NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Grid Security Exercise (GridEx II)

After-Action Report

March 2014

RELIABILITY | ACCOUNTABILITY




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

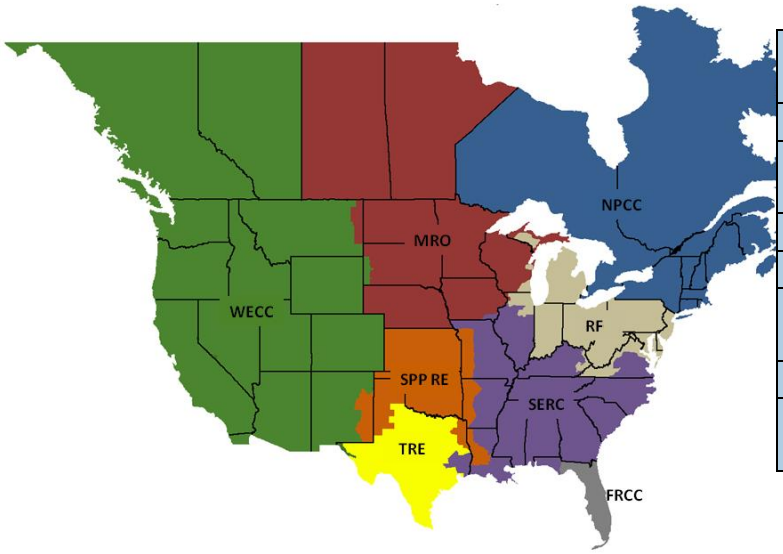
Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international electric reliability organization (ERO) whose mission is to ensure the reliability of the bulk power system (BPS) in North America, including the continental United States, Canada, and the northern portion of Baja California, Mexico. 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 is subject to oversight by the Federal Energy Regulatory Commission (FERC) and is under similar obligations in Canada, as well as a portion of Baja California Norte, Mexico. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

In 2007, FERC approved agreements by which NERC delegates its authority to monitor and enforce compliance to eight Regional Entities. The members of the Regional Entities come from all segments of the electricity industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; power marketers; and end-use customers. These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico. The footprints of the eight Regional Entities are shown on the map and corresponding table below.

NERC Regional Entities



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
TRE	Texas Reliability Entity
WECC	Western Electric Coordinating Council

Executive Summary

NERC conducted its second industry-wide grid security exercise, GridEx II, on November 13 and 14, 2013. The exercise brought together NERC, industry, and government agencies, as well as participants from Canada and Mexico. GridEx is an example of industry's ongoing efforts on cyber and physical security. It was the largest, most comprehensive effort addressing security by the electricity industry to date and serves as an example of the commitment of stakeholders to continuously improve cyber and physical security.

The NERC GridEx II scenario was built on the objectives, outreach, and findings from GridEx 2011. The exercise, a coordinated cyber and physical attack on the BPS, promoted coordination and highlighted urgent issues facing the industry. The simulated cyber attack impacted corporate and control networks, while the concurrent simulated physical attack degraded reliability and threatened public health and safety. NERC encouraged participating organizations to modify the GridEx II baseline scenario to achieve entity-specific objectives and ensure relevance to local conditions.

Over 234 organizations with more than 2,000 individuals from all key BPS functions, as well as relevant government agencies such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE), participated in the simulated exercise play. Participants received sequenced email messages that detailed scenario conditions throughout the one-and-a-half-day exercise. Based on this information, "Players" engaged in both internal response measures and external coordination activities across the industry. An Exercise Control (ExCon) cell transmitted scenario updates, simulated nonplaying entities, monitored exercise play, and recorded response activities.

GridEx II's objectives were to:

- Exercise the current readiness of the electricity industry to respond to a security incident, incorporating lessons learned from GridEx 2011.
- Review existing command, control, and communication plans and tools for NERC and its stakeholders.
- Identify potential improvements in cyber and physical security plans, programs, and responder skills.

Lessons Learned and Recommendations

Following the exercise, planners conducted a review to discuss recorded exercise communication and request input from after-action surveys. The following key lessons learned and recommendations emerged from the comprehensive review:

- **Continue to Enhance Information Sharing**
  - Exercise formal communication paths to strengthen crisis response information sharing.
  - Share information early using multiple pathways to allow analysis centers to conduct more rapid analysis and provide mitigation response.
- **Continue to Enhance NERC Coordination**
  - Expand Electricity Sector Information Sharing Analysis Center (ES-ISAC) conference call capabilities to ensure appropriate personnel can be accommodated in crisis situation briefings.
  - Clarify ES-ISAC subject matter experts' functions and membership and communicate those roles across industry.
  - Continue refinement and promotion of the ES-ISAC portal as a central coordination point and reporting tool in crisis.
- **Challenge of Simultaneous Attack**
  - Clarify reporting roles and functions within entities in the event of a coordinated cyber and physical event.
  - Estimate surge resource requirements before a crisis.
  - Continue using risk-based vulnerability assessments to potentially increase protection of physical and cyber assets.
  - Evaluate and potentially increase participation in recovery programs such as the Spare Transformer Equipment Program or the Spare Equipment Database.
- **Continue Improvement of Incident Response**
  - Assess business and operational implications of isolating IT assets during a cyber event to ensure critical functions are maintained.
  - Develop mechanisms to preserve evidence and collect forensic data following a suspected physical or cyber attack.

  - Align incident response escalation plans among business units to promote consistent response across the organization.
  - Review communications infrastructure and identify redundancies or alternatives to ensure viable communications channels during a crisis.
- **Continue Improvement of Situational Awareness Content**
  - Continue to build relationships with relevant government stakeholders to establish communication procedures prior to a crisis.
  - Filter and consolidate industry and government communication and advisories so relevant information can be processed quickly.
- **Continue to Improve the Grid Exercise Program**
  - The GridEx program has matured since GridEx 2011, and exercise participants want that growth to continue with programmatic and scope-related enhancements for GridEx III in November 2015.

Executive Tabletop

After the Distributed Play portion, an Executive Tabletop involving electricity industry executives and senior officials from the U.S. federal government took place. The goal of the Tabletop was to examine the policy-level issues and management decisions that would need to be made in the case of a Severe Event.[1] Participants in this Tabletop discussion identified a number of observations and recommendations for industry and the federal government.

- **Situation Assessment Scalability**: One of the most important aspects of responding to a crisis is the ability to quickly and accurately assess the situation, share that assessment with decision makers, and take action. The electricity industry's primary capability to perform situation assessments at the North American level is through the ES-ISAC and BPS functions. For government, the DHS National Cybersecurity and Communications Integration Center (NCCIC) serves as a centralized location where operational elements involved in cybersecurity and communications are coordinated and integrated. The ES-ISAC provides personnel to the NCCIC as needed to share information related to emerging cybersecurity threats and vulnerabilities. While coordination with the NCCIC is a good initial step toward addressing a cybersecurity threat or attack, response, communication, and coordination processes need to be scalable to meet the extraordinary challenges of a Severe Event.

- **Public Communications**: Efforts to restore electricity would be supported—or hindered—by information provided to the public through print, radio, television, and social media. The public's need for frequent, timely, relevant, accurate, consistent, and credible information would be particularly acute through a Severe Event.

- **Unity of Effort**: A unified approach is required to identify, discuss, and decide the many policy-level issues that result from a Severe Event. This requires industry executives and senior government officials at local, state, federal, and potentially international levels to be directly involved.

- **Cyber Attacks Create Unique Restoration Challenges**: Unlike storms that can be predicted and tracked with some degree of accuracy and equipment failures that tend to be random and limited in impact, cyber attacks present unique challenges for how the electricity industry restores power.

- **Physical Attacks Create Unique Restoration Challenges**: While the electricity industry has experienced occasional acts of sabotage or vandalism, a well-coordinated physical attack also presents particular challenges for how the industry restores power.

- **Mutual Aid and Critical Spares:** The extreme challenges posed by the Severe Event scenario provided an opportunity for participants to discuss how the electricity industry's mutual aid arrangements and inventories of critical spare equipment may need to be enhanced.

[1] For the purpose of this report, the term "Severe Event" means an event of a scale, scope, and duration commensurate with the GridEx II scenario; a coordinated physical and cyber attack that interrupts the reliable supply of electricity with consequential public safety and national security implications.

- **Regulatory Relief**: The electricity industry is highly regulated by mandatory standards and state and federal government regulations administered by various government agencies. Some of these regulations would constrain the operation of certain generators, and specific relief provisions should be considered before a Severe Event.

- **Legislation to Deal with Emergencies:** Existing statutes might be useful to help recovery efforts in a Severe Event (Defense Production Act, Stafford Act, etc.) but may not have been used in that capacity. A review of these statutes to determine if there is a need to develop legislation to facilitate recovery during a Severe Event would be helpful.

