NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2011 NERC Grid Security Exercise

After Action Report

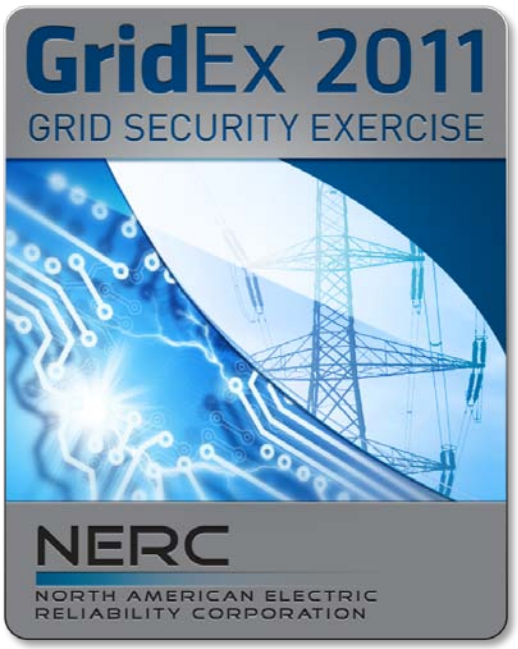
March 2012

RELIABILITY | ACCOUNTABILITY




1325 G Street, NW
Suite 600
Washington, DC 20005
202-400-3000 | www.nerc.com

Table of Contents



Executive Summary

The North American Electric Reliability Corporation (NERC) conducted the first sector-wide grid security exercise, GridEx 2011, on November 16-17, 2011. The exercise was designed to validate the readiness of the Electricity Sub-sector to respond to a cyber incident, strengthen utilities' crisis response functions, and provide input for internal security program improvements. In advance of exercise execution, a diverse group of industry stakeholders engaged in an eight month planning process to design the exercise construct, craft a relevant scenario, and recruit a representative player set. GridEx 2011 featured a hybrid discussion and operational-based exercise format that combined a geographically distributed environment for operators and a tabletop exercise for executive leadership. A scenario was crafted to fully engage the diverse stakeholder set, promote coordination during the exercise, and highlight urgent cybersecurity issues facing the sector. The scenario featured advanced persistent threat attributes that propagated across the bulk power system (BPS) and eroded trust in critical grid functions.

Seventy-five industry and government organizations from the U.S. and Canada participated in GridEx 2011. BPS entities included generation and transmission owners, reliability coordinators, independent system operators, and balancing authorities. Key government agencies such as the Department of Homeland Security, Federal Bureau of Investigation, and Department of Energy were also heavily involved. During the one-and-a-half days of live exercise play, participants received sequenced e-mail messages that detailed scenario conditions. Based on this information, players engaged in both internal response measures and external coordination activities across the sector. An Exercise Control cell managed scenario distribution, monitored exercise play, and captured response activities.

Following the exercise, an after action team reviewed player questionnaire submissions, interviews, and exercise communications. The Electricity Sub-sector achieved GridEx objectives and identified key areas for further exploration. NERC and its stakeholders will take steps to address these areas in order to enhance the ability to respond to a coordinated cyber attack on the BPS. Overall, the exercise was widely regarded across industry and government as a critical imperative in preparing the bulk power system (BPS) for a disruptive cyber event.

The GridEx 2011 findings, below, identify key themes and recommendations:

- Entities possess effective cyber incident response plans, but updates to protocols and guidelines and additional training could enhance preparedness. NERC will develop and raise cybersecurity awareness by conducting focused training opportunities for industry and policy makers to promote and emphasize incident response and recovery.
- Significant horizontal communication occurs across industry, but vertical information sharing to NERC and government agencies is limited due to concerns about compliance implications. While entities relied on the ES-IAC as the hub for information sharing and reporting, improved reporting guidance, as it relates to NERC Situation Awareness (SA) and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), could promote more information sharing. NERC will coordinate with the Critical Infrastructure

Protection Committee (CIPC), Information Sharing Task Force, to develop guidance and outreach strategies that will further enable NERC to create a secure and trusted environment necessary for information sharing.

- NERC's ES-ISAC and SA teams effectively serve a central coordination function, but further expediting the FERC review of the NERC Alert process, refining call mechanics, and activating the ES-ISAC portal could further enhance the organization's response role.
- Utilities took appropriate steps to secure the grid. Because physical intrusions into BPS infrastructure can have grave cyber implications, entities should ensure their response protocols address a coordinated threat. In partnership with industry and North American security organizations, NERC will facilitate and support the development of updated physical security guidance.
- While the NERC Emergency Standards process would expedite urgent standards development, it should be coordinated to avoid interference with core incident response activities at the entity level. NERC and industry will explore enhancements to the Emergency Standards Process that will support the overall goal of ensuring bulk power system reliability.

GridEx provided a realistic environment for organizations to assess their cyber response capabilities. NERC is applying the GridEx recommendations to further strengthen the bulk power systems preparedness and response mechanisms. To capture all relevant information in the final report, NERC is working in close partnership with public sector stakeholders, bulk power system owners and operators, and the NERC CIPC. The observations and recommendations presented in this report will undergo further analysis to help clarify these observations, assess their root causes, and develop policy enhancements and improvements. In addition to the GridEx final report, many participant organizations developed their own internal summary and observation reports.

GridEx offered Electricity Sub-sector organizations a way to test their plans and skills in a real-time, realistic environment and to gain the in-depth knowledge that only experience can provide. Participants exercised response and recovery functions that are critical to responding to a security event. The lessons learned from the exercise will provide valuable insights to guide future planning for cyber emergencies. Through the exercise interaction, participants forged and strengthened relationships across the cybersecurity community. Ultimately, GridEx served as a critical tool that allowed the Electricity Sub-sector to examine closely the growth and evolution of security capabilities.

The Electricity Sub-sector achieved GridEx objectives and identified these key areas for further exploration. NERC and its stakeholders will take steps to address the findings to enhance the ability to respond to a coordinated cyber attack on the BPS.

