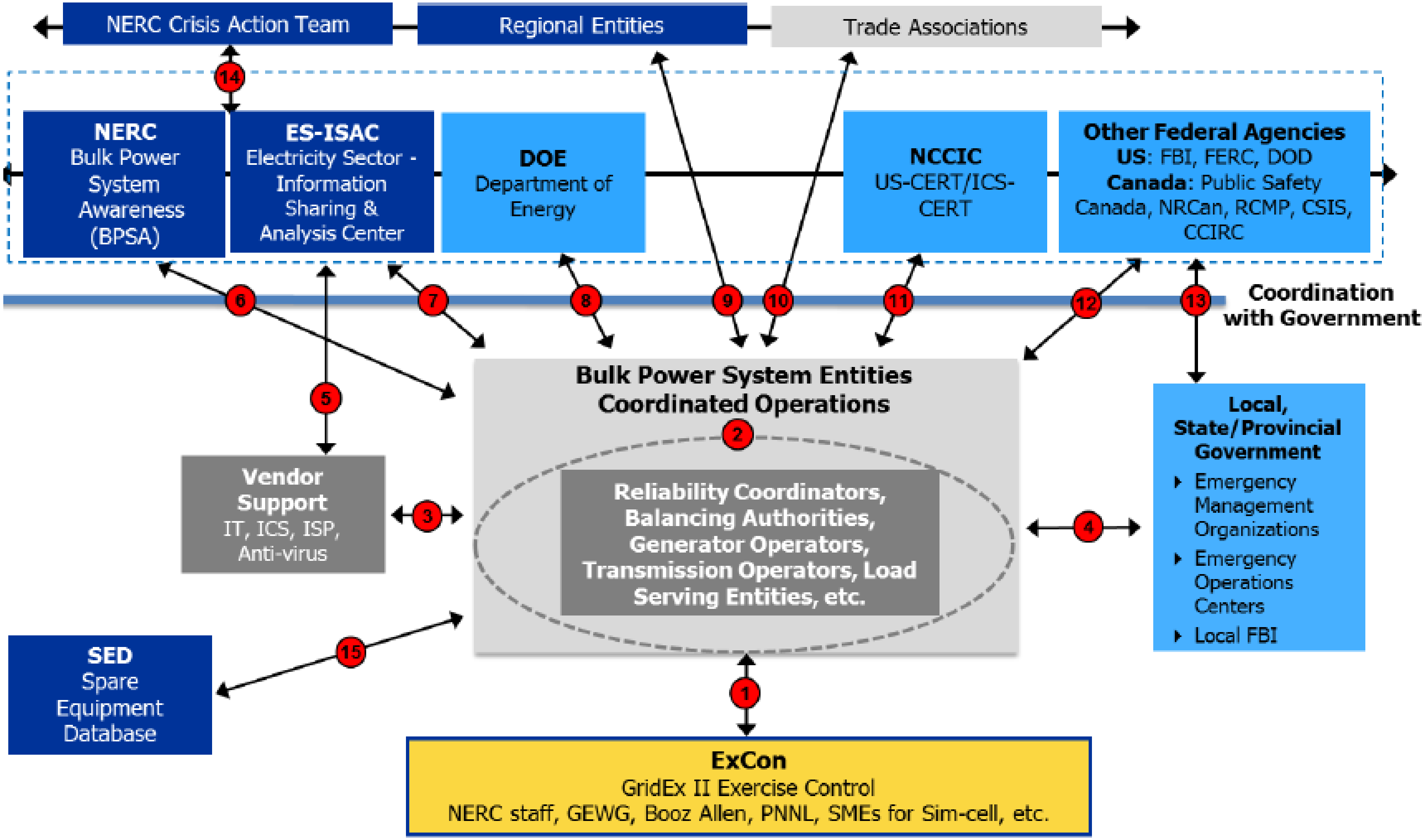
GridEx-II Distributed Play Lessons Learned

- **GridEx-II Distributed Play Lessons Learned Identified Need for:**
  - Enhanced Information Sharing—Horizontal and Vertical
  - Enhanced Coordination of Grid Security Events
  - Improved Handling of Simultaneous Attacks (Cyber, Physical & Coordinated Events to include Active Shooters)
  - Improved Incident Response Procedures and Processes
  - Improved Situational Awareness Content Sharing between Industry and Government
  - Improved 2015 GridEx Program with more **Regional Focus**