Conclusion

Participating entities found GridEx II useful for identifying opportunities to enhance their physical and cyber incident response plans. Interaction with the ES-ISAC was found to be "effective" or "very effective," and use of the ES-ISAC tools, such as the secure portal, were considered important progress since some of these tools were not available for the first GridEx. Tabletop participants agreed that the discussion provided a unique opportunity to better understand the respective challenges that both the electricity industry and government would face under extraordinary circumstances. The discussion identified opportunities to enhance how the public–private partnership must coordinate on an event of this scale, optimize efforts to mitigate impacts on public health and safety, and restore power.

NERC will continue to work closely with industry, government stakeholders, the Critical Infrastructure Protection Committee, the Electricity Sub-Sector Coordinating Council, and other relevant bodies to address the recommendations and further strengthen the electricity sector's physical and cybersecurity programs.

Introduction

Cyber and physical security have long been priorities for NERC and industry. The following report details how the grid security exercise was developed and how the lessons learned and recommendations were garnered through GridEx II.

Building on the success of GridEx 2011, the exercise was designed to exercise utilities' all-hazard crisis response functions, use and build upon existing information-sharing relationships and processes, and provide a venue for feedback on internal incident response improvements. NERC and industry expanded the exercise's participation, scope, and sophistication to position GridEx II as the largest electricity industry crisis response exercise ever conducted.

Industry leaders in cyber and physical security from NERC's Critical Infrastructure Protection Committee (CIPC) established and populated the Grid Exercise Working Group (GEWG) in February 2013. The group led the design and development of the GridEx II scenario and provided guidance on exercise mechanics and logistics.

Similar to 2011, GridEx II featured a hybrid operational-and discussion-based exercise format that combined a geographically distributed environment for operators and response personnel (Distributed Play) with a tabletop portion for executive leadership (Executive Tabletop). This report provides a summary of the planning, design, and outcomes of GridEx II.

The majority of Players participated in the Distributed Play portion from their normal places of work for one and a half days. Participants received sequenced email messages detailing simulated scenario conditions and engaged in both internal response measures and external information-sharing activities across the industry and government. As detailed in this report, GridEx II succeeded in attracting a broad representation of electricity industry stakeholders and providing them with a learning environment to enhance the security and operational restoration of the grid.

Background

As a result of society's growing dependence on electricity, the electricity grid is one of North America's most critical infrastructures. Decades of experience with hurricanes, ice storms, and other natural disasters, as well as mechanical breakdowns, vandalism, and sabotage, have taught the electricity industry how to build strong, reliable networks that generally withstand all but the worst natural and physical disasters. The industry has developed a variety of mutual aid agreements that are executed during major regional events, drawing on the resources of other utilities and contractors from outside the affected local area or region to aid in prompt restoration of electricity. The knowledge that disturbances on the grid can impact operations thousands of miles away has influenced the electricity industry's culture of reliability, affecting how it plans, operates, and protects the bulk power system.

NERC and the industry are concerned about the changing risk landscape from conventional risks, such as extreme weather and equipment failures, to new and emerging risks that might occur. The goal is to avoid or mitigate the consequences, some of which could be much more severe than previously experienced. For example, coordinated physical and cyber attacks could disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures. These threats differ from conventional risks in that they result from intentional actions by adversaries, not random failures or acts of nature.

The electricity industry continues to increase collaboration and coordination with government to address these risks. The examples below outline some of the activities NERC and industry have undertaken to enhance the industry's reliability and resilience.

Policy and Strategic Coordination

Electricity Sub-sector Coordinating Council (ESCC)

In 1998, the DOE requested NERC to help coordinate ongoing electricity industry initiatives, government partnerships, and responsibilities related to critical infrastructure protection. This role evolved to the ESCC as established by the sector coordinating council framework provided in the DHS's National Infrastructure Protection Plan in 2006. The ESCC facilitates and supports the coordination of sub-sector-wide policy-related activities and initiatives to improve the reliability and resilience of the electricity sub-sector, including physical and cybersecurity infrastructure and emergency preparedness. In August 2013, the NERC Board of Trustees (Board) approved a revised charter for the ESCC that significantly increases industry membership at the executive level. The ESCC meets regularly with the Energy Government Coordinating Council (EGCC) and conducts a variety of working group activities to improve information sharing between government and industry, emergency response planning, and the deployment of tools and technologies to support electricity industry cybersecurity.

NERC Reliability Issues Steering Committee (RISC)

The RISC is an advisory committee that reports directly to the Board and triages and provides front-end, high-level leadership and accountability for nominated issues of strategic importance to bulk power system reliability, including high-impact, low-frequency (HILF) risks. The RISC assists the Board, NERC technical committees, NERC staff, regulators, and industry stakeholders establish a common understanding of the scope, priority, and goals to develop solutions that address these issues.

The ESCC and the RISC provide a comprehensive, strategic view of the risks facing the bulk power system. They inform the industry of events and trends in risks to reliability so that NERC and the industry can prioritize efforts to address them.

Mandatory Standards

Cybersecurity Standards

In 2007, NERC was certified as the electric reliability organization (ERO) by the Federal Energy Regulatory Commission and has Reliability Standards in place that are mandatory and enforceable. These standards support the reliable planning and operation of the bulk power system across North America and include standards to mitigate risks related to cybersecurity and geomagnetic disturbances. Mandatory cybersecurity standards have been in place for the electricity industry since 2010. These standards continue to be enhanced, and Version 5 was recently approved by FERC for implementation by the industry.

This latest version includes new cybersecurity controls and extends the scope of systems that the standards protect.

Geomagnetic Disturbance Mitigation Standards

NERC developed Geomagnetic Disturbance Mitigation Standard EOP-010-1,[2] and FERC has proposed to approve it.

Information Sharing

Electricity Sector Information Sharing and Analysis Center (ES-ISAC)

Compliance with the NERC CIP standards is an important threshold for properly securing the bulk power system. However, there is no single security asset, security technique, security procedure, or security standard that, even if strictly followed or complied with, will protect an entity from all potential threats. The cybersecurity threat environment is constantly changing and defenses must keep pace. Security best practices call for additional processes, procedures, and technologies beyond those required by the cybersecurity standards. In such cases, NERC Alerts are a key element in critical infrastructure protection. NERC works through its ES-ISAC to inform the industry and recommend preventive actions. Members of NERC staff with appropriate security clearances often work with cleared personnel from federal agencies including the DHS, the DOE and its National Laboratories, and bulk power system subject matter experts to communicate sensitive information to the industry.

Classified Briefings

Twice per year, NERC's Critical Infrastructure Protection Committee hosts classified briefings for its members led by representatives from DOE, DHS, and other government agencies to share security-related information including threat updates and mitigation strategies.

Physical Security Campaign

During 2013, NERC and the industry collaborated with the DOE and DHS to conduct a series of workshops to share lessons learned and raise awareness among utility managers and local law enforcement to enhance physical security at electricity facilities.

Grid Security Conferences

NERC hosts annual Grid Security Conferences together with industry and government security professionals to provide presentations on cyber and physical security and share best practices. In 2013, NERC's third conference attracted over 300 attendees.

Cybersecurity Capability Maturity Model (C2M2)

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity, combines elements from existing cybersecurity efforts into a common tool that can be used consistently across the industry. The Maturity Model was developed as part of a White House initiative led by the DOE in partnership with the DHS and involved close collaboration with industry, other federal agencies, and other stakeholders.

Sufficiency Review Program

NERC's Sufficiency Review Program provides electricity industry entities an opportunity to review the "sufficiency" of their implementation of the NERC cybersecurity standards. Conducted separately from standards compliance audits, these reviews take a broad cybersecurity perspective and consider future versions of the standards not yet in force.

Spare High-Voltage Transformers

Many pooling/bilateral agreements exist today among industry participants to support utilities in responding to and managing bulk power system reliability if an event causes loss of transformers. NERC's Spare Equipment Database and Edison Electric Institute's (EEI) Spare Transformer Equipment Program facilitate the identification of critical spares to aid in response and recovery efforts following a HILF event.

[2] Ref. Geomagnetic Disturbance Mitigation standard http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx

High-Impact, Low-Frequency (HILF) Risks

In 2010, NERC's technical committees established four new task forces to address the HILF risks identified by the ESCC and the RISC. The task forces were composed of approximately 300 subject matter experts across the electricity industry, the scientific community, academia, manufacturers, and government agencies in Canada and the United States.

Geomagnetic Disturbance Task Force:[3] The GMDTF report provided a thorough account of historical GMDs and their impact on bulk power system reliability. The report describes U.S. and Canadian government capabilities to monitor and forecast space weather events. In May 2011, NERC published the *Industry Advisory – Planning for Geomagnetic Disturbances*[4] in an effort to provide entities with the latest guidance regarding planning and operations actions needed to mitigate the impact of a GMD. Phase 2 of the task force is currently addressing the key recommendations of the May 2011 report.

Spare Equipment Database Task Force:[5] This task force recommended mechanisms to quickly identify spare high-voltage transformers that may be available and critically needed to restore the bulk power system following a severe-impact emergency event. Their report provided the specifications for a new NERC database that was implemented in May 2012.

Cyber Attack Task Force:[6] This task force considered the impact of a coordinated cyber attack on the reliable operation of the bulk power system and identified solutions to enhance existing protection, resilience, and recovery capabilities.

