GridEx VI

Lessons Learned Report
TLP:WHITE
April 2022

RELIABILITY | RESILIENCE | SECURITY

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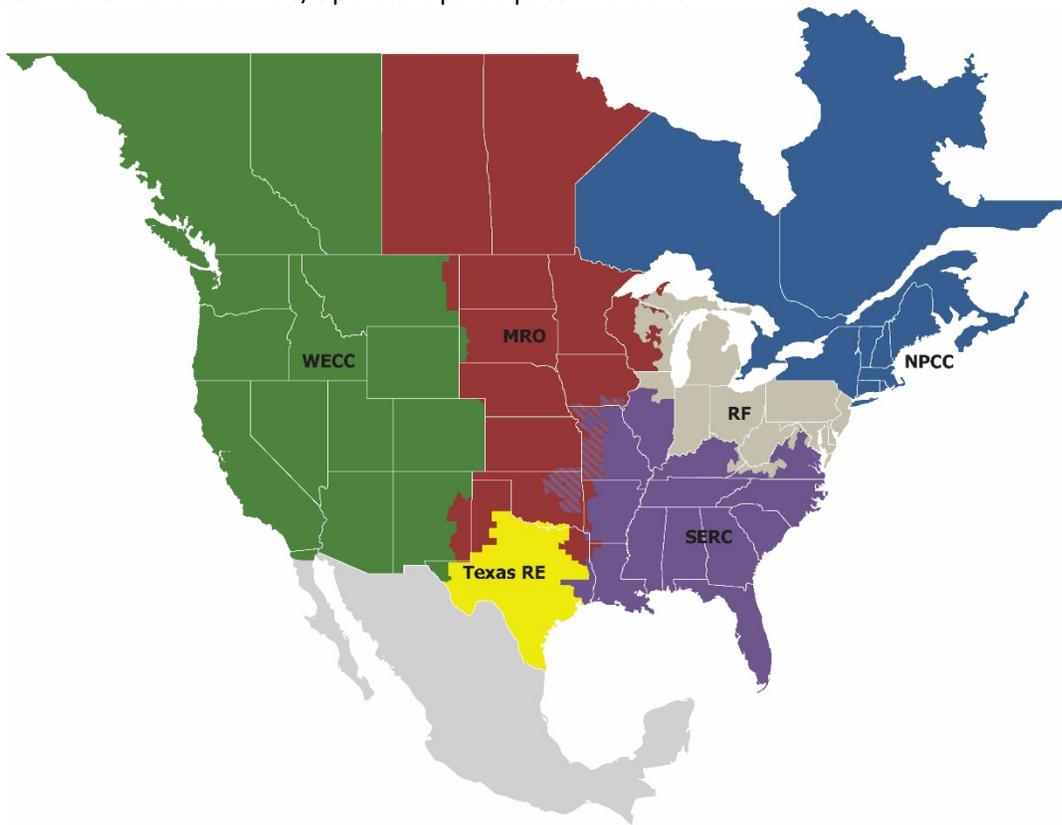
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

NERC conducted its sixth biennial security exercise, GridEx VI, on November 16–18, 2021. This grid security, emergency, and response exercise was developed, managed, and delivered by NERC's Electricity Information Sharing and Analysis Center (E-ISAC).

The E-ISAC divided play into two portions: Distributed Play, held on November 16–17, 2021, provided the opportunity for operational participants across North America to exercise the resilience of the electricity system. The Executive Tabletop, held on November 18, 2021, convened industry executives and government leadership from the United States and Canada to explore the challenges presented by a severe cyber and physical attack against the grid.

The E-ISAC challenged operational and executive participants with a single scenario that began during Distributed Play and concluded during the Executive Tabletop in which a nation-state adversary targeted the North American grid with coordinated cyber and physical attacks. GridEx VI provided participants with the opportunity to exercise their response and resilience measures and identify opportunities for advancement, fulfilling NERC's mission to assure the effective and efficient reduction of risks to the reliability, resilience, and security of the grid.

GridEx VI Goals

The GridEx series is an opportunity to explore and exercise grid security and emergency issues across North America. The E-ISAC developed distinct goals for the Executive Tabletop and Distributed Play, recognizing that the former focused on continent-wide executive and senior leadership response while the latter focused on operational response activities. The goals and underlying objectives are available in **Appendix A: Exercise Goals and Objectives**.

> **GridEx VI Executive Tabletop Goal:** Engage senior industry and government leaders in a comprehensive discussion of U.S. and Canadian security issues, extraordinary operational measures, and coordinated decisions needed to protect and restore the grid

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

- Strengthen the coordinated response to U.S. and Canadian national security implications of supply chain attacks on systems and software

- Enhance industry coordination with U.S. and Canadian federal and state/provincial governments

- Enhance electricity industry response coordination with the natural gas and telecommunications sectors

- Explore the public communications challenges that result from misinformation and disinformation

- Explore emerging security and resilience implications related to changing generation fuel mixes (traditional and renewable)

- Build consensus between the electricity industry and governments regarding the development, issuance, liability protections, and international implications of grid security emergency (GSE) orders

> **GridEx VI Distributed Play Goal:** Exercise the resilience of the North American electricity system in the face of a coordinated attack from a nation-state adversary

Organizations participating in Distributed Play typically developed exercise objectives specific to their organization's needs. The E-ISAC identified the following objectives to meet the GridEx VI Distributed Play goal:

- Activate incident, operating, and crisis management response plans

- Enhance coordination with government to facilitate restoration

- Identify interdependence concerns with natural gas and telecommunications sectors

- Exercise response to a supply chain-based compromise to critical components

- Identify common mode and cyber operation concerns across interconnections

Summary of Executive Tabletop Recommendations

Chapter 3: Observations and Recommendations provides a detailed explication of each recommendation and its associated actions. The high-level recommendations emerging from the Executive Tabletop are below:

1. **Continue to build effective communications procedures and systems to share operational information.** The electricity industry has robust grid monitoring and control capabilities that have withstood the test of emergency situations over decades of operation. However, the Tabletop scenario presented conditions that severely strained the industry's ability to communicate operational status to their many external stakeholders, including state/provincial and local government. In addition, the scenario's involvement of a nation-state adversary added a layer of complexity regarding how and with whom to share highly sensitive information.

2. **Clarify the differing crisis communications roles of the Electricity Subsector Coordinating Council (ESCC) and Reliability Coordinators (RC) with government and their members, including Canadian members.** Given the cross-border nature of the scenario, the U.S. and Canadian federal governments would be involved with the electricity industry, introducing a level of crisis communication not needed since the 2003 Northeast Blackout. While the ESCC can facilitate some of this communication, the directly-impacted RCs and utilities would be responsible for ensuring timely and effective communication and action.

3. **Continue to build effective communications procedures and systems to share security information.** Federal government mechanisms to share potentially sensitive security information with the electricity industry are challenging during normal conditions. These mechanisms would be severely strained by the incidents described in the scenario. A mutual understanding of specifically what information would be shared and how in a timely and effective manner will start to address this concern.

4. **Continue to build on understanding of GSE order development and consultation processes.** The Department of Energy's (DOE) GSE authorities are of great interest and importance to the electricity industry. During the Distributed Play portion of the exercise, several RCs used the GSE scenario inject and indicated it helped them better understand the consultation and order development process. The Tabletop discussion indicated that the U.S. electricity industry and DOE have made progress in developing a common understanding of the consultation process and initiated the discussion of possible elements that would be included in a GSE order. DOE and industry should also consider the impact of GSE orders on the natural gas industry and other critical infrastructure sectors. The recently established Energy Threat Analysis Center, which includes representatives from DOE and industry, can provide useful context during the development of a GSE order.

5. **Continue to enhance routine and emergency operations coordination between the electricity industry and natural gas providers.** The scenario included disruptions of natural gas to generating stations. Compared with the previous Tabletop two years ago, the discussion benefitted from the more robust participation of natural gas operators, the Oil and Natural Gas Subsector Coordinating Council, and natural gas trade associations in the United States and Canada.

6. **Strengthen operational coordination between the electricity industry and communications providers.** The critical interdependencies between the electricity and communications sectors are well-understood and have often been a prominent component of the GridEx series of exercises. This time, the Tabletop scenario featured a widespread loss of landline and cellular communications while electricity utilities were recovering from the cyber and physical attacks and restoring the grid. Participants agreed that the loss of communications would essentially halt the grid restoration process.

7. **Continue to reinforce relationships between governments in the United States and Canada to support industry response to grid emergencies.** Given the cross-border scope of the scenario, the Tabletop discussion was enhanced by the robust participation of senior officials from the Canadian federal and provincial governments. Participants gained a better understanding of the roles of Canada's provincial and federal governments during a grid emergency and how they differ from those of their U.S. counterparts.

Summary of Distributed Play Observations

A more detailed explanation of Distributed Play observations and their associated recommendations is included in **Chapter 3: Observations and Recommendations**. The high-level observations identified by exercise Planners and the GridEx Planning Team during GridEx VI's Distributed Play are listed below:

1. **Exercise Conduct:** Flexible exercise conduct options enabled Planners from a wide range of participating organizations to design and conduct an exercise that met their organization's needs as well as collaborate with other entities.