Introduction

On November 16-17, 2011, NERC conducted the first sector-specific, large-scale grid security exercise, GridEx 2011. The event culminated after eight months of intensive planning and recruiting efforts. The exercise was viewed across industry and government as a training success in preparing the bulk power system (BPS) for a disruptive security event.

This After Action Report provides an overview of GridEx 2011, with a focus on exercise findings and insights. The report also details key aspects of planning, execution, and the after action process. NERC will leverage lessons learned from the exercise to enhance its own response capabilities and promote cybersecurity preparedness across the BPS.

NERC initiated GridEx 2011 to validate the electricity industry's current readiness to respond to a cyber incident. The event assessed NERC's and industry's crisis response plans in an effort to strengthen security processes and capabilities. The engagement also identified areas for improvement in cybersecurity programs and incident handling capabilities for NERC and its member entities.

Modeled after the Department of Homeland Security's (DHS) Cyber Storm series, the exercise featured a distributed exercise design that enabled participants to respond to scenario events from their normal work stations. Participants consisted of representatives from NERC, Regional Entities, registered entities, and select industry and government bodies. In parallel, GridEx engaged NERC's executive decision makers, as well as senior-level government and industry stakeholders through a discussion based tabletop exercise (TTX) format. This engagement enabled leadership to assess, test, and validate existing command, control, and communication plans.

Participation

The GridEx planning team recruited player organizations through a variety of means, including a sector-wide outreach program, leveraging previous exercise relationships, and interacting with government and sector coordinating bodies. The planning team identified a core group of exercise planners to attend planning conferences, shape the objectives, support scenario design, and contribute to the after action process. In addition, from this core group of exercise planners, the planning team established two levels of organizational commitment: Full Player and Monitor/Respond (M/R). Full Player organizations fully engaged in exercise play and external coordination, while M/R entities followed the scenario progression and considered scenario implications internally. These two forms of exercise play enabled organizations to determine their level of involvement based on resources, timing, and other factors. Seventy-five organizations from the U.S. and Canada participated in GridEx 2011, including 48 utilities, 21 government and academic organizations, and six Regional Entities. Figure 1 reflects the broad representation of GridEx participants.

Figure 1: GridEx Participant List

GridEx Participants

Utilities

- Alliant Energy
- Ameren Corporation
- Arkansas Electric Cooperative
- Bonneville Power Administration
- Brookfield Renewable Power
- Burlington Electric Department
- Cal ISO
- Dayton Power and Light Company
- Duke Energy
- Duquesne Light Co.
- EDP Renewables North America, LLC
- Entergy
- ERCOT
- Georgia Transmission Corporation
- Great Lakes Power Transmission
- Hydro One
- Iberdrola Renewables
- Independent Electricity System Operator
- ITC Holdings
- Lakeland Electric
- Long Island Power Authority
- Massachusetts Municipal Wholesale Electric Company
- Midwest ISO
- National Grid
- Nebraska Public Power District
- New York Power Authority
- Northeast Utilities
- Northern Indiana Public Service Corporation
- NY ISO
- Oklahoma Gas & Electric
- Ontario Power Generation
- Orlando Utilities Commission
- Pacific Gas & Electric
- PEPCO Holdings, Inc.
- PJM
- Progress Energy
- Public Service Electric & Gas Company
- Sempra Energy Utilities
- Southern Company
- Southern California Edison
- South Mississippi Electric
- SPP - RTO
- TECO Energy
- Tennessee Valley Authority
- Western Area Power Administration
- Wisconsin Public Service
- Xcel Energy

Regional Entities

- MRO
- NPCC
- RFC
- SERC
- TRE
- WECC

Government/Academia/Other

- ABB
- Canadian Electricity Association
- Canadian Incident Response Centre
- Critical Infrastructure Criminal Intelligence/Royal Canadian Mounted Police
- DHS/National Cyber and Communications Integration Center
- DoD/Cyber Crime Center DCISE/DIB-CERT
- DOE
- Edison Electric Institute
- EnergySec
- EnerNex
- FBI
- FERC
- ICS-CERT
- Lofty Perch
- National Guard, Critical Infrastructure Protection Program
- Natural Resources Canada
- North American Transmission Forum
- Pacific Northwest National Lab
- Public Safety Canada
- University of Illinois
- Utility Services

Exercise Objectives

The planning team developed the GridEx objectives to guide recruiting, scenario development, and after action activities. The GridEx objectives included community concerns and current initiatives; however, each organization had the opportunity 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, outlined below.

Objective 1: Validate the current readiness of the electricity industry to respond to a cyber incident and provide input for security program improvements

Players achieved this objective during the execution of GridEx as entities engaged in realistic internal evaluation and incident response activities that supported grid reliability. Organizations were able to assess a number of departments including Operations, Information Technology (IT), Communications, Physical, and Cybersecurity functions. During exercise play, participants successfully engaged their protocols to guide their actions. Participating organizations identified strengths, gaps, and areas for improvement in their incident response plans and procedures. While enhancements were identified to be instituted, the industry validated its preparedness for a disruptive cybersecurity event.

Objective 2: Exercise NERC and industry crisis response plans and identify gaps in plans, security programs, and skills

GridEx 2011 enabled NERC to fully exercise its crisis response plan and assess strengths and gaps within its protocols. During the exercise, NERC distributed a series of alerts that aided in informing the electricity community on the escalating cyber incident. Entities relied on the ES-ISAC as the hub for information sharing and reporting. Player feedback and communication with NERC during the exercise enabled successful testing of their procedures and crisis response plans. In addition, participating organizations and NERC were able to assess and evaluate their incident response programming during the planning phases of the GridEx engagement.