GridEx III Challenges for ERCOT

- Improve vertical communication between utilities and ERCOT, and ERCOT with the ES-ISAC and NERC BPSA
- Distribute Exercise Control functions from NERC to ERCOT RC
- Increase level of exercise participation by State, Regional and Local Government groups
- Obtain support of ERCOT ROS Subcommittee for increased ERCOT Utility participation—Transmission and Generation

Communications in GridEx III



NERC Crisis Action Team

Regional Entities

Trade Associations

NERC
Bulk Power System Awareness (BPSA)

ES-ISAC
Electricity Sector - Information Sharing & Analysis Center

DOE
Department of Energy

NCCIC
US-CERT/ICS-CERT

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

Coordination with Government

Bulk Power System Entities Coordinated Operations

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

Vendor Support
IT, ICS, ISP, Anti-virus

Local, State/Provincial Government
- Emergency Management Organizations
- Emergency Operations Centers
- Local FBI

SED
Spare Equipment Database

ExCon
GridEx II Exercise Control
NERC staff, GEWG, Booz Allen, PNNL, SMEs for Sim-cell, etc.

Why choose 'Active'?

Organizational Benefits

- Voluntary participation
- Opportunity, if you choose, to demonstrate compliance with NERC reliability standards requirements, for example:
  - EOP-004 Event Reporting
  - EOP-008 Loss of Control Center Functionality
  - CIP-008 Incident Reporting and Response Planning
  - CIP-009 Recovery Plans for Critical Cyber Assets
- **No reporting to NERC on compliance matters as part of GridEx**

Individual Training

- NERC Certified Operators may earn up to 16 NERC continuing education hours—Operations Simulator time
- Training hours for staff with information technology or cyber security certifications
- Training hours for staff with physical security certifications
- Opportunity to cross-train staff to support other business functions

Level of Effort

- Active Organization (large)
  - One Lead Planner with multiple other Planners developing numerous custom injects
  - 10/50/100+ Players across multiple departments/functions executing crisis response procedures
- Active Organization (small)
  - One Lead Planner using ‘generic’ and a few custom injects
  - Several Players across a few departments/ functions executing crisis response procedures
- Observing Organization
  - One Lead Planner who can guide others to watch events that are occurring and discuss internal actions
- ALL – gathering and sharing lessons learned

ERCOT Regional GridEx Participation

- ERCOT ISO will be an Active Organizational Player
  - ERCOT Operations, Cyber & Physical Security, IT, Market Ops and Communications Groups will be active
  - ERCOT Operations Simulator to reflect impacts of security events
  - ERCOT Operations Team will work GridEx security events in Simulator
  - ERCOT will host White Cell for Utility “Exercise Reporting” other than Ops
    - Invite: TX-DPS and FBI
- Recommend ERCOT Members Participation
  - Generation & Transmission Owner/Operators working with Control Center
  - Report Exercise Physical & Cyber Security Events via SSRG
  - Deep-Dive analysis of Cyber Security Events below SSRG reporting level
  - Coordination and communications between security teams at neighboring and adjacent utilities, and coordination with ERCOT Security and Operations

