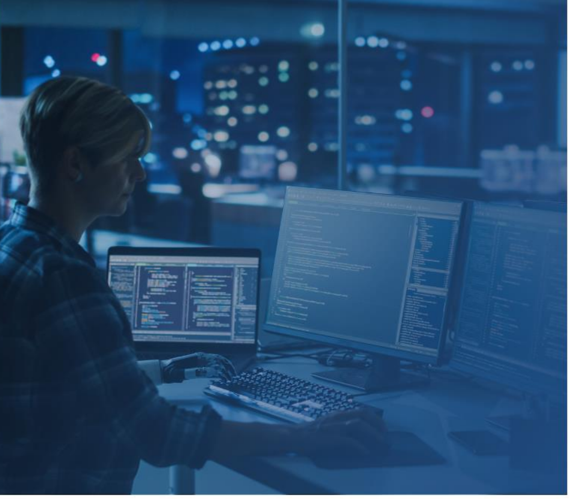
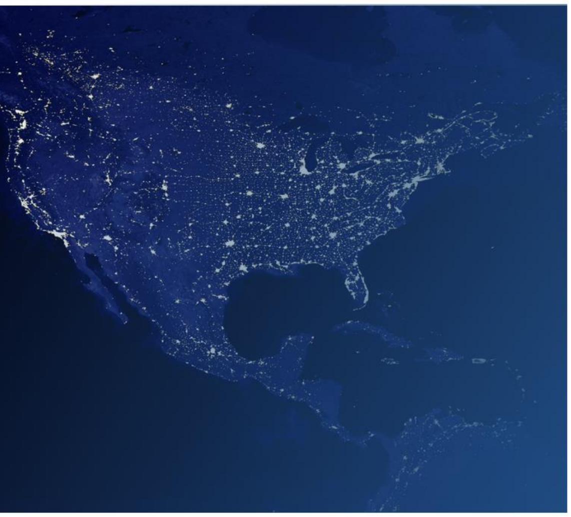




GridEx VII

Lessons Learned Report

TLP:CLEAR

April 2024

RELIABILITY | RESILIENCE | SECURITY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

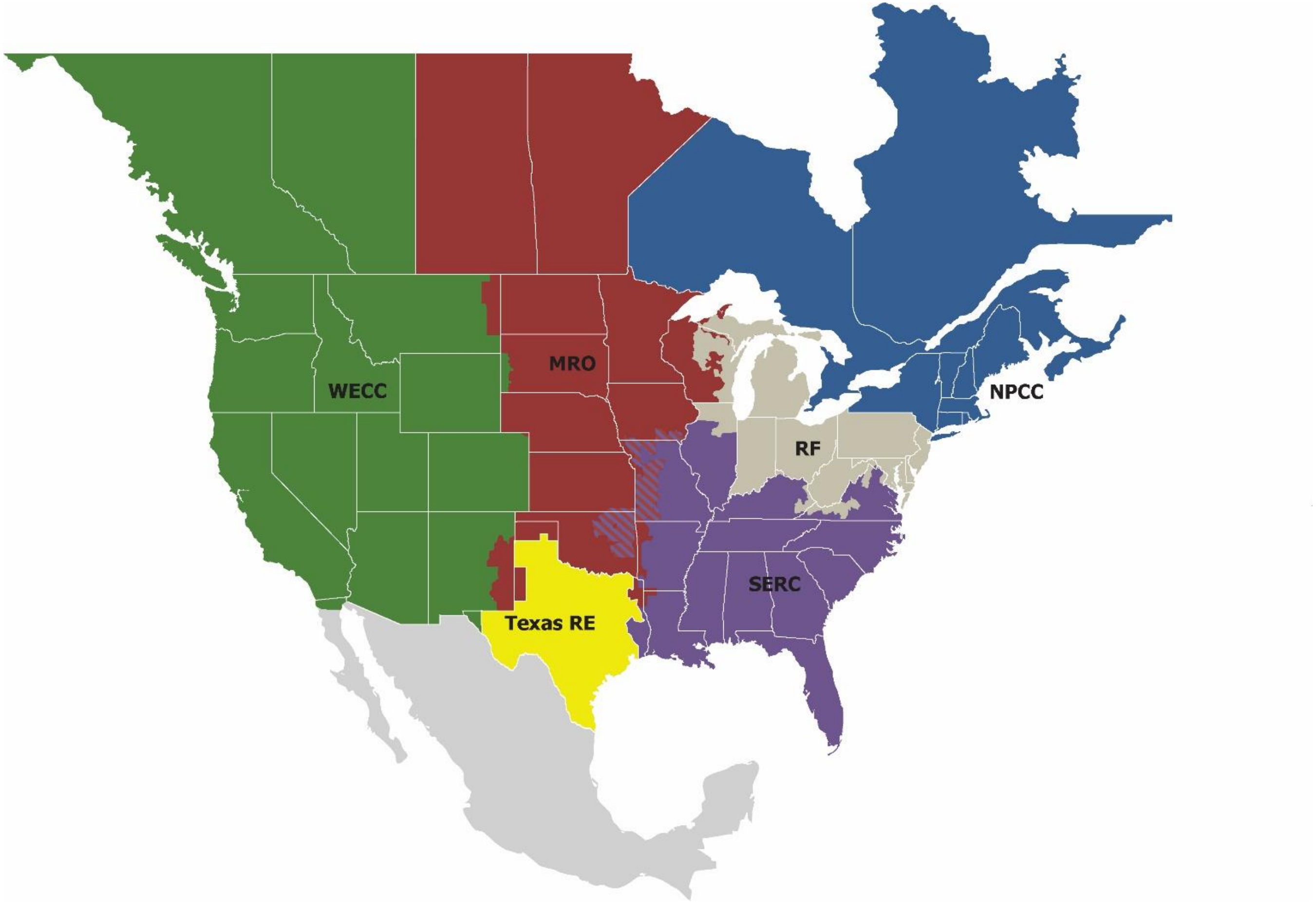
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities, is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

In November 2023, NERC's Electricity Information Sharing and Analysis Center (E-ISAC) conducted the seventh biennial GridEx. The following exercises make up GridEx:

- **Distributed Play:** On November 14 and 15, 2023, operational participants across North America exercised the resilience of the electric system in the decentralized and independent Distributed Play exercise. The E-ISAC's GridEx Planning Team developed core planning and exercise materials, which local planners across the continent used to design and conduct their own exercises for their organizations.
- **Executive Tabletop (Tabletop):** On November 16, 2023, industry executives and government leaders from the United States and Canada convened in person in Washington, D.C., as well as virtually, to explore the challenges presented by cyber and physical attacks against the electric grid and the electric market system.

This report summarizes the recommendations and observations identified through each exercise. The recommendations are intended to help electric utilities, government partners, the E-ISAC, and other stakeholders prepare for and respond to security incidents that affect the North American electricity system.

GridEx VII Goals and Objectives

The GridEx series is an opportunity to explore and exercise grid security and emergency issues impacting the North American grid. The E-ISAC developed specific goals for each portion of GridEx VII. The Tabletop focused on policy-level decisions for senior industry and government leadership while Distributed Play focused on operational response activities.

GridEx VII Executive Tabletop Goal: Engage senior industry and government leadership in a comprehensive discussion of the extraordinary operational measures needed to protect and restore the reliable operation of the grid.

To achieve this goal, the Tabletop exercise was designed to address the following objectives:

- Explore U.S. and Canadian national security implications of supply chain attacks on critical systems and software used by industry, including essential telemetry between control centers
- Enhance electric industry response coordination with the natural gas and communications sectors, which have significant interdependencies with the electric sector, for the safe and reliable operation of the grid
- Enhance industry coordination with U.S. and Canadian federal and state/provincial governments, including communications mechanisms
- Explore security and resilience implications of long-term electricity market outages, recognizing the increasing diversity of generation resources

GridEx VII Distributed Play Goal: Exercise the resilience of the North American electric system in the face of a coordinated attack from a nation-state adversary.

To achieve this goal, Distributed Play was designed to address the following objectives:

- Exercise incident, operating, communications, mutual assistance, and crisis management response plans
- Respond to imminent cyber, physical, and other threats with the potential to affect the reliable operation of the grid

- Enhance coordination with state/provincial and local governments, suppliers supporting critical operations, and industry partners to facilitate restoration
- Manage interdependencies with natural gas, telecommunications, and other critical infrastructure sectors
- Exercise response to information technology (IT) and communications system failures
- Exercise response to emergency events in a remote or hybrid environment with reduced staff availability and limited access to resources

While the E-ISAC's GridEx Planning Team developed overarching objectives for Distributed Play, participating entities were encouraged to modify these objectives or create their own to reflect their organization's priorities.

Recommendations Overview

This report provides recommendations to help inform electric industry participants, critical infrastructure sector partners, and government partners of measures that they could take to improve the collective response to cyber and physical security events that affect the North American electric grid. Additional recommendations detail how the E-ISAC can improve future iterations of GridEx. An explanation and additional details for each Tabletop recommendation are provided in **Chapter 1: Executive Tabletop**. Methodology and associated data used to develop the Distributed Play recommendations are articulated further in **Chapter 2: Distributed Play**.

Executive Tabletop Recommendations Overview

A high-level summary of the recommendations from the Tabletop is provided below. The recommendations are not listed in priority order but in the order in which they emerged during the Tabletop scenario and associated discussion.