Objective 3: Assess, test, validate existing command, control, and communication plans for key NERC stakeholders

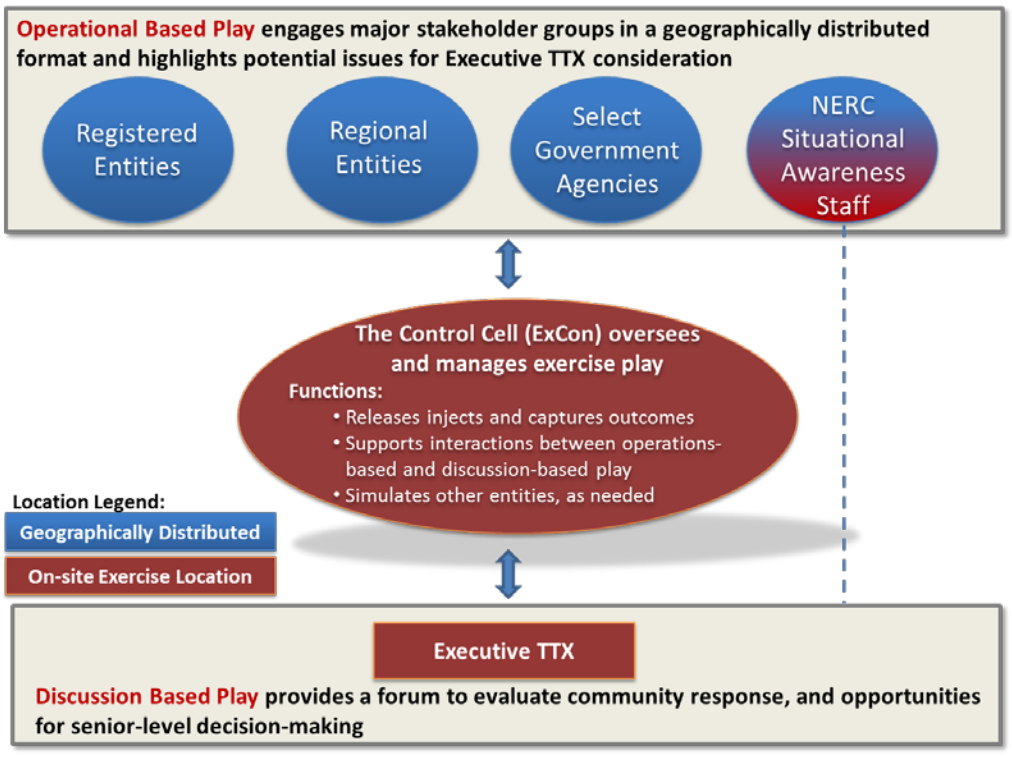
Prior to exercise execution, planners recognized the broad set of actors involved in responding to a cyber incident and the importance of proper stress testing of communications plans. The player set represented the electricity community as a whole, and enabled both internal and external communication to function successfully. Players used the player directory to identify key resources to contact. Scenario events allowed organizations to successfully test their command, control, and communications plans internally across functions and externally across the BPS. The exercise enabled players to consider alternative communications and operations approaches in a compromised environment. The planning process also promoted communication and relationship-building across the sector and across geographic borders.

Exercise Design and Scenario Construct

GridEx design embraced a combined approach with operational and discussion-based exercise tracks (see Figure 2). The operational construct featured a geographically distributed player set. The players received sequenced messages via e-mail that chronologically detailed scenario conditions. Based on this information, players engaged in both internal response protocols and coordination activities across the sub-sector, and to relevant industry and government bodies. The discussion-based Executive TTX, conducted concurrently with distributed play, focused on executive decision-making. Senior-level officials from the NERC Board of Trustees, electricity industry, and relevant government agencies participated in the Executive TTX to discuss urgent policy issues that could be escalated to an executive level. These issues included compliance concerns, widespread reliability issues, and external affairs.

During the planning phase, organizations were asked to commit to either Full Player or M/R status. Full players were expected to fully engage in exercise play. They also had the ability to tailor and adapt injects to suit their organizations' objectives and contribute to the after action process. M/R organizations received all injects, but were not required to fully engage in the exercise or report findings. M/R organizations were permitted to participate in all coordination calls, and provide limited after action feedback. An advantage for M/R organizations was participation in a sector-wide exercise without substantial resource requirements. Most players participated in GridEx from their work locations and engaged in exercise play via e-mail and other standard communications channels.

Figure 2: GridEx Construct



For each entity within the distributed player set, Controller/Evaluators (C/E) were designated to facilitate and record exercise play at the local or organizational level. C/Es ensured players were well-equipped to engage in the exercise, and liaised with Exercise Control (ExCon) throughout the event. In the distributed exercise construct, C/Es were asked to oversee interactions within their organizations and capture key observations that were not visible to the planning team within ExCon.

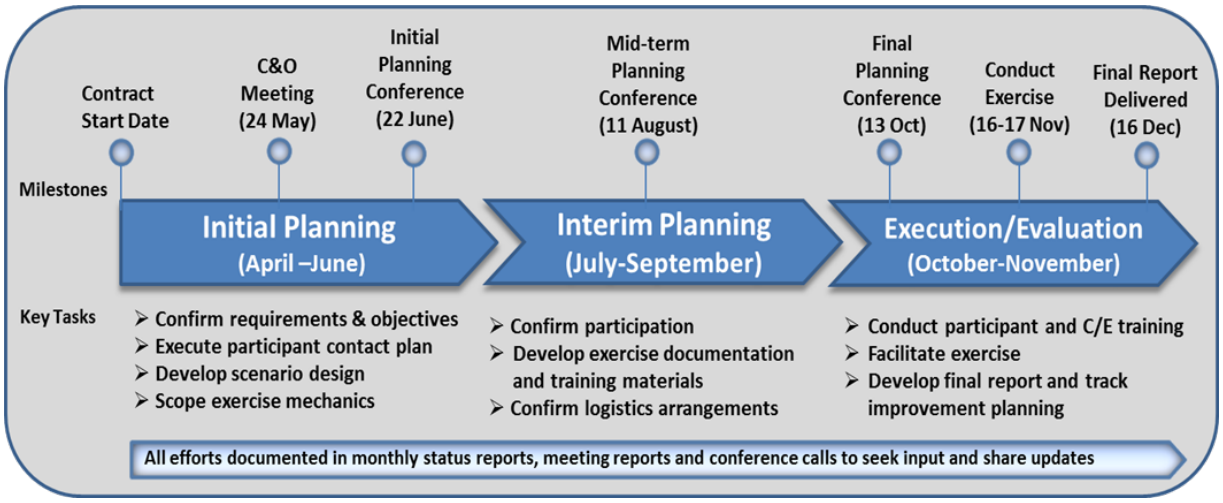
The GridEx scenario was crafted to achieve exercise objectives and fully engage the diverse GridEx stakeholder set. The scenario had broad relevance among players, promoted coordination during the exercise, and highlighted urgent issues facing the sector. While the technical feasibility of the scenario was vetted by experts across the industry, the planning team adjusted aspects of the exercise to ensure wide applicability and that players achieved exercise objectives. The scenario began notionally with physical intrusions into substations and back-up control center infrastructures. Initially believed to be copper theft, entities soon learned the intruder also committed cyber tampering. The bad actor introduced sophisticated malicious code (malware) capable of corrupting Supervisory Control and Data Acquisition (SCADA) system calculations and eroding inter-party trust relationships. The malware also tunneled to corporate networks, disrupting key business processes. The code leveraged communications Protocols as an intermediate attack vector to deliver malicious code across the North American BPS.