Severe Impact Resilience Task Force:[7] This task force assessed the industry's existing resilience capability and developed options to safely operate and restore the bulk power system through three severe-impact scenarios: coordinated physical attack, coordinated cyber attack, and a geomagnetic disturbance event. The report provided guidance to industry asset owners and operators to enhance the resilience of the bulk power system when faced with a HILF event.

Training and Exercises

Critical Infrastructure Protection Committee

NERC's CIPC provides a forum for electricity industry experts to receive training related to cyber and physical security and share information regarding good industry practices.

Grid Security Exercises (GridEx)

In 2011, NERC conducted its first security exercise on industry readiness to respond to a security incident and to identify lessons learned. The exercise involved about 75 organizations from industry, government, law enforcement, and academia. In 2012, the ESCC discussed with senior government officials the need to better understand how NERC and the electricity industry would coordinate actions with the government through a severe emergency that causes bulk power system outages that last weeks or months. The ESCC and the EGCC agreed to develop an extreme emergency exercise scenario to explore the policy-level decisions that would need to be made during the weeks or months that would follow a significant security event with national security implications. The scenario would be intentionally severe to ensure that policy-level issues would be identified beyond those yet experienced by the electricity industry. NERC proposed that this scenario be conducted as part of its planned GridEx security exercise for 2013.

[3] *Interim Report: Effects of Geomagnetic Disturbances in the Bulk Power System* http://www.nerc.com/files/2012GMD.pdf

[4] *Industry Advisory – Planning for Geomagnetic Disturbances, May 2011* http://www.nerc.com/fileUploads/File/Events Analysis/A-2011-05-10-01_GMD_FINAL.pdf

[5] *Spare Equipment Database Report* http://www.nerc.com/docs/pc/sedtf/SEDTF_Special_Report_October_2011.pdf

[6] *Cyber Attack Task Force – Final Report* http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board Accepted 0521.pdf

[7] *Severe Impact Resilience: Considerations and Recommendations* http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf

Chapter 1 – Participation

Distributed Play

The Distributed Play portion of GridEx II had twice the number of participants as GridEx 2011. Figure 1 illustrates the growth in participation between GridEx 2011 and GridEx II, along with the percentage of "Full Player" and "Monitor/Respond" organizations for each exercise.

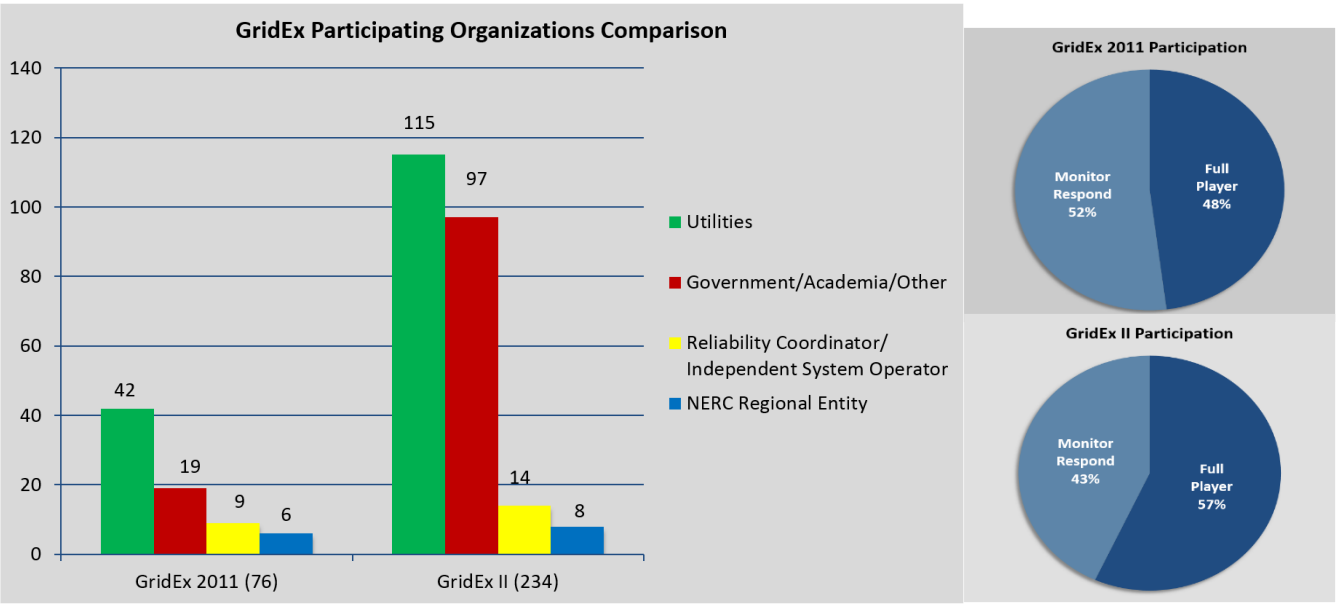


Figure 1: GridEx 2011 and GridEx II Participation Comparison

Exercise planners established two levels of organizational participation for the actual exercise play: Full Player and Monitor/Respond. Full Player organizations engaged in the planning process, exercise play, and external coordination, while Monitor/Respond entities followed the scenario progression and considered scenario implications internally. These two options for exercise play enabled organizations to select their level of involvement based on resources, timing, and other factors.

"Planners" from each organization had access to scenario specifics and materials and organized the customization of scenario events to match local objectives and system requirements. Players were given familiarization training for the exercise but were shielded from the exercise scenario. Approximately 500 Planners and 1500 Players participated in the Distributed Play exercise. The core team, which consisted of Lead Planners (one primary Planner from each organization) and members of the GEWG, participated in bimonthly planning calls, attended three main planning conferences, shaped the exercise objectives, supported scenario design, and contributed to the after-action process.

Overall, more than 2,000 individuals in 234 organizations from the United States, Canada, and Mexico participated in GridEx II. Participation consisted of:

- 115 utilities;
- 14 Reliability Coordinators (RCs) or Independent System Operators (ISOs);
- 8 NERC Regional Entities; and
- 97 law enforcement agencies, software vendors, and other affiliated organizations.

The exercise's participation level far surpassed the initial recruitment goal of 100 organizations established at the beginning of the planning process. The increase in participation is attributable to several factors, including:

- The successful incorporation of GridEx 2011 lessons learned into GridEx II;
- Returning Planners and other participants from GridEx 2011;
- A more challenging combined cyber and physical attack scenario;
- The commitment to providing learning opportunities with no compliance-related risks;
- More proactive recruiting, planning, and preparation processes;

- Availability to earn continuing education hours for individual certifications (NERC Certified Operators, Information Technology, physical security, etc.) and opportunities for organizations to meet annual Critical Infrastructure Protection (CIP) and Emergency Preparedness and Operations (EOP) compliance requirements; and
- Continued and growing capability of the industry to be prepared for and respond to cyber and physical attacks.

Executive Tabletop

The 31 participants of the Executive Tabletop portion of GridEx II were by invitation only. They included electricity industry executives representing a broad cross-section of the industry, and senior officials from the U.S. federal government. Comprehensive briefing material with scenario details and sample discussion questions had been provided to participants well in advance to help ensure that the Tabletop focused quickly on the policy issues. 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 Severe Event. Participants articulated the limitations and barriers that would need to be addressed, both independently and collaboratively, to respond.

A Member of the National Infrastructure Advisory Council facilitated the Tabletop. Those directly participating included:

- 14 electricity industry executives from the United States and Canada, representing a cross-section of investor-owned and publicly owned utilities, cooperatives, and independent system operators (e.g., chief executive officers or chief operating officers).
- 17 senior government officials (e.g., federal deputy and assistant secretaries) from the White House and several federal government departments and agencies, including the DOE, DHS, FBI, FERC and the Department of Defense.

In addition, approximately 30 individuals associated with direct participants attended the Tabletop as observers. The Tabletop was conducted as a Critical Infrastructure Partnership Advisory Council (CIPAC) meeting. CIPAC meetings help provide a known and trusted framework to foster the flow of advice and information concerning critical infrastructure protection, risks, and vulnerabilities. Federally registered lobbyists were excluded from participating.

Chapter 2 – Exercise Objectives

Distributed Play

The GridEx II Distributed Play objectives were shaped by GridEx 2011 outcomes, priorities, and ongoing initiatives that recognize the serious cyber and physical security threats facing the electricity industry. In addition to the overarching exercise objectives, GridEx II was designed with the flexibility to encourage each participating organization to create its own objectives to focus internal efforts. Through the one-and-a-half-day exercise, Players successfully achieved the three pre-established objectives for the Distributed Play event.

Objective 1: Exercise the current readiness of the electricity industry to respond to a security incident, incorporating lessons learned from GridEx 2011.

- The hybrid physical and cyber event will engage a range of security staff as well as other organizational components in crisis response. To increase industry awareness, spearphishing will be one among several potential cyber attack vectors. Recent advanced physical attack tactics will be replicated and potentially exceeded in scenario development.
- Work to build a common operating picture through information sharing between the electricity subsector and the federal government.