1. **Industry should evaluate technologies and processes that could be used to increase the resilience of Inter-Control Center Communications Protocol (ICCP) telemetry exchange between control centers.** While ICCP systems are highly reliable and supported by layers of redundant infrastructure and cyber security protections, the severity of the Tabletop scenario prompted participants to consider that the current ICCP infrastructure may not be sufficiently resilient against certain single-point-of-failure or common-mode vulnerabilities. The electric industry should consider the potential impact of a complete loss of ICCP functionality and develop recommendations for alternatives that would provide comparable capabilities. Industry should review these alternate technologies and determine if they could be applied across North America. Industry should evaluate options to maintain basic grid operation using minimal data and manual methods.
2. **Industry should evaluate opportunities to employ alternate technologies for operator voice (i.e., interpersonal) communications essential to operate the grid.** While operator voice communications are highly reliable and have robust backup facilities, the Tabletop scenario exceeded this capability. Industry should coordinate to clearly identify what specific aspects related to resilient voice communications may be improved and leverage past efforts such as those undertaken by the Electricity Subsector Coordinating Council's (ESCC) Resilient Communications Working Group. If necessary, industry should evaluate the need for alternate voice technologies with a focus on essential operator-to-operator communications. NERC will increase the resilience of its Reliability Coordinator (RC) Hotline, and the E-ISAC will evaluate hosting a centralized satellite phone book for ESCC members.
3. **Industry and government should continue discussing how to consider government priorities during a complex and prolonged power outage scenario as part of the electric industry's established restoration procedures.** RCs and electric utilities have well-practiced plans and resources in place to restore the grid and supply power to customers on a prioritized basis. However, a large-scale crisis that affects electricity and other critical infrastructure providers over extended periods will reveal new and conflicting priorities. Industry should determine the need to develop an improved restoration framework that considers government requests that may conflict with pre-established restoration priorities and recommend guiding

principles for coordinating with other critical infrastructures as needed. Industry should leverage its supply chain efforts and determine the need to improve processes to address equipment and supply shortfalls during a large-scale crisis and identify where government authorities can resolve supply chain issues.

4. **Industry should evaluate options to manage the grid reliability impacts of electricity market system or data unavailability over an extended period.** Given the importance of electricity markets as an integral part of reliable grid operations, market operators and participants should review their market rules to ensure a common understanding of how generation dispatch and financial settlements would be administered through an extended period of market system or data unavailability. Industry should coordinate to develop best practices to manage long-term unavailability with a focus on maintaining reliable grid operations. FERC and the equivalent authorities in Canada should contribute to these reviews by considering how regulatory waivers and emergency tariffs applicable to the electric and natural gas industries may help support these efforts.

Distributed Play Recommendations Overview

1. **Non-federal government partners and electric utilities should advance coordination efforts.** GridEx is an opportunity for government to collaborate with electric utilities, increase mutual understanding, and identify critical interdependencies. While it is important for regional government partners to remain proactively engaged in emergency response with electric utilities, GridEx VII Distributed Play saw an overall reduction in the number of government entities that participated. Municipal government entities, such as city, town, and county governments, as well as state energy offices would benefit from greater involvement in emergency response planning, training, and exercises, such as GridEx.
2. **Communications and response in a hybrid work environment should be further refined.** Organizations are still identifying best practices for hybrid communications since the onset of the COVID-19 pandemic. By providing an opportunity to exercise in-person and virtual response protocols, GridEx VII helped participating organizations identify challenges with hybrid response and interoperable communications with internal and external response partners.
3. **Response planning should be augmented to ensure comprehension of technical information across functional teams and external response partners.** The ability to communicate accurate and timely information to critical stakeholders when responding to events like those simulated in GridEx is essential. The GridEx scenario touches on technically complex subject matter that can require technical knowledge, making it difficult to communicate with non-technical units of an organization and external partners.
4. **GridEx should continue to evolve to provide additional support for planners from organizations of varying sizes and with different levels of experience.** While GridEx is open to organizations of all sizes, the E-ISAC recognizes that smaller asset owners and operators are a crucial part of the BPS and is committed to enabling their participation. Although the E-ISAC's GridEx Planning Team provided guides, webinars, and template materials, feedback from the After-Action Survey indicated that some smaller organizations and newer exercise planners would have benefited from additional support and guidance to scale their GridEx appropriately. Conversely, more experienced planners noted that additional materials and training on those resources could better help them develop more complex exercise play.
5. **Cyber and technical components of the GridEx scenario should continue to be developed and expanded for future iterations of GridEx.** GridEx is a grid security exercise that focuses on cyber and physical attacks on the grid and has been designed to reflect the current threat landscape. The E-ISAC's GridEx Planning Team developed a Master Scenario Event List (MSEL) with both cyber and physical attack components, and cyber incident response formed a core component of many instances of GridEx VII. However, as participating organizations have varying levels of technical cyber expertise, the GridEx Planning Team will continue seeking to deliver a scenario and associated exercise material that cater to differing levels of cyber capabilities.

Introduction

In addition to summarizing the recommendations identified during GridEx VII's Distributed Play and Tabletop activities, this report provides information on the design, delivery, and participation across both exercises. In 2023, hundreds of organizations participated in Distributed Play on November 14 and 15, while over 100 select executives and senior government officials attended the Tabletop on November 16.

Both the Distributed Play and Tabletop scenarios involved a nation-state adversary targeting the North American BPS with cyber and physical attacks. The E-ISAC developed the scenarios for both Distributed Play and the Tabletop with input from colleagues at national laboratories, subject matter experts, and experienced planners from participating organizations.

The Tabletop was conducted both in person and virtually, simulating how participants would collaborate during a real emergency. The day-long exercise involved plenary and breakout sessions to ensure that discussions were appropriately structured. The electric industry participants included chief executive officers and chief operating officers from investor- and publicly owned utilities, cooperatives, and independent system operators (ISO). Participants from other critical infrastructure sectors included senior executives from the natural gas, communications, and finance sectors. Senior officials represented key departments and agencies at the U.S. and Canadian federal, state, and provincial levels. Hagerty Consulting Vice President Brian Baker and Converge Strategies Principal Jonathon Monken facilitated the day-long event.

Methodology

Members of the GridEx Planning Team attended and observed the Tabletop and subsequent hotwash, a one-hour event to review key findings held on November 17, 2023. The GridEx Planning Team used notes from each discussion to identify and develop the recommendations identified in this report.

Owing to the nature of Distributed Play, during which utilities, government entities, and other participating organizations across North America modify their own internal exercises with the E-ISAC's core materials, the E-ISAC was not able to observe exercise play within participating entities. To collect information about Distributed Play, the E-ISAC's GridEx Planning Team asked planners to complete an After-Action Survey that collected qualitative and quantitative feedback on exercise planning and conduct. Of the 252 participating entities, 82 responded to the survey. The GridEx Planning Team also encouraged all participating entities to create their own internal after-action reports to identify strengths and areas for improvement specific to their organization. The GridEx Planning Team also hosted a hotwash for the Design Team and select lead planners to gather feedback on key findings from their organizations' exercise play.

The following chapters display additional data that informed the findings from GridEx VII.

Chapter 1: Executive Tabletop

Executive Tabletop Scenario and Conduct

The Tabletop was designed in four acts to simulate how industry and government would respond to a sophisticated, well-coordinated physical and cyber attack. During plenary and breakout sessions, facilitators led participants through discussions designed to simulate the communication and coordination that would occur during a real event.

- **Act I: A Dormant Threat Awakens.** The ICCP software used by grid operators to receive data from generation and transmission facilities is compromised and degrades operators' normal capabilities to monitor and control the grid. Operators resort to alternate and manual methods and suspend the electricity market systems that automatically dispatch and price generation. In addition, an incident occurs that may or may not be related to the ICCP outage. Voice and data communications backbone networks fail in large areas from the Gulf Coast to the upper Midwest, degrading local communications.
- **Act II: Coordinated Attack.** Transmission substations in Louisiana and Texas are subjected to cyber and physical attacks that damage high-voltage transformers, circuit breakers, and remote terminal units. The resulting power outages disrupt operations at several nationally important natural gas hubs.
- **Act III: Managing Prolonged Impacts.** Midcontinent Independent System Operator (MISO) discovers that its website has been defaced and receives a ransom demand. Its backup systems show signs of corruption, and an IT staff member critical to response cannot be reached.
- **Act IV: One Month Later.** After a massive effort, ICCP telemetry has been mostly restored. However, MISO's electricity market systems remain suspended. Repairs to damaged substation equipment are not yet complete, and power to natural gas facilities has not been restored.

Executive Tabletop Participation

The GridEx VII Tabletop convened executives and leaders from 75 organizations, leading to approximately 230 attendees representing U.S. and Canadian government agencies, the Electricity Sector Government Coordinating Council (EGCC), the ESCC, and entities impacted by the scenario.

The Tabletop scenario impacted several critical infrastructure sectors, and the E-ISAC engaged a diversity of participants to reflect the interdependent nature of the BPS. Participation in the GridEx VII Tabletop included six oil and natural gas organizations, three telecommunications organizations, two finance organizations, and one nuclear organization.

The E-ISAC also engaged participants from multiple levels of government to represent diverse involvement during an incident response. Government representation included organizations such as the Louisiana State Energy Office and State National Guard, the Canadian Centre for Cyber Security, the U.S. Department of Defense, the Royal Canadian Mounted Police, and the National Security Council. **Table 1.1** provides a full list of government agencies that participated in the Tabletop.

Table 1.1: Executive Tabletop Government Agencies

U.S. Government Agencies	Canadian Government Agencies
Cybersecurity and Infrastructure Security Agency (CISA)	Canadian Centre for Cyber Security (CCCS)
Department of Defense (DOD)	Natural Resources Canada (NRCan)
Department of Energy (DOE)	Public Safety Canada (PSC)
DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER)	Royal Canadian Mounted Police (RCMP)
Federal Bureau of Investigation (FBI)	
Federal Energy Regulatory Commission (FERC)	
Louisiana State Energy Office	
Louisiana State National Guard	
National Security Council (NSC)	
Office of the National Cyber Director (ONCD)	

Executive Tabletop Recommendations

1. **Industry should evaluate technologies and processes that could be used to increase the resilience of ICCP telemetry exchange between control centers.** The highly integrated nature of North America's grid requires operators to monitor and control the operation of generation and transmission facilities continuously without interruption, including using data from facilities outside their own jurisdiction. Robust and redundant data communications facilities (e.g., multiple communications circuits) ensure that operators have the information that they need to make decisions and share data with their colleagues at other utilities. While utilities operate their own supervisory control and data acquisition systems to monitor and control facilities within their local area, the ICCP infrastructure provides real-time telemetry and data exchange with and between neighboring utilities and Balancing Authorities (BA). RCs rely on ICCP to monitor and maintain wide-area reliability in coordination with their interconnected neighbors across North America.