Within the first two days of exercise play, operators and IT professionals engaged in incident response protocols, while working to maintain system reliability and identify the root cause. As entities observed a common pattern of suspicious behavior across the BPS, they leveraged both formal and informal communications mechanisms to share information. The simulated Reliability Coordinator Information System (RCIS) and Electric Emergency Incident and Disturbance Reports (OE-417) widely communicated observed impacts and notified relevant government agencies. NERC and the ES-ISAC served a central coordinating function by establishing a common operating picture and providing practical guidance to industry. The U.S. Federal Bureau of Investigation (FBI) worked closely with impacted entities to investigate the reported break-ins and understand the full scope of illegal activity. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), in coordination with the ES-ISAC, distributed bulletins with malware indicators and initial defense measures for entities. For a more detailed explanation of the scenario, see Appendix A.

Exercise Planning and Execution

The GridEx planning process consisted of four planning meetings that aided in the development of the scenario, exercise design, and outreach for the exercise. In addition, the planning team participated in several interim conference calls and informal discussions to expand recruitment and refine scenario elements.

Figure 3: GridEx Planning Timeline



Concept Development Phase

NERC held the Concept and Objectives (C&O) Meeting on May 24, 2011. During the C&O Meeting, the planning team discussed and reviewed the GridEx objectives, and reviewed the project timeline and key events. The group also identified exercise roles and recruitment strategies. NERC created a Steering Committee to attend all meetings and planning conferences. The Steering Committee was influential in shaping the objectives and exercise scenario and assumed an expanded role in the after action input and review process. The planning team then confirmed two levels of player participation for GridEx: Full Player and M/R. These levels enabled varying resource commitments and levels of influence during planning. During the C&O Meeting, participants took preliminary actions to develop the GridEx scenario. The scenario would focus on a cyber attack on the Electricity Sub-sector, posing reliability concerns that would trigger crisis response planning and coordination. NERC strongly encouraged the group that the scenario should be credible and realistic and reflect the current response capabilities of the sub-sector. An advanced persistent threat attack was identified to properly achieve exercise objectives. Finally, the planning team agreed the scenario should incorporate both cyber and physical elements, to the greatest extent possible.

Initial Planning Phase

During the Initial Planning Conference (IPC) on June 22, 2011, the planning team developed key themes for the scenario, reviewed DHS' cyber programs, and identified stakeholder coordination and information sharing procedures.

Given the diverse player set, planners agreed that the scenario should have far-reaching impacts to exercise the plans and processes of all players. In addition, planners determined that the scenario should escalate quickly during exercise play to fully engage incident response plans and promote coordination across the sector. After planners confirmed the scenario themes, they developed a written narrative. The narrative featured key events, timing, and expected player actions. The narrative would ultimately be leveraged to create individual injects for exercise play. The IPC also featured a discussion on the National Cybersecurity and Communications Integration Center (NCCIC) and the National Cyber Incident Response Plan. During the discussion, representatives from DHS' National Cyber Security Division (NCSD) assisted in defining parallel government activities, and sensitized the group to potential federal cyber response activities.

Another key step in the planning process was shaping stakeholder outreach activities. As planning efforts accelerated, the Steering Committee advanced scenario development and outreach efforts. To aid in the planning process, planners activated a SharePoint site as a central repository for document sharing and editing within the trusted community. Contributors could read, upload, download, and edit documents based on assigned user privileges.

Mid-term Planning Phase

The Mid-term Planning Conference (MPC) was conducted on August 11, 2011. Outreach and recruitment activities generated sector-wide interest in GridEx. DHS representatives were invited to brief the group on NCSD and NCCIC policies and procedures in place for a potential cyber incident. In addition, an ES-ISAC representative briefed the group on the organization's role in responding to a cyber incident. The group focused on maturing the scenario narrative by discussing scenario timing, attack attributes, and operational impacts.

As the scenario grew more sophisticated and nuanced, planners were reminded to maintain operational security and to keep details within a trusted circle. Throughout the mid-term planning phase, organizations continued to establish their level of participation, along with designating Lead Planners and C/Es. The distinction between Full Player and M/R organizational roles was further clarified to ensure that entities of varying resources and availability could engage at some level. By the mid-term planning phase, both the GridEx objectives and overall execution construct were confirmed.

Final Planning Phase

The Final Planning Conference (FPC) was held on October 13, 2011. During the FPC, planners added granular detail to the scenario and initiated the Master Scenario Events List (MSEL).

Facilitators also provided a final recap on the GridEx exercise construct. In addition, planners further defined the role of C/Es. For Full Player organizations, C/Es were instructed to conduct internal orientation sessions to ensure player preparation for exercise play. C/Es identified internal players that represented the broad response roles that would be engaged during conditions portrayed in the GridEx scenario. For all GridEx participants, information sharing was considered a core exercise activity. To facilitate proper information sharing, the GridEx support staff created a player directory featuring every player and C/E participating in the exercise.

In the final weeks before the exercise, planners finalized logistical and technical scenario details. The planning team communicated the after action process and requirements for both C/Es and players. The planning team created and distributed a C/E Handbook to all C/Es and M/R players. The C/E Handbook was a central reference document containing GridEx background, objectives, schedules, exercise design, and communication protocols. The planning team hosted a C/E Orientation Call to walk through the handbook and answer any final questions regarding GridEx conduct.

