NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Grid Security Exercise

GridEx III Report

March 2016

RELIABILITY | ACCOUNTABILITY



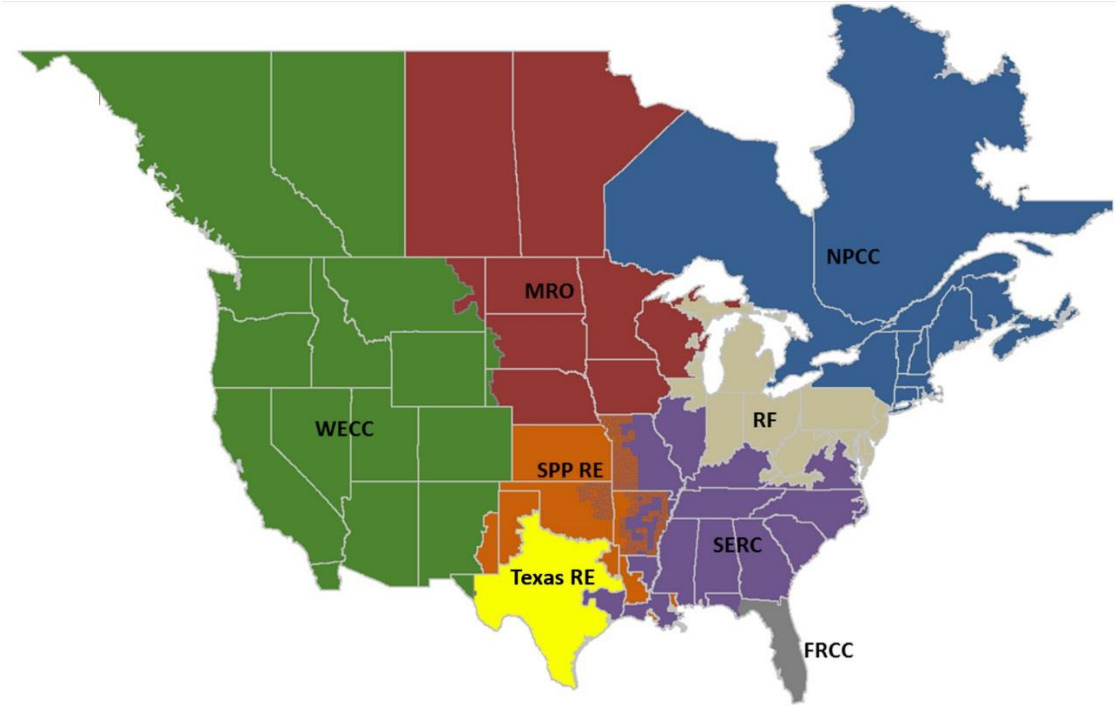

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity (RE) boundaries, as shown in the map and corresponding table below.



The Regional boundaries in this map are approximate. The highlighted area between SPP and SERC denotes 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, RE
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Executive Summary

The North American Electric Reliability Corporation (NERC) conducted its third biennial grid security and emergency response exercise, GridEx III, on November 18-19, 2015. NERC's mission is to assure the reliability of the bulk power system (BPS) and GridEx III provided an opportunity for industry and other stakeholders to respond to simulated cyber and physical attacks affecting the reliable operation of the grid. Led by NERC's Electricity Information Sharing and Analysis Center (E-ISAC), GridEx III was the largest geographically distributed grid security exercise to date. GridEx III consisted of a two-day distributed play exercise and a separate executive tabletop on the second day. More than 4,400 individuals from 364 organizations across North America participated in GridEx III, including industry, law enforcement, and government agencies.

In addition to the distributed play portion of GridEx III, a six-hour executive tabletop portion took place on November 19 that involved industry executives and senior government officials. The 32 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 III were to:

- Exercise crisis response and recovery;
- Improve communication;
- Identify lessons learned; and
- Engage senior leadership.

Distributed Play Results

NERC and participating organizations succeeded in achieving these objectives. Responding to the after-action survey, 62 percent of participants indicated the exercise met their expectations "very well" and 38 percent indicated "well."

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.

- **Coordinated Response and Communication.** GridEx III provided participants with the opportunity to exercise their incident response procedures during large-scale security events affecting North America's bulk power system. The large-scale cyber and physical attack scenario was designed to overwhelm even the most prepared organizations. GridEx III highlighted the importance of well-coordinated communications. Organizations should review documentation that describes their internal information-sharing processes in the context of a large-scale event and exercise these communication capabilities.
- **Reporting Mechanisms.** GridEx III participants observed that some aspects of the industry's information sharing and reporting tools are redundant, time-consuming to use, and provide no feedback mechanism to those who most need the information.
- **Active Participation of Operations Management, Support Staff, and System Operators.** GridEx III succeeded in providing exercise scenarios that linked the physical and cyber attacks with how system operators would respond to mitigate the impact of these attacks on bulk power system reliability. Future GridEx exercises should continue to include scenarios that prompt operations management, support staff, and field operations to interact with cyber and physical security personnel.

- **E-ISAC Information Sharing.** Participants observed that the E-ISAC portal should be enhancedfor real-time urgent communication with portal members. Participants observed that information was quickly buried within the portal, making it became difficult to highlight important information. The E-ISAC should continue to enhance the E-ISAC portal to support real-time, searchable, urgent communication and collaboration with portal members.
- **Introduction of New Exercise Tools.** While new exercise tools enhanced the exercise, there is room for continued improvement. Prior to the next exercise, functionality and volume/capacity tests should be performed.
- **Advance Exercise Planning Timelines.** Planning for the next GridEx exercise should begin earlier than GridEx III to provide organizations with more time to conduct their own planning and training activities. NERC should develop a firm delivery schedule with stakeholders, including major planning milestones, and tool development and testing at the outset of exercise planning. Future GridEx exercises should continue to provide opportunities for organizations to customize their scenario injects provided they are consistent with and support the overall NERC scenario as coordinated with their Reliability Coordinator.
- **After-Action Survey and Lessons Learned.** During the early stages of the GridEx III planning process, NERC developed a set of metrics to assess the success of the exercise that included the questions in the after-action survey. Lessons learned reports that were submitted to NERC by participating organizations provided valuable input, but a greater number of reports would provide a more complete and representative set of lessons learned. The NERC planning team should consult with participating active organizations to understand any reluctance to share lessons learned and identify ways to increase the response rate.