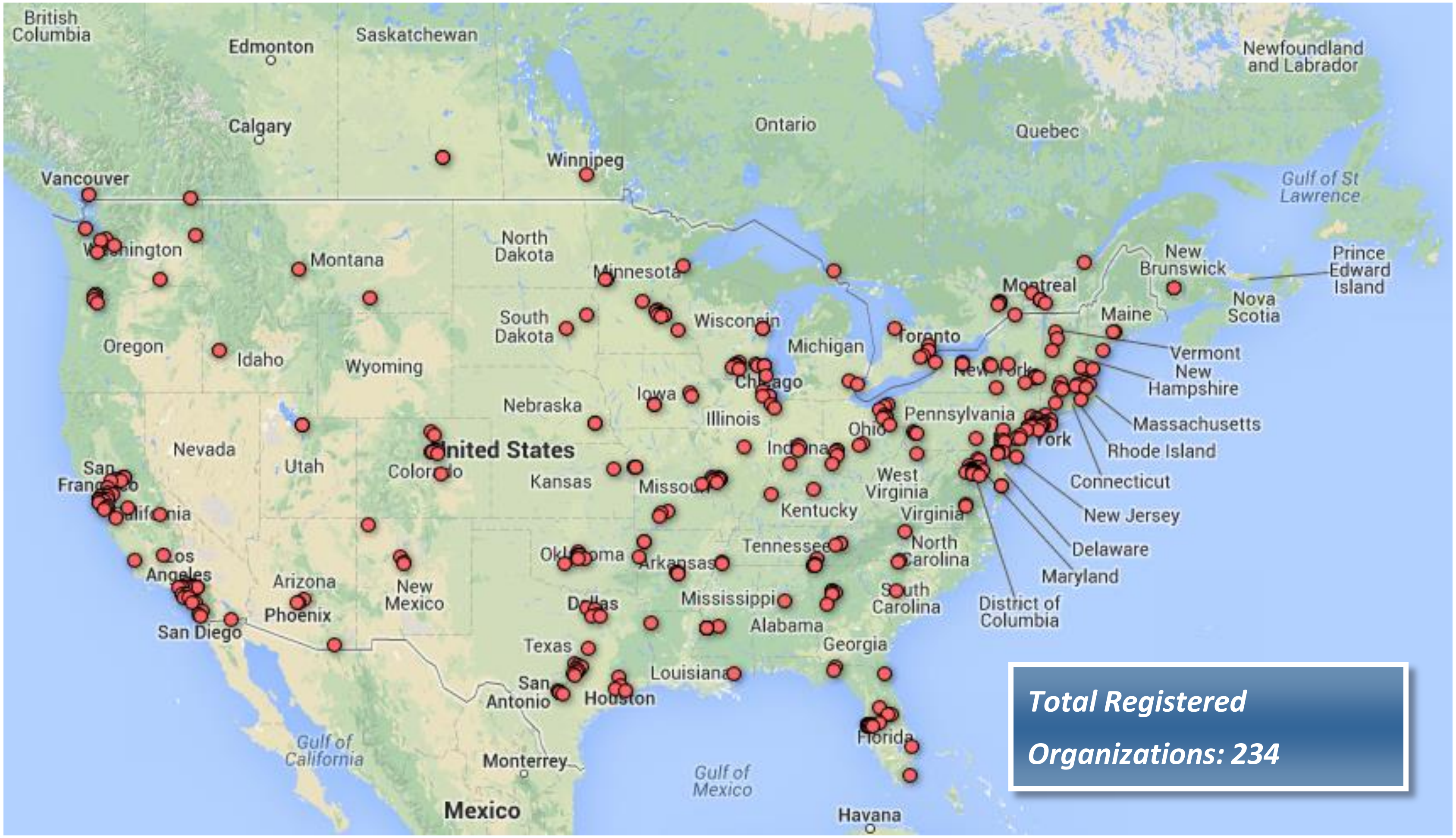
Other References

- Additional GridEx information at: http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx
- Security Questions on GridEx III in ERCOT, Contact Jim Brenton at: jbrenton@ercot.com (512-248-3043)
- Operational Questions on GridEx III in ERCOT, Contact Kelly Blackmer at: Kelly.Blackmer@ercot.com (512-248-4101)

