

GridEx V

GRID SECURITY EXERCISE

Lessons Learned Report
March 2020



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

Table of Contents

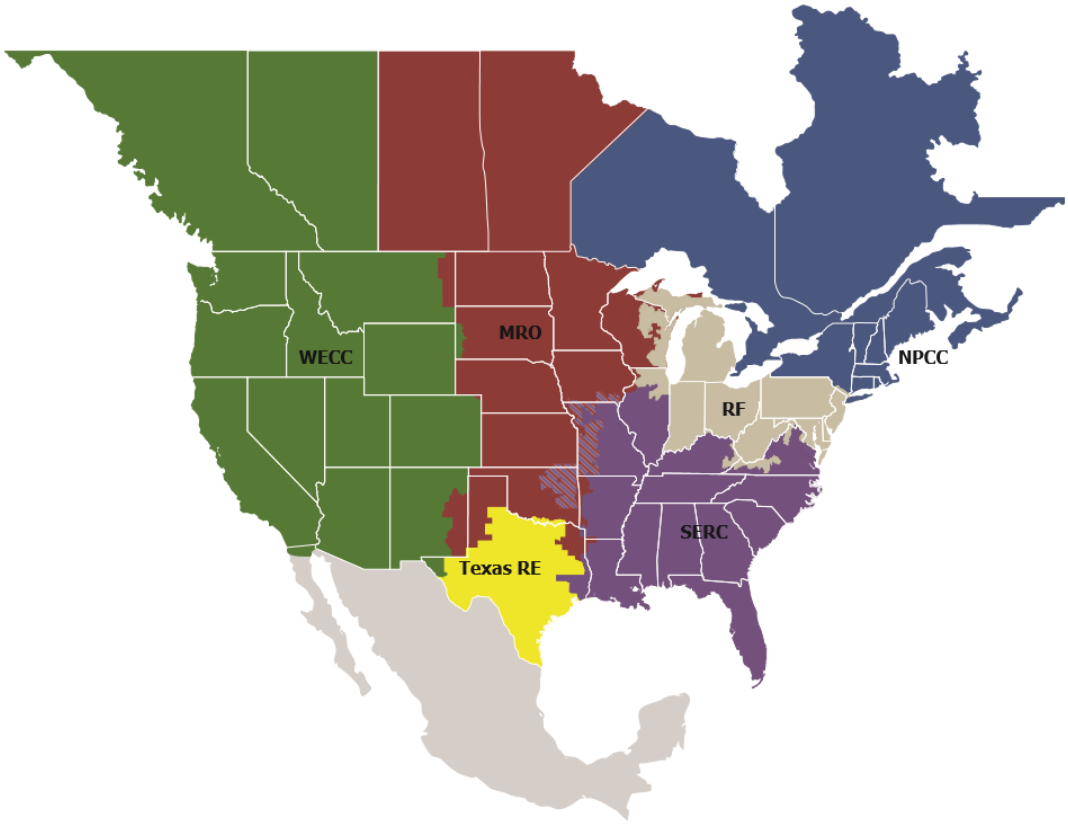
Preface

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 (REs), 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 divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



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

Executive Summary

NERC conducted its fifth biennial Grid Security Exercise (GridEx), a grid security and emergency response exercise, November 13–14, 2019. The exercise was structured as two days of distributed play and it provided an opportunity for stakeholders in the electricity industry to respond to simulated cyber and physical attacks that affected the reliable operation of the grid, fulfilling NERC's mission to assure the reliability of the North American BPS. Led by NERC's Electricity Information Sharing and Analysis Center (E-ISAC), GridEx V was the largest geographically distributed grid security exercise to date.

Additionally, NERC's E-ISAC conducted the GridEx V executive tabletop on November 14, 2019, complementing the separate North American-wide operational exercise. The Canadian Electricity Association (CEA) conducted a separate executive tabletop with the government of Canada the same day with a different, Canada-specific, scenario.

This report is labeled Traffic Light Protocol (TLP) WHITE,[1] a designation meaning that recipients may share this report freely without restriction.

GridEx V Objectives

GridEx V's objectives are listed below:

- Exercise incident response plans — Achieved
- Expand local and regional response — Achieved
- Engage critical interdependencies — Achieved
- Increase supply chain participation — Partially Achieved
- Improve communication — Achieved
- Gather lessons learned — Achieved
- Engage senior leadership — Achieved

For a more detailed assessment of exercise objectives see Appendix A: Exercise Objectives.

Executive Tabletop Recommendations

This report provides recommendations for action by the electricity industry, cross-sector partners, and government. Additional detail for each of the following recommendations is provided in the body of the report. A more detailed explanation of the tabletop recommendations is located in Chapter 3: Observations and Recommendations. Based on the tabletop discussions, it is recommended that industry:

1. **Ensure grid emergency response and restoration plans account for the complexity of national security emergencies and describe coordination with federal and state or provincial authorities.** Utilities and Reliability Coordinators (RCs) should review their grid restoration and crisis management plans and evaluate how they would identify and manage events in support of governmental national security priorities.

2. **Incorporate natural gas providers and pipeline operators into restoration planning and drills.** Natural gas providers should coordinate with natural-gas-fired generator operators to identify alternate supply arrangements in the event of a significant or sustained natural gas supply disruption. Governments at the federal and state or provincial levels in Canada and the United States should evaluate how their authorities could assist in the event of a severe natural gas supply disruption.

[1] Traffic Light Protocol (TLP) Matrix and Frequently Asked Questions (https://www.us-cert.gov/tlp)

3. **Enhance coordination with communications providers to support restoration and recovery and advocate for continued availability of 6 GHz spectrum.** Utilities should document critical communications facilities as part of their grid restoration plans. To assist with the utilities' own prioritization, they should work with providers to understand broader communication industry restoration priorities. Utilities and RCs should continue to pursue the use of resilient communications systems to enhance their ability to operate through extended disruptions of traditional communications. Electricity tabletop participants agreed that proposed changes to utility-used 6 GHz spectrum could impede resilient communications that support grid reliability during emergencies—the 6 GHz spectrum must be available to utilities during an emergency to ensure the reliable function of the grid.

4. **Build consensus with the U.S. Department of Energy (DOE) on the design, issuance, and liability protections for grid security emergency (GSE) orders issued under Section 215A of the Federal Power Act.** The U.S. government should continue to refine consultative and communications mechanisms with industry to support the development of GSE orders. Utilities agreed that a GSE should specify restoration priorities but leave the detailed engineering approach of how to achieve the priority up to the utilities and RCs. The entities responsible for implementing the order would then have the flexibility to take necessary actions while respecting safe grid operating practices and knowing the current status and overall strategy for grid restoration. DOE should collaborate with industry to consider whether to provide additional liability protections for electricity entities and supporting sectors, such as telecommunications and mid-stream natural gas companies that implement the GSE orders. This would especially apply to lawsuits from customers or others who are disadvantaged or suffer loss because of the GSE order.

5. **Identify key supply chain elements and consider the formation of shared inventory programs for the most critical components.** Tabletop participants agreed on the need to understand how critical electricity sector manufacturers would respond to a security incident and share capabilities to include in utility planning efforts. Participants also discussed the benefits of identifying key components in their systems and the supporting supply chains as well as developing a shared inventory capability for essential equipment similar to the transformer reserve.