Executive Tabletop Results

The executive tabletop engaged senior leaders in a robust discussion of the policy issues, decisions, and actions needed to respond to a major grid disruption caused by simulated physical and cyber attacks. Participants identified security and reliability challenges and opportunities to improve prevention, response, and recovery strategies. The discussion centered on three key areas: unity of messaging, unity of effort, and extraordinary measures.

Unity of Messaging

Participants explored how industry and government assess a crisis event, and receive and share information with each other and the public. Managing the challenges and opportunities related to social media was of particular interest.

Unity of Effort

While both industry and government have considerable resources at the ready to respond to crisis events, participants considered how to improve coordination during severe emergency situations. Industry needs to coordinate with local law enforcement to identify and assess the physical risks to electricity facilities and workers. Unlike how industry responds to major storms through mutual assistance, industry's capability to analyze malware is limited and would require expertise likely available from software suppliers, control system vendors, or government resources.

Extraordinary Measures

The industry operates within a regulatory framework designed within normal planning and operating criteria. Participants considered regulatory and legislative needs, as well as extraordinary government support, that could enhance timely and effective recovery under extreme circumstances that clearly exceed normal criteria.

- **Establish Priorities for Restoring Electricity Service.** When restoring power following a large-scale outage, utilities' first priorities focus on supplying electricity to re-start generation and energize transmission and

distribution lines and equipment. Second priorities include "lifeline" customers such as communications, oil and gas, water supply/treatment and hospitals.

- **Simplify Electricity System Operation Under Emergency Conditions.** North America's electricity system is operated by highly trained staff using sophisticated technology systems to forecast load, monitor electricity flows, dispatch generation, remotely operate equipment, and administer markets. In the event that these normal processes are disrupted, it may be possible to simplify how the electricity system is operated to provide basic service but at reduced levels of reliability and less economically.
- **Consider Mechanisms to Prevent Financial Defaults.** Utilities will need unprecedented levels of financial resources in order to restore their facilities and eventually resume normal operations.
- **Manage Personal and Corporate Liability Risks.** North America's bulk power system is designed and operated to meet extensive legal and regulatory requirements (e.g., environmental, safety, financial, labor, commercial). Some of these requirements may delay or prevent restoration during a large-scale event.

Introduction

GridEx III built upon the successes and lessons learned from previous exercises and, like GridEx II in 2013, consisted of a large-scale distributed-play exercise and separate executive tabletop. From the beginning of the planning process in December 2014, the NERC planning team focused on developing a planning structure, scenario, and exercise that would encourage an even greater number of participants. In order to provide clear expectations, the NERC planning team reflected on the progress made to address lessons learned from previous exercises, established planning-process milestones, and developed metrics to assess the value of the exercise.

GridEx III continued to improve upon the model established in GridEx 2011 and GridEx II, with two full days of distributed play and an executive tabletop discussion on day two. GridEx III was designed to increase utility participation, as well as state/provincial and local governments in the United States, Canada, and Mexico. NERC encouraged Reliability Coordinators (RCs) to take a lead role by planning, monitoring, and coordinating exercise play within their area.

The NERC planning team structured the exercise with the flexibility to allow organizations to determine the scope and extent of their own participation in the exercise. Lead planners at each organization decided whether their organization would participate in an "active" or "observing" capacity. This provided the flexibility for each organization to participate according to its role, available resources, and real-world operational environment.

At the conclusion of GridEx III, 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 this report.

Participation

Distributed Play Participants

An important consideration for planning GridEx III was to continue to evolve the GridEx program by designing a credible scenario, increasing active participation, and encouraging greater integration with BPS operations. In addition to inviting all NERC entities to participate in GridEx III, the NERC planning team recognized the role of RCs[1] and encouraged them to engage electricity entities within their areas to participate. This approach was very successful, and GridEx III was the largest physical and cyber grid security exercise to date, involving more than 4,400 registered individuals from 364 organizations across North America. Many entities also involved individuals from within their organizations who did not register directly with NERC for the exercise, making the actual participation rate greater. This increase in participation led to an enhanced level of communication and coordination between organizations as would be expected during a real event of this scale. As shown in Figure 1, GridEx III succeeded in attracting even greater participation[2] than previous GridEx exercises.