   While ICCP systems are highly reliable, supported by layers of redundant infrastructure and cyber security protections, the severity of the Tabletop scenario prompted participants to consider whether the existing ICCP infrastructure is sufficiently resilient against certain single-point-of-failure or common-mode vulnerabilities and whether alternate, diverse technologies and processes should be examined. Understanding the extent of redundancy and technical diversity of the ICCP infrastructure across the BPS will help identify specific areas where improvements would significantly enhance resilience in the event of a widespread failure of the existing ICCP infrastructure:[1]

   a. Industry should evaluate the potential impact of a complete loss of ICCP functionality and consider developing recommendations for alternatives that would provide comparable capabilities. For example, DOE is conducting an ICCP research initiative known as the Universal Utility Data Exchange framework, which may offer a common architecture and conceptual design for alternate ICCP functionality. Industry should review the goals and results of this initiative and seek opportunities to leverage this work to enhance ICCP infrastructure resilience. NERC's Reliability and Security Technical Committee (RSTC)[2] will consider taking on some of this analysis.

   b. Some utilities employ alternate technologies and processes similar to, but separate from, ICCP to exchange data such as control center telemetry with their RC, BA, or neighbors. Industry should review these alternate technologies and determine if they could be applied more broadly across North America.

   c. While NERC recognizes that developing, implementing, and maintaining additional full-function ICCP-like infrastructure across North America would be very costly, opportunities may exist to focus efforts on a limited set of telemetry data (e.g., fewer data points, less-frequent data sampling) sufficient to maintain reliable grid operation. Industry should evaluate options to maintain basic grid operation using minimal data and manual methods.

2. **Industry should evaluate opportunities to employ alternate technologies for operator voice (i.e., interpersonal) communications essential to operating the grid.** Tabletop participants agreed that, in the absence of all other automated or manual means to retrieve and share telemetry information needed to operate the grid, effective and efficient operator-to-operator voice communication is essential. For example, RC and BA operators need to communicate with Transmission Operators (TOP) to coordinate switching and Generator Operators (GOP) to direct dispatch. TOPs need to communicate with local utility operators who perform switching at the distribution level. While operator voice communications facilities

[1] The ICCP infrastructure is not a single network with identical installations at each electricity entity across North America. Rather, it consists of hundreds of bidirectional, always-on data links between pairs of entities that need to exchange data. Each entity's ICCP infrastructure consists of hardware, software, and telecommunications systems with varying levels of redundancy and diversity. NERC's Data Exchange Infrastructure and Testing Requirements guidance document provides examples of redundant and diverse data exchange configurations.

[2] NERC's RSTC has diverse industry stakeholder expertise to study, mitigate, and/or eliminate risks to grid reliability.

are highly reliable with robust backup facilities, the Tabletop scenario would likely exceed this capability unless alternate, diverse facilities are in place and tested.

Furthermore, while not used to operate the grid, NERC's RC Hotline is used by RCs across North America to share time-sensitive Interconnection-level information during emergencies. The RC Hotline is a high-reliability telephone-based system with backup power supplies but does not have alternate or diverse communications capability.

ESCC members typically rely on commercially available landline or cellular communications providers to communicate with each other during an emergency. For ESCC members with satellite phones, there is no central phone book or directory for ESCC members.

The Tabletop discussion regarding the necessity of operator voice communications suggested the following:

a. Industry should evaluate what specific aspects of operator-to-operator voice communications may be improved (e.g., facilities, communications providers, technologies, higher-priority operator contacts) to increase resilience beyond the redundant backups currently in place. NERC's Real Time Operating Subcommittee (RTOS)[3] will consider taking on some of this analysis.

b. Industry should leverage past efforts related to resilient communications and continue to collaborate with the communications sector.

    i. Review and update the prior work of the ESCC's Resilient Communications Working Group (RCWG) and others to address gaps in resilient communications. For example, the RCWG's Demonstration Project with the Electric Power Research Institute[4] (EPRI) tested on a pilot basis how alternate communications technologies could be used by operators to communicate and coordinate response through a blackstart and restoration scenario. The RCWG had also developed criteria to help organizations identify the criticality of their communications facilities, evaluation criteria for different communications technologies, and a self-assessment questionnaire to determine the resilience of their communications facilities.

    ii. If necessary, evaluate the need for alternate voice technologies used for operator-to-operator voice communications. In addition to landline telephone, options to be considered include satellite telephone, satellite Internet, radio, or broadband IP software-defined radio. Some examples that should be evaluated include the commercially available Starlink and EPRI's National Resilient Communications System proposal through DOE's Grid Resilience and Innovation Partnership Program.[5]

    iii. Focus these efforts on the essential communications needed between RCs, BAs, TOPs, and GOPs.

c. NERC has reviewed the reliability and backup capabilities of the RC Hotline and has contingency plans in place. NERC has identified and will implement enhancements to provide instant failover of the RC Hotline if the primary facility is lost.

d. The E-ISAC will evaluate platforms, processes, and potential costs to develop and maintain a satellite phone directory for ESCC members.

[3] NERC's RTOS supports the RSTC by providing operational guidance and technical advice related to the information technology tools and services used to support operational coordination of the BPS.

[4] EPRI's Resilient Communication Demonstration Project: Demonstration Evaluation Report

[5] DOE's Grid Resilience and Innovation Partnerships Program provides funding opportunities to enhance grid flexibility and improve resilience.

3. **Industry and government should continue discussing how to consider government priorities during a complex and prolonged power outage scenario that may conflict with the electric industry's established restoration procedures.** RCs and electric utilities have well-practiced plans and resources in place to restore the grid and supply power on a prioritized basis to customers such as hospitals, water treatment plants, and first-responder facilities. Similarly, natural gas and communications providers understand their own customers' needs and commercial obligations and prioritize accordingly. A large-scale crisis affecting electricity and other critical infrastructure providers over extended periods of time will undoubtedly reveal new and conflicting priorities. For example, natural gas-fired GOPs might ask local gas providers to prioritize supply to avoid a widespread power outage, but this may create unintended natural gas operational risks. Government authorities may be aware of security threats but unaware of how they impact the electric industry or other critical infrastructures. Despite the many challenges, priority restoration decisions would need to be made quickly during a crisis and would need the support or at least awareness of industry and government at the local, state/provincial, and federal levels.

   In some circumstances, restoration would require a great deal of spare equipment, possibly more than is available in the impacted area. The electric industry has been addressing supply chain risks in recent years from several perspectives, including cyber security risk and supply availability. A large-scale crisis might create a severe and long-term shortage of specialized equipment needed to completely restore power. Without a compelling rationale, suppliers may not be willing or able to give special priority to certain customers unless doing so aligns with their usual way of doing business, including contractual commitments and other legal obligations.

   The Tabletop discussion regarding restoration priorities suggested that industry and government perform the following:

   a. Industry and government[6] should continue to discuss the need to develop an improved restoration framework that considers government requests that may conflict with pre-established restoration priorities.

      i. Assess the existing framework, prioritization criteria, identified authorities, and how government coordinates (internally and with partners at the state/provincial and international levels) and with industry during a large-scale crisis

      ii. Recommend guiding principles to engage other critical infrastructure sectors when needed during a large-scale crisis (especially communications and natural gas) to help decide priorities and take actions

      iii. Recognize and reinforce that RCs and utilities have the ultimate authority and responsibility to operate the grid and restore customers

   b. Industry and government should continue to discuss how to leverage past supply chain efforts[7] and improve processes to address equipment and supply chain shortfalls during a large-scale crisis. Industry can identify and prioritize its own needs, but it cannot compel suppliers to accelerate production or preferentially deliver to certain utilities.

      i. Identify where government authorities can resolve supply chain issues during a large-scale crisis. For example, the U.S. Defense Production Act authorizes the U.S. president to require businesses to accept and prioritize contracts for materials deemed necessary for national defense.

[6] The ESCC serves as the principal liaison between the federal government and the electric power industry on efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC should leverage past collaborative efforts with its government counterpart, the EGCC.

[7] Ref. NERC's Supply Chain Mitigation Program regarding cyber security supply chain risk management issues.

ii. Develop and exercise a process to identify and address equipment and supply chain shortfalls during a large-scale crisis if necessary

4. **Industry should evaluate options to manage the grid reliability impacts of market system or data unavailability over an extended period.** Given the importance of electricity markets as an integral part of reliable grid operations, market systems are designed to operate with very high levels of reliability that include redundant off-site data backups and multiple Internet and communications carriers. While market operators have processes in place to suspend and restore market operations as a result of periodic short-term outages, market operators should consider developing and exercising alternate market-related mechanisms (e.g., generation dispatch, settlements, billing) sufficient to support reliable grid operations over an extended period:

   a. Market operators and participants should review their market rules to ensure a common understanding of the conditions that would render market operators unable to use market prices and systems in support of generator dispatch and financial settlements. This review should include understanding how dispatch and settlements will be administered through an extended period of market system or data unavailability.

   b. Industry should coordinate to develop best practices to manage long-term electricity market system or data unavailability with a focus on maintaining reliable grid operations. This coordination should include reviewing backup strategies, technologies, and processes that address the possibility of single points of failure. In addition, simplified market pricing models should be considered, such as cost-plus or a single clearing price rather than locational marginal pricing. Recognizing the diversity of electricity markets in the different jurisdictions across North America, the ISO/Regional Transmission Organization (RTO) Council[8] may be a valuable source of expertise to review this recommendation, consider its merits, and develop best practices.

   c. FERC should contribute to these reviews by considering how its authority over wholesale rates, regulatory waivers, and emergency tariffs may help support the electric industry's development and operation of alternate market mechanisms needed over a prolonged period of market suspension. As part of this review, in addition to deploying its market authority specific to the electric industry, FERC should consider the natural gas industry given its status as an increasingly significant cost component of electric generation. Similarly, the equivalent Canadian authorities should contribute to these reviews by considering mechanisms to provide regulatory relief under these extraordinary circumstances.