Achieved: Led by the core team, the GridEx II Planner community developed a hybrid scenario with challenging cybersecurity and physical security dimensions not yet experienced by the electricity industry. The scenario, which featured both sophisticated cyber intrusions and crippling physical attacks that significantly disrupted BPS reliability, enabled organizations to stress-test their all-hazard response capabilities. The broad-based scenario conditions also promoted coordination and information sharing to achieve shared situational awareness. Over 90 percent of entities indicated in the after-action survey that the scenario provided them the opportunity to exercise their response plans "well" or "very well."

Objective 2: Review existing command, control, and communication plans and tools for NERC and its stakeholders.

- Existing incident response/crisis action plans will be exercised at the organizational level and in coordination with other organizations. Increased early information sharing with coordination centers (e.g., the ES-ISAC) is encouraged throughout the scenario.
- Incident data, coordinated response, and mitigation measures based on condition reports will be shared through the ES-ISAC and NERC BPSA, as well as other reporting channels, to industry and government.

Achieved: During exercise play, individual entities and coordinating bodies shared information both horizontally (i.e., within their organizations and with peer organizations such as neighboring utilities) and vertically (i.e., with NERC or government organizations). Participating organizations followed entity-level policies and plans while using their operational or exercise-simulated production tools and reporting channels. Coordination centers like the ES-ISAC and the FBI's CyWatch, among others, triaged email and voice communications and disseminated information using email, secure portals, and voice calls, while NERC BPSA developed and released impact assessments. Exercise control observed frequent bidirectional vertical information flow among the entities, coordination bodies, and government agencies. About 70 percent of entities indicated in the after-action survey that their interactions with the ES-ISAC were "effective" or "very effective." About 50 percent of participating entities indicated they viewed the ES-ISAC's tools, such as their secure portal, to be "effective" or "very effective." While this suggests an opportunity for improvement, these tools did not exist at all for GridEx 2011.

Objective 3: Identify potential improvements in physical and cybersecurity plans, programs, and responder skills.

- Planners will optimize and customize scenario injects[8] to enhance relevance and realism for each Full Player organization; Monitor/Respond organizations will use generic injects.
- Player actions and findings will be captured and shared for the benefit of the electricity industry. All shared information shall be nonattributable in the after-action report and not subject to compliance enforcement.

[8] Discrete pieces of scenario event information

Achieved: Throughout the planning and scenario development process, many participating organizations identified opportunities to improve their security and crisis response polices and plans. The scenario customization process enabled entities to adapt scenario content for their local environments while maintaining consistency with the GridEx II community. Organizations identified strengths, gaps, and areas for improvements in both cyber, physical, and operational plans and protocols. These enhancements were identified due to scenario credibility, broad stakeholder representation, and established mechanisms for capturing Player actions. Over 98 percent of entities indicated in the after-action survey that the exercise was useful for identifying opportunities to enhance their cyber incident response plans; 92 percent identified opportunities to enhance their physical incident response plans.

Executive Tabletop

The objective of the Tabletop was to examine the policy-level issues and decisions that would need to be made in order to manage the impact of a Severe Event on public health and safety. Participants discussed how the electricity industry and government would coordinate their actions and identified approaches and key initiatives to enhance capabilities in the future. To meet the objectives of the Tabletop in the time available, the following items were deemed outside the scope of discussion:

- Participants discussed key messages that would be needed to inform the public and customers through radio, print, television, and social media; however, they did not actually construct messages in collaboration with communications or legal experts.
- While it is well understood that a prolonged electricity outage would have a significant impact on other critical infrastructure sectors, participants did not discuss interdependencies with other critical infrastructures in depth. Participants focused discussions on how to coordinate actions to resume a reliable supply of electricity as soon as possible.
- As this was the first Tabletop conducted by the electricity industry with the national and international implications of a Severe Event, discussions focused on communications with the federal government of the United States only and did not include the Canadian federal government or state/provincial and local governments.

Achieved: Tabletop participants agreed that the discussion provided a unique opportunity to better understand the respective challenges both the electricity industry and government would face under extraordinary circumstances and thanked NERC for taking the initiative. The discussion identified opportunities to enhance how the public–private partnership must coordinate on an event of this scale and optimize efforts to mitigate impacts on public health and safety and to restore power.

Chapter 3 – Exercise Design, Planning, and Scenario Development

GridEx II's exercise design featured both distributed and tabletop exercise tracks (see Figure 2). The Distributed Play track was geographically distributed to enable participants to engage from their regular workplaces (to the extent possible). Players from across the North American BPS learned of simulated scenario conditions through sequenced email messages. The Executive Tabletop began toward the end of Distributed Play, and while participants were informed of Player actions during Distributed Play, it was conducted separately. The Executive Tabletop featured a discussion-based format focused on executive member decision making.

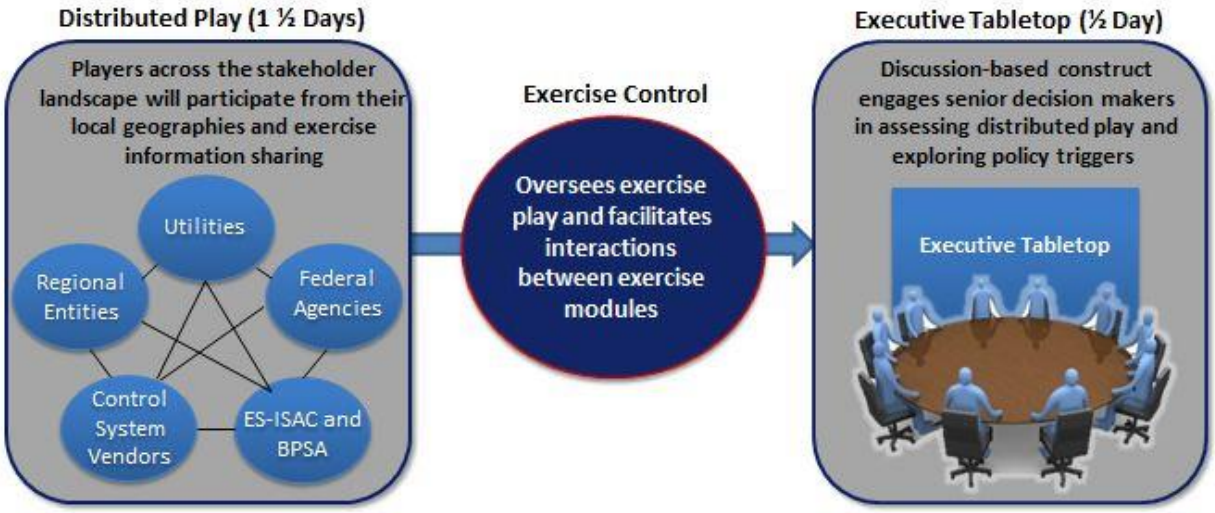


Figure 2: GridEx II Construct

While participants in the Distributed Play exercise assessed information sharing and exercised operational emergency response capabilities, participants involved in scenario elements in the Executive Tabletop highlighted urgent policy issues that would escalate to key decision makers in industry and the U.S. federal government.

NERC leadership, the GEWG, and contractor support formed the exercise core planning team (core team) and recruited participating organizations. The core team led the development of GridEx II exercise objectives to guide outreach, exercise scenario event development, and after-action activities.

Members of the core team staffed ExCon and assumed a number of roles and responsibilities, including simulating entities not participating, supporting a live phone and email help desk, and managing inject distribution. Overall, ExCon facilitated Distributed Play and ensured that key outcomes were shared with the Executive Tabletop participants.

Baseline Scenario Development

The core team was responsible for leading scenario development throughout the planning process. One of the core team's primary considerations was ensuring that scenario content was credible and realistic for utility Players. The team envisioned a determined, well-resourced adversary with robust physical and cybersecurity threat capabilities. To satisfy scenario requirements and present relevant concerns for Players, the team developed a scenario that included a Shamoon-like[9] cyber attack and other advanced persistent threats against participating utilities and some other organizations. This attack was coupled with a coordinated physical attack against a subset of transmission and generation assets developed using open-source techniques. Educating participants on spearphishing was an important subobjective as well. Exercise planners agreed that common vulnerabilities would provide a range of potential options (chosen by Lead Planners) to impact electricity

[9] Shamoon is a computer virus used for cyber espionage in the energy sector that can destroy a computer system's master boot record. It was the subject of the NERC Alert 2012-09-12-01, Industry Advisory *Foreign Energy Sector Entities Networks Impacted*.

industry entities. The scenario was crafted so that Players recognized they were working through distinct attack vectors from a determined adversary.