Questions and Answers

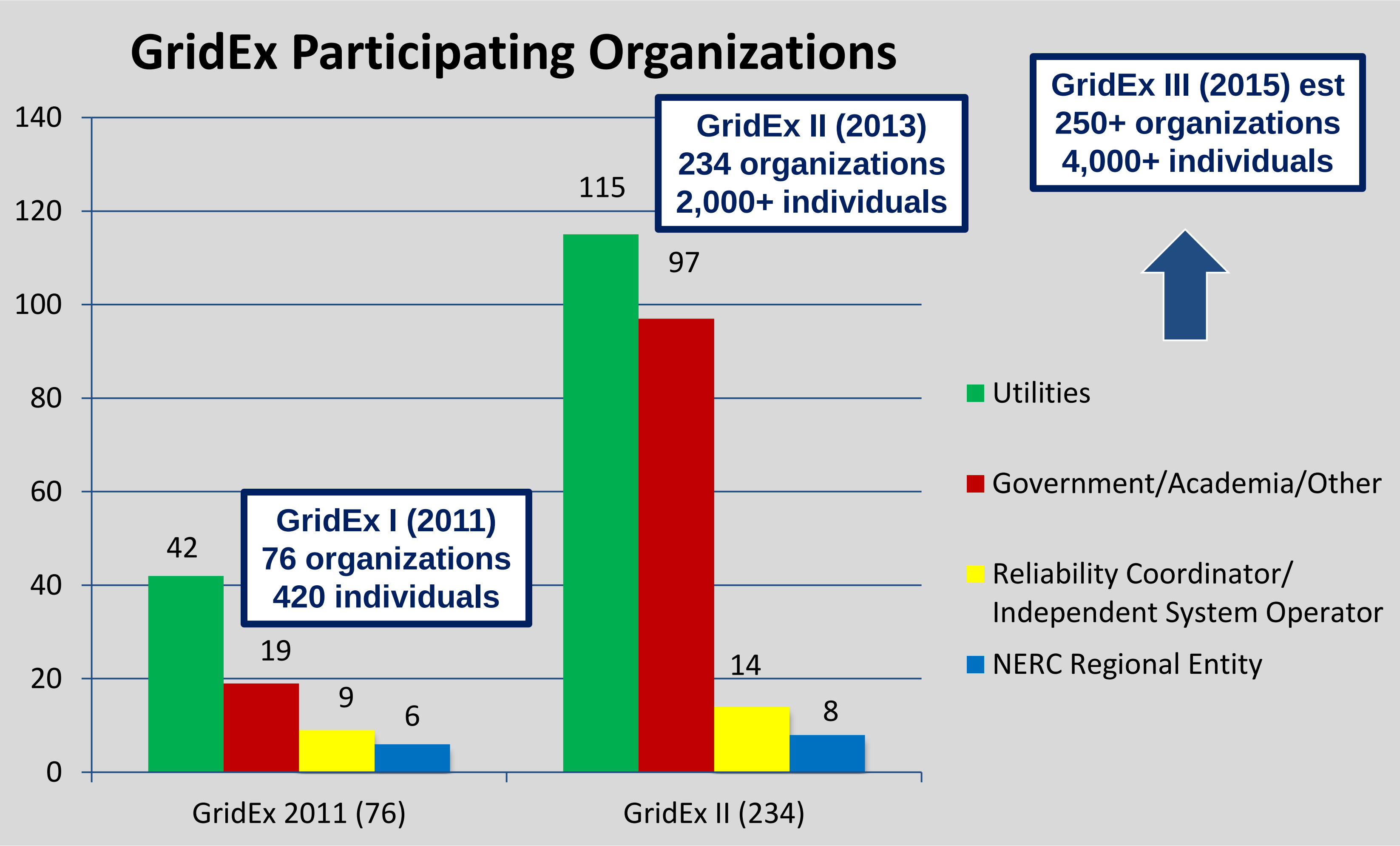
Supplemental Material

GridEx 2013 Participation



Total Registered Organizations: 234

GridEx Participation Growth



GridEx I (2011)
76 organizations
420 individuals

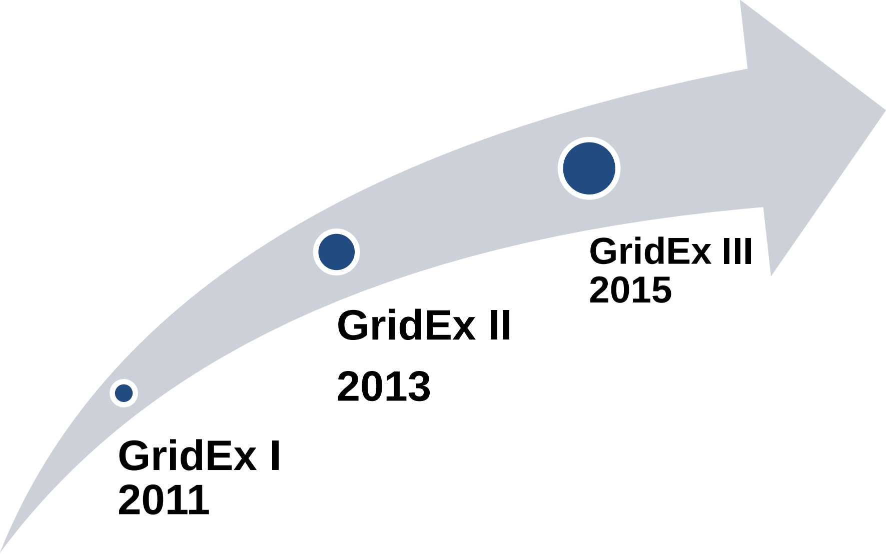
GridEx II (2013)
234 organizations
2,000+ individuals