[8] The ISO/RTO Council and its members help ensure access to affordable, reliable, and sustainable power through efficient administration of independent and transparent wholesale electricity markets.

Chapter 2: Distributed Play

Distributed Play Scenario and Conduct

Distributed Play conduct was designed to take place over two days. The E-ISAC GridEx Planning Team developed a scenario that included incidents ranging from cyber and physical attacks on substations to disinformation on social media. The GridEx Planning Team developed physical, cyber, and operational injects for the scenario in partnership with subject matter experts, GridEx planners, and partners from the SANS Institute, Idaho National Laboratory, and National Renewable Energy Laboratory to ensure their accuracy. The MSEL provided a progressive description of the national scenario, and planners were encouraged to customize it to meet their own needs. As a result, timing, content, and injects varied between participating entities.

The Distributed Play scenario was divided into five moves. Move 0 occurred a week before core exercise play, which took place on November 14 and 15 and consisted of Moves 1 through 4 as illustrated in Figure 2.1.

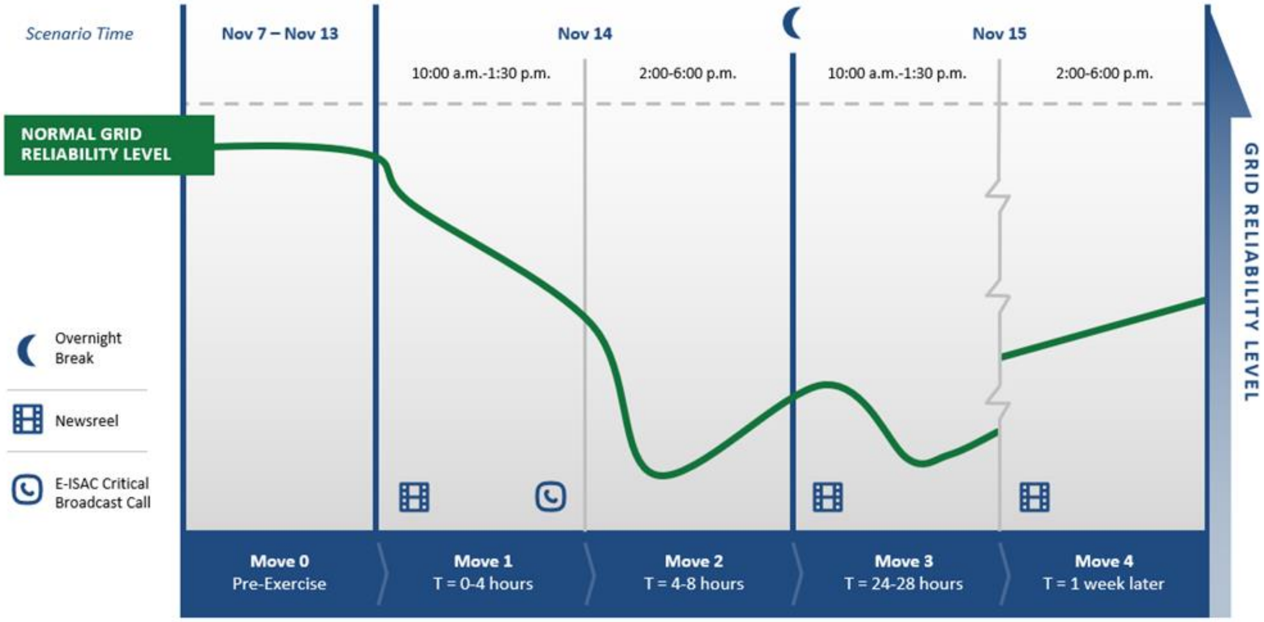


Figure 2.1: Distributed Play Scenario in Five Moves

The Distributed Play moves were as follows:

- **Move 0: The System is Vulnerable.** Move 0 set the stage for GridEx VII and took place in the week prior to November 14. MSEL injects could occur throughout Move 0 on an ad hoc basis to meet the organizational objectives of participating entities. Because the injects during Move 0 focused on investigating growing threats, not all players needed to participate.
- **Move 1: Softening the Target.** A series of cyber attacks made it harder for utilities to respond. A ransomware attack caused internal IT software and the third-party systems that operate the electric market to go out of service. An ICCP data link outage disrupted communications, and a natural gas pipeline flow disruption led to reduced generation capacity in the region.
- **Move 2: The Coordinated Attack:** A coordinated physical attack targeted multiple substations with assailants directing gunfire at critical transformer components. Several transformers, lines, and generators tripped automatically, causing outages across a large operating area. As utilities responded to these attacks, a distributed denial-of-service attack against the corporate virtual private network system rendered remote access intermittent or impossible. Meanwhile, misinformation and disinformation circulated on social media.

- **Move 3: Recovery Under Pressure.** No additional attacks occurred overnight, and recovery began under pressure from the public and local governments. However, the adversary was not finished. Transmission and distribution field breakers tripped due to unknown causes, interrupting grid supply to critical facilities. A vehicle-borne improvised explosive device detonated at a telecommunications facility, removing voice and data communications at an RC control center. The public became increasingly frustrated by power outages, and, as misinformation and disinformation continued to spread, protestors gathered and began to harass utility personnel. At 1:20 p.m., explosives detonated at equipment storage and staging areas, damaging and destroying spare equipment needed to restore service. This compounded supply chain and market disruptions.
- **Move 4: A Week Later.** Move 4 was designed as a discussion-based move and jumped ahead one week after the events in Move 3, enabling players to explore recovery and longer-term considerations. Global supply and diesel fuel shortages continued, delaying restoration and repair efforts. For the foreseeable future, no spare equipment was available, and entities had to rely on their current inventories.

Exercise Objectives

In the After-Action Survey, 60 planners shared their exact or paraphrased objectives for GridEx VII play. These objectives were broadly similar across organizations, and almost all mentioned exercising response to cyber and physical attacks as a key objective. Over half (33) of those participating entities that responded to the After-Action Survey used objectives that mentioned the importance of activating response or incident action plans. A third (21) noted communications and public information as an objective. Eight respondents highlighted coordination or interdependency identification as an objective.

Planner objectives aligned well with the E-ISAC's published objectives for GridEx VII, suggesting that the objectives developed by the E-ISAC are accurately responding to and reflecting industry needs.

After-Action Survey Results

The After-Action Survey allowed planners to share feedback about their Distributed Play conduct with the E-ISAC. Of the over 250 organizations that participated in GridEx VII, 82 completed the survey for a completion rate of 33%. Figure 2.2 highlights key statistics from the Survey.

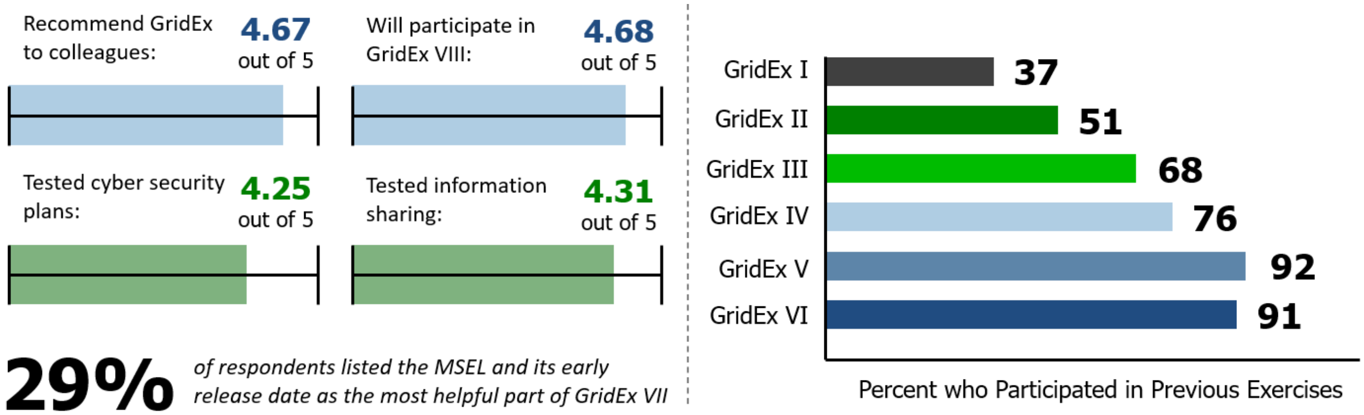


Figure 2.2: Key Highlights from the After-Action Survey

Distributed Play Coordination

GridEx is designed to allow several business units or functional teams within an organization to work together as they might during a real-world incident. To understand how organizations use GridEx, the E-ISAC's GridEx Planning Team used the After-Action Survey to capture relevant data. Of the organizations that responded, 96% indicated that their cyber security teams participated in the exercise and 94% indicated that physical security teams participated. Half of respondents engaged their legal teams in exercise play, suggesting that GridEx remains a unique opportunity to exercise internal coordination for asset owners and operators across North America **(Figure 2.3)**.