This baseline scenario development process ensured that common scenario themes were applied across the bulk power system (see Figure 3). The initial scenario narrative created the baseline Master Scenario Events List (MSEL). The MSEL consisted of three overarching moves with multiple injects transmitted within each move. The MSEL injects were delivered in a compressed exercise time frame to maximize the intensity and number of events experienced during the exercise. Injects equated to elapsed scenario (or simulated) time in about a 1:4 ratio (one hour of real time equaled approximately four hours of scenario time) as follows:

- Move 1: November 13, 2013, from 9:30 a.m. to 12:30 p.m. Eastern Standard Time (EST) equated to 9:00 a.m. to 9:00 p.m. EST on November 13, 2013, in scenario time.
- Move 2: November 13, 2013, from 1:00 p.m. to 5:00 p.m. EST equated to 9:00 p.m. on November 13, 2013 to 9:00 a.m. EST on November 14, 2013, in scenario time.
- Move 3: November 14, 2013, from 9:15 a.m. to 1:00 p.m. EST equated to 9:00 a.m. to 9:00 p.m. EST on November 15, 2013, in scenario time.

The baseline MSEL injects and supplementary materials supplied by the GEWG provided adequate content for Monitor/Respond organizations to exercise key functions without dedicating significant resources to customizing the scenario.

During the actual exercise, Planners became Controller/Evaluators (C/Es) to oversee the execution of the Distributed Play scenario and capture lessons learned from Player actions.

The MSEL translated the scenario narrative into injects that were distributed to an organization's Lead C/E or designated email alias during exercise execution. The MSEL also included Expected Player Actions (EPAs), or the anticipated responses from Players after receiving the tailored injects from their C/Es. In some cases, ExCon issued customized contingency injects (also called "2500" injects) to Lead C/Es when EPAs did not occur.

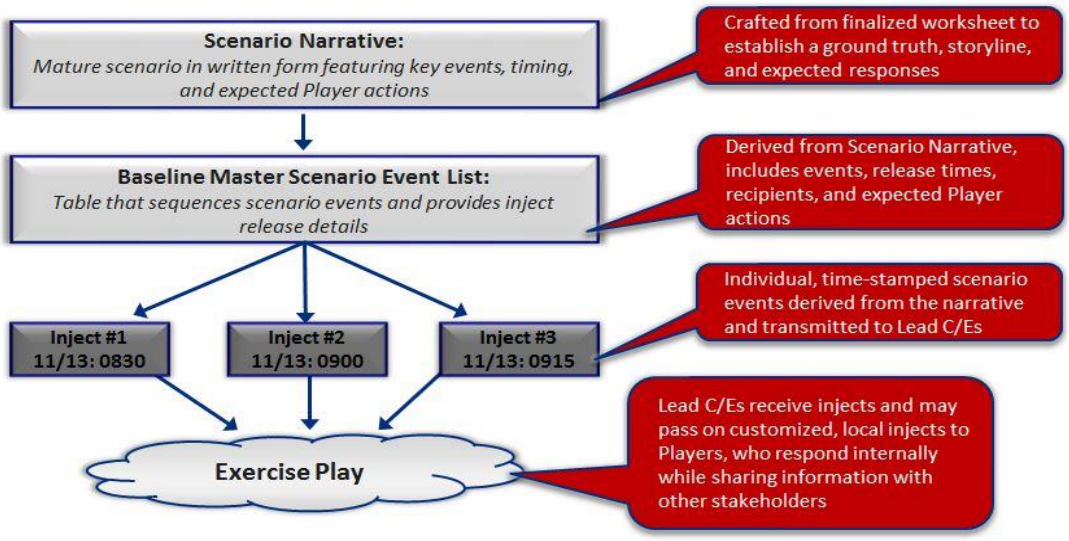


Figure 3: Scenario Development Process

Scenario Customization

Full Player organizations could tailor inject content from the baseline set developed by the core team for their respective Players (see Figure 4). Tailored injects enabled entities to exercise specific requirements and provide Players with exercise content that was consistent with their local environment for a more realistic experience. While also free to adapt the scenario to their needs, Lead Planners were advised to maintain consistency with the baseline scenario to ensure coordination across the full range of Players.

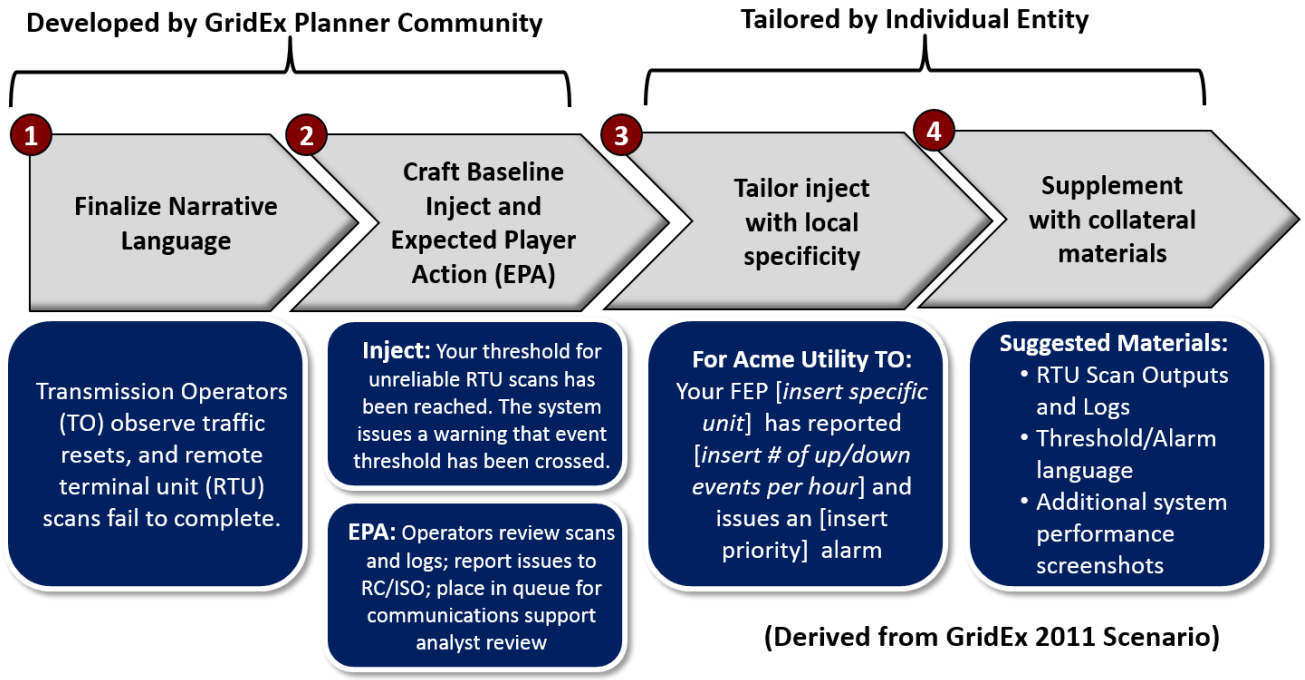


Figure 4: Example of Tailored Inject Process

Individual entities undertook scenario customization in parallel with baseline scenario and MSEL development. Once Lead Planners received the final scenario and MSEL, they were encouraged to ensure it aligned with baseline content. Tailored injects developed by Lead Planners were mapped back to the baseline MSEL so that during exercise play, all participants were tracking with the same scenario events.

Executive Tabletop Scenario

The Tabletop scenario built upon the scenario and conduct of the Distributed Play exercise. Participants were briefed on the impact of the cyber and physical attacks and recovery efforts during the Distributed Play portion. The scenario was then escalated to involve even more severe cyber and physical attacks of national and international significance. This severe attack scenario involved a second wave of multiple expanded cyber attacks that disrupted monitoring and control systems. Near-simultaneous physical attacks in the form of powerful improvised explosive devices and ballistic weapons were also targeted against key electricity facilities and infrastructures. Tabletop participants discussed their organizations' expected responses, including communication and coordination with other organizations.

Chapter 4 – Exercise Conduct

GridEx II was conducted over a day and a half, on November 13 and 14, 2013. The GridEx II Distributed Play ExCon and the Executive Tabletop session were both located at a facility in Herndon, VA. ExCon contained broad representation from the electricity industry and included NERC staff, GEWG members, industry professionals, control system experts, and regional representatives. ExCon managed and transmitted injects from a dedicated email account, monitored exercise play, liaised with C/Es, and tailored injects dynamically based on exercise outcomes. ExCon also simulated nonrepresented entities when needed, serving as telecom operators, control system vendors, and independent system operators. ExCon supported a help desk phone line and email account and responded immediately to Player and C/E questions or concerns. ExCon also hosted three C/E calls that gave Planners more visibility into distributed interactions and clarified any outstanding issues.

During this phase, Lead Planners became Lead C/Es, and Planners became C/Es for GridEx II Distributed Play. Lead C/Es served as the main points of contact between ExCon and the individual participating organizations they represented. The most important role for Lead C/Es was to send out either baseline or tailored injects to their appropriate Players. They were also Players' first point of contact for any exercise questions. Lead C/Es represented their organizations on exercise-wide teleconferences during and after the exercise.