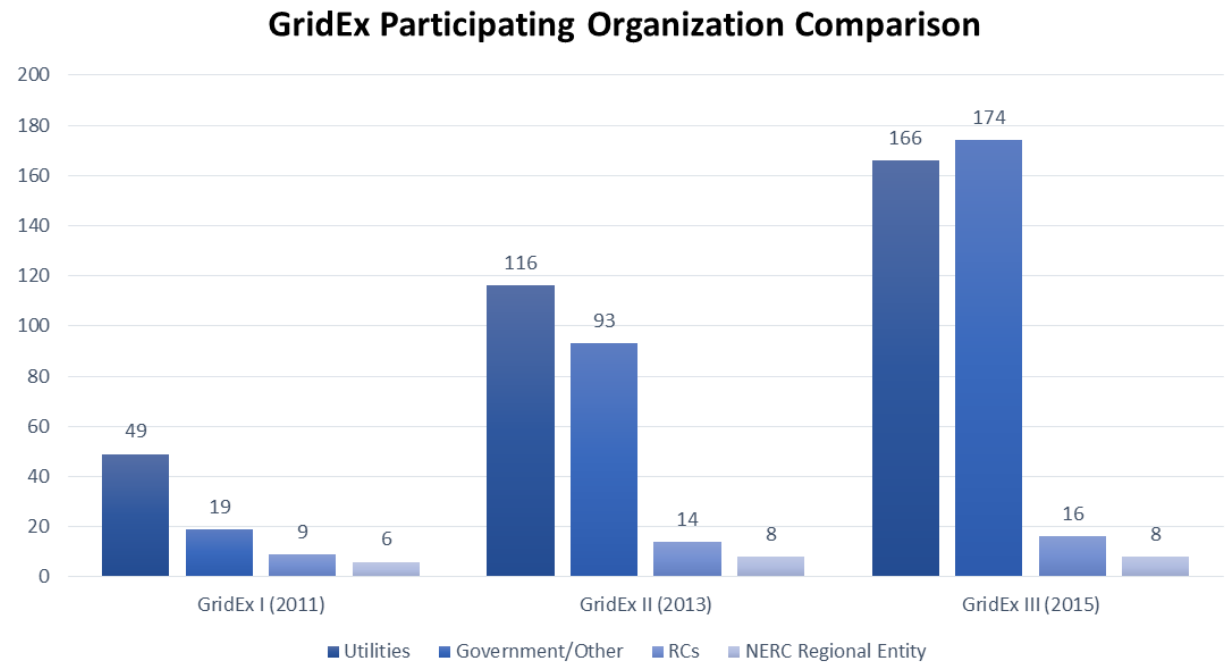


Figure 1: GridEx III Participation

Participation in GridEx III, as with all previous NERC exercises, was voluntary. Although GridEx III provided participants the opportunity to demonstrate meeting several NERC regulatory requirements related to exercises and training, NERC explicitly stated in advance that there would not be any compliance monitoring or enforcement actions related to participation in GridEx III. Organizations were invited to participate in an active or observing capacity, although NERC strongly encouraged active participation in order for organizations to get the most value from the exercise.

[1] 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.

[2] "Government/Other" includes government agencies, local law enforcement, and electricity industry vendors and suppliers.

- **Active Organizations**. Active organizations participated in GridEx III 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 III tended to be those that committed the necessary resources (i.e., lead planners and players with cybersecurity, 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, Reliability Coordinators, local law enforcement, and government authorities.
- **Observing Organizations.** Observing organizations did not respond to the scenario events as if it were a real event and did not interact with active organizations. They did however, have access to the entire range of planning documentation to use, for example, to conduct their own internal tabletop exercise. NERC anticipates that observing organizations would use GridEx III to gain experience and to participate in future exercises as active organizations.

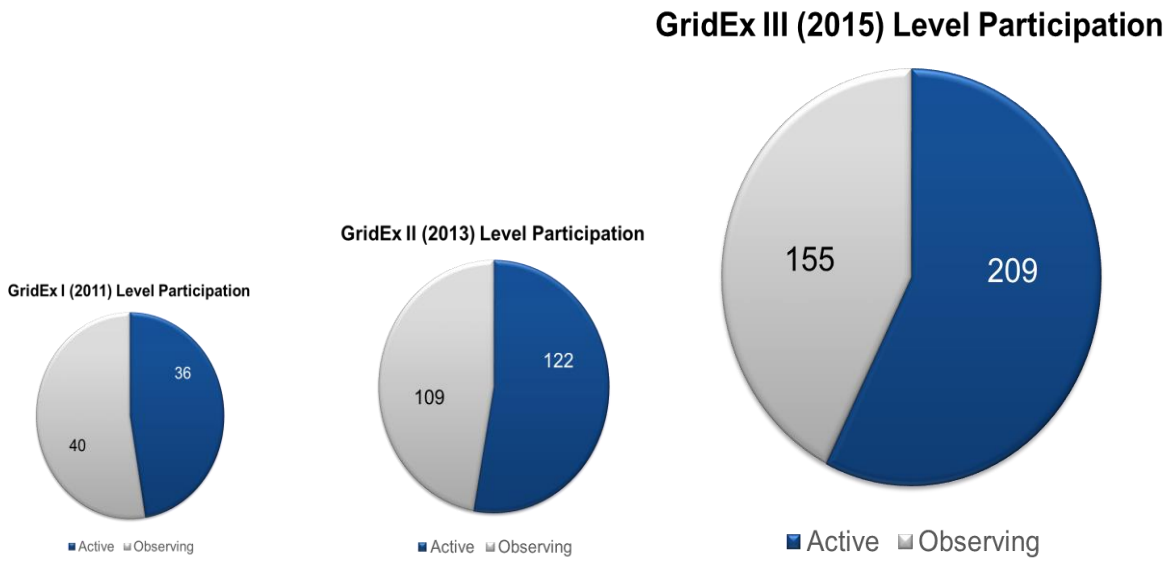


Figure 2: GridEx Participation Growth

Executive Tabletop Participants

The executive tabletop was facilitated by a former utility senior executive who advises the industry on critical infrastructure issues and serves on a presidential advisory council. The electricity industry participants included chief executives from investor and publicly owned utilities, cooperatives, and independent system operators from the U.S. and Canada. The U.S. federal and state governments were represented by senior officials from the following departments and agencies. In addition, approximately 70 individuals associated with the participants attended the tabletop as observers to provide feedback.

- White House, National Security Council
- Department of Energy
- Department of Homeland Security, including Federal Emergency Management Agency
- Department of Defense, including U.S. Cyber Command, U.S. Northern Command, North American Aerospace Defense Command
- National Security Agency
- Federal Bureau of Investigation
- National Guard

Exercise Objectives

The NERC planning team developed a set of four exercise objectives. NERC developed sub-objectives and metrics to evaluate the extent to which these objectives were met. The exercise objectives were achieved during GridEx III as described below.

Objective 1: Exercise Crisis Response and Recovery

- Increase the number of organizations and individuals who participate.