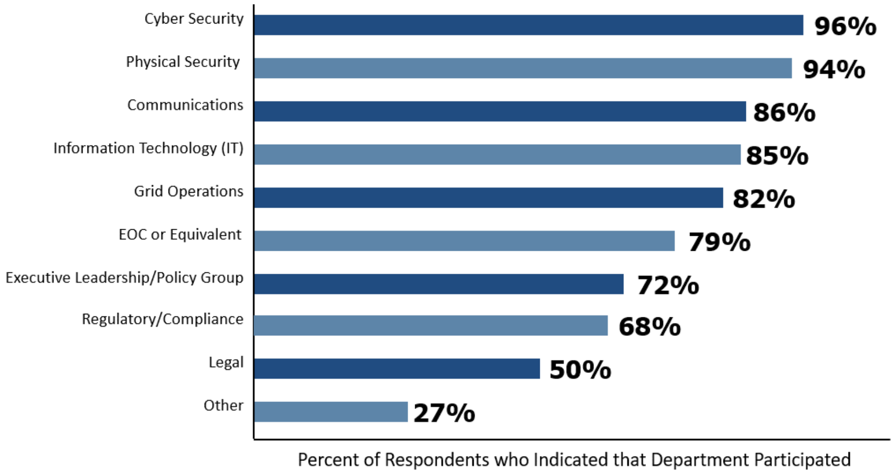


Figure 2.3: Respondents' Internal Participants

GridEx is an opportunity to exercise cyber and physical attack responses with local and regional partners. The After-Action Survey showed the average number of external partners with which planners coordinated to be four; however, the median was two. This low median suggests that a small number of entities coordinated with a very high number of external partners, while the remainder coordinated with a low number. The most common external coordinating partners were regional RCs, with 51% of respondents reporting coordination with their RC, and State/provincial governments, with 44% of respondents reporting coordination with State/provincial governments **(Figure 2.4)**.

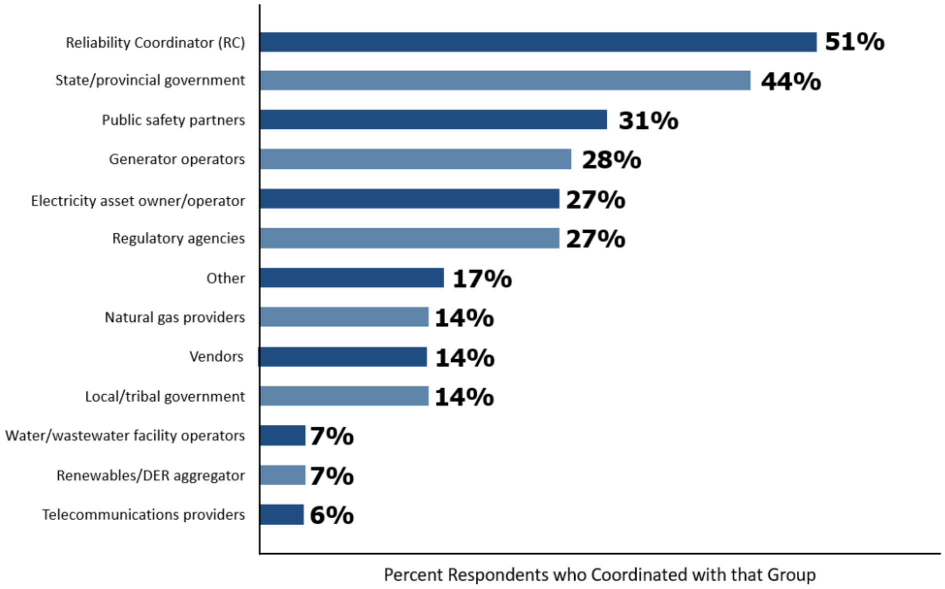


Figure 2.4: Respondent External Coordinating Partners

Respondents reported less coordination with telecommunications providers, renewable/distributed energy resource aggregators, and water/wastewater entities. One goal of the E-ISAC's GridEx Planning Team was to incorporate water/wastewater into exercise play. As such, the GridEx VII scenario included opportunities for water/wastewater coordination. However, only 7% of respondents to the After-Action Survey noted any coordination with external water/wastewater facilities. Multiple respondents also highlighted that they struggled to coordinate with external entities both within and outside the electric utilities industry.

Distributed Play Participation

Participating Organizations

GridEx VII Distributed Play had 252 registered participating organizations across North America and beyond **(Figure 2.5)**. While this is less than the 293 organizations that participated in GridEx VI in 2021, responses to the After-Action Survey suggest that over 15,000 players took part.[9] These player numbers are an estimate, however, because the E-ISAC's GridEx Planning Team only required planners to register for GridEx.

Since the exercise's inception, GridEx participation increased steadily until GridEx VI in 2021. This decrease is likely due to the COVID-19 pandemic and a change in registration requirements. As noted above, the overall number of participating organizations decreased between GridEx VI and VII, but the number of Asset Owner and Operator participants and RCs increased. The total participating organizations decreased due to a reduction in Government/Other[10] participants.

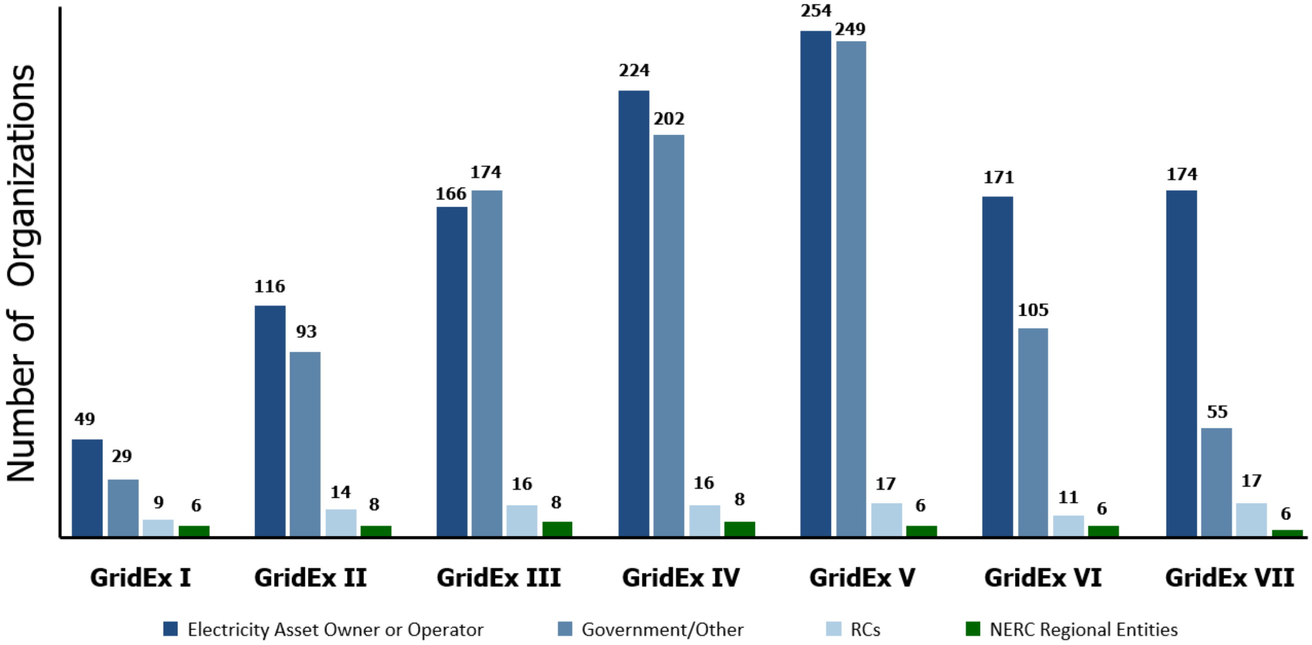


Figure 2.5: GridEx Participation by Category

To register for GridEx, entities must be E-ISAC members, a policy that took effect for GridEx VI. This change in participation requirements may explain the decrease in Government/Other participants. Additionally, organizations coordinated exercise play with entities that did not register to play in GridEx, including natural gas, water/wastewater, and government entities. As a result, the E-ISAC could not track participation from those entities.

The composition of government participants has changed from previous years. For example, in GridEx V, almost half (15% out of 31%) of government participants were from the federal government. However, in GridEx VI and VII, federal government participation decreased. As coordination during Distributed Play is primarily focused on regional (e.g., local/state/provincial) governments, this change in participation was foreseen as federal-level government participation shifts toward engagement with the Executive Tabletop. Municipal government participation also

[9] This number was calculated by averaging the estimated number of players from 70 responses to this question in the After-Action Survey for an average of 61 players per organization. With 252 participating organizations, this is a total of 15,487 players.

[10] Within the "Government/Other" category, "Other" refers to entities such as Regional Entities, trade associations, regulators, and laboratories.

decreased from GridEx V through GridEx VII **(Figure 2.6)**. Industry participants should seek to expand engagement with local, state, and provincial partners to build collective understanding of grid security incident response.