2. **Planning Material:** The GridEx Planning Team provided planning materials that offered significant value and reflected maturation in the GridEx series, but the delayed publication of certain materials limited their value.

3. **Exercise Tools:** The exercise tools enabled thousands of Players to communicate and coordinate during the exercise. Some Planners shared that they would have appreciated more information about the exercise tools during the planning process.

4. **Training Webinars:** Planner and Player training webinars effectively shared information, resources, and examples with Planners and Players in the lead-up to the exercise.

5. **Partnering with External Organizations:** Utility Planners who were part of their RC's planning process were particularly pleased with how their RC helped develop a realistic and inclusive scenario.

6. **Communications:** GridEx VI communications and resource sharing were effective tools that supported Planners throughout the planning process.

7. **NERC Play:** NERC formally participated in GridEx VI as a player and included members from the E-ISAC Watch Operations, NERC Bulk Power System Awareness (BPSA), and the ERO Communication Group, providing a valuable exercise opportunity.

Introduction

This report summarizes the recommendations identified during GridEx VI's operational and executive exercise activities, in addition to offering information on the design, delivery, and participation across both exercises. The Distributed Play portion of GridEx VI was held on November 16–17, 2021, and the Executive Tabletop portion on November 18, 2021. In previous iterations, the Distributed Play and Executive Tabletop portions were held concurrently. Responding to feedback from GridEx V, the E-ISAC bifurcated GridEx VI and developed a contiguous scenario across the two exercises.

The GridEx VI scenario centered on a nation-state adversary leveling cyber and physical attacks against the North American grid. The Tabletop scenario centered on the response to cyber and physical attacks that caused significant reliability, resilience, and security issues impacting the West Coast of the United States and Canada in addition to impacts relating to natural gas and telecommunications interdependencies as well as cross-border communications. The scenario exercised a declaration of a GSE and potential issuance of a GSE order. Incidents during Distributed Play involved nationwide impacts, including explosions tripping generators off-line, cyber attacks against industrial control systems, and physical attacks on pipelines and liquid natural gas production facilities.

The E-ISAC developed the scenarios for both Distributed Play and the Tabletop with input from colleagues at national laboratories, impacted utilities, and experienced Planners from participating organizations. The E-ISAC supported GridEx VI Distributed Play participants by developing a core exercise scenario and exercise material in addition to holding a webinar series to guide Planners through the exercise planning process. Recognizing the international scope of the exercise and the challenge of capturing all organizations' needs, the E-ISAC encouraged Planners from participating entities to customize the exercise narrative to fulfill their organization's exercise objectives and organizational priorities. Each participating organization was responsible for managing the delivery of the exercise within their organization. Consequently, each participating entity had a unique exercise experience.

The GridEx VI Executive Tabletop was held virtually for the first time, enabling wider participation from those entities responsible for responding to or managing the ramifications of the exercise scenario, such as natural gas and telecommunications partners. The day-long event was facilitated by Brock Long, executive chairman of Hagerty Consulting and former administrator of the Federal Emergency Management Agency (FEMA).

Methodology

Members of the GridEx Planning Team that designed the Tabletop scenario and observed the event identified the Executive Tabletop recommendations outlined in this report. The GridEx Planning Team drew on observations during the session and discussion points raised during a Tabletop Hot Wash for participants on November 19, 2021, to develop the recommendations in this report.

In developing observations and recommendations for Distributed Play, the E-ISAC asked Planners to complete an After-Action Survey, providing qualitative and quantitative feedback on their exercise planning and conduct experience. This feedback was supplemented by a Planner Town Hall series to which a representative selection of Planners were invited to share their views. Owing to the nature of Distributed Play, the Distributed Play elements of this report focus on observations and recommendations related to exercise planning and execution as opposed to the objectives and lessons learned that were unique to each participating organization.

Each chapter of this report leads with items related to the Executive Tabletop in recognition of the potential for North American-wide policy ramifications of the recommendations identified.

Chapter 1: Participation

Executive Tabletop Participation

The GridEx VI Executive Tabletop saw executives and leaders from 88 organizations, and almost 200 individuals in total, join the Tabletop. Participants included senior representation from U.S. and Canadian government entities and executive leaders representing U.S. and Canadian cooperatives, investor- and publicly-owned utilities, and independent system operators.

The E-ISAC took steps to diversify participation in GridEx VI to account for a wider range of perspectives when exploring the Tabletop scenario as reflected in **Figure 1.1**. This resulted in greater participation from interdependent industries, such as natural gas and telecommunications, an active role for Canadian Government partners, and wider U.S. Government representation—including representatives from state government. Organizations listed as "Other" include information sharing and analysis centers, Regional Entities, and trade associations.

The active participation of representatives from the Canadian government and interdependent industries in particular added significant value to the Tabletop as reflected in the recommendations.
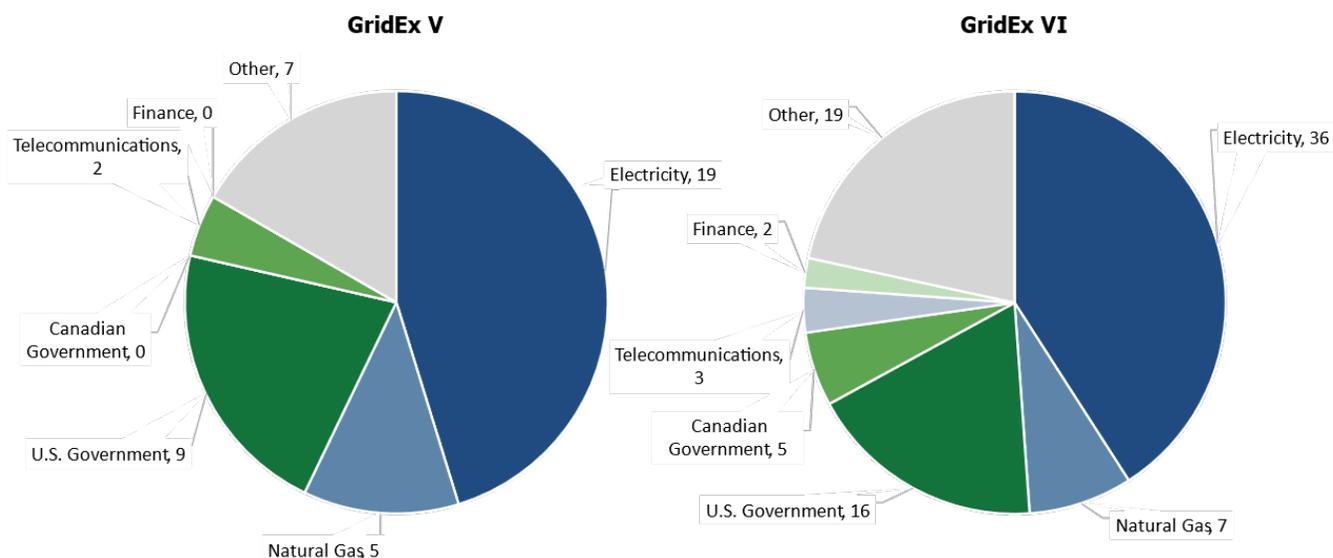
Figure 1.1: Tabletop Participation by Sector, GridEx V to GridEx VI

U.S. and Canadian government representation included the following agencies and departments:

- Canadian Centre for Cyber Security
- U.S. Department of Defense
- U.S. DOE
- U.S. Department of Homeland Security
- Natural Resources Canada
- Public Safety Canada
- U.S. White House (National Security Council)

Representatives from the states of California and Washington as well as the province of British Columbia were also in attendance.

Distributed Play Participation

During GridEx VI, a total of 293 organizations across North America and beyond participated in the exercise, down from 526 organizations in GridEx V (see **Figure 1.2**). Organizations that responded to the After-Action Survey reported that over 3,000 Players participated in GridEx VI compared to 7,000 Players in GridEx V. It is important to note that the reported number of Players in GridEx V is likely higher due to requirements for Players to register for GridEx V that was not a requirement from GridEx VI. Feedback from some organizations that participated in GridEx V but did not participate in GridEx VI cited the coronavirus pandemic and increased threat activity as reasons for not participating. This may have been compounded by exercise planning beginning in Fall 2020, coinciding with a period of increasing COVID-19 case rates globally.