GridEx III (2015) est
250+ organizations
4,000+ individuals

GridEx – A Long-Term View

Continuing Evolution

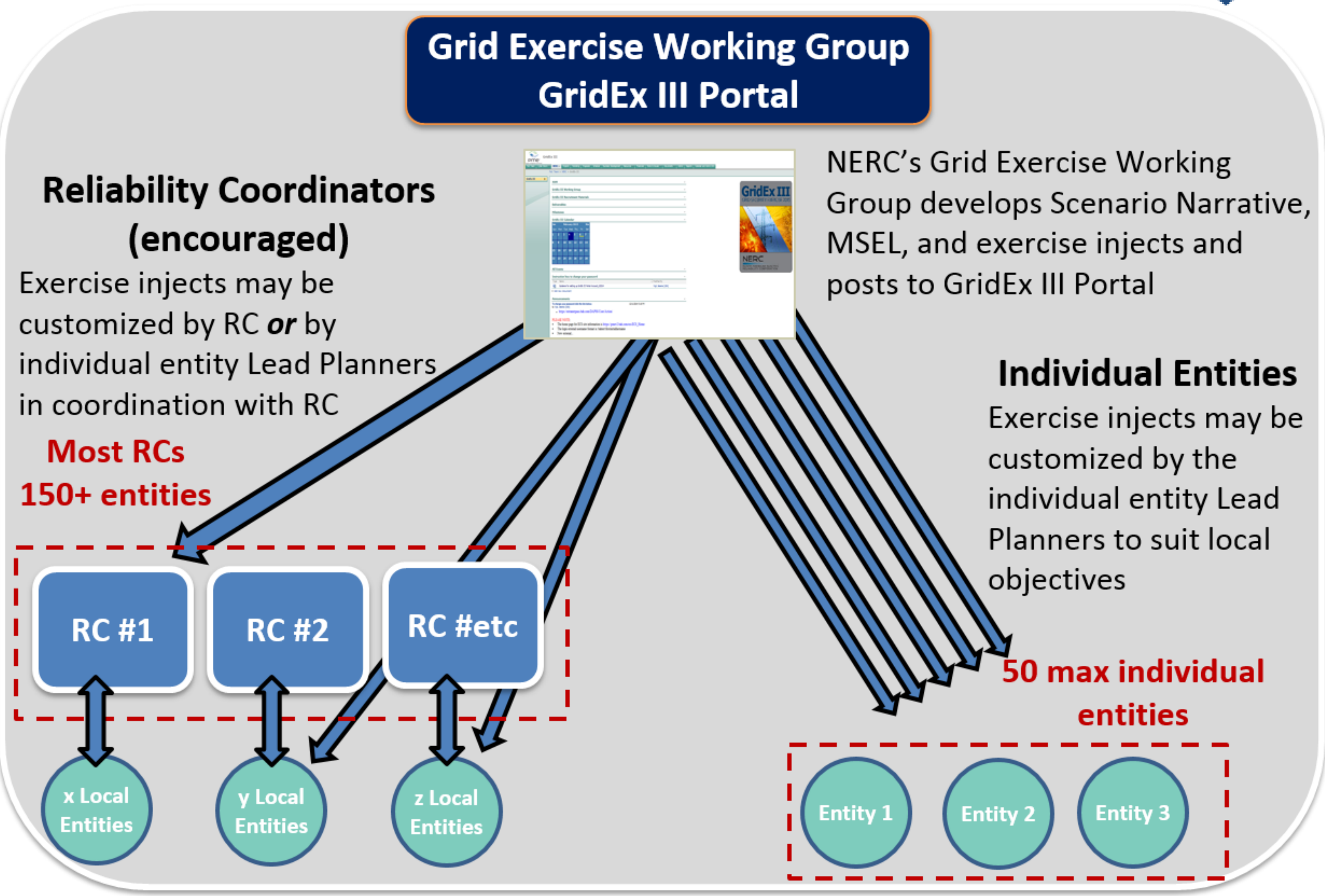
- Exercise timely, real-world scenarios
- Increase stakeholder participation and training value
- Increase integration with bulk power system operations
- **Greater state/regional and local government participation**
- Greater integration between senior industry executives and government officials
- Include other interdependent critical infrastructure sectors
- Increasingly sophisticated and realistic operational simulations