  Achieved. GridEx III participation grew by 133 organizations and more than 800 individuals compared with GridEx II. The number of active (as opposed to observing) organizations increased by 87 organizations.

- Increase the number of continuing education hours earned during the exercise.

  Achieved. Individuals participating in GridEx III earned a greater number of continuing education hours (CEH) than during GridEx II: 274 system operators and 270 others applied for CEH credits.

- Increase the extent to which entities exercise their cyber, physical, and operations response.

  Achieved. The scenario included multiple physical and cyber attacks affecting the BPS. Participants indicated in the after-action surveys that the scenario provided the opportunity to exercise cyber (84 percent), physical (92 percent) and operational (98 percent) security response plans "very well" or "well."

Objective 2: Improve Communication

- Increase the extent to which entities exercised communications processes within their organization.

  Achieved. "Very well" increased by 20 percent.

- Increase the extent to which entities exercised communications processes with their Reliability Coordinator and other neighboring entities.

  Achieved. "Very well" increased by 17 percent.

- Increase the extent to which entities exercised communications processes with law enforcement and other government entities.

  Achieved. Communications with those outside the electricity sector increased "very well" by 11 percent. Communications with other critical infrastructures stayed consistent, indicating an area for increased focus for future exercises.

- Increase the extent to which entities exercised communications processes with NERC's E-ISAC and Bulk Power System Awareness (BPSA).

  Achieved. "Very well" increased by 14 percent.

Objective 3: Identify Lessons Learned

- Identify lessons learned not identified in previous exercises.

  Achieved. NERC received a total of 25 lessons learned reports, representing 24 percent of active participating utility organizations. These reports identified actionable lessons learned and acknowledged the value of NERC's GridEx program. Early in the planning process, NERC developed a template to encourage participating organizations to identify 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 or improve future exercises of this nature.

Given the relatively low number of reports received from participating organizations, NERC will work with participants of future exercises to determine how a higher response rate can be achieved.

Objective 4: Engage Senior Leadership

- Explore what and how information is shared between industry, the public, and government.

  Achieved. The executive tabletop portion of GridEx III focused entirely on this objective.

- Explore the coordination of recovery efforts in a severe impact scenario against the reliability of the BPS.

  Achieved. Many organizations involved their senior management and crisis leadership teams in the exercise. Survey results indicated that communications between industry and government increased "very well" by 11 percent compared with GridEx II.

Exercise Design, Planning, and Scenario Development

NERC began planning GridEx III in December 2014 and conducted a series of conference calls and planning meetings with lead planners from participating organizations. A Grid Exercise Working Group (GEWG) was established by NERC's Critical Infrastructure Protection Committee (CIPC), involving industry and government subject matter experts in cyber and physical security as well as BPS operations. Members of the GEWG shaped the design and scenario of the exercise with the NERC planning team's guidance and support over the timeline illustrated in Figure 3.

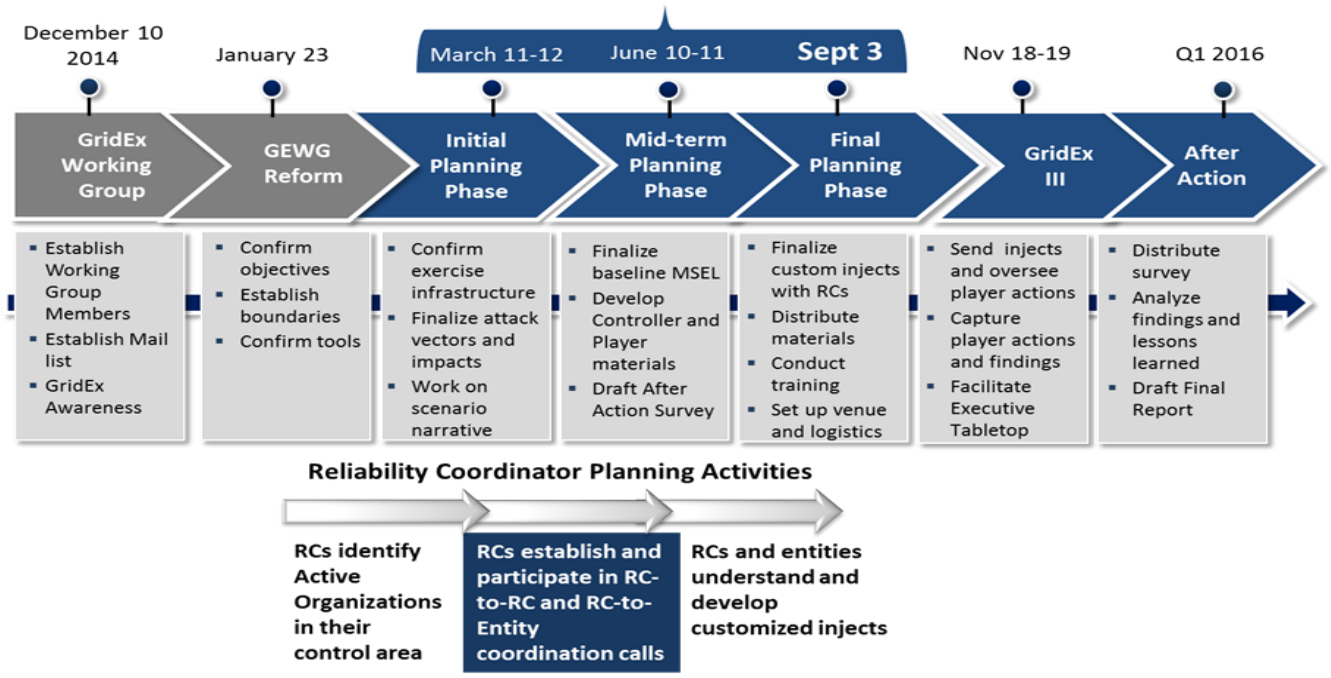


Figure 3: GridEx III Planning Timeline

To a much greater extent than GridEx II in 2013, NERC encouraged customization and coordination at the local level consistent with the overall GridEx III scenario. NERC encouraged RCs to take a lead role by planning, monitoring, and coordinating the exercise within their areas. In some areas, RCs held planning meetings and conference calls to coordinate exercise activities within their areas and with their neighbors. This enabled participants to coordinate their planning and response across a large geographic area in a more realistic fashion.