The change in participation from GridEx V to GridEx VI may also be attributed to changes in how participation was measured for GridEx VI. During GridEx VI, individuals were only required to register for GridEx VI if they wished to access planning materials via the SharePoint site or needed to use the exercise tools. In the past, all participants, including Players, were required to register. Given this change, future participation numbers are likely to be more comparable to those recorded for GridEx VI.
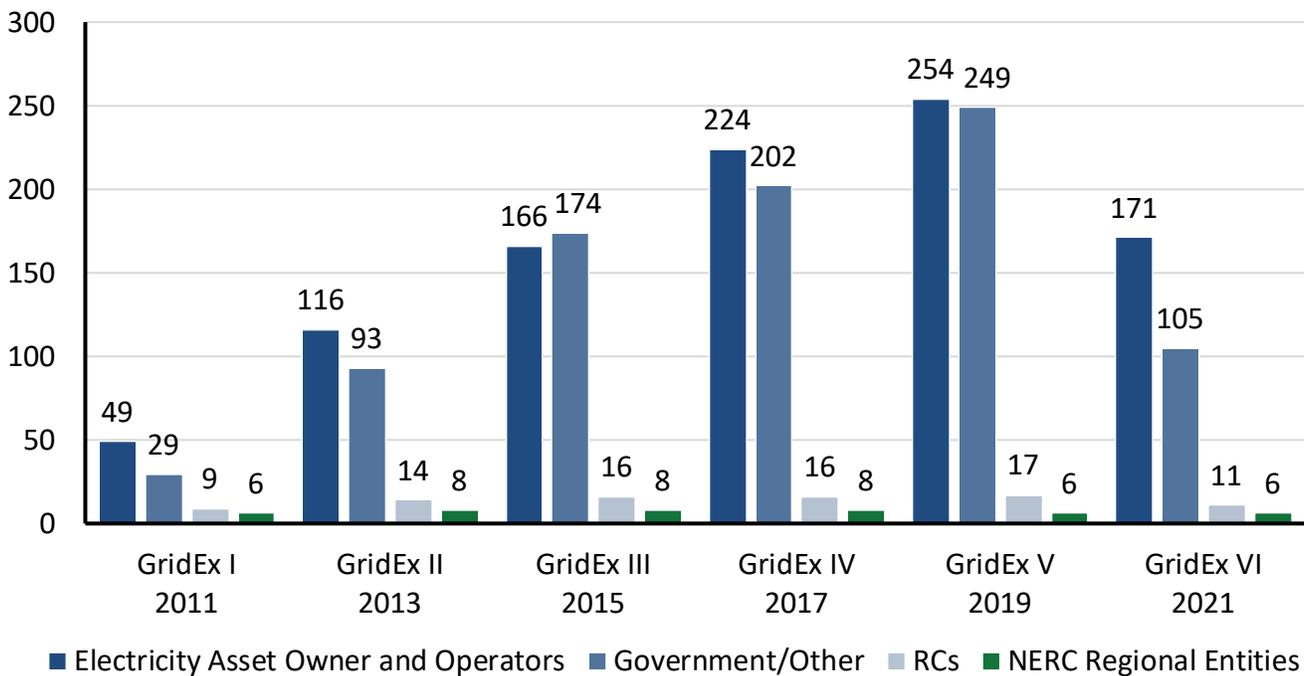
Figure 1.2: GridEx Organization Participation Since 2011

Although the majority of GridEx VI participants came from electricity utilities, other energy companies, such as natural gas utilities and water utilities, were also well represented (see **Figure 1.3**). In addition to energy participants, other organizations from the telecommunications sector, finance sector, and trade associations were also well represented.
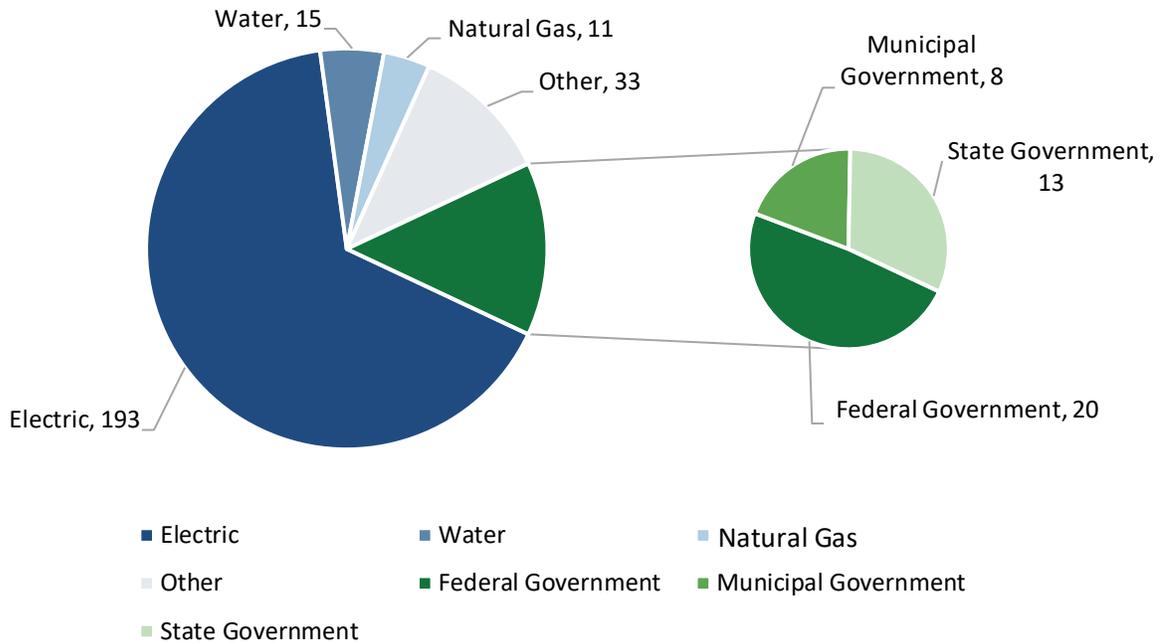
Figure 1.3: GridEx VI Participation by Organization Type

Despite the decrease in participation from previous iterations, GridEx VI still counted participation across the continent and beyond (see **Figure 1.4**). Organizations headquartered in 44 U.S. states, 8 Canadian provinces, and Mexico participated in GridEx VI. Additionally, organizations in Bermuda and New Zealand participated in partnership with other organizations in North America.
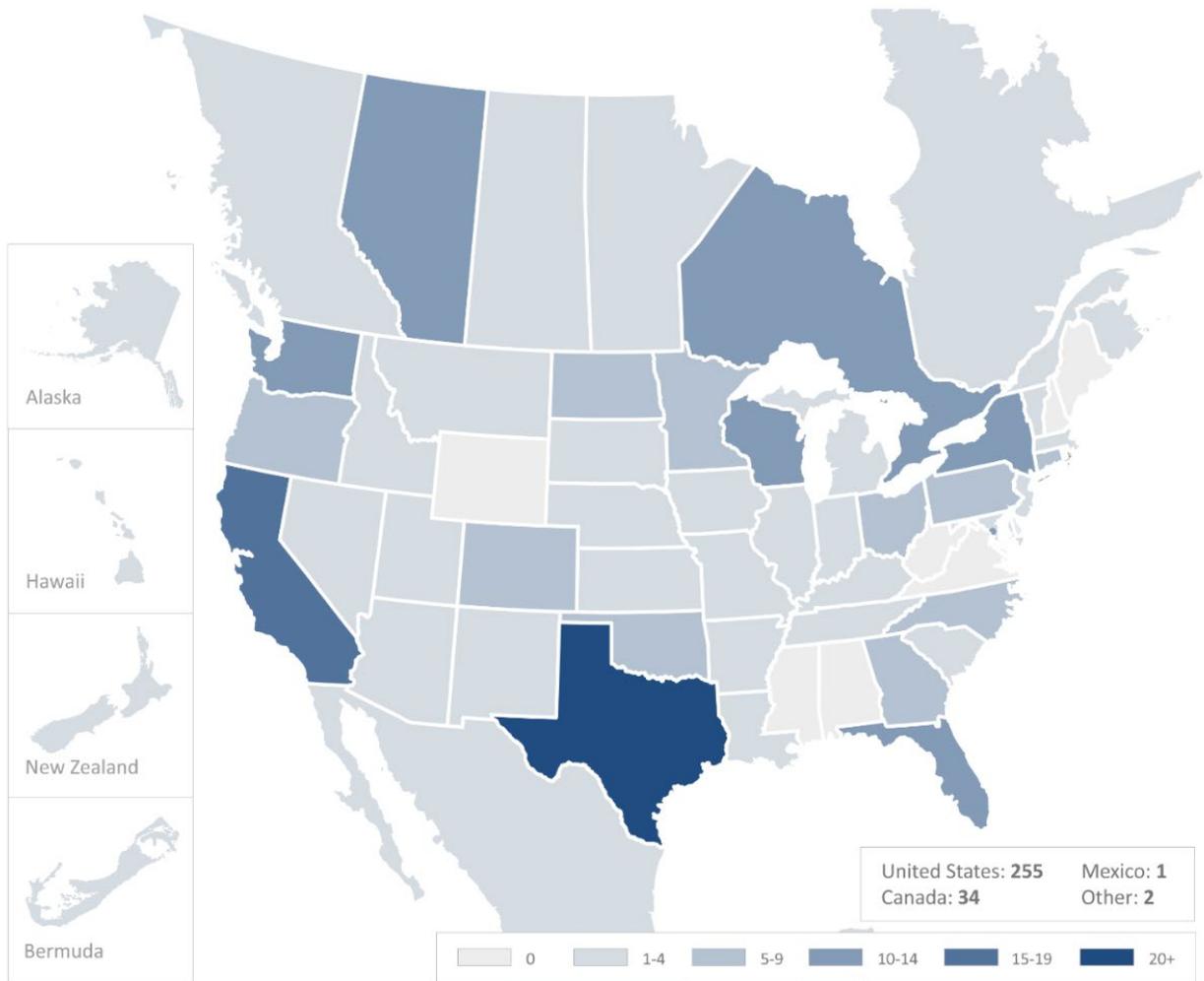
Figure 1.4: GridEx VI Participation by Geography

Chapter 2: Exercise Conduct

Executive Tabletop Scenario and Conduct

The Tabletop scenario prompted participants to assess the impact of serious cyber and physical security attacks and take the actions needed to respond; communicate effectively; restore power; and address serious public health, safety, and grid security challenges. The Tabletop exercise was designed in four phases to simulate how industry and government would respond to a sophisticated, well-coordinated cyber and physical attack. These phases were as follows:

- **Phase 1—The First Hour after the Attacks:** Challenging operating conditions further degrade reliability when the Western Interconnection splits into two islands after a transmission disturbance initially assumed to be caused by wildfires.

