NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Grid Security Exercise GridEx IV

Lessons Learned

March 2018

TLP: WHITE

RELIABILITY | ACCOUNTABILITY



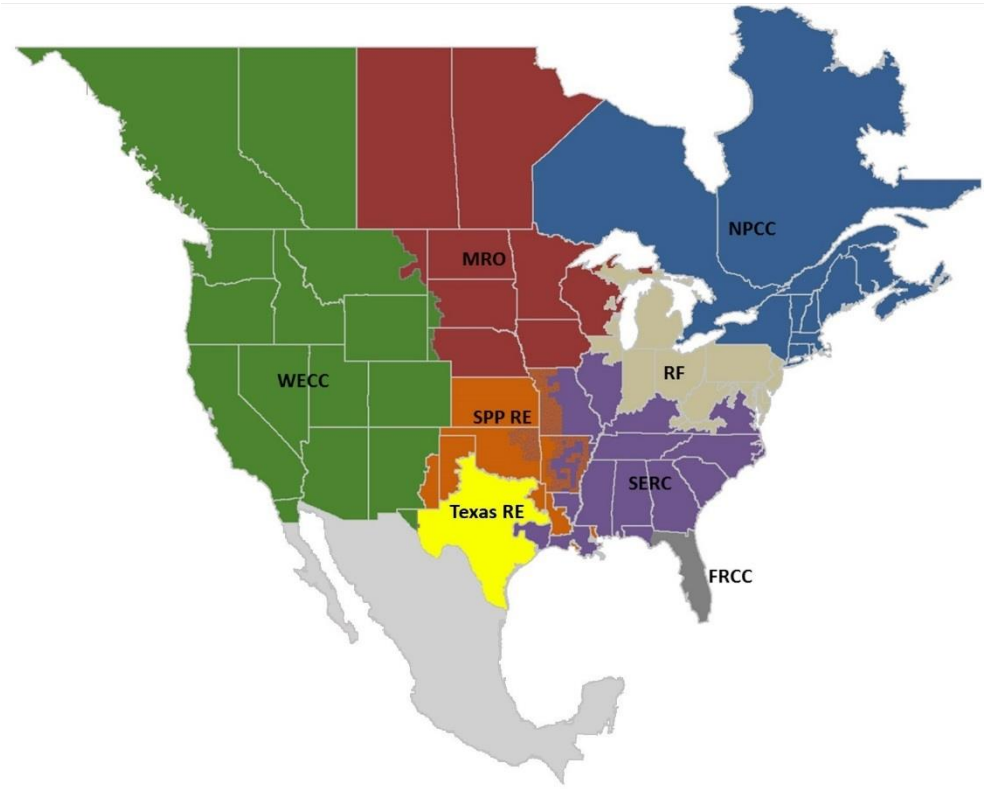

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the eight 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.

The North American BPS is divided into eight RE boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

NERC built on lessons learned from previous iterations of GridEx and from established planning-process milestones to develop the fourth grid security exercise, GridEx IV, then developed metrics to assess the value of the exercise overall.

Similar to GridEx III, GridEx IV retained the model of two days of distributed play with a separate executive tabletop on the second day. In addition, GridEx IV maintained the design goal of increasing utility participation as well as participation by other critical infrastructure organizations and state/provincial and local governments in the United States, Canada, and Mexico.

The large rise in participation from previous exercises led to GridEx IV being managed in a decentralized manner. The decentralization allowed the NERC planning team to structure the exercise with flexibility for organizations to determine the scope and extent of their own participation and to drive more customized events that they would experience during the exercise that were consistent with the high-level scenario. Lead planners decided whether their organization would operate in an "active" or "observing" capacity, what physical or cyber attack vectors their organization would experience, and what other participating organizations they would coordinate action with during the exercise. Lead planners independently distributed exercise injects within their organizations without needing to coordinate with GridEx IV's Exercise Control. The distribution of exercise injects by lead planners 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 IV, 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 on page 13 of this report.

Executive Summary

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

NERC conducted its fourth biennial (once every two years) grid security and emergency response exercise, GridEx IV, from November 15–16, 2017. With 6,500 individuals and 450 organizations participating across industry, law enforcement, and government agencies, GridEx IV consisted of a two-day distributed play exercise and a separate executive tabletop on the second day. The exercise provided an opportunity for various stakeholders in the electricity sector to respond to simulated cyber and physical attacks that affect the reliable operation of the grid, fulfilling NERC's mission to assure the effective and efficient reduction of risks to the reliability and security of the BPS. Led by NERC's E-ISAC, GridEx IV was the largest geographically distributed grid security exercise to date. Electric utilities continue to use the planning materials for separate exercises with NERC, government, and consultant support.

In addition to the distributed play portion of GridEx IV, a six-hour executive tabletop portion took place on November 16 that involved industry executives and senior government officials. The 42 participants included a cross-section of industry executives and senior officials from federal and state governments. The tabletop was facilitated as a structured discussion for industry and government to share the actions they would take and issues they would face in responding to the scenario. Participants articulated the severe limitations and barriers that would need to be addressed, both independently and collaboratively, to respond.

The objectives of GridEx IV were to do the following:

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

Distributed Play Results

NERC and participating organizations succeeded in achieving these objectives. Responding to the after-action survey, 42 percent of participants indicated the exercise met their expectations "very well" and 55 percent indicated "well" for a total positive response of 97 percent. However, 22 percent of participants responded that GridEx IV did not offer an effective opportunity for electric utilities to exercise their external communications response plans with external organizations, such as law enforcement and state emergency managers. External communication concerns should be addressed in future security exercises.

In addition to the after-action survey, participating organizations were encouraged to identify their own lessons learned and share them with NERC. NERC used this input to develop observations and propose recommendations to help the electricity industry enhance the security and reliability of North America's BPS.

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

The GridEx IV Distributed Play resulted in the following recommendations for future action by the electricity industry:

- **Increase Proactiveness of Lead Planners:** Lead planners were responsible for developing a scenario that would be tailored to their organizations' needs while operating within the overarching GridEx design. While most organizations were successful overall, some were inadequately prepared for the exercise or did not reach out to other stakeholders. Lead planners should take a more proactive role in bringing in their necessary internal players and external organizations, namely other electricity entities they operate with regularly, local law enforcement, government agencies, and utility equipment vendors.

- **Increase Participation from Law Enforcement and Other Critical Infrastructures:** GridEx IV saw greater cross-sector collaboration than previous exercises. Law enforcement participants actively coordinated with electrical entities within their areas of responsibility. However, players did not engage much with vendors. Lead planners should seek out opportunities to include the cross-sector, supply chain, and law enforcement organizations in their exercise play.

- **Strengthen E-ISAC Portal Functionality:** A "Common Operational Picture" function should be added to the E-ISAC web portal. Organizations expressed the need for more awareness of the overall North American grid and a central location to keep track of all statuses and information.

- **Enhance Public Affairs and Corporate Communications:** Utility corporate communication organizations should use their existing external communications procedures or use GridEx as a driver to develop or refine their communications procedures if they do not exist or are not suitably comprehensive; this would provide organizations with a framework and general guidelines to respond during a crisis. Additionally, an external communications procedure would include recommended actions that would be helpful in addressing misleading or false information in the social media sphere.