Baseline Scenario Development

The NERC planning team and the GEWG developed the baseline scenario for GridEx III with one important constraint: the scenario would not include grid blackstart and system restoration processes[3] as this would limit the ability of all participants to remain fully engaged throughout the exercise.

The baseline scenario was organized into four "moves" of exercise play, each lasting four hours. In response to a recommendation from GridEx II (in 2013) to provide more time for players to respond to the scenario injects in a realistic manner, exercise times matched real-time during Moves 1, 2 and 3. The exercise included only one scenario time jump between Moves 3 and 4 in order to credibly provide time for participants to develop mitigating actions to respond to the scenario. Based on this narrative, the GEWG developed the detailed master scenario event list, which consisted of over 80 individual injects that provided the tactical details to prompt players to respond.

Figure 4 illustrates the anticipated impact on grid reliability during the exercise for the distributed play and separate executive tabletop scenarios.

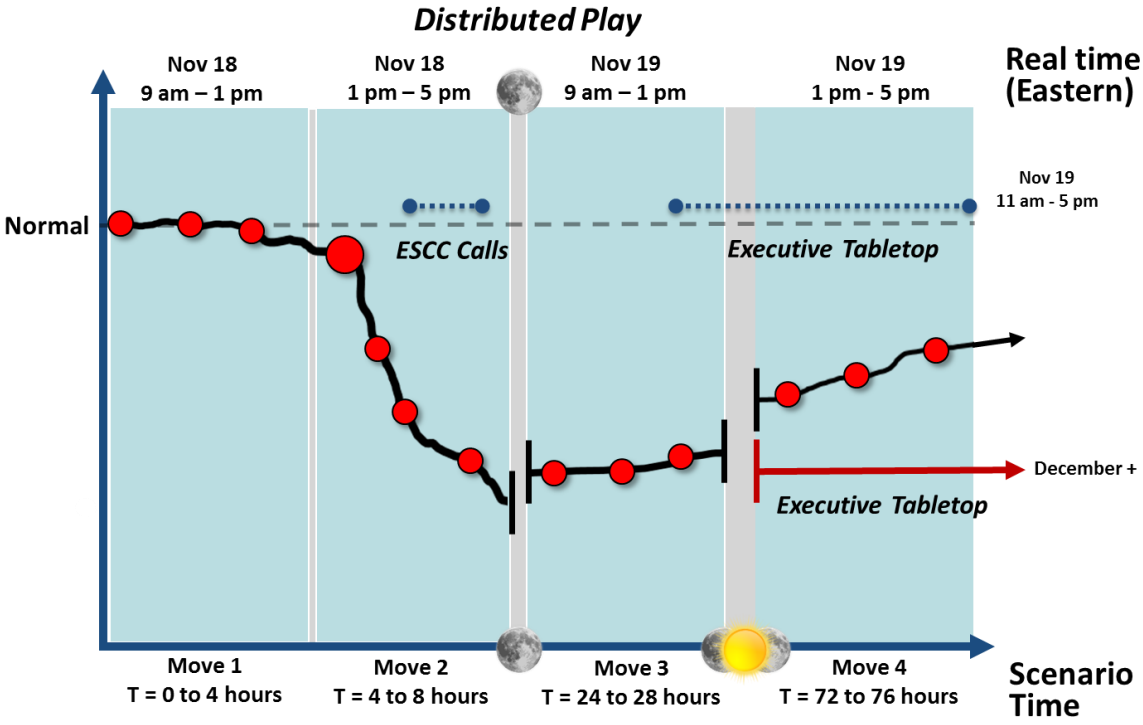


Figure 4: GridEx III Scenario Escalation Timeline

Scenario Customization

Active organizations had the option to use the baseline scenario or customize the baseline scenario to better meet their own local objectives (provided they remained consistent with the baseline scenario). The baseline scenario included different cyber and physical attack options. The simulated cyber attack options included watering hole, patch deployment, and remote access vulnerabilities affecting utility industrial control systems. 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

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

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 timeline.

Exercise Tools

NERC introduced several new tools to enhance how GridEx III was planned and conducted. The tools used during the exercise included SimulationDeck, the E-ISAC portal, RCIS reporting, OE-417 reporting, and the GridEx III Lead Planner Sharepoint portal. It should also be noted that many organizations used their own tools to simulate their various operational processes (e.g., simulators used for power system operator training).

Lead Planner GridEx III Portal

The NERC planning team created a Sharepoint portal to share exercise-sensitive materials with lead planners. Lead planners were provided access as they registered for the exercise. The NERC planning team maintained document version control. The GEWG used the portal to share draft exercise material before it was made available to lead planners.

The lead planner portal was an important tool to share exercise documents securely, but a better solution is needed for future exercises. The portal registration process was manually intensive, taking up to several days before lead planners received access. After gaining access, lead planners had to enter their login credentials each time they opened a document. These issues discouraged lead planners from regularly logging into the portal to obtain the latest draft exercise documents under development.

SimulationDeck

GridEx III introduced SimulationDeck, a web-based crisis simulation platform that supported exercise planning and execution. SimulationDeck included social media functions that simulated Facebook, Twitter, YouTube, blogs, and traditional media such as TV, newspapers, and radio. SimulationDeck served as the focal point of many exercise planning activities. The tool was used to register players in a centralized exercise directory. During the exercise it hosted simulated social and traditional media, the exercise directory, and the inject delivery tool. While SimulationDeck added a new dynamic to the exercise that allowed players to interact with increased realism, its functionality and performance needs to be improved to fully support future exercises of this scale. For example, although the NERC planning team encouraged organizations to customize their own injects, organizations were unable to use the tool's single inject delivery system, as it was dedicated to the baseline scenario only. A failure of the inject delivery tool just as GridEx III began caused some participating organizations to be concerned about the tool's reliability, although the tool was stable and functional for the remainder of the exercise.