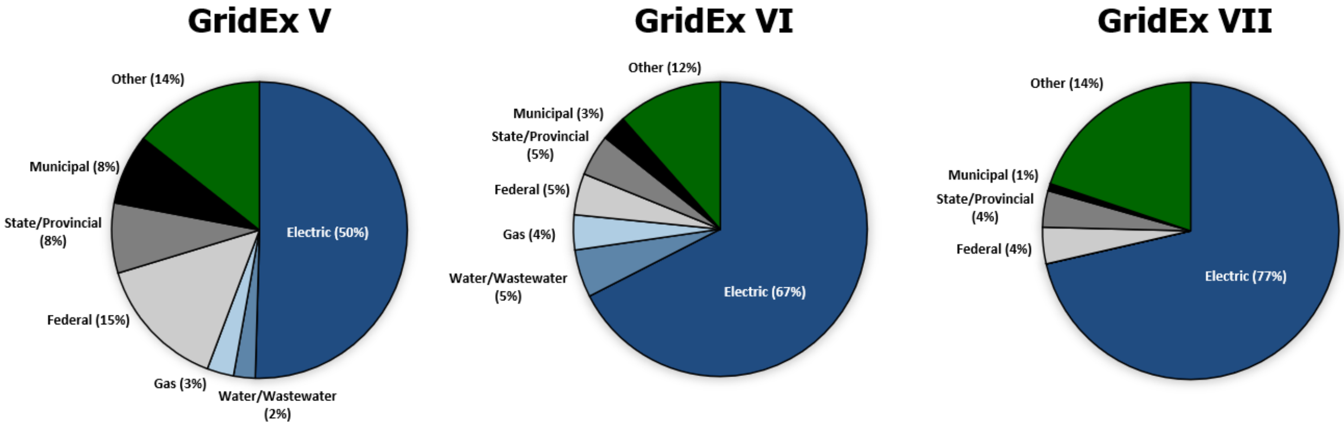


Figure 2.6: Participating Organization by Type

Natural gas and water/wastewater participation also changed. These entities made up a small portion (less than 10%) of participating organizations in GridEx V and VI, while in GridEx VII no entities that provide exclusively natural gas or water/wastewater services registered to participate.[11]

Participant Geography

GridEx involves participants from across North America and beyond. In total, entities from 44 U.S. states, seven Canadian provinces, Mexico, and New Zealand participated in GridEx VII **(Figure 2.7)**. Although many participating entities, such as RCs, operate in multiple states, **Figure 2.7** only represents the state/province/territory/country where the entity is headquartered.

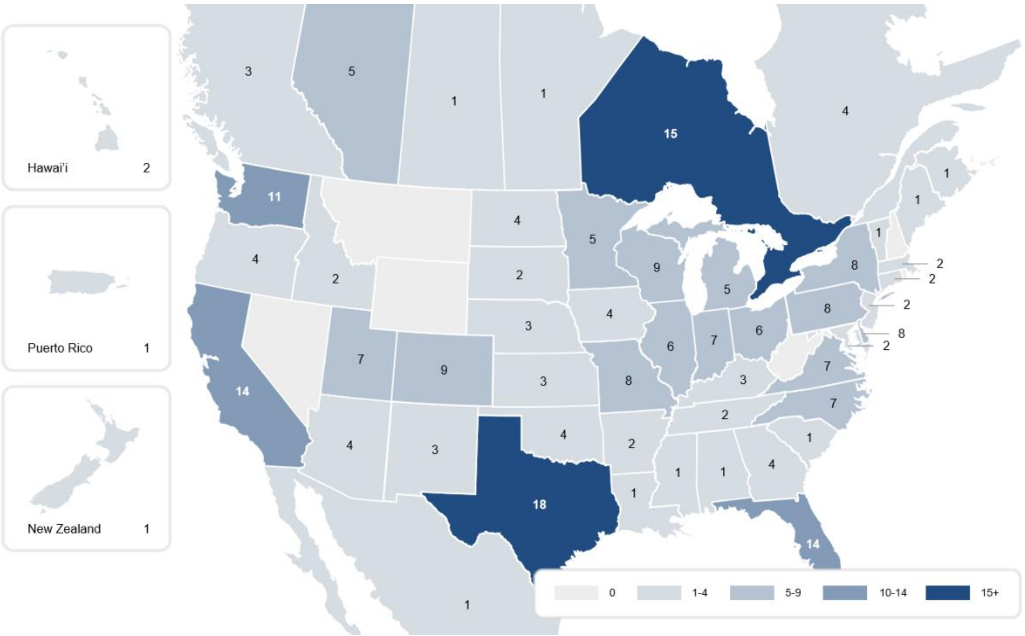


Figure 2.7: GridEx VII Participating Entities

[11] Participating utilities that provide various services, such as natural gas or water/wastewater along with electricity, have been counted as electric utilities.

The geographic composition of participants was similar between GridEx VI **(Figure 2.8)** and VII, with more populous states/provinces seeing higher participation. Outside North America, both exercises included participants from New Zealand, and GridEx VI also had a participating entity from Bermuda.

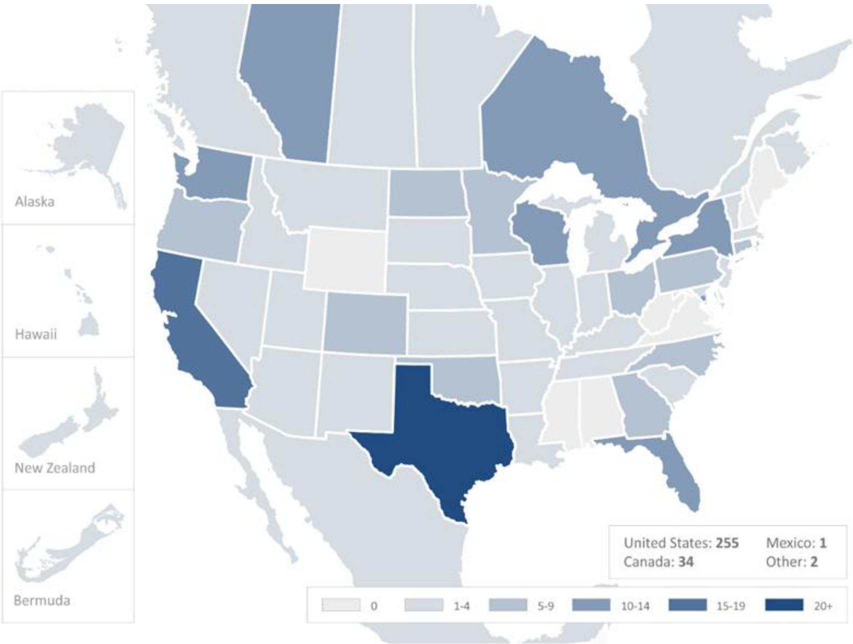


Figure 2.8: GridEx VI Participating Entities

Participating organizations represented all six Regional Entities in GridEx VII **(Figure 2.9)**. El Centro Nacional de Control de Energía, the RC structure for Mexico, also participated in GridEx VII.

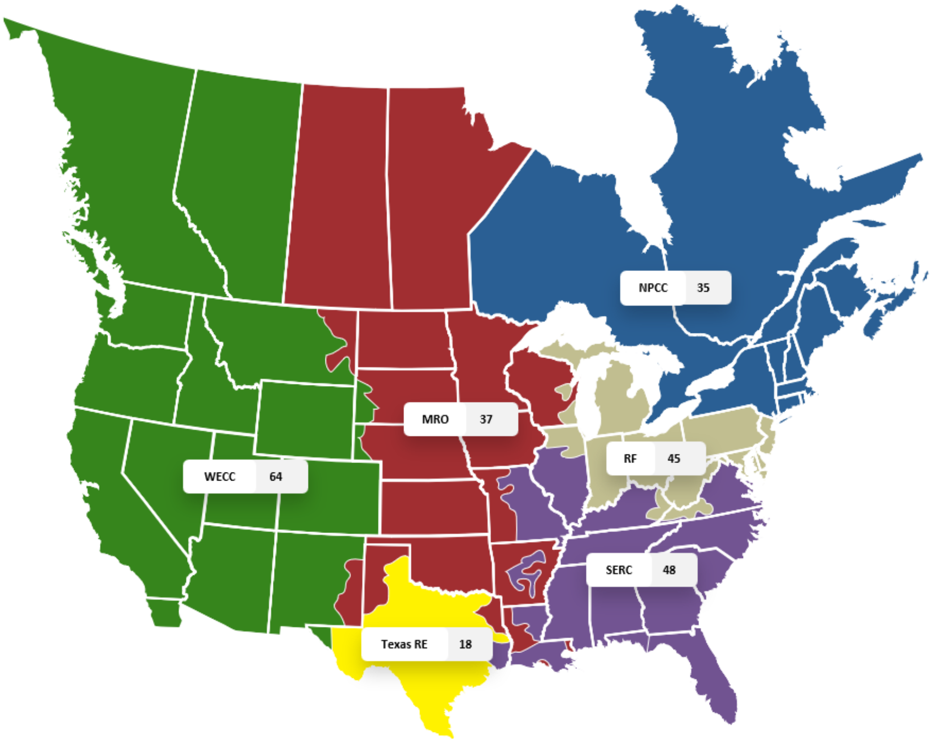


Figure 2.9: Participation by Reliability Entity

Distributed Play Recommendations

The following recommendations were developed based on the feedback provided by planners in the After-Action Survey, feedback received through exercise design, and engagement data collected by the GridEx Planning Team through exercise design and conduct.

These overarching recommendations are made with the understanding that, while many entities are already pursuing the recommendations, the recommendations do not apply equally to all entities. Nonetheless, the recommendations seek to both enhance the resilience and security of the North American BPS and improve the design and conduct of future GridEx iterations.

Recommendation 1: Non-federal government partners and electric utilities should advance coordination efforts.

Background

Electric utilities and government partners should continue proactive engagement with one another in emergency response preparation. GridEx is an opportunity for regional governments to collaborate with electric utilities, increase mutual understanding, and identify critical interdependencies. Owing to the nature of electric utility footprints, GridEx often transcends state, provincial, and county jurisdictions and involves response partners that may not otherwise exercise together.

One planner noted that their organization usually coordinated at the county level and, as such, would coordinate with county emergency managers. This approach aligns with the National Incident Management System (NIMS),[12] which advocates that emergency management is generally best coordinated from a "bottom-up" approach. However, during GridEx VII, this planner realized it was not feasible to communicate individually with each county's emergency management office in an incident that spanned many counties.[13] This case demonstrates the need for a state-level process for coordination and communication, including the ability to request assistance from law enforcement during a large-scale incident.