GridEx III Challenges

- Increasing number of utilities and government entities
- Exercise Control was overwhelmed during GridEx 2013
- Improve horizontal coordination between neighboring utilities
- **Improve vertical communication of utilities with RC/BA/TOPs and with the ES-ISAC and NERC BPSA**
- **Distribute Exercise Control functions to RCs**
- **Increase level of exercise participation by State and Regional Government groups**
- Integrate the role of the new **E**lectricity **S**ector **C**oordinating Council with their Federal Gov counterparts
- Obtain full support of NERC Ops and Planning Committees, not just the CIP Committee

Inject Development Process Planning Time Frame



Grid Exercise Working Group GridEx III Portal

NERC's Grid Exercise Working Group develops Scenario Narrative, MSEL, and exercise injects and posts to GridEx III Portal

Reliability Coordinators (encouraged)

Exercise injects may be customized by RC ***or*** by individual entity Lead Planners in coordination with RC

Most RCs
150+ entities

RC #1
RC #2
RC #etc

x Local Entities
y Local Entities
z Local Entities

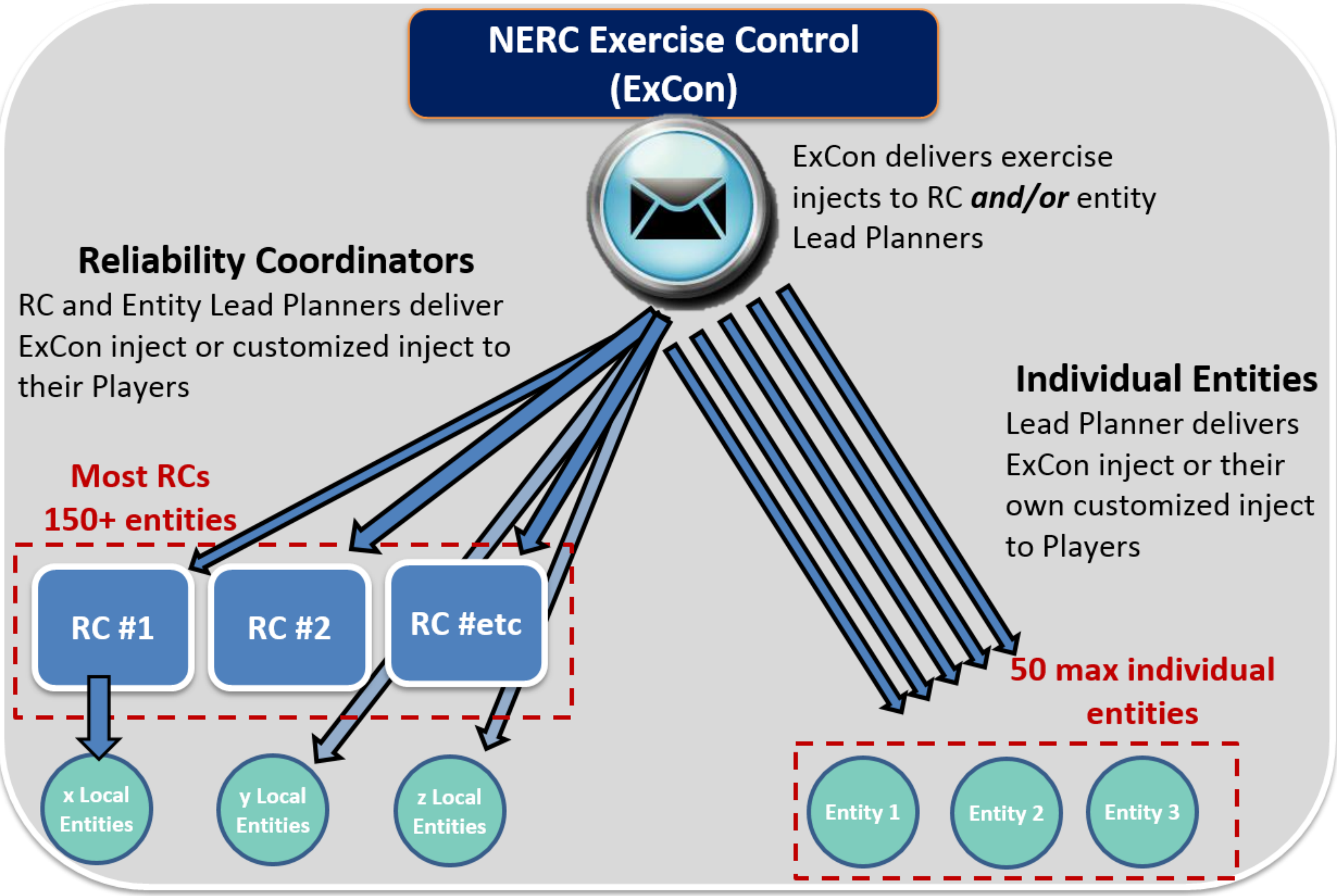
Individual Entities

Exercise injects may be customized by the individual entity Lead Planners to suit local objectives

50 max individual entities

Entity 1
Entity 2
Entity 3

Inject Delivery Process
Exercise Time Frame



NERC Exercise Control (ExCon)

ExCon delivers exercise injects to RC ***and/or*** entity Lead Planners

Reliability Coordinators

RC and Entity Lead Planners deliver ExCon inject or customized inject to their Players

Most RCs
150+ entities

Individual Entities

Lead Planner delivers ExCon inject or their own customized inject to Players

50 max individual entities

Diverse Stakeholder Organizations

Organization	Recommendation	Explanation
Reliability Coordinator	• Active, with multiple entities Active within the control area	• RC may guide the inject customization in the control area, or entities may customize injects themselves (see following slides)