- **Enhance Reliability Coordinator Communications:** The Reliability Coordinator Information System (RCIS) lacks an exercise functionality that allows operators to use the production system safely and seamlessly for training and exercises. NERC should re-platform RCIS with a built-in exercise functionality.

- **Increase Communications Resilience:** Utilities should develop and maintain communication contingency plans that use multiple technologies so that communication resiliency is maintained in the event one or more channels are lost. For example, the United States Department of Homeland Security's Wireless Priority Service (WPS) and Government Emergency Telecommunications Service (GETS) are available to United States utilities. Additionally, the E-ISAC should gain its own organic high-frequency radio system and become a member of the SHAred RESources (SHARES) High Frequency (HF) Radio Program.

- **Increase Cyber Mutual Assistance Program Participation:** The Cyber Mutual Assistance (CMA) program provides a pool of utility cyber security experts who volunteer to share their expertise with other utilities in the event of a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency.[2] NERC recommends that more utilities participate in the CMA program. Additionally, the Electricity Subsector Coordinating Council (ESCC) and the E-ISAC should engage more with the CMA program to encourage the efficient sharing of relevant information in the event, or in advance, of a cyber emergency in a manner that complies with the CMA program's non-disclosure agreement.

[2] At present, more than 140 utilities, which represent approximately 80 percent of utility customers, participate.

- **Enhance Move 0 Development:** Move 0 was intended to be an opportunity to prepare GridEx IV participants prior to the two-day exercise and provide players with hands-on training in responding to the cyber threats to be experienced in the exercise scenario. The intent and objectives of Move 0 need to be developed so as to flow seamlessly into the rest of the exercise. As the capability and scope of Move 0 increases, both physical and cyber security elements should be added.

Executive Tabletop Results

The tabletop scenario involved multiple sophisticated cyber and physical attacks that targeted the electricity industry's critical grid control systems, key generation and transmission facilities, and other critical infrastructure facilities that caused widespread and prolonged power outages. The tabletop was structured around three time frames to address the unique policy-level challenges that would arise as the scenario evolved over time:

- **One day after the attacks began:** initial situation assessment
- **Three days after the attacks began:** urgent and unresolved issues require immediate attention
- **Two weeks after the attacks began:** strategic decisions needed to take extraordinary actions

The GridEx IV executive tabletop resulted in the following recommendations for future action by industry and government:

- **Increase Utility Coordination with State and Local Governments:** Utilities should continue to build their relationships and communications capabilities with law enforcement and state and local governments to ensure information is shared early and often.

- **Enhance ESCC and EGCC communications:** The ESCC and Energy Government Coordinating Council (EGCC) play an important coordinative role and should continue to enhance their ability to share information at the national level.

- **Increase Coordination with Federal Government:** The Department of Defense and many other federal agencies will place their highest priority on stopping the attacks at their source, preventing future attacks, and identifying the adversaries. Utilities should be prepared to coordinate with local law enforcement and state-level organizations (e.g., National Guard) to secure utility facilities.

- **Ensure Unity of Public Messages:** The ESCC and the EGCC can help develop and vet public messages to ensure they are consistent with information provided by utilities to their employees and customers.

- **Increase Grid Emergency Response Capabilities:** Grid operators have extensive authorities, plans, tools, and training to operate the grid through emergency conditions. Utilities should consider how to build upon these capabilities to respond to the especially disruptive attacks presented in this tabletop scenario.

- **Increase Timeliness of NERC and E-ISAC Information:** NERC and the E-ISAC should enhance their ability to provide reliable, timely, and accurate information regarding the state of grid reliability and security threats and events.

- **Strengthen Coordination with Other Critical Infrastructures:** The interdependencies between utilities and other critical infrastructure sectors are complex. Utilities and the E-ISAC should strengthen their relationships with other critical infrastructures to consider the challenges of a severe event.

- **Develop ESCC Process for Emergency Orders:** Under this severe attack scenario, the exercise assumed that the president of the United States would declare a grid security emergency. Once that declaration is made, the Secretary of Energy may issue emergency orders to the industry to protect the grid or restore reliability. DOE, the EGCC, and the ESCC should develop consultation processes to help ensure any emergency orders are appropriate.

- **Ensure Utilities have Access to Sensitive Information:** The number of utility personnel who hold government security clearances is small and is not sufficient to share classified information under this severe scenario. Government should plan to quickly declassify information that utilities need to prevent or respond to attacks.

- **Ensure Financial Needs are Met during Recovery:** Under this severe attack scenario, utilities would need extraordinary levels of financing to maintain recovery operations. Government should be prepared to support utilities and stabilize financial markets.

- **Identify State and National Priorities:** State and federal governments should develop flexible mechanisms to identify high-priority utility customers or service areas and communicate these priorities to utilities.

- **Continue to Promote the Large Power Transformer Transportation Program:** Utilities, in partnership with the freight rail sector, should continue[3] to expand participation in the ESCC's large power transformer transportation program.

- **Continue to Promote the Cyber Mutual Assistance Program:** The CMA program provides a pool of utility cyber security experts who volunteer to share their expertise with other utilities. The CMA program should continue to enhance its capability by engaging more members and other stakeholders such as the E-ISAC, critical supply chains, and National Guard.

[3] Reference Strategic Transformer Reserve, Department of Energy Report to Congress, March 2017: https://energy.gov/sites/prod/files/2017/04/f34/Strategic Transformer Reserve Report - FINAL.pdf

Chapter 1: Participation

Distributed Play Participants

In preparation for GridEx IV, the NERC planning team was tasked with the following:

- Design a wide ranging but credible scenario
- Include all interested electricity utilities
- Involve all NERC Regional Entities and Regional Coordinators[4]
- Increase the percentage of active (rather than observing) organizations
- Encourage greater coordination between physical and cyber security personnel and power system operators

Achieving these objective allows organizations greater freedom in designing scenarios that fit their specific needs. This decentralized approach was successful as GridEx IV was the largest physical, operational, and cyber grid security exercise to date, involving more than 6,500 registered individuals from more than 450 organizations across North America. As shown in **Figure 1.1**, GridEx IV continued the upward trend of participation in the GridEx program.

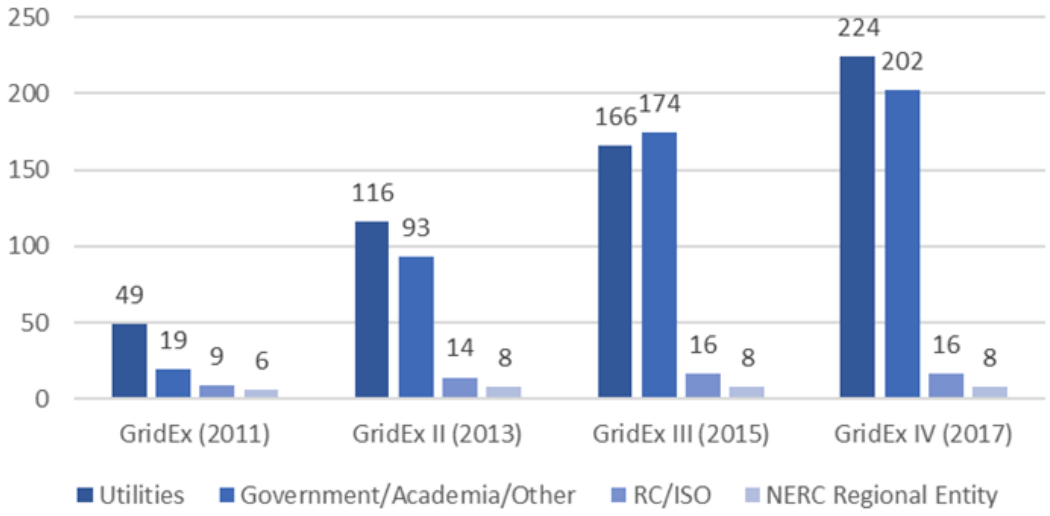


Figure 1.1: GridEx IV Participation

Participation in GridEx IV, as with all previous NERC exercises, was voluntary. Although GridEx IV provided participants the opportunity to demonstrate meeting NERC regulatory requirements related to exercises and training, NERC explicitly stated in advance that there would be no compliance monitoring or enforcement actions related to participation in GridEx IV.