- **Phase 2—The Next Morning:** Attacks on electricity and natural gas infrastructure cause widespread power outages affecting many high-priority customers, including defense-critical facilities.

- **Phase 3—Later that Day:** Telecommunications disruptions impair power system restoration activities and complicate coordination with government. Wind generation resources are disrupted by widespread control and response issues.

- **Epilogue—Two Weeks and Beyond:** The Western Interconnection is restored and customer load is eventually reconnected, but energy and capacity margins are tight for the foreseeable future. Active cyber attacks have ceased.

During plenary and breakout sessions, facilitators led participants through discussions designed to simulate the communication and coordination that would occur during a real event.

Distributed Play Scenario and Conduct

Distributed Play Scenario

The GridEx VI Distributed Play scenario saw a nation-state target the North American grid with cyber and physical attacks that spanned two days. Incidents ranged from disinformation on social media to cyber attacks that targeted industrial control systems. The E-ISAC divided the two-day exercise into four Moves. The E-ISAC also developed Move 0, which included optional material in the week preceding the exercise to prepare Players for the incidents that would follow.

The E-ISAC developed a series of physical, cyber, and operational injects in partnership with subject matter experts, expert Planners, and partners from the SANS Institute, Idaho National Laboratory, and the National Renewable Energy Laboratory to ensure that the exercise reflected the complex threat the grid faces today. The E-ISAC developed a scenario and the Master Scenario Event List (MSEL), but the Planners were encouraged to customize the scenario to meet their needs. Consequently, the timing, content, and substance of exercise play varied between participating organizations.

Figure 2.1 provides an overview of the GridEx VI exercise-wide scenario timeline and associated Moves.
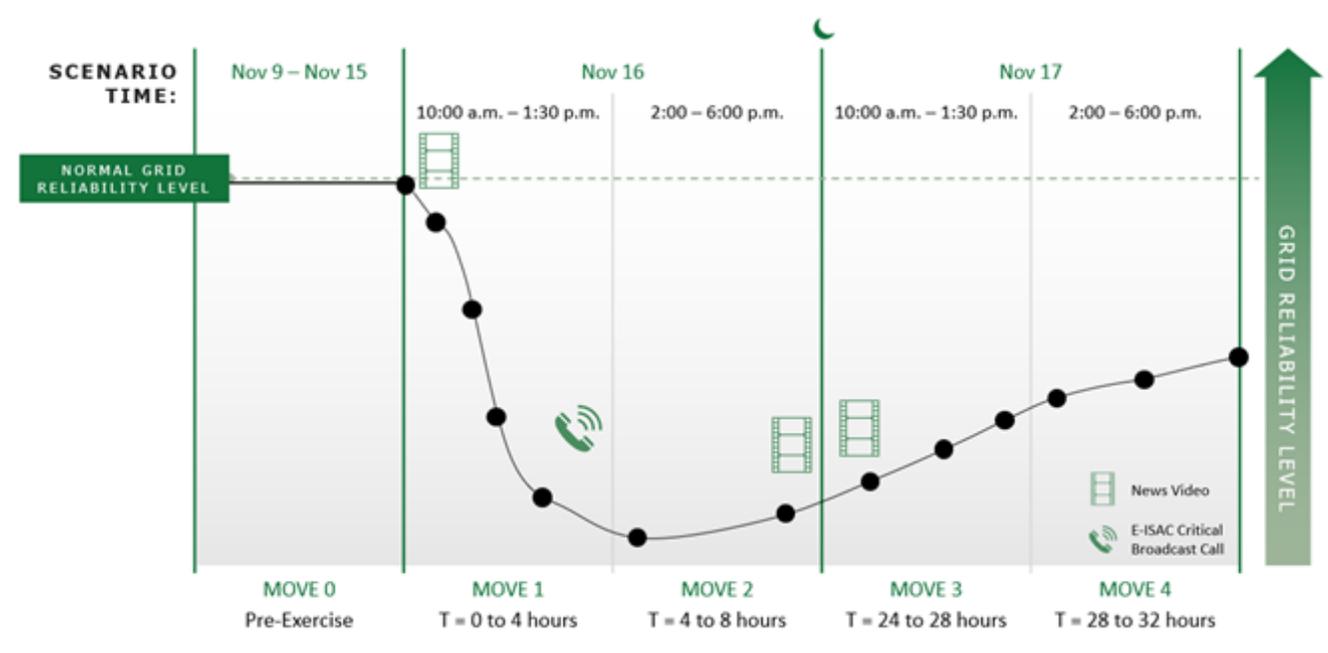
Figure 2.1: GridEx VI Timeline and Moves

The Distributed Play Moves that could be customized by participating organizations covered the following scenario events:

- **Move 0—November 9–15, 2021:** Cyber and physical security threats to the electricity sector emerged across North America. Reports from the E-ISAC, law enforcement, and other government agencies to the electricity industry indicated that adversaries were conducting aggressive cyber and physical reconnaissance of the electricity grid, telecommunications infrastructure, and natural gas facilities across North America.

- **Move 1—The Morning of November 16, 2021:** Control system faults caused generation unit outages across numerous plants followed by transmission substation system faults. Large explosions caused generators to trip off-line and transmission circuit breakers to open at multiple locations near-simultaneously.

- **Move 2—The Afternoon of November 16, 2021:** Physical attacks on pipelines and liquid natural gas production facilities disrupted natural gas supplies to generators, further constraining generation capacity and forcing transmission and distribution operators to shed load. Cyber and physical attacks also targeted telecommunications infrastructure, forcing Players to rely on backup systems.

- **Move 3—The Morning of November 17, 2021:** The adversary directly targeted critical employees, and pseudonymized social media users claimed responsibility for the attacks and threatened further incidents. Operations staff received vague but credible threats against them and their families via robocall. RCs were encouraged to discuss the impacts in case DOE pursued a GSE order that would impact their operations.

- **Move 4—The Afternoon of November 17, 2021:** Further social media threats targeted specific transmission and distribution facilities. Entities implemented emergency operations plans and worked with their partners to recover from the devastating series of attacks.

Distributed Play Conduct

Given the distributed nature of GridEx VI, NERC and the E-ISAC did not stand-up an exercise control function for GridEx VI. However, both NERC BPSA and E-ISAC Watch Operations participated fully in the exercise with NERC Communications department also expanding their participation. The E-ISAC enhanced the exercise experience by hosting a Critical Broadcast Program call for Players at the end of Move 1, and NERC BPSA also hosted a special report exercise update that offered Players a higher degree of collaboration and situational awareness.

It is likely the 2019 coronavirus pandemic impinged on organizations' ability to participate in GridEx VI. For those organizations that did participate, it is possible that the extent of their play may have been reduced by limitations to on-site exercise play and virtual working arrangements. Despite the pandemic, the distributed nature of the GridEx series allowed Planners to organize exercise play to meet the needs of their Players performing the exercise on-site, virtually, or with a hybrid approach.

To support exercise play across North America, the E-ISAC provided two exercise tools for participants: SimulationDeck (SimDeck) and the Exercise Portal. These tools enhanced exercise play by simulating real-world tools and platforms without risking real-world operations and communications.

SimDeck allowed Planners and Players to simulate the various media outlets that Players would interact with as part of their role. For example, public affairs Players could also use the platform to post content, share news clips, or simulate social media. SimDeck also hosted a simulated U.S. DOE Emergency Incident and Disturbance Report (DOE-417), NERC's Event Reporting (EOP-004), and the Reliability Coordinator Information System (RCIS) that allowed Players to simulate industry reporting and collaboration. The E-ISAC also hosted the GridEx VI After-Action Survey on SimDeck.

Additionally, the E-ISAC provided an Exercise Portal that replicated the functionality of the real-world E-ISAC Portal. During the exercise, E-ISAC shared information, such as E-ISAC reports, cyber and physical security bulletins, all-points bulletins, and Critical Broadcast Program calls to the Exercise Portal. Players posted additional information that could impact cyber security, physical security, and the function of operational technology.