E-ISAC Portal

For GridEx III, the E-ISAC developed a mirrored version of their recently-upgraded E-ISAC portal with the same functionality as the production version. E-ISAC portal members with access to the production version of the portal were able to use the portal as if it were the production environment, greatly enhancing their ability to become more familiar with the portal. The exercise was an excellent opportunity for E-ISAC portal members to learn how to use the portal during a real event.

Simulated RCIS Reporting

The Reliability Coordinator Information System (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 other RCs using an email distribution list. As an initiative unrelated to GridEx, NERC is considering rebuilding the production RCIS tool to include a separate training and drill function that would facilitate a more realistic RCIS reporting process during exercises.

OE-417 Reporting

GridEx III simulated the submission of OE-417s throughout the exercise, but did not use the production forms or processes in order to ensure that exercise information was not subject to possible Freedom of Information Act requests.

PNNL Tool

For demonstration purposes, a display tool developed by the U.S. Department of Energy's Pacific Northwest National Laboratories (PNNL) illustrated the potential impact of the scenario geographically. The map indicated the locations of the simulated scenario attacks and included a table that identified the timing of the cyber and physical attacks, the operational responses, and the volume of OE-417 reports provided to NERC and DOE. With further development, a tool of this nature may be used by ExCon during future exercises to monitor how the exercise is progressing.

FBI Virtual Command Center

During the exercise the FBI used their Virtual Command Center to aggregate and disseminate actionable, tactical information. This tool was displayed at ExCon and viewed by FBI players at participating FBI field offices across the United States.

Exercise Conduct

GridEx III was directed from a central location at the ExCon facility in McLean, VA, November 18-19, 2015. ExCon included NERC staff and contractors, certain GEWG members, government representatives, industry experts, and SimulationDeck staff. ExCon was responsible for distributing the scenario injects, monitoring progress, simulating organizations not participating in the exercise, and providing help desk support. All events were simulated.

Despite initial issues with the SimulationDeck website and inject distribution tool, ExCon was able to deliver injects to lead planners who in turn delivered the appropriate injects to their own players. As Move 1 unfolded, utility players began to experience unusual control system operation and received reports of substation break-ins and UAV surveillance. With a high degree of uncertainty surrounding the nature of the unfolding events, players worked to respond to the events according to their roles in the exercise. As Move 2 began, players experienced an escalation in malware intrusions and coordinated physical attacks. These events caused communications disruptions and generation and transmission outages. Simulated media injects added realism to the scenario (ref. Figure 5). During Move 2, the E-ISAC and NERC's BPSA group conducted a conference call with members of the E-ISAC portal to share information received and to provide an overview of the status of grid reliability. The Electricity Subsector Coordinating Council (ESCC) conducted a conference call just after the E-ISAC call to share information. At the end of the day on November 18, players were continuing to look for ways to prevent, protect, and mitigate the impacts of the cyber and physical attacks.

Figure 5: Simulated News Broadcast

BPSA developed and maintained geographic overviews of the situation across North America. Throughout the exercise BPSA developed and maintained a continent-wide awareness of the locations, types, targets, and impacts of reported attacks, as well as suspicious activities, noteworthy media actions, and operational anomalies. On November 18, BPSA received reports regarding 88 physical security events, 23 cybersecurity incidents, 10 suspicious activities, and 47 impacted electricity assets. On November 19, BPSA received reports regarding 18 physical security events, eight cybersecurity incidents, and six suspicious activities. On November 19, BPSA received no additional reports regarding impacted electricity assets. The E-ISAC received 69 telephone calls, emails, or reports from participants regarding cyber attacks. The E-ISAC portal received 52 discussion and request-for-information postings from exercise participants.

During the second day of the exercise on November 19, copycat attacks and inaccurate social media reports further stressed utilities that continued to work with RCs and others to maintain grid reliability by implementing emergency control actions including load shedding and rotating outages.

Observations and Recommendations

Distributed Play

NERC fulfilled its GridEx III 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 resulting from GridEx III, 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 NERC 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.[4] While some of the observations and recommendations relate to lessons learned by participating organizations as a result of their responses to the exercise scenario, many of them relate to how the exercise was planned and conducted. This is a result of the relatively low number of lessons learned shared by participating organizations, and NERC anticipates this input will increase for future exercises.

This section provides a summary of the input NERC received from participating organizations that submitted after-action survey responses and lessons learned documents. These observations and recommendations identify opportunities to enhance the security and reliability of the North America's BPS. NERC and other industry groups should coordinate their efforts to address these recommendations by developing new or enhancing existing guidelines on behalf of the industry, for example. Industry groups include:

- NERC's Planning Committee (PC), Operating Committee (OC), and Critical Infrastructure Protection Committee (CIPC)
- North American Transmission Forum (NATF)
- North American Generator Forum (NAGF)
- Electricity Subsector Coordinating Council (ESCC)
- Trade associations

Observation 1: Coordinated Response and Communication. GridEx III provided participants with the opportunity to exercise their incident response procedures during large-scale security events affecting North America's electricity system. The large-scale cyber and physical attack scenario was designed to overwhelm even the most prepared organizations. GridEx III highlighted the importance of well-coordinated communications. GridEx III provided the opportunity to test communications processes and tools (e.g., testing satellite phone capacity and functionality) when normal forms of communication, such as email and phone, are unavailable. Lessons learned from some organizations indicated that day-to-day communication mechanisms, roles, and responsibilities during such an event would be insufficient.