E-ISAC invited organizations to participate in an active or observing capacity but strongly encouraged active participation so that organizations could get the most value from the exercise. The types of participation are outlined as follows:

[4] As defined by NERC's functional model, Reliability Coordinators are the highest authority responsible for the day-to-day operation of the bulk power system. There are 16 Reliability Coordinators across North America: http://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx

- **Active Organizations:** Active organizations participated in GridEx IV by assigning staff prepared to respond to the scenario as if it were a real event according to their role (e.g., cyber and physical security, power system operations, plant operations, crisis management). Active organizations that benefited the most from participating in GridEx IV were those that committed the necessary resources (i.e., lead planners and players with cyber security, physical security, and operations responsibilities) early in the exercise planning process. Response activities included sharing information and coordinating efforts with other active organizations consistent with what would be expected during a real event. Active organizations included utilities, RCs, local law enforcement, and government authorities. Consistent with the rapidly growing size of the exercise, GridEx IV continued the upward percentage of active participants vs. observing organizations (see **Figure 1.2**).

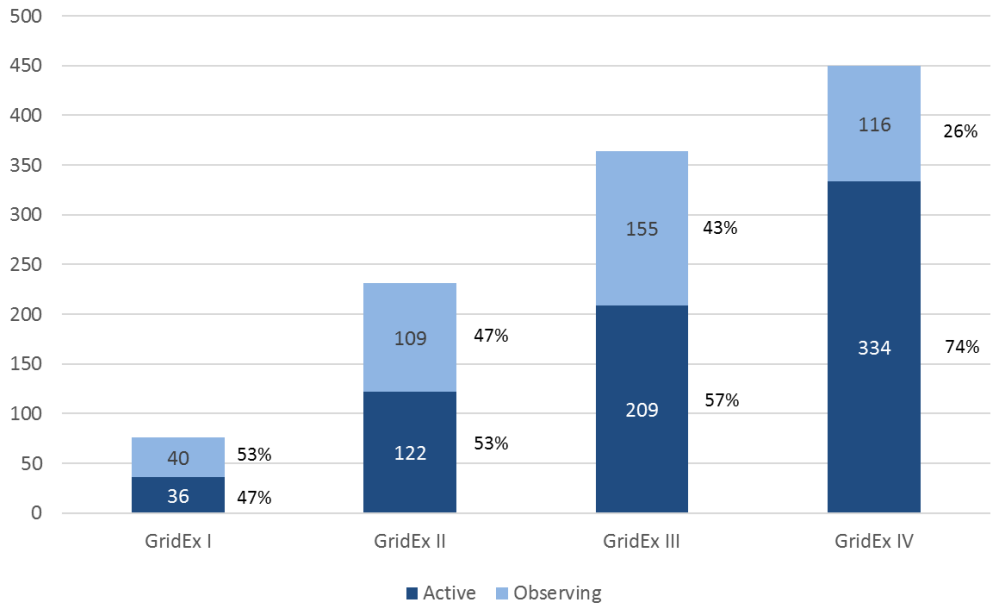


Figure 1.2: Electricity Sector Active vs. Observing Participants

- **Observers:** Observing organizations did not respond to the scenario events and did not interact with active organizations. However, they did have access to the entire range of planning documentation to use (e.g., to conduct their own internal tabletop exercise). Observer status has proven to be a great way of introducing the GridEx program to new organizations; a total of 30 percent of the observers from GridEx III became active participants in GridEx IV. NERC was particularly encouraged that observers from the water and natural gas sectors participated and anticipates engaging in more active cross-sector coordination in future exercises.

Executive Tabletop Participants

The tabletop was facilitated by a former senior Department of Defense (DOD) official who asked participants to discuss the decisions and actions they would take as the scenario evolved. Participants also discussed the support that might be needed from other critical infrastructure sectors and government agencies. The electricity industry participants included chief executive officers from investor-owned utilities and publicly owned utilities, cooperatives, Independent System Operators, and Regional Transmission Organizations. Other critical infrastructure sectors included representatives from financial services, communications, natural gas, and critical manufacturing. United States federal and state governments were represented by senior officials from the following departments and agencies:

- White House, National Security Council

- Department of Energy (DOE)
- DHS, including Federal Emergency Management Agency (FEMA)
- DOD, including U.S. Cyber Command, U.S. Northern Command
- Federal Bureau of Investigation (FBI)
- National Guard: Illinois and Wisconsin
- States of Maryland and Virginia

Chapter 2: Exercise Objectives

NERC developed six primary exercise objectives with each containing sub-objectives and metrics to help determine the level to which each objective was met. As described below, all six exercise objectives were accomplished.

Objective 1: Exercise Crisis Response and Recovery—Achieved

- **Increase the number of participating organizations and individuals:** GridEx IV participation grew by 86 organizations and more than 1,800 individuals compared with GridEx III. The number of active organizations increased by 17 percent with 74 percent of participants serving in an active role. South Carolina participated in GridEx as part of their annual cyber exercise program, providing a model for future state participation.
- **Increase the extent to which entities exercise their cyber, physical, and operations response:** The scenario included multiple physical and cyber attacks that affected the BPS. Participants indicated in the after-action survey that the scenario provided the opportunity to exercise cyber, physical, and operational security response plans with respondents, indicating a minimum of 96 percent "very well" or "well."

Objective 2: Expand Local and Regional Response—Achieved

- **Involve local law enforcement in the emergency response plan:** Eight state police forces participated in GridEx IV.
- **Coordinate with State National Guard for cyber and physical incident response**: Six State National Guards fully participated in GridEx IV. In the case of Wisconsin and South Carolina, both states used GridEx IV as their annual statewide cyber exercise.
- **Coordinate with FBI field offices for incident response in regards to cyber and physical attacks against the grid**: A total of 29 FBI field offices participated in GridEx IV.
- **Coordinate emergency response with state emergency managers:** A total of 17 state emergency management agencies participated in GridEx IV.

Objective 3: Engage Critical Interdependencies—Achieved

- **Involve cross-sector entities in GridEx IV:** GridEx IV saw the participation of four gas utilities, five water utilities, and two telecom companies. NERC expects cross-sector entities to play a larger and more active role in GridEx V.