Chapter 3: Observations and Recommendations

Executive Tabletop Recommendations

1. **Continue to build effective communications procedures and systems to share operational information.** The electricity industry has robust grid monitoring and control capabilities that have withstood the test of emergency situations over decades of operation. However, the Tabletop scenario presented conditions that severely strained the industry's ability to communicate operational status to their many external stakeholders, including state/provincial and local government. In addition, the scenario's involvement of a nation-state adversary added a layer of complexity regarding how and with whom to share highly sensitive information:

   a. RCs and utilities should review their crisis management plans and assess the extent to which these plans and capabilities may need to be enhanced:

      i. Define the roles of individuals responsible for communicating with employees, industry colleagues, customers, government (including emergency responders and law enforcement), and the media.

      ii. Provide the infrastructure and resources required to support these communications roles through an extended period of continuous 24-hour operation. It is important to ensure that key personnel (e.g., control room operators, field technicians) are not distracted by frequent or burdensome requests for information.

      iii. Understand the nature of the information that will be needed and provided, including information that may be difficult to know with certainty or will change over time and become overtaken by events (e.g., estimated times to restore power to customers, future actions).

      iv. Develop a set of frequently asked questions and response templates that cover a wide range of emergency conditions. Include "as of" or "valid through" times with information and, where possible, indicate the degree of confidence in the information (e.g., "confirmed" or "initial assessment indicates" or "likely that").

   b. Similarly, NERC and the Regional Entities should review their crisis management plans and capabilities and assess the extent to which these may need to be enhanced to remain effective for such an extreme scenario. While NERC and the Regional Entities do not have operational roles, they have intimate knowledge of industry organizations, issues, and technology and can help government entities understand the overall situation and the strategies being employed to restore grid reliability:

      i. Define the roles of individuals responsible for communicating with employees, RCs, utilities, trade associations, the ESCC, the Energy Government Coordinating Council (EGCC), state/provincial and local governments, regulators, and the media. Given the diverse roles of the many entities involved, it may be necessary to establish a limited number of trusted points of contact to avoid duplication of effort. Schedule updates to take into account when information becomes available and time stamp reports to avoid confusion as the situation changes over time.

      ii. Provide the infrastructure and resources required to support these communications roles through an extended period of continuous 24-hour operation.

      iii. Understand the nature of the information that will need to be provided and received without getting into unnecessary levels of detail or speaking on behalf of specific utilities.

   c. Communications between local emergency operation centers and the electricity sector should be enhanced. The ESCC should work with the National Association of State Energy Officials to design and disseminate a model to assist utilities in planning, development, and testing of interoperable tactical communications at local to state/provincial levels.

2. **Clarify the differing crisis communications roles of the ESCC and RCs with government and their members, including its Canadian members.** Given the cross-border nature of the scenario, the Canadian and U.S. federal governments would be involved with the electricity industry, introducing a level of crisis communication not needed since the 2003 Northeast Blackout.[1] While the ESCC can facilitate some of this communication, the directly-impacted RCs and utilities would be responsible for ensuring timely and effective communication and action.

   a. The ESCC should continue communicating its crisis coordination role broadly across the electricity sector as well as with other interdependent sectors. As part of this outreach, the ESCC should document how its role to provide information and advice to the U.S. federal government is distinctly separate from that of operating entities and RCs. For example, to speed restoration, the EGCC should coordinate through DOE Energy Response Organization/Emergency Support Function #12 with FEMA's National Continuity Program and Integrated Public Alert & Warning System on continuity of communications concepts and identify opportunities and solutions for integration/enhancement with existing assets at critical control centers.

   b. While several Canadian entities and Electricity Canada are ESCC members, there is no organization equivalent to the ESCC in Canada. That said, Canadian industry and government groups will communicate and coordinate on relevant national security and emergency management matters through a variety of formal and informal mechanisms. Electricity Canada should continue to work with its members and Canadian government partners to leverage and mature these channels and to make communication and coordination mechanisms more resilient.

   c. The ESCC and Canadian entities should continue to improve two-way information flow and pursue opportunities for mutually beneficial partnerships.

3. **Continue to build effective communications procedures and systems to share security information.** Federal government mechanisms to share potentially-sensitive security information with the electricity industry are challenging during normal conditions, and these mechanisms would be severely strained by the incidents described in the scenario. Approaches that require security clearances or one-day read-ins, access to specialized facilities (e.g., a sensitive compartmented information facilities with secure video teleconference capabilities) are not feasible to support rapid industry response; however, in emergency situations, there are some options (e.g., downgrading information) that allow for these constraints to be addressed. During the Tabletop discussion, government representatives provided assurance that the relative speed and volume of information flow would increase during a real incident, but the practical effects of these assurances are not widely understood and have not been exercised or implemented at scale during a real incident. A shared understanding of specifically what information would be valuable, where this information originates, which recipients can act on it and therefore have a priority need to know, and the anticipated value in those actions that can be taken will start to address this concern.

   a. NERC should establish a working group to clearly articulate the critical information requirements the industry needs to maintain or restore the reliability and security of the grid. To the extent possible, this should leverage established frameworks for similar endeavors.[2]

   b. U.S. DOE and the Department of Homeland Security should work with the electricity industry to review existing information products, their content, any information-sharing limitations, and the mechanisms to convey that information in a timely manner. A detailed gap analysis should be performed to improve the

---

[1] Ref. Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations: https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf
[2] Ref. U.S. Joint Staff J7's Commander's Critical Information Requirements Insights and Best Practice Focus Paper: https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/ccir_fp4th_ed.pdf?ver=2020-01-13-083331-097

quality and timeliness of information needed by government and the electricity industry in the United States and Canada.

c. Similarly, the Canadian federal government departments should work with their electricity industry and Electricity Canada to enhance how sensitive information will be shared across Canadian entities and with U.S. counterparts.

4. **Continue to build on understanding of GSE order development and consultation processes.** DOE's GSE authorities are of great interest and importance to the electricity industry. During the Distributed Play portion of the exercise, several RCs used the GSE scenario inject and indicated it helped them better understand the consultation and order development process. The Tabletop discussion indicated that the U.S. electricity industry and DOE have made progress in developing a common understanding of the consultation process and initiated the discussion of possible elements that would be included in a GSE order. DOE and industry should also consider the impact of GSE orders on the natural gas industry and other critical infrastructure sectors.

The recently established Energy Threat Analysis Center, which includes representatives from DOE and industry, can provide useful context during the development of a GSE order.

a. DOE should work with the ESCC to further refine the consultation process that would be used when a GSE order is being considered. DOE noted that their GSE authority has so far never been used, so any first use would need to be highly consultative to clearly determine the desired outcomes of the order. To do so, it would be necessary for all parties to appreciate the operational and technical complexities and avoid unknown or unintended consequences. It is likely that the consultation and development process would differ depending on the nature of the initiating event. Several hypothetical crisis scenarios with different national security and public safety characteristics should be developed to help DOE and the industry understand which organizations absolutely need to be involved in the consultation process and what communication mechanisms will be used. It will be important to clearly distinguish between the roles of federal and state governments, the ESCC, and that of the electricity entities responsible for ultimately implementing any GSE order. The Fixing America's Surface Transportation Act, which amended the Federal Power Act by adding Section 215A (outlining the GSE authority), outlines the applicable emergency threats and incidents to which a GSE applies. The procedural rule is also clear on what entities are to be considered in the consultation process. GSE orders will be drafted to be extremely clear in terms of which entities would be required to implement them and what would be required of those entities.

b. The ESCC and EGCC should review the elements included in GSE orders as provided by DOE. Understanding these elements would help to familiarize others with the orders, the procedural rule, and the consultation process.

Per the scenario, an outcome of the GSE order could be to identify particular customer loads for restoration that might differ from the utility's standing prioritization that was developed with safety and social welfare foremost in mind. The working group should discuss how utilities prioritize their customers and how this sequence might change as outages extend from hours into days.

Industry should continue to develop several hypothetical crisis scenarios with different national security and public safety characteristics to help DOE and the industry understand which organizations absolutely need to be involved in the consultation process and what communications mechanisms will be used.

c. Industry should confer and study the existing statutory language to understand what "liability protections" are allowed by statute and how they may apply to their operations. DOE cannot expand nor limit the protections that are set by statute.

    d.   DOE should consider if GSE orders impact the natural gas industry and other sectors.

        The U.S. federal government could consider creating a comprehensive register that identifies and explains the different capabilities and tools that the whole of government could make available to industry in a crisis. Referencing DOE's Energy Waiver Library[3] could support this effort.

5. **Continue to enhance routine and emergency operations coordination between the electricity industry and natural gas providers.** The scenario included disruptions of natural gas to generating stations. Compared with the GridEx V Tabletop two years ago, the discussion benefitted from the more robust participation of natural gas operators and natural gas trade associations in the United States and Canada, some of whom are part of the natural gas industry's National Mutual Assistance Program. In responding to the scenario, natural gas participants noted the limited number of alternate paths to supply natural gas to generating stations in the event of a serious transmission pipeline disruption. On the other hand, options do exist to re-allocate natural gas supply to priority customers. This would require government regulators to be prepared to waive tariff requirements and potentially provide liability protections. For example, government regulators may prioritize residential and certain industrial customers (e.g., natural-gas-powered generation) over other industrial customers.

    a.   The ESCC, the Oil and Natural Gas Subsector Coordinating Council, and the National Association of State Energy Officials should consider establishing a joint working group[4] to consider the impact of natural gas supply disruption on electricity generation through a range of scenarios, including the impact to resilience from a single energy source net-zero policy. The working group should include electricity, natural gas, and government regulatory representatives. The group should focus on a certain geographic area to ensure that discussions are based on real infrastructure capabilities, constraints, and options. This regional approach would provide a model that could be applied to other jurisdictions across North America.

    b.   To help accelerate these efforts at a strategic level, the Tri-Sector Executive Working Group[5] should be expanded beyond electricity, financial services, and communications sectors to include natural gas production, transmission, and distribution. Alternatively, one could consider an all-energy membership by including oil and natural gas. The Tri-Sector Executive Working Group should include regulatory agencies in the process to help ensure regulatory requirements are identified and considered.