6. **Continue to grow participation in the Electricity Subsector Coordinating Council (ESCC) cyber mutual assistance (CMA) program.** Utilities should consider activating the CMA program as a resource for supporting response and recovery efforts in a cyber incident in advance of, or in the event of, disruption of electric or natural gas service. The CMA program provides resources (e.g., information sharing, services, personnel, equipment) that can assist an entity during an incident.

7. **Continue to strengthen the operational industry and government coordination between the United States and Canada.** NERC, in partnership with CEA, should invite Canadian government representatives to be part of the next GridEx executive tabletop and continue to use a scenario with an incident scope that includes Canada and the United States.

Summary of Distributed Play Observations and Recommendations

For a more detailed explanation of exercise observations, see Chapter 3: Observations and Recommendations. Based on the distributed play, the planning team made the following observations and recommendations:

1. **The flexible scenario structure enabled exercise planners to customize their GridEx experience and maximize learning to improve their organization's incident response preparations and capabilities.** It is recommended that:

a. Exercise planners should continue to customize the scenario to meet their own learning objectives. GridEx should continue to recognize the diverse needs of participating utilities and provide additional scenario examples to illustrate how GridEx can relate to their functional entity role (e.g., transmission operator, generator operator, distribution entity).

b. Planners should consider how to customize the scenario by deciding which operational processes they want to exercise within their organization. Clear operational goals will help planners decide which cyber or physical security scenario injects to use.

2. **Early planning allowed planners to benefit from the scenario's flexibility, but planners whose organizations joined later struggled to adequately prepare for the exercise.** It is recommended that:

a. NERC should continue to make information available to planners at least six months in advance of execution, giving them maximum time to prepare their organizations.

b. NERC should consider making some planning documents publicly available. Some organizations struggled to access documents during the planning stage due to security measures, such as two-factor authentication and firewall incompatibility. NERC should designate some exercise documents TLP:WHITE and post them to NERC's website. These publically available documents would give new organizations a clearer picture of the commitment necessary to effectively participate in GridEx.

c. NERC should consider facilitating an "experienced planner" program that pairs experienced planners with new planners to help them navigate the planning process. With several iterations of GridEx successfully completed, many veteran planners are available to help new planners manage and prioritize their planning responsibilities.

d. The E-ISAC will continue facilitating partnerships between observers and organizations actively involved in GridEx.

3. **While many utilities used GridEx to strengthen their relationships with RCs, law enforcement, and government agencies, others lacked the resources needed to coordinate responses to the challenges in the scenario.** It is recommended that planners for future GridEx exercises:

a. Encourage RCs to work with utilities in their areas to coordinate scenario development. RCs are well positioned to pair utilities with local government resources and neighboring critical infrastructure partners.

b. Encourage planners to reach out to law enforcement and emergency responders for support in GridEx. In GridEx's current format, each organization should coordinate with government and cross-sector incident response partners as they would in an actual event.

c. Planners should enhance utility-government partnerships, such as embedding U.S. Department of Homeland Security (DHS) protective security advisers with utilities or liaising with DHS watch centers and state fusion centers.

4. **GridEx distributed play and the GridEx executive tabletop should occur on different dates so that leadership teams can achieve maximum training value for their organizations.** Based on this observation:

a. NERC will move the executive tabletop to another time separate from distributed play.

5. **Some participants were confused or overwhelmed by the Move 0 scenario:**

    a. The GridEx planning team will consolidate and shorten Move 0 injects from three weeks to one or two weeks in future exercises.

    b. NERC should provide Move 0 E-ISAC Exercise Portal notifications as an opt-in at registration.

6. **Responses to the cyber injects in GridEx were overwhelmingly positive and participants requested new cyber security inject material for GridEx VI.** Based on this observation:

    a. The GridEx program will continue to use its relationship with DOE and national laboratories to seek out leading-edge cyber training capabilities to facilitate more cyber challenges. This relationship will allow organizations to seek a more immersive cyber security exercise experience.

7. **GridEx V saw an expansion in the scope of crisis communication tools and their adoption.** Based on this observation, for future exercises:

    a. The GridEx planning team will move GridEx registration to a separate website away from SimulationDeck. This move will assist in focusing player use of SimulationDeck solely as a means for exercise crisis communications.

    b. Utility exercise planners should consider developing more interaction between communications players and other exercise players to increase relevance of communications and SimulationDeck play. For instance, planners could structure reports of incidents or threats in the public domain to have relevance for physical security; communications players could also share how their organizations successfully addressed incidents.

8. **The E-ISAC Exercise Portal succeeded as an information sharing portal for utilities and RCs, but the Critical Broadcast Program (CBP) coordination call access caused confusion in some organizations.** For future exercises:

    a. The E-ISAC should consider conducting CBP communications via multiple means, such as a prerecorded briefing posted to the E-ISAC Portal, creating a security "podcast," or a live dial-in capability.

9. **The ESCC used the GridEx V distributed play to successfully test a new series of staff- and executive-level coordination calls that it would use at the outset of a no-notice incident as well as an activation of the CMA program.** Based on this observation:

    a. Electric entities should consider pre-identifying a public information officer and an operations lead to participate in the staff-level coordination calls if asked by the ESCC Secretariat as part of their incident response planning protocols. These protocols should consider that executive-level participation may be required for some calls that include ESCC leadership and senior executives from the federal government.

    b. NERC and the E-ISAC should consider developing a portion of the GridEx VI distributed play that would have a common scenario multiple electric entities use. This portion of the exercise would help facilitate ESCC participation and allow for easier integration and testing of industry-wide capabilities, such as CMA and spare transformer programs, during the exercise.

Introduction

NERC held the fifth Grid Security Exercise (GridEx) November 13–14, 2019, throughout North America to improve the security and resilience of the electricity industry. GridEx has evolved to focus on the unity of effort and message among industry, government, the Electric Reliability Organization Enterprise, and interdependent critical sectors at a strategic, operational, and tactical level. The growth in participation numbers and diversity of participants at all levels is a positive sign of industry preparedness and understanding of the collective threats facing the sector.

To ensure proper focus on the various objectives across multiple levels of industry, the exercise planners separated the executive tabletop and distributed scenarios to maximize both recommendations and observations as well as deliver on the training objectives vital to utility cyber and physical security preparedness. The executive tabletop played a scenario that focused on the extraordinary operational measures necessary to restore the grid in the northeast United States and southern Ontario, Canada, following a severe combined cyber and physical attack on the electricity and natural gas transmission systems. U.S. and Canadian chief executive officers and executives worked with government officials to establish restoration priorities, achieve unity of effort with the natural gas and telecommunications industries, and ensure proper coordination with Canadian authorities. The recommendations can help government and industry on both sides of the border enhance operational coordination during incidents.

In developing the GridEx V distributed play, the NERC planning team built on lessons learned from previous iterations of the exercise, established planning-process milestones, and developed metrics to assess the value of the exercise overall. GridEx V maintained the design goal of increasing utility participation as well as participation by other critical infrastructure organizations and provincial or state and local governments in the United States, Canada, and Mexico. Building on the success of the decentralized planning structure used in GridEx IV, NERC encouraged planners to customize a baseline exercise scenario to meet their organization's needs. The need to facilitate participation by an ever-growing number of organizations with disparate scales and levels of preparedness drove a decentralized planning approach. The decentralization enabled organizations to determine the scope and extent of their own participation and to drive the events they would experience during the exercise, consistent with the baseline scenario. Planners decided whether their organizations would operate in an "active" or "observing" capacity, what physical or cyber attack vectors their organizations would experience, and what other participating organizations they would coordinate action with during the exercise. Planners independently distributed exercise injects within their organizations and without needing to coordinate with GridEx V Exercise Control. This distribution of exercise injects allowed each organization to participate according to its role, available resources, and real-world operational environment without creating massive logistical and communication hurdles.