Objective 4: Improve Communication—Achieved

- **Increase the extent to which entities exercised communications processes within their organization:** A total of 99 percent of after-action report respondents indicated "very well" or "well."
- **Increase the extent to which entities exercised communications processes with their RC and other neighboring entities:** A total of 72 percent of after-action report respondents indicated "very well" or "well."
- **Increase the extent to which entities exercised communications processes with law enforcement and other government entities:** A total of 78 percent of after-action report respondents indicated "very well" or "well."
- **Increase extent to which participants will engage secondary and tertiary means of communication (e.g., SATCOM, HF, WPS, GETS):** Many lessons-learned reports received from organizations highlighted the importance of alternative communication methods during a crisis event. In particular, many agencies discovered that their employees were unaware or unfamiliar with alternate communication at their disposal

or that some of the methods were insufficient in satisfying organizational requirements; as such, NERC will continue to incorporate secondary and tertiary means of communication in future exercises.

- **Increase the extent to which entities exercised communications processes with NERC's E-ISAC and Bulk Power System Awareness departments:** A total of 91 percent of after-action report respondents indicated "very well" or "well."

Objective 5: Gather Lessons Learned—Achieved

- **Identify lessons learned not identified in previous exercises:** NERC received a total of 25 lessons-learned reports. These reports identified actionable lessons learned, acknowledged the value of NERC's GridEx program, and were used to inform this report. Early in the planning process, NERC developed a template to encourage participating organizations to identity their lessons learned and, where appropriate, share with NERC without attribution to individual organizations. These lessons learned help industry identify possible initiatives to enhance response to cyber and physical attacks and 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 times is part of a much larger trend across an enterprise. As such, NERC should encourage participating organizations to share all their lessons learned as this presents an opportunity to identify and improve problem areas.

Objective 6: Engage Senior Leadership—Achieved

- **Explore what and how information is shared between the electricity industry, the public, and government:** The executive tabletop portion of GridEx IV focused entirely on this objective. In addition, many state governors' offices, state emergency management agencies, and senior management crisis response teams participated in GridEx IV.

Chapter 3: Exercise Design, Planning, and Scenario Development

Planning for GridEx IV began in March 2016. NERC conducted a series of conference calls and planning meetings with lead planners from participating organizations in order to gather input on the exercise time line and on any boundaries that needed to be set. Continuing with the development model of GridEx III, NERC's Critical Infrastructure Protection Committee (CIPC) established the GridEx Working Group (GEWG), which consists of industry and government subject matter experts in cyber and physical security as well as BPS operations. With the NERC planning team's guidance and support, members of the GEWG shaped the design and scenario of the exercise over the timeline illustrated in **Figure 3.1**.

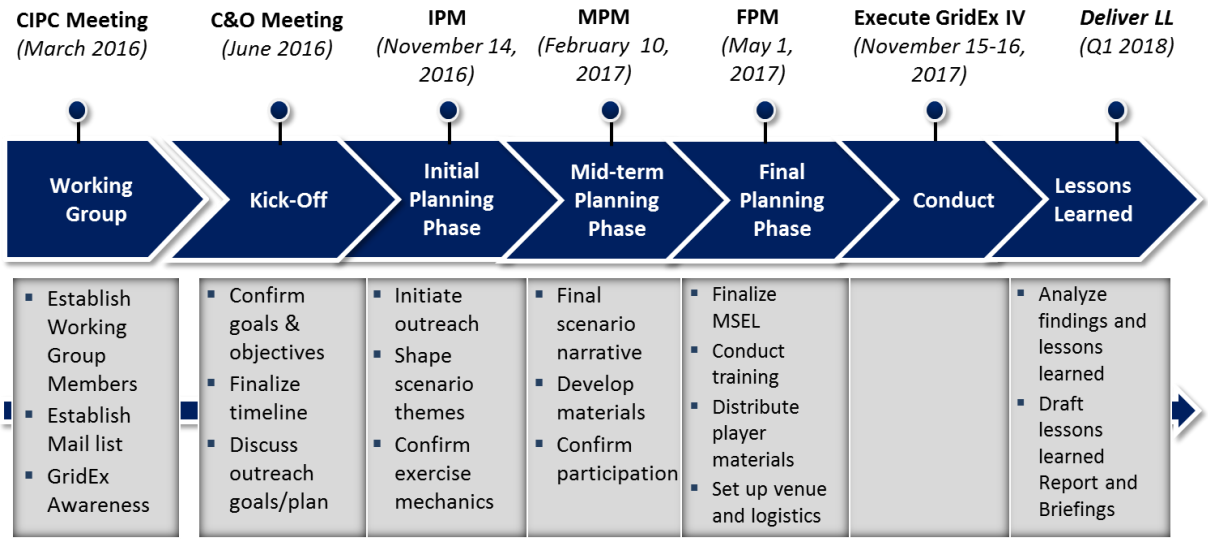


Figure 3.1: GridEx IV Planning Timeline

NERC continued the development model of encouraging customization and coordination at the local level. This allowed organizations to tailor the exercise so that it was both more realistic to their players and addressed their incident response training needs. However, with GridEx IV being designed with greater decentralization, NERC gave RCs a larger role in coordinating the exercise scenario within their operational footprint. This involved RCs holding planning meetings and conference calls with their neighbors and associated utilities in order to coordinate exercise activities.

Baseline Scenario Development

The NERC planning team and the GEWG did not include grid blackstart and system restoration processes[5] in GridEx IV; doing this would limit the ability of all participants to remain fully engaged throughout the exercise. This is also consistent with the GridEx III scenario.

The baseline scenario was structured into four "moves" (i.e., chronological sequences of scenario events) with each move lasting four hours. The scenario injects[6] for each move were conducted in real-time with 30-minute breaks between moves to give players and planners time to discuss lessons learned, identify problems, and to catch-up on real-world activities as necessary. Responding to feedback from GridEx III, all time jumps were removed for GridEx

[5] System restoration drills and exercises are regularly conducted by electricity entities (ref. NERC Reliability Standard EOP-006-2).

[6] The injects are events, typically planned through entries on the master scenario events list, that lead planners must put into play, including directives, instructions, and decisions. Exercise planners provide injects to exercise players to drive exercise play towards the achievement of objectives. Injects can be written, oral, and/or transmitted via any means.

IV, making each move's exercise time align with real world time. Moves 1, 2, 3, and 4 occurred on November 15–16, 2017; an overview of actions can be seen in **Figure 3.2**.