6. **Strengthen operational coordination between the electricity industry and communications providers.** The critical interdependencies between the electricity and communications sectors are well-understood and have often been a prominent component of the GridEx series of exercises. This time, the Tabletop scenario featured a widespread loss of landline and cellular communications while electric utilities were recovering from the cyber and physical attacks and restoring the grid. Participants agreed that the loss of communications would essentially halt the grid restoration process.

    a.   The Tabletop scenario once again highlighted that, in the case of essential grid communications services, there is an urgent need to consider technical alternatives that have rudimentary functionality and high reliability in case of an extreme telecommunications disruption. This is not a trivial initiative. With the advent of real-time electricity market systems, new types of generation with different operating characteristics, and distributed energy resources, operating today's grid is much more complex than in decades past and requires the exchange of commensurately more data to maintain reliability, resilience, and security. The electricity industry should leverage past research efforts, including that of the ESCC's Resilient Communications Working Group, and engage the communications sector and government to consider alternate capabilities, such as cloud-based solutions and utilities with their own private fiber-

---

[3] U.S. Department of Energy | Energy Waiver Library: https://www.energy.gov/ceser/energy-waiver-library
[4] NERC's Reliability and Security Technical Committee and their Electricity-Gas Working Group could assist with this initiative.
[5] The Tri-Sector executive Working Group: https://www.cisa.gov/tri-sector-executive-working-group

optic networks. The Tri-Sector Executive Working Group could sponsor this initiative and provide the necessary strategic direction and support. Such initiatives should engage government at the local, state/provincial, and federal levels (e.g., FEMA's National Continuity Programs).

    b.   At the local level, electricity utilities and their communications providers should examine their respective service restoration plans and consider how they may be optimally coordinated to provide mutual support. For example, during an electricity outage, electricity crews would prioritize areas where communications cell towers or switching offices have exhausted their backup batteries and generator fuel. During a communications outage, communications providers would prioritize grid control centers and other critical electricity facilities.

7.   **Continue to reinforce relationships between governments in the United States and Canada to support industry response to grid emergencies.** Given the cross-border scope of the scenario, the Tabletop discussion was enhanced by the robust participation of senior officials from the Canadian federal and provincial governments. Participants gained a better understanding of the roles of Canada's provincial and federal governments during a grid emergency and how they are different from those of their U.S. counterparts.

    a.   Depending on the geographic scope of future Tabletop scenarios, NERC should continue to invite senior state and provincial government officials who would demonstrate their prominent roles during a real event.

    b.   RCs in Canada should consider making their provincial and federal government stakeholders aware of DOE's GSE authority in the event a GSE order is developed and issued in the United States. Per the procedural rule at 10 C.F.R. Part 205, DOE can include the Canadian federal government within the consultation process prior to the issuance of an order. DOE and the Canadian federal government should consider further discussions on the appropriate method and protocol to coordinate during this process.

        Canadian industry's inclusion in the consultation process warrants further discussion/study. Canadian industry and government participants reaffirmed their desire to be included in the consultation process.

    c.   Canadian industry and government departments acknowledged the need to enhance how sensitive information will be shared across Canadian entities and with U.S. counterparts.

Distributed Play Observations and Recommendations

The observations gathered for this report incorporate feedback from 57 After-Action Survey responses, the GridEx Planning Team, and notes from the post-exercise Planner Town Hall series. The following observations and recommendations identify opportunities to enhance the security, resilience, and reliability of the North American BPS, organized from the most generic to more detail-oriented issues:

1. **Flexible exercise conduct options enabled Planners from a wide range of participating organizations to design and conduct an exercise that met their organization's needs as well as collaborate with other entities.** Similar to GridEx V, the GridEx VI Planning Team created a template schedule for Planners to follow that ensured organizations across North America could participate in GridEx VI at approximately the same time.

   Planners shared that two days of exercise play allowed them to sufficiently explore the exercise scenario and associated response activities. While some Planners felt that a two-day exercise was too long, other Planners recognized that two days provided the flexibility they needed.

   Additionally, while all registered Planners understood E-ISAC's role in Distributed Play, the GridEx Planning Team received communications from non-participating organizations with questions about Distributed Play and how they could participate in the two weeks leading up to the exercise. While the GridEx VI Fact Sheet is publicly available on the E-ISAC and NERC websites, it shares general information about the exercise and planning process, not the specifics of the distributed play exercise.

   ## Recommendations

   a. The E-ISAC should continue to emphasize that Planners can customize both the content and duration of their exercise play. The E-ISAC should share more detailed recommendations with Planners on how to customize their exercise in a way that allows for coordination with partner organizations, such as recommended approaches for customization based on lessons learned from experienced GridEx Planners.

   b. The E-ISAC should post additional information about Distributed Play on the E-ISAC website so organizations that have not participated in GridEx previously could understand how to participate, the benefits of participation, and what the planning process entails. The GridEx Fact Sheet should include a more detailed explanation of the distributed nature of the exercise. Additionally, documents like the GridEx Frequently Asked Questions, Planner Checklist, and Planner Recommendations should be made TLP:WHITE so that organizations that are considering GridEx participation can gain a more detailed understanding of the planning process and the benefits of participating.

2. **The GridEx Planning Team provided planning materials that offered significant value and reflected maturation in the GridEx series, but the delayed publication of certain materials limited their value.** The Scenario Narrative and MSEL gave Planners the flexibility to develop a customized exercise that met their organization's objectives. Some participating organizations made few adjustments to the GridEx VI MSEL, while others created a new MSEL and injects using the Scenario Narrative as a starting point. The GridEx VI MSEL included fewer injects than previous iterations and did not include expected Player actions, which made it easier for Planners to customize the injects.

   The GridEx Planning Team created more cyber inject supporting material compared to previous iterations. Planners felt that the cyber material was realistic, thought-provoking, and useful, and 98% of Planners agreed that GridEx VI provided an opportunity to test their cyber security response plans. One Planner noted that offering the cyber material in smaller technical portions, such as packet captures and hash files, allowed Planners to focus their efforts and enhance exercise play. The physical security injects offered realism to Players, with the personal targeting of staff provoking discussion during the exercise. Additionally, 98% of Planners felt GridEx VI tested their physical security response plans.

Planners noted that the news report videos added an element of realism to exercise play and offered Players a unique way to engage with the narrative. Several Planners felt that the news report videos were shared with them too late, consequently making it difficult to incorporate into their exercise play. Overall, materials that were delayed or posted too close to exercise conduct could not be used without delaying participating organizations' planning timelines or making modifications to exercise play.

The E-ISAC should publish essential planning material at least six months in advance of the exercise and communicate revised release timelines for lower-priority material if delays are expected. For materials that have longer development timelines or are delayed, the GridEx VII Planning Team should consider whether publishing an initial version of the material would be appropriate and offer value to Planners.

Recommendations

a. The E-ISAC should publish essential planning material at least six months in advance of the exercise and communicate revised release timelines for lower-priority material if delays are expected. For materials that have longer development timelines or are delayed, the GridEx VII Planning Team should consider whether publishing an initial version of the material would be appropriate and offer value to Planners.

   i. The E-ISAC should share the news report videos with Planners earlier or provide Planners with the scripts for the videos so they can incorporate video content into their customized scenario.

b. The GridEx VII Design Team should focus the Scenario Narrative and MSEL around a few scenario threads (e.g., cyber security thread, physical security thread) that evolve through the exercise Moves. The Design Team should create a similar number of injects as was developed for GridEx VI and continue to ensure the content is relevant and easily customizable for participating organizations.

c. The E-ISAC should provide Planners with additional information on how to navigate and customize the MSEL in Excel for their organizations as well as to include information on which columns to hide or delete to facilitate spreadsheet navigation. This information should be included in a Planner training webinar early in the planning process as well as any other materials that share guidance on customizing the MSEL.

d. The E-ISAC developed cyber inject supporting material as well as Planner and Player guides and held a webinar that explained how to use cyber-related exercise material. These resources were useful and the E-ISAC should continue to provide them to Planners and Players as well as to develop other products to assist Planners.

e. The E-ISAC should continue to develop physical security injects and inject supporting material, such as photos, videos, and press releases.

3. **The exercise tools enabled thousands of Players to communicate and coordinate during the exercise. Some Planners shared that they would have appreciated more information about the exercise tools during the planning process.** According to the After-Action Survey, 88% of respondents agreed or strongly agreed that the exercise tools were sufficient to support their organization's GridEx VI. The exercise tools were most actively used during Move 1 at which time several attacks became apparent to Players (see **Figure 3.1**).