The GridEx II scenario was divided into three moves. Moves 1 and 2 were conducted on November 13, and Move 3 was November 14. The exercise featured mock news videos and a cyber training video. The videos provided context and set the stage for GridEx II participants (see Figure 5). The first mock news video was shown at the start of Move 1, and the second, along with the cybersecurity training video, was shown at the end of Move 2. As detailed in the Scenario Narrative, each exercise move presented a series of scenario events; Players were asked to respond to these injects. During exercise play, ExCon monitored interactions and ensured Players were fully engaged in the activity.

Figure 5: GridEx II Mock News Video

GridEx II's ExCon room was divided into two discrete areas: one for ExCon participants and one for observers. The participant section had four pods set up with three phones on each table. Each pod had a specific role with ExCon members assigned to certain duties: simulating entities, fielding help desk requests, gathering context for the Executive Tabletop, and monitoring Electric Emergency Incident and Disturbance (OE-417) reports and Reliability Coordinator Information System (RCIS) traffic. The final pod served as a command and control center with NERC leadership and contract support staff to oversee both the overall exercise and ExCon functions. The observer section featured tables lined up classroom style, facing ExCon activities, which allowed observers to monitor the exercise proceedings.

As key scenario events unfolded, different visual tools were displayed on large screens to provide situational awareness. One dedicated monitor displayed the inject timeline and status of inject release. A Pacific Northwest National Laboratory (PNNL) tool displayed exercise communications between participating organizations during the exercise. The tool captured all external (sent outside an organization) email exchanges across the broad Player set and provided a visual output of exercise communication (see Figure 6). The tool displayed the dense volume of scenario inputs from ExCon (center of image) and responses from the Player set. The tool assisted ExCon in observing communications trends in near real time and also supported after-action analysis.

Figure 6: PNNL Visual Output of Move 1 Communications

Figure 7 illustrates GridEx II's key scenario events over the day and a half of the Distributed Play session (the light blue left section of the figure). When live exercise play concluded, ExCon hosted a hotwash teleconference for the C/Es and

Monitor/Respond Planners. This meeting provided an opportunity for participants to report initial insights and give feedback on the exercise. The hotwash officially concluded the GridEx II exercise.

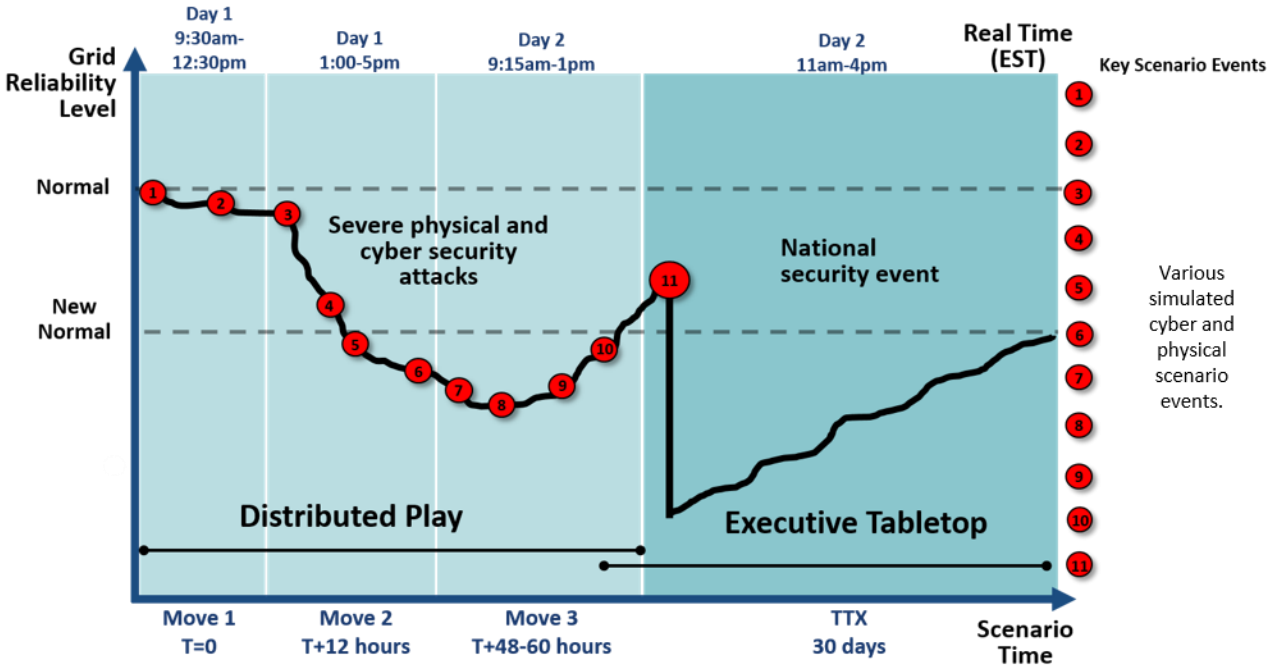


Figure 7: GridEx II Scenario Escalation Timeline

Executive Tabletop

On November 14, 2013, the Tabletop began with a briefing to the electricity industry and government participants on the attacks and response during the Distributed Play scenario. The scenario was then dramatically escalated to the Severe Event caused by key scenario event #11 in Figure 7. The simulated cyber and physical attacks quickly rose to national and international significance with a magnitude clearly exceeding the electricity industry's normal capability to respond and mitigate. Tabletop participants accepted the Severe Event as within the realm of possibility. In doing so, lessons learned could then be addressed, and the electricity industry would be better positioned to respond to less extreme events. Participants discussed their organizations' responses and concerns, including communication and coordination with other organizations. Other than a short break, the Tabletop ran continuously for over five hours and was structured through three time periods, each of about 75 minutes, as outlined in Table 1. Participants discussed the many unique challenges associated with responding to a Severe Event and how these challenges might be addressed.

Table 1: Agenda Outline

Severe Event Scenario	Sample Discussion Topics
One Hour After: Initial Situation and Response	• What those affected knew and did not know • Capabilities to respond • Extraordinary challenges related to decisions that needed to be made by the electricity industry • Policy-level issues that needed to be addressed by government • Coordination between the electricity industry and government • Partial return of electricity supply • Extraordinary resource requirements and prioritization of scarce resources
Two Days After: Increasing Response	
One Month After: Longer-Term Challenges	

Chapter 5 – GridEx II Lessons Learned

Distributed Play Lessons Learned

NERC developed the GridEx II findings through a comprehensive review and analysis of exercise outcomes, including real-time exercise control observations, exercise communications, hotwash feedback, after-action survey results, and an after-action teleconference with Lead Planners. Lead Planners completed the after-action survey to provide the most extensive review of both exercise planning and conduct. Aggregated exercise trends and specific examples support the key lessons learned. No entity names or defining characteristics are included.

Lesson Learned #1: Continue to Increase Information Sharing

Horizontal information sharing among entities remained strong; vertical communications have increased in both volume and quality since GridEx 2011.

Lesson Learned #1 Recommendations Summary

- Exercising formal communication paths strengthens crisis response information sharing.
- Sharing information early using multiple pathways (e.g., OE-417s, RCIS, ES-ISAC Portal, etc.) allows analysis centers to conduct more rapid analysis and provide mitigation response.

Supporting Observations and Recommendations

a) Bulk power system entities readily communicated throughout the exercise at a level well beyond that of GridEx 2011. Utilities shared information laterally with other entities to gain situational awareness on current conditions, specifics on attacks, and potential mitigations. This information sharing enabled asset owners and operators to gain a more comprehensive picture of unfolding events and confirm sector-wide trends such as the spearphishing attempts, compromises of control networks, and physical attacks. Industry communicated according to internal policies and protocols, but information sharing was also highly relationship-driven. While relationship-based exchanges are useful, more formal communications paths and points of contact should be incorporated in organizational procedures. In addition to point-to-point communication, the exercise reinforced the RCIS as a major source of industry operational communication, with 43 posts observed on the simulated RCIS message board from the 14 participating RCs. Overall, entities reported that exercise interactions succeeded in strengthening existing crisis response communications channels and forging reporting paths previously underutilized in security exercises.

b) Several communications "centers" participated during the exercise, illustrating more robust vertical reporting and information sharing. ES-ISAC was a key industry resource, receiving reports from 64 percent of the Full Player entities. The FBI was active at both the division and headquarters levels with 20 field offices engaging industry stakeholders during GridEx II. The DOE also observed an increase in reporting, with 67 OE-417 reports submitted during exercise play. This was a substantial increase from the fewer than 10 OE-417s submitted during GridEx 2011 and could be attributed in part to clearer pre-exercise documentation, increased participation, and a more severe scenario that clearly met the reporting threshold, but is also consistent with stronger vertical reporting observed during exercise play.

c) NERC and the ES-ISAC coordinated with key government stakeholders including the DOE, FBI, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and the National Infrastructure Coordinating Center (NICC). This coordination included frequent communication with the DOE Energy Response Center, coordinated release of advisories with ICS-CERT, and physical attack information sharing with NICC Watch Operations. Although some duplication and redundancy arose during exercise play, the consistent sharing pattern enhanced awareness between industry and government. During the exercise, participants developed and issued 13 Watch List entries and three NERC Alerts: one Advisory Alert (Level 1) and two Recommendation Alerts (Level 2).