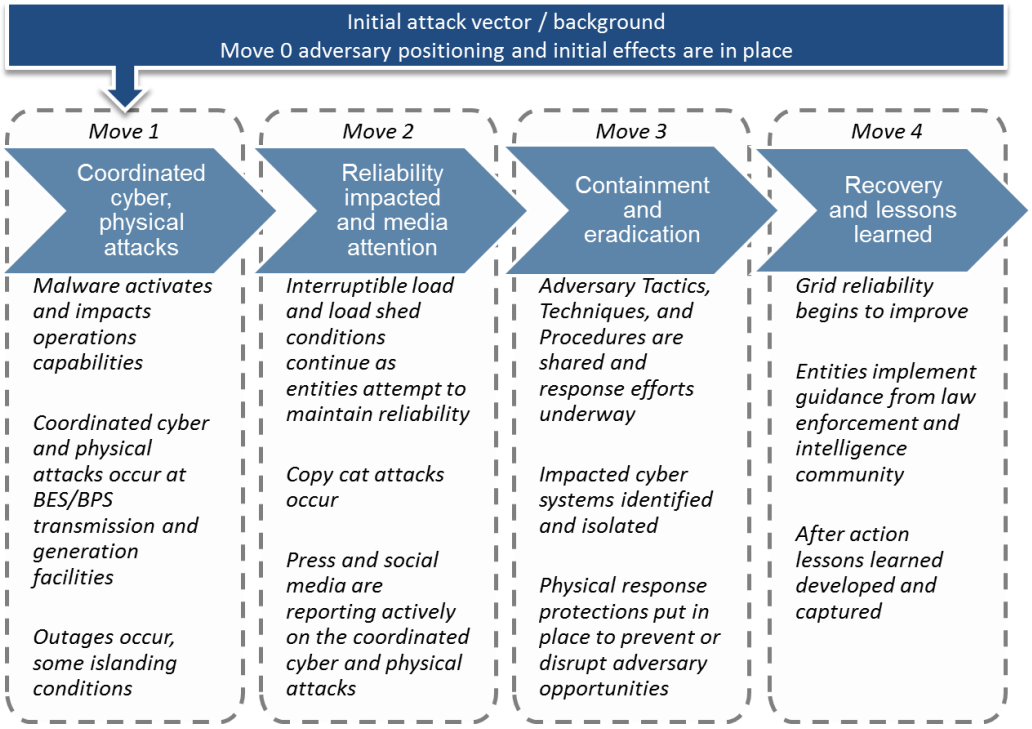


Figure 3.2: GridEx IV Moves

GridEx IV included a "Move 0" in the weeks leading up to November 15–16, 2017 (Moves 1, 2, 3, and 4). The "Move 0" event was focused on adversary preparation, reconnaissance, and execution activities that would lead into cyber attacks coordinated with physical attacks during the two-day exercise itself. This design allowed participants to focus on their response actions, information sharing, and restoration activities almost immediately at the start of the two-day exercise. It is important to note that Move 0 was not a prerequisite to participating in GridEx IV; if organizations did not have any player participate, they would still be able to kick off the exercise at Move 1 without a need for additional information.

Figure 3.3 illustrates the anticipated impact on grid reliability during the exercise for the distributed play. In order to begin the exercise in a degraded grid reliability level, Move 1 began with a degraded state and major "cyber booms" occurred early in Move 1, allowing Moves 3 and 4 to be dedicated more toward recovery and continuity operations.

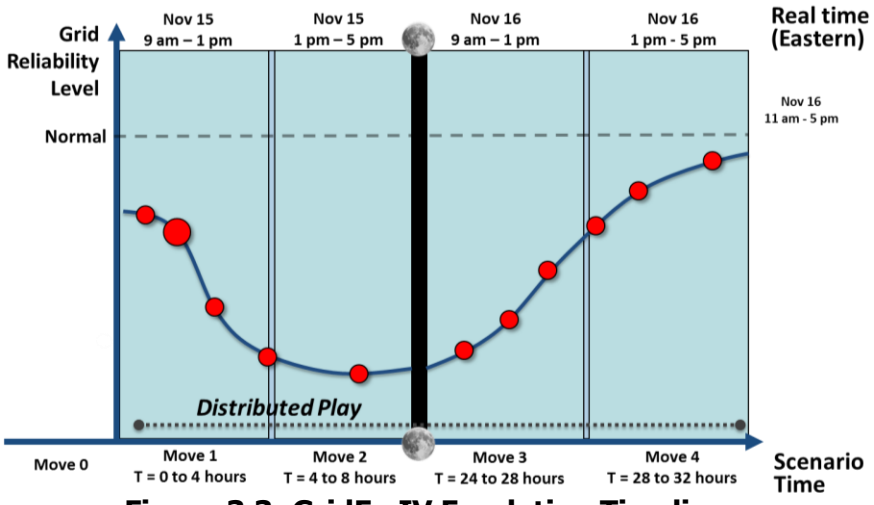


Figure 3.3: GridEx IV Escalation Timeline

Scenario Customization

Active organizations had the option to use the baseline scenario or customize it to better meet their own objectives, provided that they remained consistent with the baseline scenario. Responding to feedback from GridEx III, the scenario was completed six months prior to the start of the exercise to ensure organizations had plenty of time to tailor the exercise to their needs.

The baseline scenario included different cyber and physical attack options. The simulated cyber attack options included watering hole, patch deployment, and remote access vulnerabilities that affected utility industrial control systems (ICSs). Simulated physical attack scenarios impacted transmission and generation facilities.

By simulating attacks on their own assets and operations technology systems, players were able to exercise their own processes in a more realistic manner. The NERC planning team worked with RCs who coordinated with lead planners in their areas to maintain a consistent wide-area view of the impacts on the BPS, taking into account the customized attacks in order to ensure all participants remained consistent with the baseline scenario time line.

Exercise Tools

NERC maintained the same suite of exercise tools but enhanced some of their functionality for easier exercise play[7] based on feedback from GridEx III. Many organizations used their own tools to simulate their various operational processes (e.g., simulators used for power system operator training). The tools used during the exercise included the following:

Lead Planner GridEx IV Portal

The NERC planning team created a SharePoint site to share exercise-sensitive materials with lead planners who were provided access as they registered for the exercise. Throughout the planning process, the lead planner GridEx IV portal was the central hub to share information and provide updates to participating organizations. The portal also effectively served as a resource center for lead planners during the exercise itself as it held copies of all the exercise handbooks and quickstart guides.

While the portal proved to be an invaluable tool to prepare organizations for the exercise, some lead planners did not access the site until within two weeks of November 15, 2017. At that point, it was too late for these individuals

[7] This included adding organizations' favorites to SimulationDeck as well as a relaunch of the E-ISAC portal with enhanced functionality.

to adequately prepare for the exercise. In the future, additional effort should be made to ensure that lead planners routinely check materials on the portal.

SimulationDeck

SimulationDeck primarily served as a virtual social media environment and exercise directory in GridEx IV. The platform was used to generate social media functions that imitate Facebook, Twitter, YouTube, blogs, and traditional media (e.g., television, newspapers, and radio). All of the SimulationDeck functions could be used by individual organizations to fit their needs and scenario.

SimulationDeck performed well in its function in GridEx IV; however, it did experience periods of slowdowns and lagging performance. Part of the slowdown was attributed to the initial news clips that were posted on the site's homepage, which hogged significant bandwidth. Website administrators quickly resolved this problem by posting subsequent videos on a separate server, preventing interference with player activities. In the future, SimulationDeck should allocate double the required resources to handle the initial logins as this is where the site was most stressed.

E-ISAC Exercise Portal

The E-ISAC developed a mirrored version of their legacy E-ISAC portal with the same functionality as the production version. E-ISAC members with access to the production version of the portal were able to use it as if it were the production environment, greatly enhancing their ability to become more familiar with the portal and use it during a real event.

GridEx IV proved to be an effective way of finding areas of improvement for the legacy E-ISAC portal. In particular, it was found that the categories in the pull-down menus were insufficient to describe each electrical incident, too many groups received irrelevant messages by default, and the site did not have Common Operational Picture functionality. In response to these issues, and incorporating similar lessons learned from GridEx III, the E-ISAC launched a new portal in December 2017 and will continue to improve information sharing capabilities and access by stakeholder trust groups.