However, some Planners shared that there was a lack of clarity surrounding what the tools could be used for. This created difficulties around how to develop tool-specific injects earlier in the planning process when organizations were developing their customized scenarios and MSELs. As a result, some Planners opted not to use the platforms or did not create many tool-specific injects. Some Planners also believed that the testing period for the exercise tools was too short.
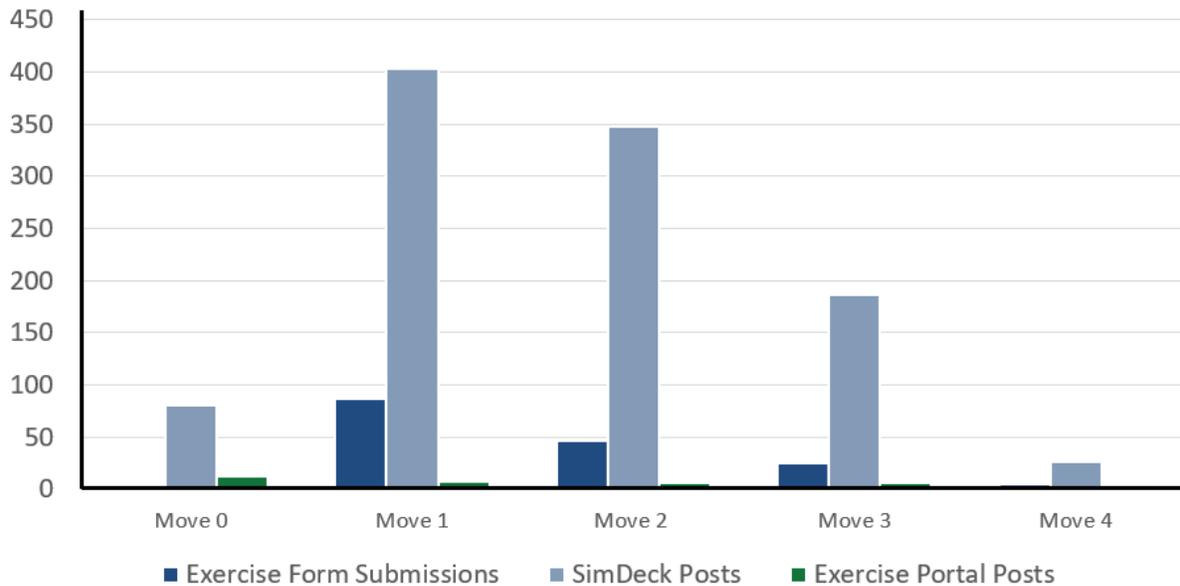
Figure 3.1: GridEx VI Exercise Tools Usage

During GridEx VI, Players had the opportunity to use SimDeck to simulate social and traditional media as well as collaboration and event reporting functions. The simulated RCIS and event reporting functions mimicked their real-world counterparts and added realism to the exercise. The simulated social and traditional media was engaging and made the exercise more connected across participating organizations. During GridEx VI, only Players that used media, collaboration, and event reporting functions in their day-to-day roles were encouraged to use SimDeck. Technical difficulties in past iterations of GridEx and a short testing period for GridEx VI also deterred some Planners from using SimDeck.

Players also had the opportunity to use the E-ISAC Exercise Portal to simulate the real E-ISAC Portal during the exercise. The removal of Exercise Portal email notifications was frustrating for some Players. During GridEx VI, Players who used the Exercise Portal were not notified when other Players created postings, requiring certain Players to repeatedly need to check the Exercise Portal. Disabling Exercise Portal notifications was a recommendation from GridEx V as Players received an overwhelming number of emails during the exercise.

Recommendations

a. The E-ISAC should provide detailed examples of SimDeck and Exercise Portal postings so that Planners understand what they will need to build as they develop their scenario. The GridEx Planning Team should include these examples in Planner training webinars.

b. The E-ISAC should provide Planners a full month to familiarize themselves with the exercise tools and test the platforms before the exercise. The E-ISAC should share guidance with Planners on what to test during this period and release practice injects for Planners to see and interact with. At the same time, Planners should have all necessary access, guidance, and training to fully test the exercise tools.

c. The E-ISAC should continue to use all media, collaboration, and event reporting functions in SimDeck and should post more exercise-wide injects on the platform during exercise conduct. All Players, including those that do not use media, collaboration, and event reporting functions in their day-to-day roles, should be encouraged to use SimDeck during the exercise to create a greater sense of cohesion.

d. The E-ISAC should explore options for Players to turn Exercise Portal notifications on or off during exercise conduct.

4. **The Planner and Player training webinars effectively shared information, resources, and examples with Planners and Players in the lead-up to the exercise.** During GridEx VI, the GridEx Planning Team developed eight Planner training webinars and one Player training webinar, more than in any previous GridEx. The additional webinars developed for GridEx VI added value for Planners, particularly those who were less experienced in the GridEx series. Some more experienced Planners felt that some webinars were too high-level and that practical examples of exercise planning, development, and delivery would have been more beneficial. Other Planners found the high-level content to be valuable.

Recommendations

a. The E-ISAC should deliver a similar number of Planner and Player training webinars in future iterations of GridEx. If appropriate, the GridEx Planning Team should consider delivering some of the training webinars as videos or town hall events, depending on the content and purpose of the session.

b. The E-ISAC should expand the role of experienced Planners in the webinars and incorporate working sessions for Planners into the Training Plan. Experienced Planners should share tips and resources for planning the exercise as well as examples of deliverables, such as injects, exercise plans, and evaluation materials:

   i. The E-ISAC should segment Planner training webinars and other training materials by experience. Training materials should be developed for both new Planners and experienced Planners, and it should be clear to Planners what resources are most relevant to their experience level.

5. **Utility Planners who were part of their RC's planning process were particularly pleased with how their RC helped develop a realistic and inclusive scenario.** Some RCs conducted their own training webinars and created additional planning resources for their customers that took some of the burden off Planners at those utilities. Many entities do not work with their RC, authorities, or the E-ISAC unless security or emergency issues arise, so working with these organizations during the planning process helped them to better understand the roles of RCs, balancing authorities, and the E-ISAC.

Recommendations

a. The E-ISAC should encourage greater coordination between Planners and other external organizations, such as RCs, balancing authorities, neighboring utilities, law enforcement, and government agencies.

b. The E-ISAC should continue to encourage all RCs to participate in GridEx VII and conduct outreach to involve them early in the planning process. While the E-ISAC will continue to lead exercise design and support, if RCs are involved early in the planning process, they will be prepared to serve as an additional resource for utilities throughout the planning process.

6. **GridEx VI communications and resource sharing were effective tools that supported Planners throughout the planning process.** According to the After-Action Survey, 98% of respondents agreed or strongly agreed that the E-ISAC was effective at sharing information and providing high-level situational awareness throughout the planning process. The GridEx VI Planning Resources Site was well-organized and contained helpful planning resources. It was convenient to host all planning resources in one central location that Planners could return to at any time. The GridEx Planning Team sent communications when key planning resources were posted to the site, but not all new or updated resources were communicated. However, additional communications about new planning resources would have been helpful for a few Planners. Some Planners also encountered SharePoint access issues that inhibited their ability to use the GridEx VI Planning Resources Site. Additionally, the GridEx inbox was responsive to Planners' questions, concerns, and access and registration issues throughout the planning process.

Recommendations

a. The E-ISAC should continue to use SharePoint or a similar platform to publish Planner resources throughout the planning process. The E-ISAC should also continue to use the GridEx inbox to respond to inquiries from Planners and other individuals with questions or concerns about GridEx.

   i. The E-ISAC should provide Planners with information about how to subscribe and unsubscribe from SharePoint notifications and release additional communications when any major planning resources are posted to the site.

b. The E-ISAC should publish a TLP:WHITE document with information about registration and SharePoint access so that Planners who have registration or access issues know how to troubleshoot and who to contact for further support.

7. **NERC formally participated in GridEx VI as a player and included members from the E-ISAC Watch Operations, NERC BPSA, and the ERO Communication Group, providing a valuable exercise opportunity.** E-ISAC Watch Operations was able to effectively exercise operating procedures for triaging and ticketing reports. Secure messaging and incident response ticketing platforms proved valuable tools for internal communication throughout exercise conduct, and one analyst suggested developing the role of automation to enhance Watch Operations' response in future iterations of the exercise.

NERC BPSA was able to effectively exercise normal operating procedures during GridEx VI through collecting incoming data, analyzing the information, and reporting appropriately system status. Throughout play, two NERC staff volunteers assisted the core BPSA staff with all play duties, replicating what would be required in a similar non-drill situation. The NERC Situational Awareness for the Federal Energy Regulatory Commission (FERC), NERC, and Regional Entity tool was especially useful during GridEx VI, providing a geospatial description of the threat landscape. The NERC Situational Awareness for FERC, NERC, and Regional Entity tool images were shared with the E-ISAC, Regional Entities, executive management, and government partners throughout GridEx VI. Secure messaging was successfully utilized during play between NERC BPSA and the regional situational awareness teams. NERC BPSA did not specifically know how they would receive mandatory reporting during play due to an unexpected but necessary security workaround with SimDeck the week before the event. Furthermore, NERC BPSA believed there was some lack of coordination with RCs prior to GridEx VI that resulted in the governmental conference call portion of the exercise not having full player involvement. Members of NERC Communications department found GridEx VI valuable and identified opportunities for deeper exercise play in GridEx VII.