Lesson Learned #2: Continue to Improve NERC Coordination

NERC has improved its coordination functions by clarifying ES-ISAC and BPSA roles and capabilities. While significant progress has been made since GridEx 2011, NERC should continue to calibrate its operational response and coordination functions, specifically in regard to providing time-sensitive wide-area information to the industry, and should inform industry and government of this capability.

Lesson Learned #2 Recommendations Summary

- Expand ES-ISAC conference call capabilities to ensure appropriate personnel can be accommodated in crisis situations.
- Clarify ES-ISAC subject matter experts' (Hydra team) functions and membership, and communicate roles across industry, especially to cybersecurity and operations personnel.
- Continue refinement and promotion of ES-ISAC portal use as a central coordination point and reporting tool in crisis.

Supporting Observations and Recommendations

a) The ES-ISAC observed a far higher percentage of reporting entities—64 percent—compared to 10 percent during GridEx 2011. This is likely due to increased awareness across industry since 2011 regarding the ES-ISAC's role within both the scenario development and the training that exercise participants received prior to the exercise. Another consequential difference, addressing an observation from GridEx 2011, was the Board-approved policy to "firewall" the ES-ISAC from the NERC Compliance Monitoring and Enforcement Program to promote the free flow of information to the ES-ISAC.[10]

b) The ES-ISAC, in partnership with NERC BPSA, hosted four industry-wide coordination calls that were widely attended by cybersecurity, physical security, operations, and management personnel from industry entities. The calls provided real-time impact assessments, reliability status, and potential mitigation measures. Participants found the ES-ISAC and NERC BPSA roles more coordinated and less redundant than in GridEx 2011; this time, participants noticed the ES-ISAC's and BPSA's discrete functions, as well as the value each brought to respective entities. Unlike GridEx 2011, the ES-ISAC was able to conduct unscheduled coordination calls based on conditions and need, rather than more scripted teleconferences. Coordination calls were effective overall; however, participants encountered technical issues and capacity constraints related to the conference call infrastructure that limited participation.

c) The ES-ISAC stood up two Hydra teams composed of core groups of impacted entities. Some entities noted that Hydra should be more inclusive and broader in its membership, but this may have been an artifact of the exercise, as the composition of Hydra teams has been reported as robust during recent real cybersecurity incidents. Others lacked an awareness of Hydra's role and function during a crisis event. Much of the BPS operating community is not aware of the Hydra teams' capabilities, what information and guidance can reasonably be expected, how quickly this information can be made available, and how it will be communicated to industry.

d) NERC activated its internal Crisis Action Team (CAT) as conditions worsened and threatened BPS reliability. The group convened five times to brief NERC leadership on the status of the affected systems and operating entities and to coordinate information flow from the ES-ISAC and NERC BPSA. While the CAT did not exist in 2011, in GridEx II the group successfully engaged NERC senior leadership in high-level updates and saw opportunities to improve the level of detail received.

e) NERC's ES-ISAC also made improvements to its incident response tools and mechanisms since GridEx 2011. The ES-ISAC portal was not yet in place during GridEx 2011, but it was functional in GridEx II; ES-ISAC staff posted 13 Watch List entries during the exercise. Entities reported that the portal was an efficient tool for reporting information that should be imbedded in internal response plans. In addition, BPSA's impact assessment outputs have improved in both fidelity and usefulness. They effectively generated a common operating picture to entities across the BPS, although the timely dissemination of these assessments presents an opportunity for improvement. Despite these advances, many utilities were still unclear on proper reporting thresholds and formats or how to enroll in the ES-ISAC portal and configure the system to receive Watch List entries according to individual needs. Those who did not use the ES-ISAC portal reported a lack of standardized reporting protocols and minimal visibility into how these reports were aggregated to relay situational awareness back to stakeholders. Some participants expressed the need for greater understanding of how mandatory reporting and voluntary information sharing are captured and used by NERC during an incident. This observation also aligns with the 2013 CIPC Electricity Sector Information Sharing Task Force recommendation[11] to position NERC as the central hub for information sharing and to reduce complexity and redundancy of the reporting process.

[10] http://www.nerc.com/files/Updated%20ES-ISAC%20Firewall%20Approval%20(13%20Mar%202013).pdf

[11] http://www.nerc.com/comm/CIPC/Electricity%20Sector%20Information%20Sharing%20Task%20For1/Electricity%20Sector%20Information%20Sharing%20Task%20Force%20Report.pdf

Lesson Learned #3: Challenge of Simultaneous Attack

Widespread, simultaneous, coordinated cyber and physical attacks on BPS infrastructure have the potential to pose significant electricity reliability, prioritization, resource allocation, and interdependency challenges. Entities should review cyber and physical security plans to ensure preparedness for simultaneous events.

Lesson Learned #3 Recommendations Summary

- Clarify reporting roles and functions within entities should a coordinated cyber or physical event occur.
- Estimate surge resource requirements prior to a crisis and consider potential source of support in a resource-constrained environment.
- Continue use of risk-based vulnerability assessments to potentially increase protection of physical and cyber assets.
- Evaluate and increase as needed participation in the STEP and Spare Equipment Database.

Supporting Observations and Recommendations

a) Entities were able to manage degraded conditions stemming from both the cyber and physical attacks, but significant constraints and coordination challenges emerged. Many entities took broad perspectives of both IT and physical degradation and acknowledged potential resource shortages during the height of the attacks. Planners observed communication among operations, cybersecurity, and physical security personnel through joint briefings and coordinated status updates. Although the cyber and physical interactions were valuable for coordinated response, formalized communication between the two groups with appropriate operations groups during crisis situations would enhance enterprise-wide coordination. Reporting roles and responsibilities could also be better clarified to address confusion on submission thresholds and sources within individual entities. This clarification would strike the appropriate balance between ensuring that all relevant parties receive information they need to respond to the situation without overwhelming organizations with a mass of unanalyzed and potentially less relevant data.

b) A severe attack on both cyber and physical assets can have significant second- and third-order impacts across the enterprise that inhibit response capabilities and exacerbate the crisis. For example, some entities reported that the cyber attack conditions degraded physical security surveillance assets, a factor to consider when facing physical attack vectors. Utilities should consider the dependencies of physical security monitoring processes on cyber systems that might not be available during a cyber attack.

c) The coordinated attacks allowed entities an opportunity to consider the demand for resources and the potential shortage of external surge capabilities. Entities acknowledged that independent contracted security personnel may not be available if they are receiving similar urgent requests from neighboring utilities. Demand for IT support should also be considered in a large-scale event. Entities can use the scenario as an opportunity to estimate potential requirements and consider available surge resources prior to a major incident. During GridEx II, some utilities considered solutions to address resource scarcity, such as cross-training staff members on multiple response functions.

d) The scenario allowed the consideration of employee safety and security concerns during the widespread simulated physical attacks. The GridEx scenario provided an opportunity to further clarify policies and guidance for potential life safety issues.

e) The planning and conduct of GridEx II provided an opportunity for entities to evaluate and identify their physical infrastructure security statuses and postures. Entities may further reduce the vulnerability of their high-value, limited-quantity assets through vulnerability assessments conducted by qualified physical security experts.

f) Given the broad and destructive nature of the attacks, spare equipment programs, such as NERC's Spare Equipment Database (SED), the Edison Electric Institute's Spare Transformer Equipment Program (STEP), and the DHS Recovery Transformer (RecX) program, offer potential resources for replacement of high-voltage transformers. Because quick, cost-effective replacement of transformers and other expensive BPS equipment continues to be a challenge, asset owners who are not already participating in these programs should be encouraged to evaluate and participate in STEP and SED.

Lesson Learned #4: Continue Improvement of Incident Response

Industry continues to refine and enhance its all-hazard incident response plans and protocols. The broad set of scenario conditions stress-tested these plans, sensitized participants to potential threats, and helped to identify areas for further strengthening.

Lesson Learned #4 Recommendations Summary

- Assess business and operational implications of isolating IT assets during a cyber event to ensure critical functions are maintained during a crisis.
- Develop mechanisms to preserve evidence and collect forensic data following a physical or cyber attack.
- Align incident response escalation plans among relevant business units to promote a consistent response posture across the enterprise.
- Review communication infrastructure and identify redundancies or alternatives to ensure viable communications channels in crises.