At the conclusion of GridEx V, NERC asked participating organizations to complete an after-action survey and encouraged organizations to share with NERC any lessons learned that may be relevant to the industry as a whole. NERC used this information to develop the observations and recommendations provided in the Chapter 3: Observations and Recommendations section of this report. While some of the observations and recommendations relate to lessons learned by participating organizations, many of them relate to exercise planning and execution. As GridEx has grown to accommodate more participants, NERC has placed greater responsibility on organizations to manage their own exercise play and collect findings internally.

After-action survey responses indicated the following:

- 96% of respondents felt GridEx V met their expectations with 65% indicating "very well" (up from 42% in GridEx IV).

- 97% of respondents felt GridEx V was planned and managed to meet their needs with 64% indicating "very well" (up from 38% in GridEx IV).

Chapter 1: Participation

Distributed Play Participants

More than 7,000 players from 526 organizations participated in GridEx V, up from the 450 organizations and an estimated 6,000 players who participated in GridEx IV. While the bulk of participants continue to come from the electric utilities that the E-ISAC supports,[2] participation has broadened (see **Figure 1.1**) among interdependent industries, including natural gas utilities, water utilities, and telecommunications companies.

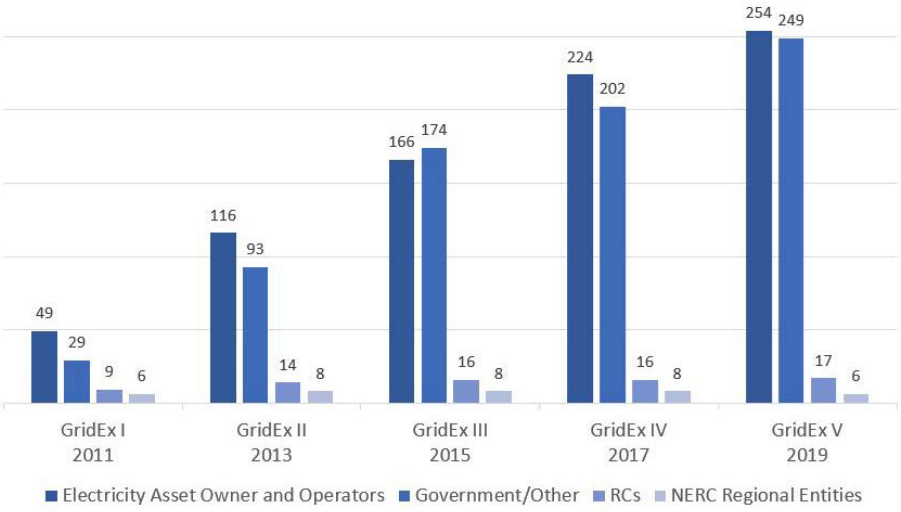


Figure 1.1: Growth in GridEx Organization Participation Since 2011

Participation has also grown among governmental organizations: GridEx V counted participating organizations from the United States, Canada, Mexico, New Zealand, Australia, and the United Kingdom (see **Figure 1.2**).

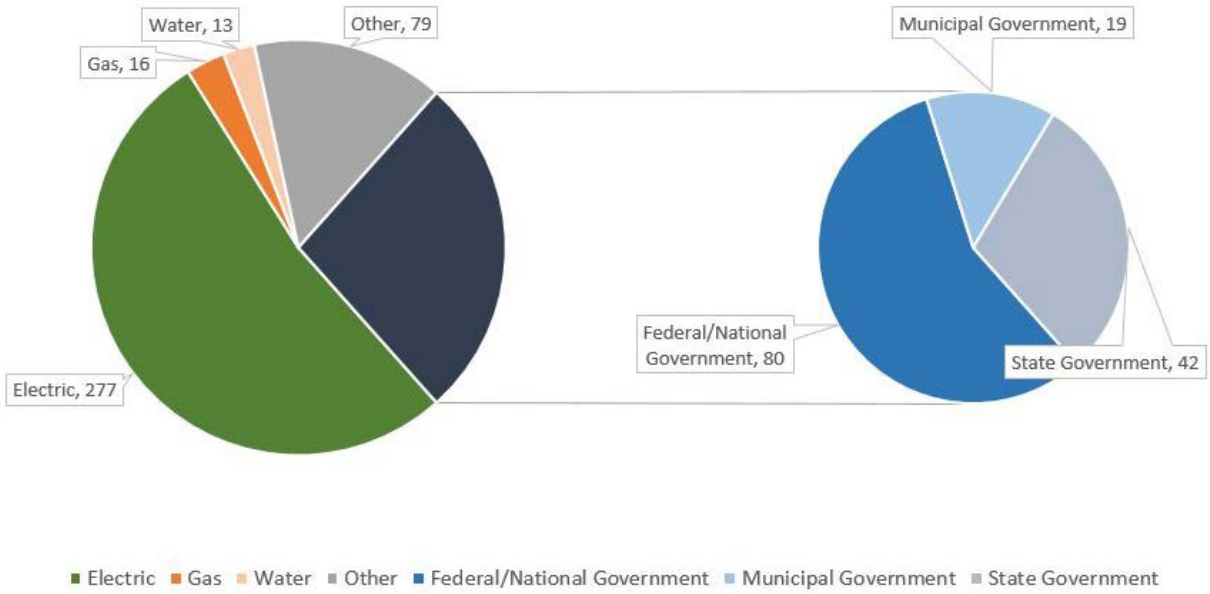


Figure 1.2: GridEx V Participation by Organization Type

[2] Public power utility participation increased from 53 utilities in GridEx IV to 100 in GridEx V.

Executive Tabletop Participants

More than 100 executives and staff from the electricity industry, cross sector partners, and government attended the executive tabletop. Electricity industry participants included U.S. and Canadian chief executive officers and chief operating officers from publicly- and investor-owned utilities, cooperatives, and independent system operators. Participants from other critical infrastructure sectors included representatives from natural gas and telecommunications industries as well as a major automation, protection, and controls manufacturer. U.S. federal government senior officials from the following departments and agencies also attended:

- White House, National Security Council
- Department of Energy (DOE)
- Department of Homeland Security (DHS)
  - Cybersecurity Infrastructure Security Agency (CISA)
  - Transportation Security Administration (TSA)
  - Federal Emergency Management Agency (FEMA)
- Department of Defense (DOD)
- Federal Bureau of Investigation (FBI)
- Federal Energy Regulatory Commission (FERC)

With the support of the National Governors Association, a representative from the State of New York represented the state perspective based on the scenario.

Chapter 2: Exercise Conduct

Executive Tabletop Conduct and Scenario

The GridEx V Executive Tabletop was separate and distinct from the distributed play scenario. The change in approach from previous GridEx years facilitated specific conversations around the extraordinary operational measures needed to restore the grid. Based on feedback from previous tabletops, GridEx scenario planners decided to take a different approach that focused on a scenario narrative that was coherent to a geographic area of the grid and technically defensible. These details enabled a more realistic conversation between industry and government, and produced learning and recommendations that would benefit the entire industry.