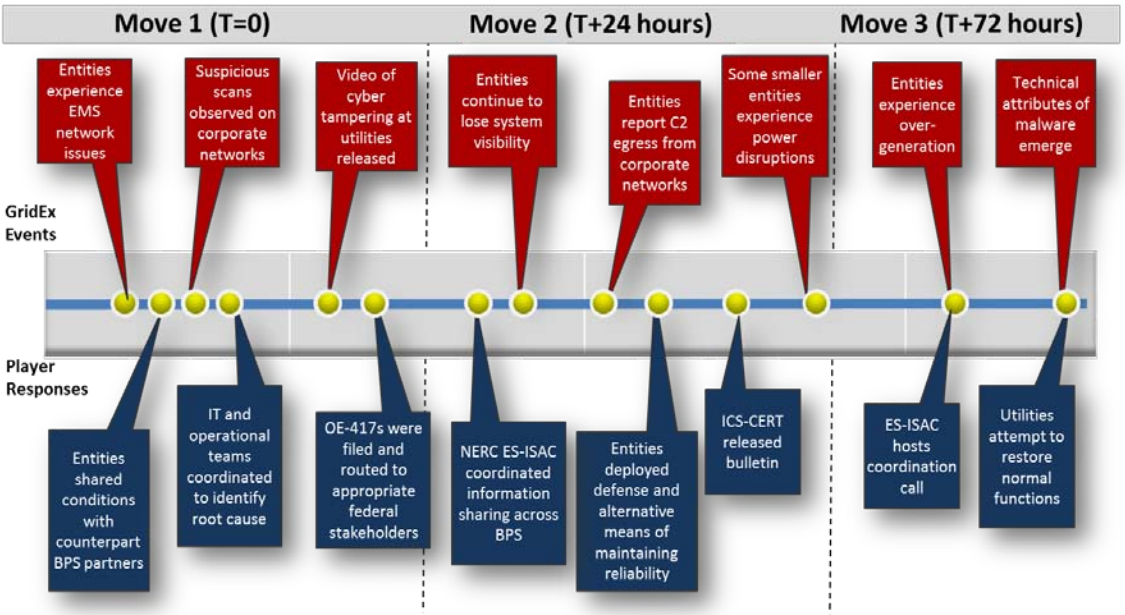
Exercise Execution Phase

GridEx was conducted over a day-and-a-half, on November 16-17, 2011. ExCon consisted of a broad representation of the Electricity Sub-sector, including NERC staff, industry professionals, control system experts, and regional representatives. They 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 non-represented entities when needed, serving as telecom operators, control system vendors, and independent system operators. ExCon supported a help desk phone line and email account, responding immediately to player and C/E questions or concerns. The ExCon also hosted three C/E calls that gave planners more visibility into distributed interactions and clarified any outstanding issues.

The GridEx scenario was divided into three moves. Moves One and Two occurred on November 16, 2011 and with Move Three occurring on November 17, 2011. Planners initiated both exercise days with mock news videos that established a context for exercise play and generated enthusiasm for the GridEx activity among players. As detailed in the Scenario Narrative (see Appendix A), each exercise move presented a series of scenario events to which players responded. During exercise play, ExCon monitored interactions and ensured players were fully engaged in the activity.

Figure 4 below illustrates GridEx scenario events and corresponding player actions as observed by ExCon. Following the conclusion of live exercise play, ExCon hosted a hotwash teleconference for the C/Es and M/R players. This hotwash provided an opportunity for participants to report initial insights and give feedback on the exercise and officially concluded the GridEx engagement. NERC's contractor, Booz Allen Hamilton, delivered the After Action Report to NERC on December 16, 2011.

Figure 4: Scenario Activities by Move



GridEx Findings

The GridEx 2011 findings were developed through the review and analysis of exercise data, stakeholder interviews, and hotwash feedback. C/E calls and the final exercise hotwash provided initial field observations for organizing after action findings. The GridEx planning team reviewed After Action Questionnaires from each of the participating organizations to identify common themes and insights. The planning team also conducted individualized interviews with key stakeholders in ExCon to gain real-time assessments of exercise interactions. Finally, the team merged insights from the Executive TTX with distributed outcomes to ensure the findings reflected an integrated perspective.

Finding #1: Entities effectively applied internal security protocols and cyber incident response measures in an effort to maintain grid reliability and mitigate the impacts of a sophisticated cyber attack. Information sharing across business units and departments occurred frequently, but areas for improvement emerged.

Supporting Observations and Recommendations

- Participating entities successfully activated internal cyber incident response command structures and external crisis management teams to address both technical impacts and broader public-facing implications. Internal policies and procedures promoted order in an unpredictable situation, but the need to update and refresh guidelines was widely acknowledged. The exercise reinforced the importance of maintaining a Cyber Security Incident Response Plan in advance of an actual incident. Several entities learned that some internal policies were outdated due to infrastructure upgrades, staff turnover or new Critical Infrastructure Protection (CIP) requirements. In addition, some entities noted the importance of updated and current intercommunications plans between operational-level staff and senior management in a rapidly evolving crisis environment.
- Operational and IT staff shared impact assessments and attack implications as the scenario escalated. Several entities noted that this interaction represented the first time these functional groups had successfully coordinated efforts during a security incident or drill. While some organizations readily shared information across functions, others worked in isolation and struggled to recognize implications for both operational and IT assets. In the early phases of the scenario, some business units such as generation and transmission operators also noted that cross-department information sharing could have occurred in a more proactive manner. Entities can develop training scenarios that would promote more understanding of operations/IT interdependencies and reinforce cross-functional coordination.
- Entities reported the need to establish clearer thresholds that can rapidly distinguish a common operational issue from a major cybersecurity incident. While scenario escalation ultimately led players to activate their cyber incident protocols, some entities

were delayed in acknowledging the full scope of the event. Complicated protocols and diverse infrastructure can lead to tentative responses to infrequent events. Incident response plans should establish clearly defined thresholds that clarify expectations and the level of urgency based on a specific set of operational metrics. Some entities also applied weather event response protocols to the cyber sabotage scenario. While some operational parallels exist, organizations should distinguish cyber response doctrine from those employed during a weather emergency.