Supporting Observations and Recommendations

a) IT professionals and operators followed incident response plans and protocols to contain and mitigate impacts to both the corporate and operational network. Measures included reinforcing firewalls, isolating corporate networks, coordinating with vendors who provide support by remote access, and moving toward manual operations. While many entities did consider the operational impact of isolating network infrastructure, some reported that a more formalized review of enterprise system dependencies could bring to light networking issues that need to be addressed. Some utilities struggled with balancing the need to contain the spread of malware with the need to maintain operability of core business functions. Other utilities noted that preserving evidence and collecting forensic data would be difficult when the affected systems are needed to support reliable bulk power system operation. A thorough review, followed by prioritization of critical systems across the enterprise, would help decision makers choose the best steps in a crisis. In addition, some entities indicated that while their plans are well suited for disruptive weather events, they should be enhanced to recognize major cyber events that are not predictable and not as well understood.

b) GridEx II's diverse set of baseline scenario attack vectors heightened the awareness of potential threats facing the industry. Entities built on their knowledge of cyber attacks and experienced the nature and implications of spearphishing attacks, distributed DDoS conditions, control network penetration, and physical security risks. The realistic nature of GridEx II exercise play reinforced the importance and urgency of safeguarding the bulk power system from both cyber and physical threats.

c) Entities' abilities to customize the scenario enabled a broad set of participation from functional areas within participating entities. Utilities reported that Players from business continuity/emergency management, call centers, control systems, corporate communications, IT security, energy trading, generation operations, law enforcement, physical security, senior management, and transmission operations engaged in exercise play. The diversity of functional areas enabled entities to identify interdependencies, redundancies, and gaps in incident response. Entities identified the need to eliminate duplicative reporting requirements among functional areas and address misalignment in shared escalation procedures.

d) Entities reported that participation in GridEx II enabled them to vigorously exercise both internal and external reporting requirements. Asset owners reported conditions to RCs, ISOs, Regional Entities, the ES-ISAC, and government agencies. While acknowledging the importance of information sharing, some participants noted that the reporting effort can absorb key resources. Entities should streamline reporting by ensuring the appropriate reporting thresholds and requirements are clearly documented and integrated into incident response plans.

e) When responding to crisis events of this magnitude, entities identified vulnerable communications channels without redundancies. Although email and phones were available for exercise purposes, participants acknowledged that these communications channels could also have been degraded or not functional, given the severe scenario conditions, and some participants exercised this scenario by switching to alternate communications facilities (e.g., system operators used voice communications not dependent on voice over Internet protocol). Utilities should consider alternative, out-of-band communications capabilities in significantly disruptive events to ensure the organization can communicate internally and exchange information with external parties.

f) While planners observed more internal response coordination between IT and operational functions, some "stovepiping" of response activities was still evident. IT, operational, and other utility lines of business should identify triggers to share information regularly in a cyber event that could impact both functions.

Lesson Learned #5: Continue Improvement of Situational Awareness Content Development

Industry and government stakeholders such as the ES-ISAC, DOE, ICS-CERT, and FBI play a key role in promoting situational awareness across the sector and disseminating products to better inform incident response teams. More coordination on the release of this content could consolidate the effort.

Lesson Learned #5 Recommendations Summary

- Continue building relationships with relevant government stakeholders to establish communication expectations in advance of crises.
- Filter and consolidate industry and government communication and advisories so relevant information can be processed quickly by asset owners.

Supporting Observations and Recommendations

a) Entities reported that the FBI's robust participation at both the division and headquarters level was extremely valuable for forging and reinforcing relationships between industry and law enforcement. The regional involvement provided local context and enabled entities to exercise real reporting mechanisms and points of contact. The FBI was able to exercise real tools, such as its FBI Liaison Alert System (FLASH), to promote situational awareness of ongoing attacks. Division/headquarters involvement also helped to support the information aggregation process as attack patterns escalated and grew more widespread. Entities should establish or enhance communication relationships with local FBI field offices.

b) ICS-CERT distributed four alerts: 1) a "stagesetter" advisory to warn against future activities, 2) reports of corporate network intrusion, 3) reports of operational network attacks, and 4) advisories on the identified vulnerabilities. The advisories provided asset owners and operators an impact summary, timeline, analysis of events, and recommended mitigation measures. ICS-CERT coordinated closely with the ES-ISAC and the FBI to validate information and ensure a consistent message. Entities reported that ICS-CERT reinforced its role in a major incident and that they found the alert content important for responding to the attacks. While the information disseminated was valuable for restoring grid reliability, some entities reported duplicative guidance and products from, for example, ICS-CERT and ES-ISAC, which reflects the collaboration necessary in building these recommendations. Better consolidation and coordination when releasing similar information could reduce the amount of resources entities need to determine similarities themselves while maintaining parallel communications pathways for mitigation information.

c) The DOE received many more OE-417s during GridEx II than during 2011. OE-417s were one of the most readily used reporting mechanisms and were shared with other key partners for situational awareness. DOE's Energy Response Center coordinated response measures with FERC, the ES-ISAC, and DHS. One improvement to this process is to inform the operating community in real time of these coordinated efforts—if not actively involving them in the coordination—to allow entities to become aware of these additional sources of information.

Executive Tabletop Observations and Recommendations

Participants in this Tabletop discussion identified a number of recommendations for industry and the federal government.

These recommendations are intended to enhance the resilience of the electricity infrastructure during a Severe Event. While the postulated Severe Event is viewed as highly unlikely, the exercise was designed to stress the system. The recommendations below merit further investigation to continue enhancing the electricity industry's resilience for a wide variety of more probable, but less severe, events of national significance.

Information Sharing Between Industry and Government

- **Situation Assessment Scalability**: One of the most important aspects of responding to a crisis is the ability to quickly and accurately assess the situation, share that assessment with decision makers, and take action. The electricity industry's primary capability to perform situation assessments at the North American level is through the ES-ISAC and BPS functions. To do this, NERC depends on information provided by the industry's more than 1,900 publicly owned and investor-owned utilities, cooperatives, and independent system operators. For government, the DHS

National Cybersecurity and Communications Integration Center serves as a centralized location where operational elements involved in cybersecurity and communications are coordinated and integrated. The ES-ISAC provides personnel to the NCCIC as needed to share information related to emerging cybersecurity threats and vulnerabilities. While coordination with the NCCIC is a good initial step toward addressing a cybersecurity threat or attack, response, communication, and coordination processes need to be scalable to meet the extraordinary challenges of a Severe Event, as well as one that goes beyond cybersecurity or involves physical threats or attacks.

- **Public Communications**: Efforts to restore electricity would be supported—or hindered—by information provided to the public through print, radio, television, and social media. The public's need for frequent, timely, relevant, accurate, consistent, and credible information would be particularly acute through a Severe Event.

Operational Decision Making

- **Unity of Effort**: A unified approach is required to identify, discuss, and decide the many policy-level issues resulting from a Severe Event. This requires industry executives and senior government officials at local, state, federal, and potentially international levels to be directly involved.

- **Cyber Attacks Create Unique Restoration Challenges**: Unlike storms that can be predicted and tracked with some degree of accuracy and equipment failure that tends to be random and limited in impact, cyber attacks present unique challenges for how the electricity industry restores power.

- **Physical Attacks Create Unique Restoration Challenges**: While the electricity industry has experienced occasional acts of sabotage or vandalism, a well-coordinated physical attack also presents particular challenges for how the electricity industry restores power.

- **Mutual Aid and Critical Spares:** The extreme challenges posed by the Severe Event scenario provided an opportunity for participants to discuss how the electricity industry's mutual aid arrangements and inventories of critical spare equipment may need to be enhanced.

Legal and Regulatory Authorities

- **Regulatory Relief**: The electricity industry is highly regulated by mandatory standards and state and federal government regulations administered by various government agencies. Some of these regulations would constrain the operation of certain generators, and specific relief provisions should be considered prior to a Severe Event.

- **Legislation to Deal with Emergencies:** Existing statutes might be useful to help recovery efforts in a severe event (Defense Production Act, Stafford Act, etc.) but may not have been used in that capacity. A review of these statutes to determine if there is a need to initiate emergency legislation to facilitate recovery during a Severe Event would be helpful.

Chapter 6 – Conclusion

In the Distributed Play after-action survey, 100 percent of entities indicated that GridEx II met their organizations' expectations "well" or "very well." NERC's GridEx II Distributed Play session successfully provided the electricity industry with a learning opportunity to strengthen both internal and sector-wide crisis response plans. It exercised the readiness of industry and government to respond to coordinated cyber and physical attacks and identified potential improvements in industry programs, plans, and responder skills. The exercise also served as an opportunity to enhance information-sharing capabilities. Participants considered the exercise a successful training event that delivered substantial return on time and resource investments. The event reinforced the value of sector-wide exercises and the need to plan future training events.

The core team, along with Planners and Players, worked closely to strengthen relationships, evaluate cyber and physical incident response plans, and identify opportunities for improvement. NERC will continue to work closely with industry entities, government stakeholders, CIPC, and other relevant bodies to address the recommendations from GridEx II and continue to mature the program while planning and executing GridEx III.

At the conclusion of the Tabletop, participants thanked NERC for taking the initiative to propose the exercise and committing the necessary executive leadership and technical resources. All agreed that the collaborative relationship between the federal government and the electricity industry to address matters related to critical infrastructure has improved greatly and continues to mature.

While the Tabletop was extremely valuable, there is now an opportunity to leverage this "proof of concept" by drilling down to the necessary levels of detail to act on the ideas discussed. The time and effort invested by electricity industry executives and senior officials of the federal government who participated in the Tabletop will then materially enhance the reliability and resilience of the electricity industry in the face of a Severe Event. The ESCC and the EGCC should review the recommendations in this report and decide how best to act on each of the recommendations.