GridEx Executive Tabletop Goal and Objectives

> Engage senior industry and government leaders in a comprehensive discussion of the extraordinary operational measures needed to protect and restore the reliable operation of the bulk power system (BPS).

To achieve this goal, GridEx V aimed to do the following:

- Exercise the operational response of electricity utilities and their Reliability Coordinator (RC) to severe cyber and physical attacks
- Review the coordinated operation of electricity utilities and natural gas providers during a severe emergency
- Explore developing and implementing extraordinary operational measures needed to protect and restore the operation of the grid, especially DOE grid security emergency (GSE) orders under the Federal Power Act and other emergency authorities
- Review the mechanisms to request and provide mutual assistance, including coordination facilitated by the Electricity Subsector Coordinating Council (ESCC) and the Energy Government Coordinating Council (EGCC)
- Examine emerging best practices to mitigate the impact of attacks on supply chain providers to the electricity industry

Tabletop participants discussed security and electricity reliability challenges, interdependencies with other critical infrastructures, and coordination with government agencies. For the first time in GridEx history, the participants went beyond high-level policy issues and debated the extraordinary operational measures needed to respond to a coordinated cyber and physical attack scenario causing a widespread blackout across New York State and Southern Ontario, Canada. This U.S.–Canada operational perspective focused the policy-level discussions beyond generalities to discuss which policy decisions would be effective or would create unintended consequences.

Cyber and Physical Security Attack Scenario

The tabletop prompted participants to assess the impact of serious cyber and physical security attacks and take actions needed to respond, communicate effectively, restore power, and address serious public health, safety, and grid security challenges.

The scenario included the following things:

- Cyber attacks targeting utility control systems
- Physical attacks targeting key electricity generation and transmission facilities and natural gas transmission
- Impacts of cyber and physical attacks, including widespread and prolonged electricity outages affecting large population centers

- Response actions and coordination efforts of many organizations, including electricity utilities and other key critical infrastructure sectors, supply chains, the E-ISAC, law enforcement, and government agencies

Tabletop exercise planners designed three phases to simulate how industry and government would respond to a sophisticated, well-coordinated cyber and physical attack scenario:

- **Phase One: Immediate Operational Response during the First Hour**—Widespread, unexplained power outages occur in northeast United States and southern Ontario, Canada.
- **Phase Two: Near-Term Extraordinary Operational Measures**—Power outages persist across the northeast United States and southern Ontario, Canada, with other critical infrastructures affected.
- **Phase Three: Extraordinary Operational Measures after the First Day—**Some power is restored, but serious critical infrastructure outages persist.

Facilitators led participants through each of these three phases during plenary and breakout sessions that were designed to simulate the communications and coordination that would occur among entities during a real event. Prior to the tabletop, NERC provided participants with a handbook that included technical and operational scenario details with sample questions to consider in advance. This enabled participants to contribute in an open, transparent, and well-informed manner.

Distributed Play Conduct and Scenario

The GridEx V planning team directed the distributed play portion from a central location at the exercise control facility in McLean, Virginia, November 13–14, 2019. The planning team oversaw and monitored the status of exercise tools to ensure they remained operational throughout the exercise.

The baseline scenario initiated degraded grid reliability early in Move 1; see **Figure 2.1**, which illustrates the general grid reliability level throughout the exercise.

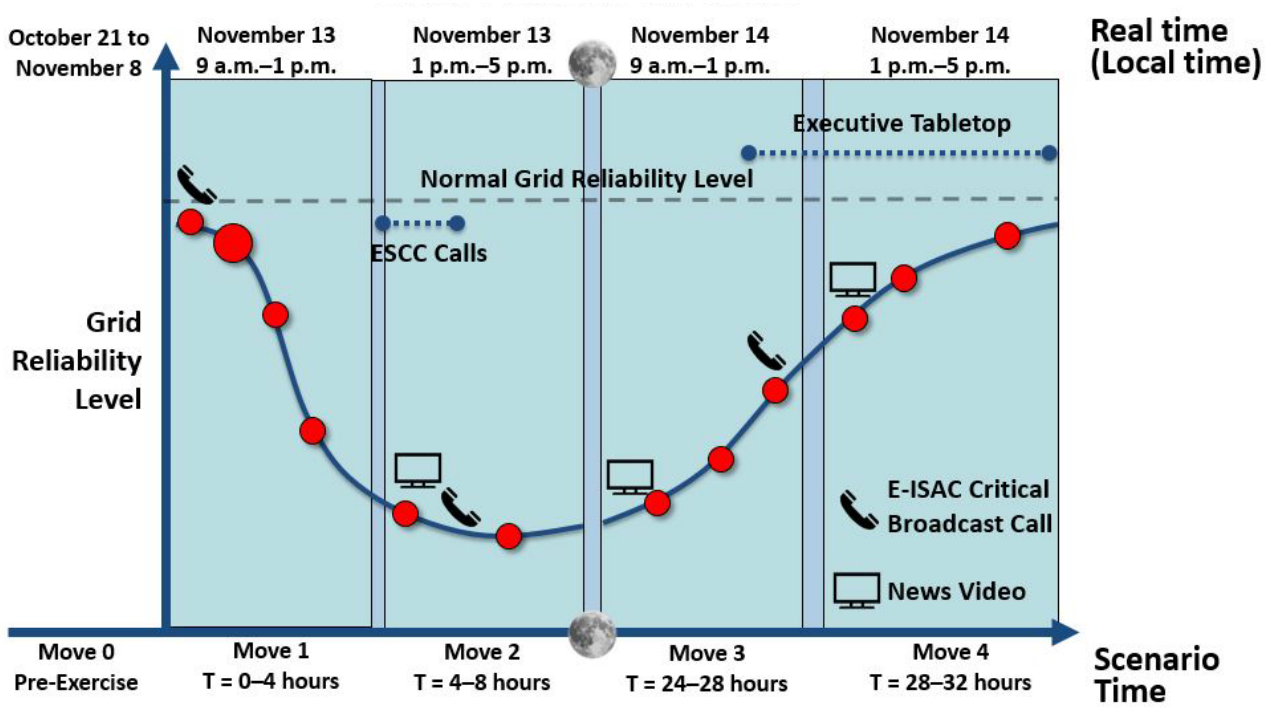


Figure 2.1: Baseline Scenario Timeline

Move 0: The exercise prologue provided players with information that suggested that cyber and physical security threats against the electricity industry were growing, although no information identified the targeted facilities. Various reports stated that nation-state conflicts around the world were escalating in the form of targeted cyber attacks and physical surveillance against critical infrastructures. European transmission operators experienced a cyber-attack-induced system disturbance that impacted over 10 separate countries, including at least one instance of a cyber breach affecting an electricity utility. Reports from the E-ISAC, the FBI, and DHS to the electricity industry indicated that adversaries were aggressively conducting cyber and physical reconnaissance of electricity grid, telecommunications, and natural gas facilities across North America. The adversaries were well-resourced and possessed considerable technical knowledge, skills, and motivation.