Simulated RCIS Reporting

The RCIS production reporting tool was not used for the exercise in order to avoid compromising its availability for real-time operations. As an alternative, the NERC planning team provided a generic email address for RCs to submit RCIS messages that were then distributed by Exercise Control (ExCon) to RCIS users using an email distribution list.

For future exercises, it is expected that RCIS will develop an exercise option to create a more realistic reporting process. In addition, the NERC planning team will advise organizations not to submit RCIS forms in PDF format as this created processing difficulties and presented a cyber-security vulnerability as PDFs can be embedded with malware.

OE-417/EOP-004 Reporting

GridEx IV simulated the submission of OE-417s[8] and EOP-004s[9] throughout the exercise through exercise forms sent to generic email addresses. However, organizations did not use the production forms or processes to ensure that exercise information was not subject to possible Freedom of Information Act requests.

Some organizations did not have the exercise forms at the start of the exercise. In the future, the NERC planning team will ensure templates are available to lead planners in August prior to GridEx V. Some organizations used RC-level custom tools (built with SharePoint-type software) that caused significant readability challenges for the E-ISAC and NERC's Bulk Power Situation Awareness.

[8] https://www.oe.netl.doe.gov/docs/OE417_Form_03312018.pdf
[9] https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-4.pdf

Vendor Helpdesk

The Vendor Helpdesk was created to simulate electricity industry vendors that were not participating in the exercise. Organizations could send messages to the generic email address if their particular exercise called for contacting the vendor of their equipment.

The Vendor Helpdesk did not receive a single email or phone call during the course of GridEx IV. For future exercises, this function will either not be used or greater emphasis will be placed on incorporating electricity industry vendors into GridEx V directly with individual utilities.

FBI Virtual Command Center

During the exercise, the FBI used the Virtual Command Center (VCC) to collect, aggregate, and share actionable, tactical information. FBI players viewed and updated the VCC while coordinating with their energy partners at all participating FBI field offices across the United States and at ExCon. The VCC could prove to be a valuable common operating platform for utilities in the real world and in the exercise.

Chapter 4: Exercise Conduct

GridEx IV was directed from a central location at the ExCon facility in McLean, Virginia, November 15–16, 2017. ExCon included NERC staff and contractors, certain GEWG members, government representatives, industry experts, and SimulationDeck staff. ExCon was responsible for monitoring progress and providing help desk support. Exercise players participated from their locations including corporate offices, generating stations, transmission substations, and control centers across North America.

Move 1 began on the morning of November 15, 2017. Operators and IT staff observed anomalous behaviors and some failures of energy management and other systems. Adversaries launched coordinated physical attacks at predetermined sites using vehicles to deliver explosive packages to damage and disable generation and transmission facilities. The attacks caused local and large-scale outages across the BPS, but the attacks were not impactful enough to cause cascading outages or interconnection-wide effects. News and social media reports regarding the physical and cyber attacks increased dramatically.

In Move 2, it became clear to participants that the attacks were large-scale and coordinated with facilities affected in multiple Regions across North America. The E-ISAC led an industry-wide situational awareness conference call to provide a summary of shared information and to report on impacts to the grid. Other critical infrastructure sectors (e.g., natural gas and communications) were also impacted, further complicating crisis response and recovery efforts. Participants continued to share information to identify vectors of the cyber attack. Industry also coordinated with local law enforcement and emergency services to respond to the physical attacks.

Move 3 then began on November 16, and participants started the day as if crisis response efforts had continued overnight. News videos and E-ISAC broadcast calls supplied information summarizing the night's events and set the stage for new scenario injects (See **Figure 4.1**).

Figure 4.1: Simulated News Broadcast

In some large metropolitan areas, system operators implemented emergency procedures such as rotating load shedding and voltage reductions to maintain BPS reliability. The E-ISAC conducted conference calls to review the

situation, provide support to participants, and issue bulletins and portal postings as new information became available. By mid-day, repair crews made progress in switching and isolating facilities in an effort to restore or bypass damaged and destroyed equipment, activating mutual assistance arrangements. Information sharing stayed steady. At the end of Move 3, ExCon paused the exercise to allow organizations to catch up on scenario injects and ensure objectives were accomplished.

Move 4 focused on participants' response actions during recovery of cyber systems and physical assets. Entities prioritized repairs and worked to restore service to customers. Law enforcement, supplemented by National Guard or similar forces, secured affected facilities so utility crews could assess damages and begin to make emergency repairs. NERC and the electricity industry continued to share information using E-ISAC portal postings and alerts, watchlist updates, and the RCIS. The Industrial Control System-Cyber Emergency Response Team (ICS-CERT) and other organizations continued to provide updates regarding the malware alert, indicators of compromise, and mitigation recommendations. The cyber attack vectors were identified and mitigated. Entities continued to work through recovery steps of their cyber incident response plans and retained data needed for forensic analysis.

GridEx IV distributed play ended after Move 4. **Figure 4.2** details the number of RCIS and OE-417 reports that utilities submitted over the course of the exercise, indicating where exercise play was the most intensive.

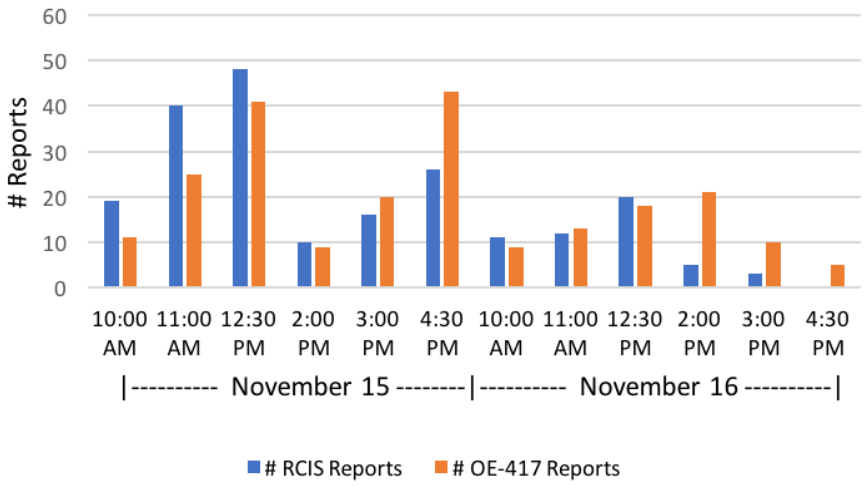


Figure 4.2: RCIS and OE-417 Reports

Chapter 5: Observations and Recommendations

Distributed Play

This chapter provides a summary of the input NERC received from participating organizations that submitted after-action survey responses and lessons learned documents.