Recommendations

a. E-ISAC Watch Operations should maintain their expanded exercise participation in future iterations of GridEx.

b. E-ISAC Watch Operations should continue to use secure messaging and incident response ticketing platforms for internal communications.

c. NERC BPSA should continue to expand exercise participation in future iterations of GridEx.

d. The GridEx Planning Team should facilitate earlier engagement and planning between NERC BPSA and RCs to build a shared understanding of exercise planning and activities.

e. NERC BPSA and the E-ISAC should employ a more realistic, normal RCIS analysis process during GridEx play.

f. NERC, through the ERO Communication Group, should consider expanding the ERO Enterprise communications exercise play.

Chapter 4: Conclusion and Next Steps

GridEx VI Distributed Play and Executive Tabletop activities provided a unique opportunity to exercise the resilience of the grid and provide a forum for industry and government leaders to explore grid security issues. With the support of participants and Planners, the E-ISAC identified a series of recommendations to both enhance the resilience of the grid and improve the delivery of GridEx VII.

Next Steps

In preparation for the GridEx VII Executive Tabletop, the E-ISAC reconvened Tabletop participants in March 2022 to seek concurrence on the recommendations and identify champions to advance them. From the discussion, the E-ISAC identified the following next steps:

- The E-ISAC will coordinate with the ESCC and the EGCC to develop an action plan to address the recommendations in this report, assign ownership, decide how best to act on each of the recommendations, and provide periodic status updates to monitor progress in preparation for GridEx VII in 2023.

- NERC and the E-ISAC are committed to continue enhancing the GridEx program to meet the challenges posed by the ever-evolving threat environment. The E-ISAC will consider suggestions made by participants for the next Tabletop:

    - **Interdependencies with the Natural Gas and Telecommunications Sector:** Build on the positive contribution of the natural gas and communications participants at GridEx VI by inviting a similar 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 Participation:** Encourage the participation of state and provincial government representatives consistent with their prominent roles during regional emergencies.

    - **Policy and Operations**: Thanks largely to the active participation of industry executives, the GridEx VI Executive Tabletop successfully addressed policy matters within the context of operational realities. The next Tabletop should continue this approach with the following:

        - A scenario that is regional in scope, involves the United States and Canada, and recognizes the extent to which the recommendations in this report have been addressed

        - A focus on a few key issues

        - A virtual format with breakout sessions to simulate communications during a real event

In preparation for the GridEx VII Distributed Play, the E-ISAC has identified the following next steps:

- The E-ISAC will post additional information about Distributed Play on the E-ISAC website so that organizations that have not participated in previous iterations understand how to participate in GridEx VII and what the planning process entails.

- The GridEx VII Planning Team will include RCs and the Design Team in scenario development so that simulated operational impacts are as realistic as possible and the scenario is designed with the end-user in mind.

- The GridEx VII Planning Team will work more closely with RCs throughout the planning process so that RCs can serve as an additional resource for their customers during GridEx planning. This will also strengthen the relationship between RCs, balancing authorities, the E-ISAC, and their customers.

- The GridEx VII Planning Team will develop exercise planning materials with the observations and recommendations from this report in mind.

Appendix A: Exercise Goals and Objectives

Executive Tabletop Goal and Objectives

The goal of the GridEx VI Executive Tabletop was to engage senior industry and government leaders in a comprehensive discussion of U.S. and Canadian security issues, extraordinary operational measures, and coordinated decisions needed to protect and restore the grid. The underlying objectives are listed below.

Objective 1: Strengthen the Coordinated Response to U.S. and Canadian National Security Implications of Supply Chain Attacks on Systems and Software

The GridEx VI Executive Tabletop scenario referenced software supply chain attacks that affected industry's ability to respond to attacks. While there was limited discussion during the Tabletop, the Planning Team recognizes that supply chain issues are being addressed by other industry initiatives.

Objective 2: Enhance Industry Coordination with U.S. and Canadian Federal and State/Provincial Governments

Canadian and U.S. government representatives from the appropriate departments and agencies participated actively throughout the exercise. Future iterations of the GridEx Executive Tabletop should continue to involve Canadian government and industry participants to further strengthen cross-border grid security response efforts.

Objective 3: Enhance Electricity Industry Response Coordination with the Natural Gas and Telecommunications Sectors

The GridEx VI Executive Tabletop scenario featured massive impacts on natural gas and telecommunications infrastructure and capabilities. The natural gas sector and telecommunications sector were well represented in the exercise and made significant contributions to the discussion. The GridEx Executive Tabletop should continue to involve natural gas and telecommunication participants and continue to explore natural gas and telecommunication interdependencies as they relate to the reliability, resilience, and security of the grid.

Objective 4: Explore the Public Communications Challenges that Result from Misinformation and Disinformation

The GridEx VI Executive Tabletop discussion did not focus on misinformation and disinformation challenges. These challenges were recognized during the exercise, but given the limited time, participants focused their discussion on the most critical issues and decisions they would need to make. The E-ISAC should explore expanding the role of misinformation and disinformation in the Distributed Play portion of GridEx VII during which time corporate communications teams from participating entities can explore the issues arising in greater depth.

Objective 5: Explore Emerging Security and Resilience Implications Related to Changing Generation Fuel Mixes (Traditional and Renewable)

The GridEx VI Executive Tabletop scenario included discussion of impacts to solar and wind generation, leading to meaningful discussion between participants. The E-ISAC should use future Tabletops to further explore the security and resilience implications of changing generation fuel mixes as well as the impact to resilience that electrification policies will have on the North American energy systems.

Objective 6: Build Consensus between the Electricity Industry and Governments Regarding the Development, Issuance, Liability Protections, and International Implications of GSE Orders

The GridEx VI Executive Tabletop scenario featured a thorough discussion on the implications of GSE orders. The discussion fostered a better understanding between the electricity industry and U.S. and Canadian governments. Further discussions between industry and government could deepen the shared understanding across the sector and explore in greater detail the relevant capabilities and authorities the U.S. government might employ in response to a GSE.

Distributed Play Goal and Objectives

The goal of GridEx VI's Distributed Play was to exercise the resilience of the North American electricity system in the face of a coordinated attack from a nation-state adversary. The underlying objectives are listed below.

Objective 1: Activate Incident, Operating, and Crisis Management Response Plans

The injects in Moves 1 and 2 focused heavily on the immediate response to an attack targeting the grid. The injects featured cyber, physical, and operational impacts, including a cyber attack on hydroelectric facilities and a physical attack on natural gas pipelines. Planners overwhelmingly agreed that GridEx VI gave them the opportunity to exercise a variety of response plans as shown by the following After-Action Survey results:

- 98% of After-Action Survey respondents agreed or strongly agreed that GridEx VI provided them with an opportunity to exercise their organization's cyber security and physical security response plans.

- 96% of After-Action Survey respondents agreed or strongly agreed that GridEx VI provided them with an opportunity to exercise their organization's operational response plans.

Objective 2: Enhance Coordination with Government to Facilitate Restoration

The GridEx VI scenario included widespread attacks on critical infrastructure, a disinformation campaign, and a nation-state threat that required local, state, and federal government coordination. According to the After-Action Survey, 91% of respondents agreed or strongly agreed that GridEx VI provided them with an opportunity to exercise external communications, media, and response plans with government stakeholders (e.g., law enforcement, local or state/provincial government). The E-ISAC should ensure GridEx VII maintains the opportunity for government–industry cooperation.

Objective 3: Identify Interdependence Concerns with Natural Gas and Telecommunications Sectors

The GridEx VI scenario featured attacks that impacted natural gas and telecommunications sectors and required coordination between those sectors and the electricity industry. According to the After-Action Survey, 79% of respondents agreed or strongly agreed that GridEx VI provided them with an opportunity to exercise external communications, media, and response plans with the natural gas subsector. Additionally, 76% of respondents agreed or strongly agreed that GridEx VI provided them with an opportunity to exercise external communications, media, and response plans with the telecommunications sector. The E-ISAC should incorporate more opportunities for participating organizations to engage natural gas and telecommunications partners in GridEx VII.

Objective 4: Exercise Response to a Supply Chain-Based Compromise to Critical Components

The GridEx VI scenario included injects that targeted third parties and the supply chain in Moves 0 and 3, including a spearfishing campaign that targeted third parties as well as a cyber attack that targeted third parties with remote access to electric utilities. One Planner noted that their Players found the cyber security injects focused on malware, ransomware, and supply chain issues to be of particular value. The E-ISAC should continue to provide detailed cyber-related injects and inject supporting material to enhance the cyber play of participating organizations.

Objective 5: Identify Common Mode and Cyber Operation Concerns across Interconnections

The GridEx VI scenario featured multiple cyber security impacts, and Planners shared that the additional cyber training materials were an improvement upon previous iterations of the exercise. According to the After-Action Survey, 98% of respondents agreed or strongly agreed that GridEx VI provided them with an opportunity to exercise their organization's cyber security response plans. GridEx VII should encourage Planners to explore the implications of common mode and cyber operation concerns between utilities in more detail.