Move 1: On the morning of November 13, 2019, the E-ISAC posted notice about a Critical Broadcast Program (CBP) call via the E-ISAC Exercise Portal to inform players of a possible imminent threat against the grid due to a perceived spike in threat reporting against the North American electricity industry. The E-ISAC shared information regarding an active malware campaign targeting industrial control systems. Utilities reported anomalous behaviors within their operational technology networks, and others reported physical surveillance activities and small-scale physical attacks. Utility operators reported serious problems with their control systems and suspected a cyber intrusion compromised them. Already challenged by the generation shortfall, operators lost situational awareness capabilities and resorted to manual methods to monitor and operate the grid. More serious physical attacks damaged generation, transmission, and distribution facilities via direct attacks and fuel supply disruptions. Grid operators shed customer load and avoided the cascading outages that could have caused an interconnection-wide blackout.

Move 2: A prerecorded video of simulated media reports (see **Figure 2.2**) described the attacks and scope of the power outages in this portion of the exercise. Reporting over five million homes without power, the media relied on unverified reports as well as social media information. The ESCC Secretariat hosted a staff-level coordination call with federal government partners (i.e., DOE, DHS, and FBI) and two utilities that played the role of impacted entities. Following that call, the ESCC co-chairs conducted an executive-level conference call with its members, leadership from the impacted entities, and senior federal government officials to share information regarding the situation and align public messaging. The E-ISAC conducted a CBP call to share what industry and government partners had reported so far as well as provide next steps for organizations. Adversaries continued using social media to profile their successes. Utility executives and the government responded to customer and media demands to know what was happening and what they were doing to secure public safety and restore power.

Figure 2.2: Simulated News Broadcast

Move 3: The third move began with another prerecorded video of media reports that described the attacks and power outages that had occurred the previous day. At this point, NERC and DHS responded to news outlets as adversaries continued antagonistic activities against electricity infrastructure in follow-up coordinated attacks. A new

E-ISAC CBP call shared new information from DHS about the specifics of the malware campaign as well as suggesting steps towards mitigation.

The impact of the power outages continued to grow, and water treatment plants without power or backup generator fuel supplies ceased to operate. Fortunately, telecommunications services had largely been restored. Physical attacks continued, this time against coal-fired generating plants, transmission towers, and distribution substations. Cyber attacks continued and included apparent copycat attacks using hacking tools readily available on the Internet. Social media posts by adversaries and affected public continued to raise anxieties and fears.

Move 4: The final set of prerecorded media reports highlighted how industry and government were working together to restore power. Industrial control systems vendors released a software patch needed to remediate infected systems, and utilities worked to install the patches on their production systems. Physical attacks became less frequent, providing utilities with the opportunity to assess the situation, prioritize actions, and begin the repairs needed to restore operation. Utilities requested support from mutual aid partners through traditional and cyber mutual assistance (CMA) networks for grid restoration efforts.

At the end of Move 4, planners concluded the exercise, reviewed the status of exercise play, responded to questions from their players, and began to identify lessons learned.

While each participating organization ran its own distributed exercise, players across the exercise interacted on SimulationDeck, an online platform that hosted applications mimicking social media like Facebook™, Twitter™, and YouTube™ as well as traditional media like television, newspapers, and radio. To enhance realistic training value, GridEx V planners created adversary and customer profiles for players to interact with that allowed them to publish their own press releases and social media postings throughout the exercise. Players used SimulationDeck extensively, publishing more than 1,300 posts, a 50% increase from posts during GridEx IV. SimulationDeck also hosted exercise-specific versions of the Reliability Coordinator Information System and the system disturbance EOP-004 and OE-417 reporting forms. These exercise tools enabled players to report and share information as they would during an actual event. Over the course of the exercise, players submitted 201 Reliability Coordinator Information System forms, 195 OE-417 forms, and 38 EOP-004 forms—a significant increase over previous years.

Chapter 3: Observations and Recommendations

Executive Tabletop Recommendations

Exercise planners gathered feedback from the ESCC Secretariat, a trusted-agent planning team of electricity and natural gas industry experts, and executives present at the tabletop, and produced several recommendations to drive industry resilience and security. These recommendations identify opportunities to enhance utility planning and coordination with government and cross-sector partners and the vendor community to support the security and reliability of the North American BPS. Based on this feedback, this report recommends that industry:

1. **Ensure grid emergency response and restoration plans account for the complexity of national security emergencies and describe coordination with federal and state or provincial authorities.** Electricity utilities and their RCs have well-established processes in place, reinforced by NERC's Reliability Standards, to coordinate operations through normal and emergency events, such as severe storms. However, emergencies with national security implications add layers of complexity beyond the control of the electricity industry that could disrupt or delay grid restoration activities. These complexities include urgent life safety concerns: key messaging to alert, inform, and provide assurance to the public; international coordination; and national defense priorities. Within this high degree of uncertainty, utilities and RCs would make operational decisions to stabilize the grid. Specific activities include:

    a. Utilities and RCs should review their crisis management plans and evaluate how they would manage events with national security implications. For example, a crisis management plan should specify who on a crisis management team is responsible for monitoring and coordinating national security-related issues with federal, provincial, state, and local government officials.

    b. During a national security emergency, utilities should not expect immediate response or support from national defense resources because the focus on their primary missions, including protecting military installations. Utilities, in partnership with DOE and DOD, should identify critical military facilities within their service territory in their grid restoration plans and plan for how they can prioritize them for restoration.

    c. RCs and utilities periodically conduct blackstart and grid restoration exercises and should include government facility managers and law enforcement to observe industry response and address security-related issues. This would provide government and law enforcement with an appreciation of the issues and priorities to address as part of the grid restoration process. The ESCC should work with state associations, such as the National Governors Association, to ensure state and provincial emergency managers and law enforcement are aware of these opportunities.

2. **Incorporate natural gas providers and pipeline operators into restoration planning and drills.** With natural-gas-fired generation now being a significant portion of North America's electricity generation capacity, natural gas supply is a critical fuel required to maintain grid reliability and support restoration operations. Utilities with natural-gas-fired generation and natural-gas-fired generator operators should coordinate with natural gas providers to identify alternate supply arrangements that may be feasible in the event of a significant or sustained natural gas supply disruption. These supply options should evaluate the regulatory requirements and recognize consequential trade-offs, such as prioritizing natural gas supply for electricity generation over other industrial, commercial, or residential natural gas customers. Additionally, interstate pipeline operators typically do not own title to the natural gas they transport; this could complicate decisions needed to reroute natural gas supply to meet electricity restoration priorities. It is recommended that:

a. Utilities with natural-gas-fired generation and natural-gas-fired generator operators should work with their RC to identify dual-fuel capabilities that could mitigate the impact of a sustained natural gas supply disruption and document these capabilities and limitations in their grid restoration plans.

b. Utilities should incorporate natural gas providers and pipeline operators into planning, coordination, training, and exercises for electric system restoration.

c. Governments in Canada and the United States at the federal and state or provincial levels should evaluate which of their authorities could assist in the event of a severe natural gas supply disruption. For example, the TSA has certain authorities to protect the people and facilities associated with critical natural gas pipeline operations, and state public utility commissions often have jurisdiction over intrastate pipelines and local distribution companies and add additional supply requirements that may need to be addressed. The ESCC should work with the Oil and Natural Gas Subsector Coordinating Council as well as the Downstream Natural Gas-ISAC, American Gas Association, Interstate Natural Gas Association of America, and the National Association of Regulatory Utility Commissioners to ensure cross-sector planning that supports the availability of fuel for generation occurs.