- Based on scenario conditions, utilities undertook the appropriate measures to protect assets, mitigate impacts, and maintain grid reliability. These steps included disconnecting the communication protocol networks, relying on manual operations, performing forensics to identify root cause, and isolating corporate networks to contain propagation. While these steps were consistently taken in a coordinated fashion, entities must continue to evaluate the resource requirements and operational implications of such measures. For example, several utilities did not fully recognize the staffing requirements of extended manual operations. Cross-training personnel to perform multiple functions in a crisis situation could alleviate some staffing constraints.
- The exercise highlighted a heavy reliance on e-mail, teleconferencing, and other technology that enables coordination in crisis conditions. In a potentially compromised environment, where communications mechanisms could be untrustworthy, alternate information sharing mechanisms and protocols should be developed.

Recommendations Summary

- Review and refine incident response plans and protocols to ensure applicability and relevance to operational environment
- Establish clearer thresholds to distinguish common issues from major cyber incidents
- Strengthen communications channels between IT and operational personnel
- Identify alternative communications means in crisis situations

Finding #2: Horizontal communication that occurred among utilities was extremely robust but vertical information sharing can be improved. While BPS entities shared information readily, communication with NERC and government agencies, were often not as frequent or comprehensive.

Supporting Observations and Recommendations

- A broad representation of the BPS, including generation and transmission operators, reliability coordinators, balancing authorities, and independent system operators exchanged information as scenario impacts escalated. This information exchange

enabled players to validate conditions and acknowledge the coordinated nature of the sabotage. Entities relied heavily on RCIS posts to gain better situational awareness of conditions across the BPS. For example, RCIS was the first mechanism to broadly disseminate the possibility of cyber tampering originally considered to be copper theft.

- The quality of information sharing and reporting to NERC's ES-ISAC and relevant government agencies was not as frequent or comprehensive as the communication occurring across the BPS. Several entities did report break-ins and potential cyber sabotage to the FBI, but not to other relevant bodies. Despite the assurance that NERC reporting would not be used for compliance purposes, several entities expressed hesitation in sharing sensitive information regarding compromised critical cyber infrastructure. One entity indicated that it was contacting corporate legal for "permission" to report to the ES-ISAC. This trust deficit significantly impeded entities' willingness to share information that could have supported the ES-ISAC's role in ensuring grid reliability. As a result, ES-ISAC's information gathering content was often limited to OE-417 filings and hampered by the NERC Standard EOP-004 time requirements. NERC has recently taken additional steps to clarify this separation between compliance and the ES-ISAC. Further publicizing and communicating ES-ISAC responsibilities will address concerns about compliance repercussions stemming from entity reporting, and will likely enhance vertical information sharing. NERC can also better reinforce the benefits and incentives for reporting upwards.
- Some entities reported that a lack of clear and consistent reporting protocols inhibited their ability to share information vertically. Utilities cited the overlapping nature of certain compliance procedures found in NERC Standards CIP-001, CIP-008, EOP-004, and the OE-417, which created redundancies in a period of severe resource constraints. Reporting to NERC can be streamlined to reduce duplication and clarify information sharing channels. An updated Incident Reporting Guidelines document with improved guidance on non-regulatory information sharing and a reporting flow chart can help to illuminate the vertical communication protocols that NERC relies on during a major cyber event. Entities also acknowledged the need to review their own protocols for sharing information vertically and clarify what constitutes a reportable event.
- While regional entities supported coordination in their respective areas, information sharing between registered entities, regional entities and NERC can be improved. Regions hosted calls with their impacted entities, but NERC was not consistently invited to these interactions. Some utilities also reported that they were not included in region-specific update calls. In an unfolding emergency, utilities should ensure that both their regional entities and NERC are included in status updates. Conversely, NERC should include the appropriate regional entities on communications to utilities.

Recommendations Summary

- Establish a process or mechanism that enables NERC to capture relevant and/or urgent RCIS post content to strengthen incident response
- Conduct ES-ISAC outreach and communicate incentives to improve vertical information sharing
- Update and disseminate NERC incident reporting guidelines that reduce redundancies and clarify reporting channels with a vertical communications flow chart

Finding #3: NERC fulfilled its role as the central coordinating body for maintaining reliability across the BPS. By developing alerts and hosting industry coordination calls, NERC promoted information sharing and coordinated mitigation efforts to counter the scenario impacts. Although information sharing mechanisms did promote broader awareness, the exercise identified several areas for refinement and clarification.

Supporting Observations and Recommendations

- The ES-ISAC and NERC SA coordinated with ICS-CERT to craft and transmit two ICS-CERT alerts during the exercise. The ICS-CERT team developed timely and actionable guidance on the notional GridEx malware. The ES-ISAC reviewed this content and incorporated it into NERC Alerts for impacted entities. Although the sequence of events did include some exercise artificialities, NERC was able to reinforce its relationship with ICS-CERT and strengthen its NERC Alert process. The alerts promoted awareness of the situation quickly, giving impacted entities mitigation solutions to maintain reliability. NERC should continue to refine its communications channels to ensure that it can disseminate critical information to its stakeholders before they learn of it through media or other sources. A joint information center that can coordinate NERC/DOE/Federal Energy Regulatory Commission (FERC) messaging could support the rapid release of consistent information and avoid a surprise where entities first learn of unfolding events from the media.
- While the ES-ISAC and NERC SA developed and transmitted NERC Alerts rapidly during exercise play, real-world constraints could hamper the expeditious release of urgent updates. The ES-ISAC is bound by requirements stemming from Section 810 of its Rules of Procedures that require up to a possible five day review time by FERC for approvals prior to release. This requirement could adversely affect NERC's ability to share real-time information and guidance to registered entities during disruptive events.
- NERC Hydra exchanges and larger coordination calls were effective in fostering a common operating picture among entities. Although NERC can further clarify call mechanics, most entities found them helpful and informative. Several utilities expressed concern about the security of the conference bridge, particularly unauthorized participation from media. NERC frequently refreshes bridge security access codes to prevent non-essential organizations from participating. NERC conducts separate calls for media and other non-BPS stakeholders. Existing security measures

should be widely publicized to registered entities to promote confidence and broader participation in calls.