Recommendations

a) Organizations should review documentation that describes their internal information-sharing processes in the context of a large-scale event. This will enhance current situation awareness of staff at system operations, field locations, security, and other business areas. Documentation should be examined to identify opportunities to align incident response by different parts of the organization.

[4] Ref. E-ISAC Code of Conduct http://www.nerc.com/gov/Annual%20Reports/ES-ISAC_Code_of_Conduct%20(FINAL%203%2011%2015)docx.pdf

b) Organizations should test the capability of their alternative communications facilities and equipment. Future GridEx exercises should explicitly include opportunities to exercise these communication capabilities.

Observation 2: Reporting Mechanisms. Reporting tools and related processes (i.e., OE-417, CIP-008, EOP-004, RCIS, and E-ISAC portal) used by the industry should be reviewed in order to eliminate redundancies, increase timeliness, and enhance information quality. GridEx III participants observed that some aspects of these information sharing and reporting tools are redundant, time-consuming to use, and provide no feedback mechanism to those who most need the information. The larger number of active participants and increased information flow because of the severity of the GridEx III scenario highlighted these issues.

Recommendations

a) Review the various tools and reporting processes used by the industry[5] to identify opportunities to improve the efficiency and effectiveness of the information sharing process.

Observation 3: Active Participation of Operations Management, Support Staff, and System Operators. NERC succeeded in designing an exercise scenario that linked the physical and cyber attacks with how system operators would respond to mitigate the impact of these attacks on BPS reliability. To a much greater degree than previous GridEx exercises, GridEx III simulated physical and cyber impacts that required system operators to take immediate control actions even though the attacks may have affected the tools they use to do their jobs. Cyber attacks targeted the electricity industry's corporate networks and critical control systems, physical attacks targeted key generation and transmission facilities, and system operators and field staff responded as the events unfolded in real-time. In order to create conditions that would satisfy local objectives and system functionality, NERC encouraged RCs, consistent with their system operation roles, to take the lead in planning GridEx III with utilities in their areas. The response to the question related to operational response in the after-action survey received the highest percentage of all "very well" responses (63 percent).

Recommendations

a) Continue to leverage the essential role of RCs to help ensure that the scenarios for future GridEx exercises are credible, customized to reflect local conditions, and effectively coordinate generation, transmission, and system operations in the context of cyber and physical security events.
b) Future GridEx exercises should continue to include scenarios that prompt operations management, support staff (such as corporate communications), and field operations to interact with cyber and physical security personnel.

Observation 4: E-ISAC Information Sharing. During the months leading up to GridEx III the E-ISAC structured a new watch center organization, upgraded the E-ISAC portal, and began training newly hired staff. By design, the GridEx III scenario provided the flexibility for customized scenarios at each organization. This exercise artificiality, while valuable for participating organizations, made it challenging for the E-ISAC to perform analysis, as most incidents were unique to each organization and no common indicators existed. These factors prohibited the E-ISAC's ability to provide clear guidance and mitigation measures. Participants highlighted this as an area for future exercise improvement. Participants identified that the E-ISAC portal needed enhancements to handle real-time, urgent communication with portal members. During the exercise, information was quickly buried within the portal and it became difficult to highlight important information.

[5] Ref. for example, Recommendations for Improving Information Sharing, NERC CIPC Electricity Sector Information Sharing Task Force, May 2013. While this report suggests opportunities to streamline the various reporting processes, further work is required to recognize real-time versus after-the-event information needs.

Recommendations

a) The E-ISAC should continue to enhance the E-ISAC portal to support real-time, searchable, urgent communication and collaboration with portal members. The automated tools used by system operators to monitor events affecting the reliability of the BPS may provide examples of these capabilities, recognizing the very different sources and types of data involved.
b) The E-ISAC should continue to develop and mature its capabilities including training the watch operations team, enhancing internal communications capabilities, and developing a prioritization method for responding to and disseminating information to industry.
c) Future GridEx scenarios should be designed to focus E-ISAC analysis on a reasonable and credible subset of the player responses to certain scenario injects (as opposed to attempting to analyze all player responses to their own customized injects).
d) For future GridEx exercises, consider enhancing the Move 0 scenario (i.e., prior to the start of the exercise) to provide a more credible period of time for the E-ISAC to receive information from participants and analyze emerging threats and vulnerabilities.

Observation 5: Introduction of New Exercise Tools. Exercise tools were rated as "more than adequate" or "adequate" by 75 percent of survey respondents, indicating that these new tools certainly enhanced the exercise. However, there is room for improvement. InjectDeck, part of the SimulationDeck tool, was configured to automatically distribute the baseline scenario injects via email from ExCon to lead planners. However, many organizations chose to customize their own scenario injects and therefore did not need to receive the baseline injects from SimulationDeck. Instead, they simply distributed their own injects according to the baseline scenario timeline.

Recommendations

a) The inject distribution tool for future exercises needs to be dynamic enough to adapt to the customization of each organization's scenario injects. Lead Planners should be able to create their own injects within the tool to use for distribution. Alternatively, organizations could develop their own inject distribution mechanisms (e.g., email).
b) Enhance exercise management and communications tools to increase load capacity during large-scale exercises. Perform functionality and volume/capacity tests in advance of the exercise. Provide training in advance of the exercise on the tools for lead planners to deliver to their participants, especially corporate communications participants who would make posts for their organizations during the exercise.
c) Consider enhancing the social media simulator to include a notification feature to alert users when new content has been posted to the various sections of the tool. These notifications should be customizable to allow users to receive alerts on different platforms (e.g., email, text).

Observation 6: Advance Exercise Planning Timelines. In response to feedback received following GridEx II, the NERC planning team adopted a more aggressive timeline to provide more time for lead planners to conduct their own planning activities. Additionally, NERC encouraged RCs to take a lead role by coordinating entities within their areas. Both of these changes for GridEx III marked a large shift in the exercise planning structure, and were well received as they improved the ability of participating organizations to customize the scenario and prepare their players. Feedback from the survey and lessons learned reports indicated that training players for the exercise should be improved in future exercises. Feedback indicated that the training offered for players, one and a half months prior to the exercise, was too soon as some organizations had not yet identified who in their organization would participate.