3. **Enhance coordination with communications providers to support restoration and recovery and advocate for continued availability of 6 GHz spectrum.** Perhaps the most important interdependency between critical infrastructure sectors is electricity generation and communications. Communications providers rely on a reliable and continuous supply of power to their facilities, and electricity generation relies on communications for operations-critical voice and data communications.

a. Electricity utilities and their communications providers should enhance their understanding of each other's critical facilities and relative priorities in the event of a prolonged power or communications outage. Utilities should document the critical communications facilities as part of their grid restoration plans and understand from communication providers how critical facilities fit in their own prioritization plans to inform utility prioritization.

b. While landlines remain the primary communications path and many utilities have their own alternative communications paths (e.g., fiber, microwave, radio), utilities' preferred infrastructure for voice communications during emergencies is via wireless services. Electricity utilities and their communications providers should enhance their understanding of each other's wireless infrastructure facilities and priorities.

c. Utilities and RCs should continue to pursue the use of resilient communications systems (e.g., the ESCC's resilient communications pilot) to enhance their ability to operate through extended communications disruptions.

d. The electricity industry has expressed concerns to the Federal Communications Commission regarding the proposed expansion of unlicensed access to the 6 GHz frequency band due to the potential interference with communications systems used by utilities to monitor and operate the grid. The 6 GHz spectrum must be available during an emergency to ensure the reliable operation of the grid, and any changes to the use of the spectrum need to account for this interdependency. Utility participants agreed it would be in the best interests of resilience within the communications and electricity industries to protect critical bands of the 6 GHz spectrum.

e. Participants from the natural gas industry provided helpful insight regarding how electricity and natural gas suppliers coordinate their efforts to respond to shortfalls in natural gas supply. NERC and the ESCC should ensure that prominent wireless communications providers, in addition to wired and fiber

providers, participate in the next GridEx in order to focus on electricity communications interdependencies and discuss respective priorities. Additional local electric and telecommunications service territory studies leading up to GridEx would enhance understanding and improve planning factors to account for these critical interdependencies.

4. **Build consensus with DOE on the design, issuing mechanisms, and liability protections for GSE orders issued under Section 215A of the Federal Power Act.** Participants agreed that an order would help government clarify national security priorities to industry during a GSE. Participants discussed opportunities for further consensus building between the electricity industry, interdependent cross-sector partners, and government.

   a. Government should continue to refine consultative mechanisms with industry to support the development of GSE orders. Government and industry should collaborate to develop the parameters of content required and communications design to improve efficiency during implementation of an order. This collaborative effort could result in a template and specific industry consultative mechanisms for DOE to accelerate drafting orders to address the full range of potential GSE scenarios. Industry and government participants acknowledged that no documents could account for the unknown within the extreme events that may trigger a GSE, but a more defined starting point will save precious time during intelligent adversary attacks.

   b. Although a GSE order would not apply to Canadian entities, due to the interconnected nature of the North American grid, it may impact Canadian entities. The development of more specific consultation mechanisms than the outline provided in 10 CFR § 205.380 should also include Canadian industry and government representatives.

   c. DOE should ensure that a GSE order clearly states the intended objectives without specifying technical or operational details. This would provide the entities responsible for implementing the order with the flexibility to take the necessary actions while respecting safe grid operating practices and knowing the current status and overall strategy for grid restoration. RCs and utilities serving the affected areas would be in the best position to develop the grid restoration process to meet the GSE order's intended objectives. The GSE order should also address aspects that may be outside the responsibility or direct control of electricity entities (e.g., natural gas supply contracts entered into by generators' fuel marketing). Grid facilities and equipment critical for grid restoration (i.e., blackstart generation, primary and secondary restoration paths, substations, and loads) are identified in grid restoration plans, which are regularly exercised and enable operators to assess the options available under various circumstances. DOE, in consultation with DHS and DOD, should accelerate sharing information with RCs regarding defense-critical electric infrastructure so RCs may discern how this infrastructure could be referenced in their grid restoration plans.

   d. DOE, the ESCC, and NERC should develop a mechanism to communicate a GSE order in a timely and secure manner to meet the needs of various audiences. The mechanism should recognize that some will need sufficient detail to implement the order (e.g., directly impacted entities, the ESCC, NERC), others need to be aware at a more general level (e.g., indirectly impacted entities, state and local governments), and others at the most general level (e.g., the public). The mechanism should address the risk that adversaries will seek to disrupt normal means of industry–government communication and provide a means to authenticate proper distribution and receipt.

   e. DOE should collaborate with the electricity industry to consider how additional liability protections may be provided for electricity entities that implement the GSE orders, especially regarding lawsuits from customers or others who are disadvantaged or suffer loss as a result of the GSE order. The federal

government should also evaluate how a GSE order might impact interdependent cross-sector partners, including liability, in the telecommunications and midstream natural gas sectors.

5. **Identify key supply chain elements and consider the formation of shared inventory programs for the most critical components.** While the scenario focused on one prominent supplier to the electricity industry, participants agreed on the need to understand how other critical manufacturers within the electricity supply chain would respond to a security incident. Given the scenario focus of an attack conducted through protective relays, participants discussed the possibility of developing an equipment reserve for the most critical grid components, such as a "strategic relay reserve" or inter-utility mutual assistance programs similar to those used for large power transformers, to ensure an adequate supply of critical equipment in an emergency. To explore this issue further, industry should undertake the following activities:

   a. The ESCC and its working groups should engage with other manufacturers in the electricity supply chain to share their respective security incident response capabilities, including the means to communicate industry-wide through a trusted channel—such as the E-ISAC.

   b. Given the pervasive potential risk from the supply chain threat vector, NERC, the North American Transmission Forum, and the North American Generator Forum should continue their various initiatives (e.g., developing industry guidance for vendor-identified incident response measures) to address supply chain management risks.

   c. Participants noted that a critical component stockpile, such as a protective relay reserve similar to the transformer reserve, could fill a critical component gap in a cyber attack against the grid. The ESCC and its working groups should consider how to develop such a reserve to support industry.

6. **Continue to grow participation in the ESCC CMA program.** The ESCC's CMA program, consisting of more than 160 electricity and natural gas utilities, provides a legal framework for participating electric and natural gas utilities to request or respond to requests for assistance in advance of or in the event of a cyber emergency. CMA allows impacted-utilities to augment their response capabilities through assistance that may take the form of information sharing, personnel, services, and equipment. CMA is a voluntary program that include investor-owned, public power and cooperatives as well as regional transmission organizations and independent system operators; there is no cost to participation. To further the impact of CMA:

   a. Utilities currently not participating should sign onto the program non-disclosure agreement to have the ability to request resources from industry peers in the event of a cyber emergency. The ESCC and relevant trade associations should continue to promote this capability, including to independent power producers.

   b. Utilities already participating in the program should continue to socialize the CMA activation process internally within their organizations to increase the likelihood of success in invoking CMA in the event of a cyber emergency.