- As scenario impacts eroded confidence in conventional communication means, entities considered more trusted mechanisms for sharing information. Since information sharing via standard email or teleconference could be rendered untrustworthy, entities noted that the ES-ISAC portal would address the trust gap by providing a reliable and secure mechanism for sharing information. Entities encouraged the accelerated activation of portal functionality. The ES-ISAC can better educate industry on such services through presentations and awareness activities.

Recommendations Summary

- Support the revision of FERC review and pre-approval requirement of NERC Alerts to ensure timely release of information and guidance to registered entities
- Clarify and disseminate information regarding NERC conference bridges to promote confidence in the security and confidentiality of coordination calls
- Expedite the activation and availability of ES-ISAC portal to enhance trusted information sharing channels and increase awareness of existing ES-ISAC tools to industry

Finding #4: NERC's ES-ISAC and Situational Awareness (SA) teams collaborated closely to support a coordinated BPS response to the GridEx scenario. Despite generally effective coordination, improvements can be made in defining individual roles and responsibilities during a High Impact, Low Frequency events.

Supporting Observations and Recommendations

- NERC's SA staff and the ES-ISAC coordinated closely in developing an attack sequence and hosting industry conference calls to promote situational awareness. The ES-ISAC successfully tested its Cyber Events and Analysis workflow to obtain a strong understanding of unfolding events. While conference calls were well-run and informative, roles and expectations require further definition. Players noted some overlap in reporting content and felt agenda items could be better streamlined. Developing call scripts to communicate standard messages could help address this issue.
- During the rapidly evolving scenario events, NERC SA and the ES-ISAC uncovered some redundancy and parallel responsibilities. While the two groups are heavily reliant on one another to coordinate with regions, gather information from BPS entities, develop guidance and host information sharing forums, some confusion around their respective duties could inhibit responsiveness in a cyber event. The development of formal roles and responsibilities between NERC ES-ISAC and the SA team, agreed upon by teams and senior leadership, would address overlapping functions. These decisions should be communicated to stakeholders, as some entities expressed confusion regarding their individual purviews. The ES-ISAC, in coordination with NERC SA, should consider developing outreach presentations to registered entities to highlight and reinforce its incident response role.

Recommendations Summary

- Streamline coordination call facilitation by developing standardized call scripts
- Clarify incident response roles and responsibilities between NERC ES-ISAC and SA teams to reduce overlap and enhance responsiveness

Finding #5: Entities responded to initial physical intrusion information with conventional measures but cyber threats should be considered when addressing BPS break-ins.

Supporting Observations and Recommendations

- Upon learning of a physical break-in at substations or back-up control centers, several entities engaged their physical security procedures and reported the apparent copper theft. The scenario highlighted the need to proactively evaluate physical intrusions as an avenue for more disruptive cyber tampering. While conventional copper theft is commonplace across the BPS, security personnel should be sensitized to the cybersecurity implications of a seemingly innocuous event.
- Once cyber tampering was confirmed at facilities across the U.S. BPS, entities consistently reported the situation to appropriate law enforcement authorities. This information was successfully routed vertically through RCIS and, ultimately, in OE-417 reports.

Recommendations Summary

- Sensitize staff to cybersecurity threats stemming from physical intrusions
- Ensure incident response protocols address combined physical/cybersecurity considerations

Finding #6: While the NERC Emergency Standards process could effectively develop binding standards in response to an imminent issue regarding the bulk power system, the process could interfere with core incident response activities at the entity level.

Supporting Observations and Recommendations

- Entities' primary focus during GridEx was mitigating malware impacts and maintaining grid reliability. Players expressed concern that the Emergency Standards directive could divert scarce resources from ongoing recovery efforts to a less mission-critical activity.
- Utilities had little awareness or visibility into the Emergency Standards program. Players expressed concern that the Emergency Standards provision could divert scarce resources from ongoing recovery efforts to a less mission-critical activity. To ensure efficacy and support for the process, NERC should more broadly communicate its function and requirements. NERC can also clarify if the standards are permanent or

have some form of "sunset" provision. Conversely, entities must designate the appropriate personnel to address Emergency Standards directives, should they occur. Utilities reported issues with executing the confidentiality agreements sent as part of the Emergency Standards activation. Several participants noted that the requested turn-around timeframe for the agreement was impractical, while others did not understand the context in which the confidentiality was being assigned.

Recommendations Summary

- Consider resource requirements and improved process for entities to address NERC Emergency Standards in the midst of a security event
- Use the Hydra community to socialize and test Emergency Standards procedures
- Consider pre-negotiating confidentiality agreements prior to invoking the Emergency Standards development activity

Conclusion

GridEx 2011 provided an opportunity to test the Electricity Sub-sector's crisis response plans, and evaluate the community's current readiness to respond to a cyber incident. The exercise also served as an opportunity to enhance collaboration and strengthen industry security processes and capabilities. Participants considered the exercise a successful training event that delivered substantial return on time and resource investments. To reinforce the value of sector-wide exercises, entities expressed a strong interest in participating in future GridEx engagements.