NERC fulfilled its GridEx IV planning role by providing the exercise design, planning logistics, and baseline scenario without needing to oversee or monitor the details of how individual organizations planned or participated in the exercise. In an effort to enhance the quality of the observations and recommendations that resulted from GridEx IV, the NERC planning team developed a set of quantitative metrics and a template that organizations could use to document their own lessons learned. Participating organizations were not required to share the details of their internal lessons learned outside their own organizations. However, participating organizations were encouraged to share any generic lessons learned with the E-ISAC in order to identify opportunities for improvement across the industry. NERC assured organizations that any lessons learned shared with NERC would be subject to the protections of the E-ISAC Code of Conduct.[10] While some of the observations and recommendations related to lessons learned by participating organizations as a result of their responses to the exercise scenario, many of the participating organizations related to how the exercise was planned and conducted. NERC anticipates industry-specific crisis response improvement input will increase in future exercises.

The following observations and recommendations identify opportunities to enhance the security and reliability of North America's BPS:

Observation 1: Increase Proactiveness of Lead Planners

The rapid growth and participation in GridEx has evolved into operating in a largely decentralized manner instead of a "one-size, fits-all" distributed play. While the distributed play approach has been successful in the past, this caused some communication issues to arise during GridEx IV. Lead planners were responsible for developing a scenario that would be tailored to their organizations' needs while operating within the overarching GridEx design. While lead planners were successful overall, some were inadequately prepared for the exercise or did not reach out to other stakeholders (such as local law enforcement or ICS product vendors), perhaps believing that the E-ISAC or GridEx planning team would provide exercise injects or bring in the necessary organizations.

Recommendations:

- A small number of lead planners were confused about the scenario or felt they had insufficient time to synthesize new information and incorporate it into their own exercises. Accordingly, messaging from the GEWG regarding high level exercise information should become more frequent. This should include notifications when information is added to the GridEx IV planning portal, reminders for upcoming deadlines, and overall expectations for lead planners. In addition, the Master Scenario Event List (MSEL) and exercise development should adhere to the time line to minimize confusion and allow for a greater synthesis of information.
- Lead planners should take a more proactive role in bringing in their necessary players, namely other electricity entities they operate with regularly, local law enforcement, government agencies, and utility equipment vendors. Increased messaging from the GEWG is needed to encourage organization outreach and that the NERC exercise planning team is a resource but not responsible for making decisions for any organization.

[10] https://www.eisac.com/Documents/E-ISAC_Code_of_Conduct.pdf

- The final planning meeting was held on May 8, 2017, more than six months before the start of the exercise. The six-month timeframe gave organizations ample time to incorporate the final scenario into their customized exercises and was routinely praised in after-action reports. During this period, some lead planners did not engaged in the process and were scrambling to find exercise tools and had many questions in the final days leading up to the exercise. The NERC exercise planning team should increase the number of tool training and Q&A sessions between the final planning meeting and exercise start to keep lead planners engaged.

Observation 2: Increase Participation from Law Enforcement and Other Critical Infrastructures

Other critical infrastructure organizations registered for GridEx for the first time with four oil and natural gas companies, five water utilities, and two telecommunication companies. These organizations chose observer status, but this opens the door for expanding their participation in future GridEx exercises. Six supply chain vendors also participated in the exercise, serving as points of contact in ExCon for any organization simulating malfunctions with third-party hardware or software. Unfortunately, the vendors were not used by players to the extent desired with none of the vendors receiving calls during the exercise and no emails being received by the Vendor Helpdesk email account. In contrast, with 29 FBI Field Offices and 7 state police forces registered for GridEx IV, law enforcement participation was fruitful and provided the opportunity for law enforcement to coordinate with electrical entities within their areas of responsibility.

Recommendations:

- Lead planners should seek out opportunities to include the cross-sector, supply chain, and law enforcement in their exercise play. Exercise designers should solicit GEWG members who have included such entities to share the successes they have achieved through these connections in GridEx.
- Greater emphasis needs to be placed on encouraging supply chain and operations technology vendors to participate with their utility customers in GridEx. Industries and vendors should share information during an attack situation as complications can easily arise. Future scenarios should be designed to include a more prominent role for vendors, possibly including vendor participant(s) on the GEWG. Additionally, there should be increased messaging and strong encouragement for lead planners to bring in the various vendors of their equipment. Outreach at user conferences or company-vendor matchmaking exercises in the planning phases provide additional avenues to increase vendor participation.
- Utilities expressed a desire to work more closely with their local law enforcement agencies as they would certainly be called upon during any cyber or physical attack on a utility. An additional concern cited by many survey respondents was determining the exact role of state and federal government during a grid emergency. Similar to the previous recommendation, increased messaging is needed from the NERC planning team to encourage organizations to take the initiative in engaging government partners to enhance the quality of their exercises.

Observation 3: Strengthen E-ISAC Portal Functionality

The E-ISAC portal is designed to serve as a central hub for information, mitigation, and response related to physical and cyber attacks occurring on the grid. In the after-action survey, organizations were asked about the E-ISAC's effectiveness at sharing information and providing high-level situational awareness, providing clear guidance and mitigation measures, and providing effective collaboration tools through the E-ISAC portal. Of the respondents, a total of 21 percent found the portal "very effective," and 49 percent said "effective." A total of 26 percent said "somewhat effective" and 4 percent said "not effective"; these were the lowest percentages of all survey questions marking the need for improvement. Notably, the E-ISAC launched a new E-ISAC portal following GridEx IV, which should address many of the legacy portal shortcomings.

Recommendation:

- The E-ISAC should consider adding a "Common Operational Picture" function to the portal. By adding this capability, it would satisfy the desires of many organizations who felt they could use more awareness of the overall North American scenario and have visibility in a central place to keep track of all statuses and information.

Observation 4: Enhance Public Affairs and Corporate Communications

SimulationDeck offered a unique opportunity for corporate communicators to engage with simulated customers and adversarial misinformation during the GridEx IV cyber and physical attacks. Eighty-seven utilities used this simulated environment to alert, educate, and inform stakeholders about electricity outages without fear of being misinterpreted by entities outside the exercise. Many organizations found that their external messaging was "ad hoc" and that they did not have an external communications playbook. In addition, they lacked well-defined thresholds on when and how to engage social media misinformation.

Recommendations:

- Utility corporate communication organizations should use their existing external communications procedures, or use GridEx as a driver to develop or refine procedures if they do not exist or are not suitably comprehensive. This would provide organizations with a framework and general guidelines to respond during a crisis. Additionally, an external communications procedure would include recommended actions that would be helpful in addressing misleading or false information in the social media sphere.
- A corporate communications subteam should be established within the GridEx Working Group. This sub team will be responsible for creating scenario injects that are specific to electricity industry external affairs personnel.

Observation 5: Enhance Reliability Coordinator Communications

RC organizations played a critical role in GridEx IV by sharing information and coordinating grid reliability actions with the utilities in their areas as well as with their neighboring RCs. However, since there is no exercise functionality within RCIS, email was used to simulated RCIS functionality. As a result, the process of writing, transmitting, and retransmitting the information was manpower intensive, prone to human error, and incapable of relaying information in real-time.

Recommendation:

NERC should re-platform RCIS with a built-in exercise functionality. This will allow operators to use the production system safely and seamlessly for training and exercises.

Observation 6: Increase Communications Resilience

Primary communication paths were simulated to be degraded or disrupted. GridEx IV provided an opportunity to practice contingency plans so that players activate alternate emergency communication paths. These communications would be used to maintain contact with internal personnel, emergency managers as well as first responders. The E-ISAC simulated a communications blackout in the National Capitol Region, which interrupted a broadcast call to exercise participants. The SHARES HF radio program transmitted a brief message on behalf of the E-ISAC to alert utilities of the situation and to stimulate use of backup communications.