7. **Continue to strengthen the operational industry and government coordination between the United States and Canada.** The involvement of Canadian participants has grown with each successive GridEx tabletop. In addition to the separate video teleconference, executives from three interconnected Canadian utilities and RCs participated in the tabletop in McLean, Virginia. As a result, participants were able to address the challenging scenario with first-hand knowledge of how they would respond. The initial video conference link with the tabletop in Ottawa reinforced the growing U.S.–Canada dialogue on electricity security issues and was foundational for future exercises. Participants agreed that future exercises should continue to include

coordination play within the North American electricity industry, as well as with the U.S. and Canadian governments. For the next GridEx, exercise planners should:

a. Use a scenario with an incident scope that includes Canada and the United States when designing the next GridEx executive tabletop.

b. When designing the next GridEx executive tabletop, NERC and the Canadian Electricity Association should invite Canadian government representatives (e.g., the Privy Council, Natural Resources Canada, Public Safety Canada) to participate in-person. In addition to federal government participants, NERC should invite government representatives at the provincial and state levels to further explore additional operational issues.

Distributed Play Observations and Recommendations

The observations gathered for this report were compiled from the feedback of those on the exercise planning team, interviews with the Grid Exercise Working Group, and lessons learned gathered from 148 after action surveys. These observations and recommendations identify opportunities to enhance the security and reliability of the North American BPS:

1. **A flexible scenario structure enabled exercise planners to customize their GridEx experience and maximize learning to improve their organization's incident response preparations and capabilities.**
   Building on the success of GridEx IV's methodology, GridEx V continued the model of flexible, organization-specific exercise planning. For distributed play, each planner had the opportunity to customize their scenario, emphasizing their cyber, physical, and communications resilience as they chose. Some organizations could include physical security threats in their scenario while others might forego physical security play altogether. This flexibility was intended to allow organizations with different scales and priorities to all participate in the same exercise, deriving optimal benefit for their organizations, while retaining the opportunity to interact with external organizations during exercise play. After action survey results show that planners responded overwhelmingly in favor of the flexible survey format; however, some planners felt overwhelmed by the range of options and faced difficulty determining which options they should include in their own organization's planning.

Recommendations

a. NERC should continue to encourage exercise planners to customize the scenario to meet their own learning objectives. GridEx should continue to recognize the diverse needs of participating utilities and provide additional scenario examples to illustrate how GridEx can relate to their functional entity role (e.g., transmission operator, generator operator, distribution entity).

b. When considering how to customize the scenario, planners should start by deciding which operational processes they want to exercise within their organization. Clear operational goals will help planners decide which cyber or physical security scenario injects to use.

2. **Early planning allowed planners to benefit from the scenario's flexibility, but planners whose organizations joined later struggled to adequately prepare for the exercise.**
   Exercise scenario planning was finalized 10 months prior to execution, giving planners the time to develop customized scenario injects for their organizations. NERC also conducted regular, on-going training webinars and opportunities for question-and-answer sessions over the six-month lead-up to the exercise; this addressed a need identified after GridEx IV to finalize the master scenario events list at an earlier date while

maintaining engagement with planners to avoid fall-off. Organizations that joined the exercise at a later date, however, faced limitations in taking advantage of the available exercise material and tools.

Recommendations

a. NERC should continue to make information available to planners at least six months in advance of execution, giving them maximum time to prepare their organizations.

b. Consider making some planning documents publicly available. Two-factor authentication and firewall incompatibility made it difficult for some organizations to access documents during the planning stage. Reducing barriers to planning document access will reduce barriers to entry for organizations; this can be accomplished by making some of the exercise information TLP:WHITE and posting on NERC's website and give new organizations a clearer picture of the commitment participation in the exercise will require.

c. NERC should consider facilitating a "planner mentor" program of pairing experienced planners with new ones to help them navigate the planning process and get up to speed. With several iterations of successfully completed exercises behind GridEx, there are many veteran planners who could help new planners manage and prioritize their planning responsibilities.

d. The E-ISAC will continue facilitating partnerships between observers and organizations actively involved in GridEx.

3. **While many utilities used GridEx to strengthen their relationships with RCs, law enforcement, and government agencies, others lacked the resources necessary to coordinate responses to the challenges in the scenario.**
DHS's CISA, the FBI, numerous state agencies, local law enforcement, and National Guard units committed resources to GridEx. However, because of the individual planning responsibilities each organization took on in GridEx V, engagement with government agencies was largely dependent on existing relationships. In keeping with the GridEx V objectives, NERC will continue encouraging utility and government incident response cooperation through exercises (e.g., GridEx, Liberty Eclipse) and security conferences like GridSecCon.

Recommendations

a. Encourage RCs to work with utilities in their areas to coordinate scenario development. RCs are well positioned to pair utilities with local government resources and neighboring critical infrastructure partners.

b. Encourage planners to reach out to law enforcement and emergency responders for support in GridEx. In GridEx's current format, it is incumbent on each organization to coordinate with government and cross-sector incident response partners as they would in an actual event.

c. Planners should enhance utility-government partnerships, such as embedding DHS protective security advisers with utilities or liaising with DHS watch centers and state fusion centers.

4. **GridEx distributed play and the GridEx executive tabletop should occur on different dates so that leadership teams can achieve maximum training value for their organizations.**
Coinciding with distributed play, some senior executives from active organizations participate in an executive tabletop. The necessary preparation and participation prevents them and their staff from fully taking part in the distributed exercise.

Recommendation

a. NERC should move the executive tabletop to another time period separate from distributed play exercise.

5. Some participants were confused or overwhelmed by the Move 0 scenario.

Move 0 is the "world building" phase within GridEx preceding Move 1. E-ISAC members received three to five exercise threat notifications a day during the three weeks prior to the start of GridEx V. Players felt the Move 0 notifications were successful in conveying a sense of rapidly increasing threat level against the North American grid. Some participants felt the length of Move 0 was drawn out and wished there was more flexibility on selecting notifications.

Recommendations

a. The GridEx planning team will consider consolidating and shortening Move 0 injects from three weeks to one or two weeks.

b. NERC should provide Move 0 E-ISAC Exercise Portal notifications as an opt-in at registration.

6. Responses to the cyber injects in GridEx were overwhelmingly positive and participants have requested new cyber security inject material for GridEx VI.

A fictitious malware called MOOSESCEPTER,[3] which was created by Idaho National Laboratory through DOE's National Exercise Program, was used as the principal adversary cyber malware campaign within GridEx V. In the exercise, electricity industry cyber security professionals faced a problem set that included artifacts, signatures, and suspicious files. Respondents described the MOOSESCEPTER scenario inject material as "exciting," "original," and "truly challenging."

Recommendation

a. To facilitate more cyber challenges, the GridEx program will continue to use its relationship with DOE and national laboratories to seek out leading-edge cyber training capabilities. This will allow organizations to seek a more immersive exercise cyber security experience.

7. GridEx V saw an expansion in the scope of crisis communication tools and their adoption.

NERC encouraged planners to delegate planning for crisis communications play to a separate communications planner during the planning phases of GridEx V. Recognizing that crisis communications is an integral part of crisis response, NERC has encouraged planners to include their organization's crisis communications and public relations staff in the exercise. To facilitate this inclusion, NERC provided an enhanced SimulationDeck tool for communications staff to use during the exercise to simulate their media posts. The training NERC provided to these communications planners led to expanded use of SimulationDeck in GridEx V with more than 1,300 posts, a 50% improvement on GridEx IV adoption. Most survey respondents felt GridEx V afforded a strong opportunity to exercise their external communications with those responding "very well" rising from 18% to 40% and those responding "not well" falling from 18% to 8%.

Recommendations

a. Move GridEx registration to a separate website. This will assist in focusing player use of SimulationDeck solely as a means for crisis communications.