Regional Entities	• Observing	• Some Regional Entities may have crisis coordination roles and may work with RCs to determine if an Active role is required. **No compliance-related participation.** • Regional Entities will be integrated into lessons learned process
US Department of Energy	• Active	• US DOE, Infrastructure Security and Energy Restoration • Natural Resources Canada, Energy Security Division
Local / State 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)	• 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 Stakeholder Organizations (con't)

Organization	Recommendation	Explanation
Cross-sector ISACs and organizations	• Observing	• ES-ISAC will invite specific interdependent sectors (e.g. Nuclear, Down-stream Natural Gas, Communications, Financial, Water, etc.)
Support Vendors / Consultants	• Active (**only** by invitation from participating utility)	• 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	• ES-ISAC will share information with key stakeholders (e.g. Canadian Security Intelligence Service, National Security Agency, etc.) • Utilities may invite Active or Observing regional participation (e.g. National Guard, etc.)
Federally Funded Research and Development Centers / Academia	• Observing	• ES-ISAC will invite

Key Planning Dates for GridEx III

- March 11-12 – Initial Planning Conference--COMPLETED
  - Jacksonville CIPC Meeting
  - Finalize attack scenario and impacts
- June 10-11 – Mid-term Planning Conference--COMPLETED
  - Atlanta CIPC Meeting
  - Finalize detailed baseline scenario--MSEL
- September 15-16 – Final Planning Conference
  - NOLA CIPC Meeting
  - Finalize customized scenarios with Reliability Coordinators and train Players
- November 18-19 – GridEx III takes place
- December 15-16 – Hot Wash of GridEx at Atlanta CIPC Meeting
- March 2016—GridEx After-Action Reports published