As noted above, Distributed Play participation saw an overall reduction in the number of government entities that participated in GridEx VII as compared to GridEx VI. The makeup of these government participants also changed, primarily as a result of reduced municipal government participation. Responding to a grid security incident will likely require involvement from government partners at all levels. However, it is particularly important for municipal government entities, such as city, town, and county governments, to be involved in emergency response planning, training, and exercises such as GridEx, considering that these entities may be the first level of government responding to a real-world incident.

State energy offices could also benefit from greater participation in GridEx. In 2021, the bipartisan infrastructure law required all states to submit state energy security plans to receive federal financial assistance. These plans assess threats and vulnerabilities to the energy system in each state and are typically authored by the states' energy offices. The requirement places a renewed emphasis on the role of state governments in responding to energy disruptions. Given the level of coordination necessary for a large-scale incident and the evolving risk to the energy sector, it is important that electric utilities and entities from all levels of government advance their coordination efforts for energy disruptions. However, planner registration data indicates that no state energy offices registered to participate in GridEx VII.

[12] First issued in 2004, NIMS is maintained by the Federal Emergency Management Agency and is intended as a guide for all levels of government, nongovernmental organizations, and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. The latest revision was completed in 2017 (https://www.fema.gov/emergency-managers/nims).

[13] One planner responding to the GridEx VII Distributed Play After-Action Survey noted that their organization coordinated with 80 counties during its exercise.

In addition, there was limited evidence of interdependent partners, such as natural gas and water/wastewater asset owners and operators, registering to participate in GridEx VII. The E-ISAC's GridEx Planning Team built coordination opportunities into the exercise by developing an MSEL that referenced impacts to natural gas and water/wastewater partners. It is possible that independent partners participated in GridEx VII alongside local electricity entities without registering separately; however, noting the limited registration to participate from these entities, planners may benefit from more support in identifying and demonstrating the benefit of participation to natural gas and water/wastewater partners.

The GridEx Planning Team provided resources (such as the Planner Directory, which contained a running list of every participating organization, their RC, and the associated planner's contact information) to help planners find local or regional participants. A training webinar dedicated to securing external participation was also provided. Additional support in finding partners and building buy-in could increase external participation.

Recommendations

- **Electric utilities should engage their local and state/provincial government partners in grid security response planning and exercises.** Most electric utilities are likely to coordinate primarily with their local or state/provincial governments and response personnel as opposed to federal partners. GridEx registration data indicated that there is room for greater utility–local government engagement in GridEx activities and beyond. For example, establishing a jurisdiction-wide quarterly coordination meeting or planning smaller, topic-specific exercises with local and county government partners could strengthen mutual understanding and enhance response efforts.
- **Government entities, including municipal government and state energy offices, should expand engagement with electric utilities to enhance GridEx participation and their understanding of grid security impacts.** In a changing operational environment in which the federal government is expecting state governments to engage more on energy security, government entities have a responsibility to engage electric utilities to understand grid security incident response and consequence management. GridEx provides one opportunity for the electric industry and government entities to exercise coordination and communication; however, it is also important that this collaboration extends beyond GridEx. Implementing and practicing coordinated response plans through planning efforts and other exercises is vital to effective and efficient response during an emergency incident. Furthermore, such engagement provides an opportunity for states to raise awareness of their energy security planning efforts.
- **RCs and large utility operators should brief the offices of state governors and state emergency management directors on emergency response plans for a grid-related incident.** While it is important for government entities to further engage with electric sector preparedness plans, larger entities throughout the electric industry should also engage directly with state governments, particularly if leadership is newly elected or appointed.
- **The E-ISAC should continue engaging government partners to encourage their participation in GridEx.** The E-ISAC's GridEx Planning Team should expand efforts to engage state government partners in preparation for GridEx in recognition that GridEx planning serves as an opportunity for electric utilities and state governments to improve mutual understanding of grid security response priorities and responsibilities. This could include further engagement with experienced planners among local, state, and provincial government partners and greater planning coordination with entities such as the National Governors Association (NGA) and National Association of Regulatory Utility Commissioners (NARUC).
- **The E-ISAC should explore options to track non-member participants that do not formally register for the exercise.** Between GridEx V and VI, the E-ISAC changed the requirements to register and participate in GridEx. Starting in GridEx VI, entities wishing to participate were required to have an active E-ISAC Portal account to register. This may have contributed to the decrease in registered participants in GridEx VI, with GridEx VII seeing a similarly reduced number of registered participating organizations compared to GridEx V. However,

evidence suggests that entities such as government and cross-sector partners may still be participating alongside electric utilities during GridEx but not registering due to the changes in requirements. While there has been a reduction in regional government registration, participants still report a high level of engagement with government partners. The E-ISAC should explore alternative methods of tracking "non-registered" participants to ensure the most accurate account of participation in GridEx. Exploring alternative methods for GridEx participation may help ensure that GridEx remains accessible to the government and cross-sector partners upon which electric utilities rely.

Recommendation 2: Communications and response in a hybrid work environment should be further refined.

Background

GridEx VII marked the second GridEx to be held after the onset of the COVID-19 pandemic, and participating organizations have greater familiarity with hybrid response environments that involve both in-person and virtual response. Nonetheless, organizations are still identifying the best practices for hybrid communications.

After COVID-19 began, organizations made different decisions about managing in-person and remote work, and it may no longer be possible for all responders to meet in a single room to coordinate. Consequently, it is important to continue developing best practices for response in a hybrid environment. GridEx VII provided an opportunity to test hybrid response protocols during two days of intense exercise play. For example, one organization planned for remote and in-person response by identifying a secure information-sharing system for its executive team. However, during GridEx VII, some players realized that not everyone who needed to share sensitive information had the necessary access to the software, demonstrating the challenge of hybrid environments when responding to extraordinary operational circumstances.

Another finding from GridEx VII relating to in-person response exposed the importance of identifying a backup location for in-person staff if the primary location is unusable or inaccessible. For example, one planner noted that the original location identified for in-person response was inaccessible due to simulated public unrest. Given this, the planner's organization determined that a secondary location should be identified, added to applicable emergency response plans, and communicated to personnel and external partners.

Planners also noted the need for interoperable communications with response partners. While organizations often have their own internal communications networks built with systems like Microsoft Teams or Google Workspace, it can be challenging to communicate with external parties on these systems. GridEx provided the opportunity to exercise information-sharing structures and shared accounts in a blue-sky environment. For example, one planner noted that, during GridEx VII, certain substations' 911 calls would be routed to a law enforcement territory outside their actual jurisdiction due to the substations' proximity to the border of two territories. Identifying effective and resilient methods of communication between utilities and response agencies could enhance multi-agency incident response efforts.

Recommendations

- **Organizations should identify and establish an interoperable method of communication that can be used internally and externally during a grid security incident.** Given the vast array of platforms and software available to communicate virtually, it can be challenging to find a system that works within and across organizations. Security protocols and access barriers further complicate this issue. These systems should be documented and communicated to all necessary parties. While GridEx provides an opportunity to exercise communications systems, standalone communications-specific drills could ensure that organizations have appropriate communications tools in place.

- **Organizations should identify and articulate a clear plan for primary and secondary in-person response locations.** This information should be documented and communicated internally and to relevant external partners.
- **To create a realistic exercise, planners for GridEx should continue inviting their players to participate as they would in a real-world incident.** In-person and virtual participation that reflects an organization's operational norms will help ensure that the exercise accurately identifies gaps in plans and systems.

Recommendation 3: Response planning should be augmented to ensure comprehension of technical information across functional teams and external response partners.

Background

The ability to communicate accurate and timely information to critical stakeholders when responding to events like those simulated in GridEx is critical. The GridEx scenario touches on technically complex subject matter that can require technical knowledge, which in turn can make it difficult to communicate with non-technical units of an organization and its external partners.

GridEx provides the opportunity to convene personnel from different business units and organizations, including non-electric industry stakeholders, to discuss complex response and restoration of the electric grid. However, communicating technical information can be challenging for non-technical personnel, potentially hampering the response to an incident. Government responders may not have a background in the electric industry and need more support understanding the implications of certain attacks or response actions. The same may be true of non-electric utility partners, such as those responsible for water/wastewater. These organizations may need to have power restored as a priority but not be able to interpret communications from electric utilities.

Just as technical knowledge could make it difficult to communicate with external partners, some planners found that it was a challenge internally as well. Corporate functions such as communications, security, and customer care were not always comfortable with grid security incident response processes, making it difficult for them to support responders and the operational needs of the organization. The Incident Command System, part of NIMS, advocates for common terminology during incident response. Common terminology allows diverse organizations to work together efficiently by clearly identifying organizational functions, resource descriptions, and incident facilities without using colloquial terms, or "jargon." Establishing and distributing guidance for common terminology may help make communications more efficient and effective during an emergency.

One planner also noted that, beyond the platforms used to communicate internally and externally, different utilities within the same area each have their own organizational response plans, each with their own thresholds and terminology, which can make coordination across utilities more difficult. One organization noted that emergency response protocols were not well understood by all responders and used GridEx VII as an opportunity to share and validate these procedures. As a result, planners identified cross-functional education as a key outcome from their GridEx VII.

Recommendations

- **Organizations within the same area should share information and organizational plans, such as emergency operations plans or handbooks, to establish a common operating picture.** Regional Entities and RCs could benefit from supporting or even leading this coordination.
- **Asset owners and operators should consider developing internal training for non-technical personnel to provide a base understanding of technical but critical topics.** This is especially pertinent for communications personnel and organizational leadership. Existing external training is also available to provide personnel with additional knowledge of critical topics, particularly regarding incident response. The Federal Emergency

Management Agency (FEMA) has a full catalog of freely available online courses that cover topics such as the Incident Command System (ICS) and cyber basics for personnel throughout an organization.