[3] The cyber inject material was developed specifically for GridEx by the Department of Energy's Idaho National Laboratory and was presented and discussed with planners during GridEx planning webinars.

b. Consider developing more social media interaction between communications players and other exercise participants to increase relevance of communications and SimulationDeck play. For instance, planners could structure reports of incidents or threats in the public domain to have relevance for physical security; successful addressing of incidents could be reported by communications players as well.

8. **The E-ISAC Exercise Portal succeeded as an information sharing portal for utilities and RCs, but the CBP coordination call access caused confusion in some organizations.**
An exercise-specific mirror of the E-ISAC Portal replicated the information sharing functionality of the E-ISAC. While 79% of respondents felt the E-ISAC was effective in providing collaboration tools through the E-ISAC Exercise Portal, 92% of respondents felt the E-ISAC was effective at sharing information and providing high-level situational awareness in the exercise, up from 70% in GridEx IV. Most of the GridEx V threat information shared was restricted to E-ISAC asset owner and operator members (as it is in real-life). Some respondents were confused as to why their organizations did not have access to the portal while other respondents felt the CBP call did not sufficiently reflect the way a critical communication at the start of an event would be sent.

Recommendation

a. The E-ISAC should consider conducting CBP communications via multiple means, such as a prerecorded briefing posted to the E-ISAC Portal, creating a security "podcast," and/or a live dial-in capability.

9. **The ESCC used the distributed exercise play to successfully test industry-government coordination at the outset of a no-notice incident as well as an activation of the CMA Program.**
In 2019, the ESCC updated its playbook to include a new series of staff- and executive-level coordination calls with the federal government that are used at the outset of a no-notice incident. These calls are designed to quickly share information on disaster impacts and response operations as well as align industry and government messaging regarding the incident. The new series of calls was tested as part of the GridEx V distributed exercise play on November 13. During the exercise, the ESCC and the CMA Program each successfully tested the resilient communications capabilities that are being developed by the Council's Research and Development Committee.

The CMA Program was successfully activated during distributed exercise play to share information as well as resources. Participation in CMA exercise play increased from GridEx IV to GridEx V and incorporated both regional and national play.

Recommendations

a. As part of their incident response planning protocols, electric entities should consider pre-identifying a public information officer and an operations lead to participate in the staff-level coordination calls if asked by the ESCC Secretariat. These protocols should also consider that executive-level participation may be required for some calls that include ESCC leadership and senior executives from the federal government.

b. NERC and the E-ISAC should consider developing a portion of the GridEx VI distributed play that would have a common scenario used by multiple electric entities. This portion of the exercise would help facilitate ESCC participation and allow for easier integration and testing of industry-wide capabilities, such as CMAs and spare transformer programs, during the exercise.

Conclusion and Next Steps

At the conclusion of GridEx V, participants agreed that the exercise helped reinforce the need to continue to build on the collaborative relationships between the electricity industry, cross-sector partners, and government necessary to mitigate ever-evolving security risks against the North American grid.

Next Steps

- The exercise identified opportunities to improve the E-ISAC's timely and actionable communications to its members through its CBP. Future CBPs will use multiple means to reach stakeholders, such as an All-Points Bulletin, prerecorded briefings posted to the E-ISAC Portal, creating a security "podcast," and/or a live dial-in capability.
- The GridEx planning team will include RCs in scenario development so that the simulated operational impacts designed for GridEx VI are realistic and act as a regional scenario baseline for distributed play.
- The ESCC and the EGCC should review and prioritize 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 VI in November 2021.
- NERC and the E-ISAC are committed to continue enhancing the GridEx program to meet the challenges posed by the ever-evolving threat environment. Participants suggested topics for a next executive tabletop that included the following:
  - **Interdependencies with the Communications Sector:** Build on the positive contribution of the natural gas participants at GridEx V by inviting a similar level of participation from the communications sector to the next tabletop.
  - **North American Scope:** Continue to build on the increasing participation of Canadian utilities, RCs, and government, including Mexican entities as appropriate.
  - **Critical Supply Chains**: Build on the positive contribution of the supply chain provider who participated in GridEx V by including other critical providers in the exercise.
  - **Policy and Operations**: Thanks largely to the active participation of industry executives, GridEx V successfully addressed policy matters within the context of operational realities. The next executive tabletop should continue this approach with the following:
    - Scenario that is regional in scope and involves the United States and Canada
    - Focus on a few key issues
    - Breakout sessions to simulate communications during a real event

Appendix A: Exercise Objectives

Objective 1: Exercise Crisis Response and Recovery

Achieved: The scenario included multiple cyber and physical attacks affecting the BPS. Participants indicated in the after action survey that the scenario provided the opportunity to exercise cyber security, physical security, and operational incident response plans with 97% indicating "very well."

Objective 2: Expand Local and Regional Response

Achieved: A total of eight National Guard units, 29 FBI Field Offices, and 26 state governments participated in GridEx V, expanding participation with state and local law enforcement.

Objective 3: Engage Critical Interdependencies

Achieved: GridEx V saw an increase in the participation of other interdependent organizations, including 16 natural gas utilities,[4] 13 water utilities, and three telecom companies (up from four, five, and two respectively); this is a trend NERC hopes will continue in GridEx VI.

Objective 4: Increase Supply Chain Participation

Partially Achieved: Only three major electric industry supply chain vendors officially registered for GridEx V, although the number of participating vendors may have been greater. It is incumbent upon participating organizations to include supply chain partners in their response plans. Some organizations chose to engage with their supply chain partners during the exercise while others did not.

Objective 5: Improve Communication

Achieved:

- 97% of respondents indicated that GridEx provided a "very good" or "good" opportunity to exercise their internal communications response plans.
- 92% of respondents indicated that GridEx provided a "very good" or "good" opportunity to exercise their external communications response plans with other electricity industry entities.
- 82% of respondents indicated that GridEx provided a "very good" or "good" opportunity to exercise their external communications response plans with other non-electricity industry organizations (with 39% replying "very good," up from 28% in GridEx IV).
- 77% of respondents indicated that GridEx provided a "very good" or "good" opportunity to exercise their external communications response plans with other critical infrastructure sectors.

Objective 6: Identify Lessons Learned

Achieved: NERC received 148 after action surveys, 120 of them from electric utilities. These reports identified actionable lessons learned, acknowledged the value of NERC's GridEx program, and informed this report. Early in the planning process, NERC developed a template to encourage participating organizations to identify their lessons learned and share them with NERC without attribution to individual organizations, where appropriate. These lessons learned help industry identify possible initiatives to enhance response to cyber

[4] Of the 277 electric entities that participated in GridEx V, 56 are also natural gas entities.

and physical attacks or improve future exercises of this nature. NERC recognizes that, in some cases, organizational lessons learned may be particular to the individual company; however, what may seem to be a unique lesson learned to an organization often is part of a much larger trend across an enterprise. NERC encourages participating organizations to share their lessons learned that can possibly reduce cyber and physical security risk across the BPS.

Objective 7: Engage Senior Leadership

Achieved: The executive tabletop focused entirely on this objective, and its results are included in this report. In addition, many states' governor's offices, state emergency management agencies, and senior management crisis response teams participated in GridEx V. Senior industry and government also participated in an ESCC coordination call that was part of the distributed play exercise on November 13.