Recommendations:

- The E-ISAC should gain its own organic HF radio system and become a member of the SHARES program. This will enable use of the SHARES frequencies without requiring a FCC license to transmit, providing an avenue to communicate with E-ISAC members in this type of emergency.
- The United States Department of Homeland Security's WPS and GETS are available to United States utilities and NERC should encourage their adoption in the electricity sector.
- Utilities should establish communication contingency plans that use multiple technologies so that communication resiliency is maintained in the event one or more information paths are lost.

Observation 7: Increase Cyber Mutual Assistance Program Participation

The need for Cyber Mutual Assistance (CMA) was highlighted in 2015 following the executive tabletop portion of the NERC GridEx III exercise, and was underscored by the December 2015 cyber attack in Ukraine. The CMA program was developed through an industry-wide collaborative process and officially launched as a program of the ESCC in 2016. During GridEx IV, 42 electric companies participated in the CMA program as a reaction to the exercise scenario. The CMA Program provides a pool of utility cyber security experts who volunteer to share their expertise with other utilities in the event of a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency.

Recommendations:

- More utilities should participate in the CMA program.
- The ESCC and the E-ISAC should engage more with the CMA Program to efficiently share to encourage the efficient sharing of relevant information in the event, or in advance, of a cyber emergency in a manner that complies with the CMA program's non-disclosure agreement.
- The CMA program should continue to engage with potential partners and external stakeholders to discuss how best to be prepared to communicate about and respond to cyber emergencies when they arise.

Observation 8: Enhance Move 0 Development

Move 0 was intended to be an opportunity to prepare GridEx IV participants prior to the two-day exercise and provide players with hands-on training experience in responding to the cyber threats to be experienced in the exercise scenario. Move 0, which launched during the E-ISAC's grid security conference (GridSecCon), focused on adversary preparation, reconnaissance, and execution activities with players reacting to attacks in real time, sharing information, and engaging in simulated containment activities. Move 0 proved that incorporating hands-on simulations into GridEx was feasible and valuable and will be expanded in future GridEx iterations. Several planning and organizational changes should be made to decrease any confusion surrounding Move 0 and its relation to subsequent exercise moves.

Recommendations:

- Many distributed play participants did not attend GridSecCon and therefore did not get the Move 0 explanation there.[11] Final scenario and injects for Move 0 need to be completed and given to lead planners at least 60 days prior to execution to allow adequate preparation time.
- The GEWG needs to more clearly define the intent and objectives of Move 0 and ensure that Move 0 is developed to flow seamlessly into the rest of the exercise. Move 0 injects should be fully integrated into the GridEx MSEL to allow lead planners to better incorporate the events of Move 0 into their own customized

[11] NERC's annual Grid Security Conference: http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridSecCon.aspx

scenarios. Additionally, keeping Move 0 in the MSEL gives organizations the opportunity to do their own training regardless of whether they attend GridSecCon.

- As the capability and scope of Move 0 increases, more physical security elements, not just cyber, should be added. Preoperational planning for cyber effects and reconnaissance activities also should be considered.

Executive Tabletop

The tabletop reinforced the need to continue building on the collaborative relationships between the electricity industry and government. Participants recognized the progress made in a number of areas to address the recommendations of the 2013 GridEx II and 2015 GridEx III executive tabletops. They also acknowledged the need to continue efforts in other more challenging areas, such as unity of message and effort.

Recommendations:

- The ESCC and 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 V in November 2019. Participants highlighted two recommendations for particular attention from the perspective of maintaining reliable grid operations:
  - **Increase Grid Emergency Response Capabilities:** Address the need for emergency communications capabilities during severe events.
  - **Ensure Utilities have Access to Sensitive Information:** Quickly recognize threats that may affect multiple critical infrastructure sectors.
- The recent NIAC report[12] to the president of the United States that recommends the formation of a Strategic Infrastructure Coordinating Council should be supported as a framework for addressing not only high-level electricity issues but also related issues with key strategic sectors having critical interdependencies (e.g., communications, financial services, transportation, and water.)
- NERC and the E-ISAC are committed to continue enhancing the GridEx program to confirm the progress being made and meet the challenges posed by the ever-evolving threat environment. Participants suggested topics for a next executive tabletop that included the following:
  - **Increase Participation with Other Critical Infrastructure Sectors:** Build on the positive contribution of the representatives from other critical infrastructure sectors who participated in the tabletop. Broaden participation to include all life-line sectors.
  - **Increase State-Level Participation in Future Exercises:** GridEx state-level participants should encourage other states to participate in future exercises. This could occur through organizations like the National Governor's Association, National Fusion Center Association, and the Adjutants General Association of the United States.
  - **Consider Security of Generator Fuel Sources:** Consider whether the diversity of fuel sources (today and into the future) presents a vulnerability to common mode failures or disruptions.
  - **Review Secure Industrial Control System Architecture**: Consider whether industrial control systems (specifically Supervisory Control and Data Acquisition Systems and Energy Management Systems) are adequately architected with security foremost in mind.

[12] Reference NIAC report "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure (August 2017)": https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

- **Identify Critical Supply Chains:** In recent years, utilities have improved their ability to acquire, transport, and replace large transmission power transformers. Consider identifying critical supply chains for other equipment that could be vulnerable to attacks (e.g., long manufacturing lead-times, shortage of highly-specialized technical expertise).
- **Review Monitoring of Machine-to-Machine Communication and Artificial Intelligence:** Consider establishing robust monitoring and oversight of machine-to-machine interfaces and artificial intelligence to ensure that cyber security risks are sufficiently known and controlled.
- **Consider Including Tactics:** Consider structuring the next executive tabletop or other exercises to determine if tactical capabilities are in place to execute policy-level decisions. Examples include the following:
    - Template orders to implement FAST Act orders
    - More focused regional-level scenario to test our understanding of who decides what, when, and how
    - Focus on a few key issues
    - Exercise ESCC/EGCC coordination with detailed scenarios to prompt specific decisions and how they would be implemented

Conclusions

Feedback from GridEx IV participants indicate that the exercise continues to provide industry and government participants with a valuable learning opportunity to strengthen their internal crisis response capabilities, including how they coordinate with others. Participants understand that physical and cyber security incidents could disrupt the reliable operation of the BPS, and GridEx IV allowed security staff and power system operators to identify the threats and quickly respond as they would in a real-world event. GridEx IV reinforced the need to continue building on the collaborative relationships between the electricity industry and other critical infrastructure sectors and government.

The exercise identified opportunities to improve the E-ISAC's information-sharing capabilities in today's evolving threat environment. The E-ISAC continues striving to achieve its vision of being "a world-class, trusted source of quality analysis that rapidly shares electricity industry security information."

NERC and the E-ISAC will continue to work closely with industry and government stakeholders to enhance industry's readiness and further evolve the GridEx program based on the recommendations and lessons learned gathered. The security landscape in North America is dynamic and requires constant vigilance and agility. Events and coordination like GridEx ensure industry is as prepared as possible. NERC remains focused on our mission to assure the reliability and resilience of the BPS, which is inextricably tied to grid security.