Recommendations

a) Planning for the next GridEx exercise should begin earlier than GridEx III in 2013 to provide organizations with more time to conduct their own planning and training activities. Conceivably this would mean

starting planning in September or October for an exercise in November of the following year. NERC should develop a firm delivery schedule with stakeholders including major planning milestones and tool development and testing at the outset of exercise planning.

b) Future GridEx exercises should continue to provide opportunities for organizations to customize their scenario injects provided they are consistent with and support the overall NERC scenario as coordinated with their RCs.

c) Each participating organization should train their own players. The NERC planning team should continue to develop a training package for lead planners to deliver to players within their organization at a time individual organizations deem appropriate.

Observation 7: After-Action Survey and Lessons Learned. During the early stages of the GridEx III planning process, NERC developed a set of metrics to assess the success of the exercise which included the questions in the after-action survey.

In addition, NERC provided lead planners with a lessons learned template to help them document their observations and provide feedback to NERC. NERC received 25 lessons learned reports from participating organizations, representing about 24 percent of active participating utility organizations. The reports that were submitted provided a great deal of valuable input, but a greater number of reports from participating organizations would provide a more complete and representative set of lessons learned.

Recommendations

a) The NERC planning team should use similar after-action survey questions for the next GridEx in order to measure the extent to which objectives are achieved, and to assess the evolution of the GridEx program.

b) The NERC planning team should consult with participating active organizations to understand any reluctance to share lessons learned and to identify ways to increase the response rate.

Executive Tabletop

The executive tabletop engaged senior leaders in a robust discussion of the policy issues, decisions, and actions needed to respond to a major grid disruption caused by simulated physical and cyber attacks. Participants identified security and reliability challenges and opportunities to improve prevention, response, and recovery strategies. The discussion centered on three key areas: unity of messaging, unity of effort, and extraordinary measures.

Unity of Messaging

Participants explored how industry and government assess a crisis event, and receive and share information with each other and the public. Managing the challenges and opportunities related to social media was of particular interest.

- **Assess the Situation.** The industry and government need mechanisms to develop a common view of the evolving situation from two perspectives: the impact on the delivery of electricity to consumers, and the intelligence information needed by the industry to respond and recover, considering ongoing or follow-on attacks are likely.

- **Communicate with the Public.** The industry and government need to provide the public with meaningful information so they are aware of the situation and what is being done about it. This helps individuals decide what they need to do to look after their own interests. Utilities and government at all levels, local, state/provincial, and federal, will need to communicate with the public. Social and traditional media capabilities drive an ever-increasing demand for timely and accurate information. Widespread and prolonged power outages will disrupt the ability of traditional media (television, radio, print) to function.

Unity of Effort

While both industry and government have considerable resources at the ready to respond to crisis events, participants considered how to improve coordination during severe emergency situations.

- **Resolve Physical Risks to Personnel.** Industry needs to coordinate with local law enforcement to identify and assess the physical risks to electricity facilities. Utility workers will not begin to perform site assessments or begin repairs to electricity system facilities until they are satisfied their work environment is safe.
- **Resolve Cyber Threats and Malware.** Industry needs to coordinate with government to identify and assess the cyber risks, likely by visiting the affected facilities. Unlike how industry responds to major storms through mutual assistance, industry's capability to analyze malware is limited and would require expertise likely available from software suppliers, control system vendors, or government resources. Electricity system recovery and restoration would be delayed or may not begin until the nature of the cyber risks are understood and mitigation strategies are available.

Extraordinary Measures

The industry operates within a regulatory framework designed within normal planning and operating criteria. Participants considered regulatory and legislative needs, as well as extraordinary government support, that could enhance timely and effective recovery under extreme circumstances that clearly exceed normal criteria.

- **Establish Priorities for Restoring Electricity Service.** When restoring power following a large-scale outage, utilities' first priorities focus on supplying electricity to re-start generation and energize transmission and distribution lines and equipment. Second priorities include "lifeline" customers such as communications, oil and gas, water supply/treatment and hospitals.
- **Simplify Electricity System Operation Under Emergency Conditions.** North America's bulk power system is operated by highly trained staff using sophisticated technology systems to forecast load, monitor electricity flows, dispatch generation, remotely operate equipment, and administer markets. In the event that these normal processes are disrupted, it may be possible to simplify how the electricity system is operated to provide basic service but at reduced levels of reliability and less economically.
- **Consider Mechanisms to Prevent Financial Defaults.** Utilities will need unprecedented levels of financial resources in order to restore their facilities and eventually resume normal operations.
- **Manage Personal and Corporate Liability Risks.** North America's bulk power system is designed and operated to meet extensive legal and regulatory requirements (e.g., environmental, safety, financial, labor, commercial). Some of these requirements may delay or prevent restoration during a large-scale event.

Conclusions

In responding to the distributed play after-action survey, all of the participating organizations indicated that GridEx III met their expectations "well" or "very well." NERC's GridEx III distributed play exercise successfully provided industry with a learning opportunity to strengthen both internal and coordinated crisis response plans. The exercise also served as an opportunity to enhance the industry's information-sharing capabilities. Participants considered the exercise a successful training event that delivered a substantial return on the time and resources they invested.

Participants of the executive tabletop agreed that the tabletop helped to reinforce the need to continue to build on the collaborative relationships between the electricity industry and government. Participants recognized the progress made to address the recommendations of GridEx II in 2013. They also acknowledged the need to continue efforts in other more challenging areas.

NERC will continue to work closely with industry and government stakeholders to address the recommendations from GridEx III to enhance the industry's readiness and further evolve the GridEx program.