- **Develop or review existing standards for communicating critical response information across organizations' work functions.** The GridEx scenario identified technical topics that required additional context or explanation when communicating within and between organizations. Exercises are a good opportunity for organizations to identify areas of common confusion. Organizations should identify these areas, standardize communications protocols regarding any issues, and train on them so they are expected and understood.

The preceding three recommendations are focused on industry-related improvements, whereas recommendations 4 and 5 below focus on improvements related to GridEx exercise planning and development.

Recommendation 4: The E-ISAC should continue to evolve its support for planners from organizations of varying sizes and with different levels of experience.

Background

While GridEx is open to organizations of all sizes, the E-ISAC recognizes that smaller asset owners and operators are a crucial part of the BPS and is committed to enabling their participation. Although the E-ISAC's GridEx Planning Team provided guides, webinars, and template materials, feedback from the After-Action Survey indicated that some smaller organizations and newer exercise planners would have benefited from additional support and guidance to scale their GridEx appropriately. Conversely, more experienced planners noted that additional materials and training on those resources could better help them develop more complex exercise play.

The GridEx Planning Team delivered the MSEL—a key document provided to planners that provides a detailed narrative to drive exercise play—earlier in the planning process than in GridEx VI. Many planners noted that receiving the MSEL earlier benefited their planning process, allowing them to begin developing their GridEx exercise earlier. The GridEx Planning Team sought to ensure that the MSEL included injects that were applicable to all participating entities, spanning small rural electric cooperatives and large transmission organizations. The resulting MSEL was complex and may have been challenging to navigate, particularly for new planners or smaller organizations.

For GridEx VII, the MSEL included a restoration-focused, discussion-based Move 4, which included discussion questions for planners to tailor to their organizations. One planner noted that this element of the exercise allowed their organization to consider long-term restoration and recovery efforts, which they had not been able to do previously. Planners provided positive feedback to the E-ISAC on Move 4, and this may be an area for further innovation.

Recommendations

- **The E-ISAC's GridEx Planning Team should explore approaches to packaging key materials, such as the MSEL and the Planner Handbook, by the final planning meeting (FPM) to increase usability for organizations with fewer resources or new planners.** Versions of these materials will still include detailed information necessary for well-resourced and experienced organizations to develop challenging exercises, while alternative versions will cater to organizations with fewer resources or newer planners.
- **The E-ISAC's GridEx Planning Team should update the training webinars to contain more of the content that planners find particularly helpful.** Content might include additional tutorials on Exercise Tools, such as SimDeck, or expanded explanations of inject supporting material. The E-ISAC's GridEx Planning Team should

also continue to highlight planning perspectives from asset owners and operators and from other types of participating organizations, such as RCs.

- **The E-ISAC's GridEx Planning Team should continue exploring innovative exercise structures.** The recovery-focused, discussion-based Move 4 appeared to be valuable to participants. The E-ISAC's GridEx Planning Team should consider other format customization by the Midterm Planning Meeting (MPM) for planners to make meaningful adaptations to GridEx play.
- **The E-ISAC's GridEx Planning Team should seek to understand why some organizations have stopped participating in GridEx.** This could include direct outreach prior to the Initial Planning Meeting (IPM) to entities that previously participated in GridEx but have not participated in recent iterations. Understanding their rationale may also help the E-ISAC's GridEx Planning Team identify barriers to participation and mitigate them for future iterations.

Recommendation 5: Cyber and technical components of the GridEx scenario should continue to be developed and expanded for future iterations of GridEx.

Background

GridEx is a grid security exercise that focuses on cyber and physical attacks on the grid and has been designed to reflect the current threat landscape. In accordance with this threat, the E-ISAC's GridEx Planning Team developed an MSEL with both cyber and physical attack components to the scenario. The Idaho National Laboratory notably assisted the GridEx Planning Team with developing realistic, detailed cyber components for the MSEL.

However, several planners responding to the After-Action Survey noted that they would have benefited from more intricate and complex cyber injects and associated materials, such as examples of indicators of compromise for cybersecurity players to investigate. Conversely, some planners noted that they were not comfortable using the cyber-related material because they did not have the necessary subject matter expertise. Irrespective of comfort level, the After-Action Survey indicated that cyber incident response formed a core component of many GridEx exercises, demonstrating the importance of the GridEx Planning Team responding to the threat environment and participant need by developing appropriate cyber material.

Recommendations

- **The E-ISAC's GridEx Planning Team should continue to develop complex cyber injects within the MSEL to allow planners to create a robust cyber scenario if appropriate for their organization.** While not all organizations will use complex cyber injects, the GridEx Planning Team will work with cyber subject matter experts to ensure that organizations that do wish to exercise a more robust cyber scenario are provided with cyber injects prior to the FPM that allow for a sophisticated and challenging exercise.
- **The E-ISAC's GridEx Planning Team should provide more detailed guidance on cyber-related injects and inject supporting material for planners.** The GridEx Planning Team will prepare uniform cyber injects with coinciding guidance from subject matter experts on how to use and implement the injects and accompanying inject supporting material. This will provide planners with a better understanding of how each inject and supporting material can be used and employed during the exercise.

Chapter 3: Conclusion and Next Steps

GridEx VII provided an opportunity for the E-ISAC's members and their partners to exercise grid security response in the face of simulated cyber and physical attacks from a nation-state adversary. The E-ISAC's GridEx Planning Team has identified a series of recommendations to enhance the resilience of the grid and improve the delivery of GridEx VII.

Executive Tabletop Next Steps

At the conclusion of the Tabletop, participants agreed that the Tabletop helped reinforce the need to continue building on the collaborative relationships between the electric, natural gas, and communications industries and government.

In preparation for the GridEx VIII Tabletop, the E-ISAC reconvened Tabletop participants in March 2024 to validate the recommendations listed in this report and gain consensus from industry and government leaders. With consensus from participants and planners, the Planning Team proposed the following preliminary next steps in anticipation of GridEx VIII:

- Tabletop participants from the ESCC and EGCC should review the recommendations in this report and provide strategic direction (e.g., priority, scope, timing) to industry and government groups that will work to address the recommendations.
- NERC, through the E-ISAC, is committed to continue enhancing the GridEx program to meet the challenges posed by the ever-evolving threat environment. The E-ISAC will work with industry and government partners to consider the following suggestions made by participants for the next Tabletop:
    - **Resilient Communications:** Explore options to enhance the resilience of ESCC communications
    - **Interdependencies with the Natural Gas and Communications Sectors:** Build on the positive contribution of the natural gas and communications participants at GridEx VII by inviting a similar or enhanced level of participation to the next Tabletop
    - **North American Scope:** Continue to attract industry executives and senior government officials from the appropriate U.S., Canadian, and Mexican entities
    - **State and Provincial Government Participation:** Continue to encourage the participation of state and provincial government representatives consistent with their prominent roles during regional emergencies
    - **Policy and Operations:** The GridEx VII Tabletop successfully addressed policy matters within the context of operational realities without unnecessary technical details. The next Tabletop should continue this approach with a scenario that includes the following components:
        - Is regional in scope, involves the United States and Canada, and considers the extent to which the recommendations in this report have been addressed
        - Helps the industry understand how government authorities may assist the industry through a large-scale crisis
        - Focuses on a few key issues similar to GridEx VII
        - Supports a virtual format with breakout sessions to simulate communications during a real event, as was done during GridEx VII

Distributed Play Next Steps

While some of the recommendations in this report apply to entities across industry and government, the E-ISAC will be exploring the following next steps derived from Distributed Play with the intent of enhancing the impact of GridEx VIII exercise play:

- **Engagement:** The E-ISAC will explore ways to further engage partners in the design and delivery of and participation in GridEx VIII:
  - During GridEx VIII planning, the E-ISAC will expand endeavors with electric asset owners and operators to encourage more engagement and coordination with government partners.
  - The E-ISAC will also increase outreach to government partners during GridEx VIII planning with the intention of involving government partners more throughout the planning process and connecting government partners to appropriate electric utility partners.
  - Prior to the commencement of registration for GridEx VIII, the E-ISAC will explore alternative methods of tracking non-registered participants.
  - Using participation metrics collected over the past several GridEx iterations, the E-ISAC will reach out prior to the beginning of GridEx VIII planning to organizations whose participation in GridEx has decreased or stopped to better understand the rationale behind the changes in their participation.
- **Accessibility:** The E-ISAC will explore options to make GridEx VIII as accessible as possible for a diverse range of participants, be that utilities, interdependent partners, or government entities. This may include repackaging GridEx materials for different scopes of participation and adjusting the webinar series.
  - Prior to the commencement of the GridEx VIII webinar series, the E-ISAC will develop a training curriculum that meets the needs of planners as expressed in the GridEx VII After-Action Survey and GridEx VII webinar surveys.
- **Materials:** During GridEx VIII planning, the E-ISAC will develop materials, such as the MSEL, to be innovative and more accessible to a variety of organizations and capabilities. Redesigned and packaged materials will be communicated throughout the GridEx VIII planning meetings (e.g., IPM, MPM, FPM) to ensure that participating entities are up to date and aware of changes and newly available options. The E-ISAC will pursue opportunities to develop more valuable exercise materials for its members. This may include more robust cyber material and more options to customize the scope, extent, and duration of play in addition to ensuring that the materials that the E-ISAC produces reflect the needs of its diverse membership.
  - During GridEx VIII planning, the E-ISAC will work with cyber subject matter experts to develop cyber injects that are more robust to challenge organizations that desire a more complex cyber scenario while also developing standardized cyber injects with detailed guidance on the use of inject supporting material. All materials will be developed by the FPM, and the E-ISAC will explore the use of a training webinar to provide cyber inject-related training to planners.