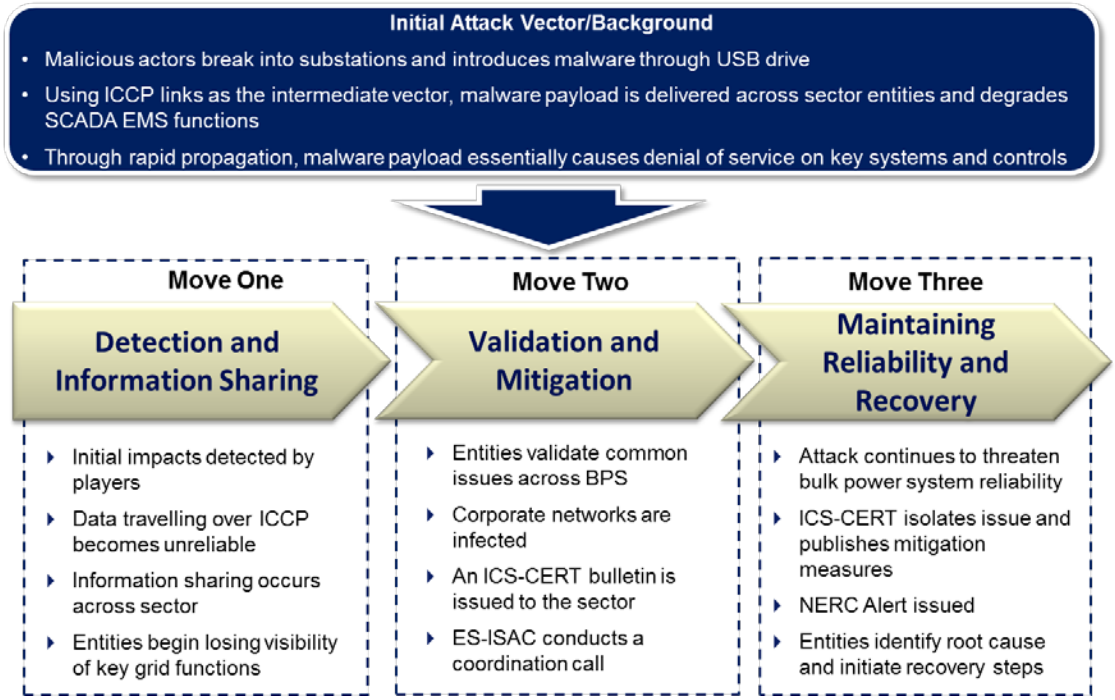
The Electricity Sub-sector successfully achieved its objectives and identified key areas for further exploration during both the planning and execution phases of GridEx. Participants worked together during planning and exercise play to strengthen relationships, evaluate cyber incident response plans, and expose issues for improvement. After participating in GridEx, the sub-sector is better positioned to effectively participate in future industry and government sponsored exercises like GridEx 2013, Cyber Storm 4 and the National Level Exercise 2012. In addition, the Electricity Sub-sector is taking steps to address the findings to enhance its ability to respond to a coordinated cyber attack on the BPS.

Appendix A: GridEx Scenario Narrative

Introduction

The NERC GridEx scenario was crafted to achieve exercise objectives and fully engage the broad GridEx stakeholder set. The scenario had broad relevance among players, promoted coordination during the exercise, and highlighted urgent issues facing the sector. A malware attack with attributes of an advanced persistent threat was developed to realize desired scenario conditions and achieve exercise objectives. The malicious code (malware) compromised the industrial control system (ICS) environment and eroded inter-party trust relationships. As players detected anomalous activity and lost control of systems, they began to share information, coordinate response measures, and mitigate impacts. While the technical feasibility of the scenario was vetted by experts across industry, some liberties were taken to ensure broad applicability and the achievement of exercise objectives.

Scenario Concept Diagram



Overview of Initial Attack Vector and Malware Behavior

Although the exercise began with the assumption that malicious code had already infiltrated critical cyber assets within the BPS, a back-story or "ground truth" was crafted to establish the scope and impacts of the attack.

Prior to Move One of exercise play, a motivated adversary with a desire to cause disruption to the power grid had devoted significant resources to developing malware that attacked grid functions. The code leverages communications protocols as an intermediate attack vector to deliver malicious code across the North American bulk power system. Once delivered, the

malware corrupted core systems and their functions. The malware required two vital pieces of information to work – network address information and operator credentials. The attacker gained unauthorized access to several substations and back-up control centers (BUCC) and inserted a low profile data device between the keyboard and the computing workstations in these locations to capture administrative credentials and other sensitive data for later use in crafting malware.

Upon introduction, the sophisticated malware sensed anti-virus/anti-malware products in use, maintained a small footprint, and supported numerous operating system-based payloads that could be launched from within the master payload located at one of the drop locations. The malware communicated with other copies to share information in a 'mesh'-based methodology so that if any one node was discovered, the communications of that node did not reveal nodes belonging to other cells. The malware was designed to run adjacent to main reporting processes and opened ports usually assigned to permitted functions (so that intrusion detection was not triggered), transferred the binary or mapping information, and shut down. A number of hidden binaries were included in the master binary. These additional binaries were small applications designed to run inside existing critical systems. The malware also had the ability to travel from the ICS environments to the corporate network through trusted links. Once there, the worm sought to find egress points out of the network.

Exercise Phases / Moves

The exercise was structured around three phases or "moves" that simulated three discrete blocks of time. To simulate the passage of time, a notional 24 hours passed between Move One and Move Two, and 48 hours passed between Move Two and Move Three. Each move was initiated by new information that updated players' situational awareness and understanding of the current environment.

Move One (T-Zero): Detection and Information Sharing

In Move One, sector entities and organizations began observing abnormal activity in their operational environment. Network operations were sluggish and an overall system slow-down was detected. Operators observe traffic resets and remote terminal unit (RTU) scans fail to complete. It appears that timing relationships and signals are corrupted, endangering the electricity sector's remote assets.

The malware has created plausible changes in unit outputs that remain within the unit's operating limits. Impacted entities begin to identify alternative means of relaying data, including verbal communications and other manual approaches. Entities also consider deploying manpower to substations to address reliability concerns with remote assets. While the source of the issues is not yet understood, IT staff begins forensics measures and attempt to clean systems. Utilities, BAs and RCs share information on the conditions and validate a common pattern of suspicious conditions across the BPS. Players become suspicious of communications protocol traffic and begin to focus on this channel as a source of abnormalities. Meanwhile, market dispatch issues arise due to data anomalies complicating the arrangement of imported power (interchange). The disturbance and current conditions necessitate entities to issue Electric Emergency Incident and Disturbance Reports (OE-417) to the appropriate authorities.

As Move One concluded, entities continued to lose visibility and experienced difficulty managing load. An RCIS bulletin revealed that cyber tampering at major utilities' key locations had been detected.

Move Two (T+24 hours): Validation and Mitigation

In Move Two, entities continued to experience reliability concerns as summer peak demand exacerbated load balancing issues. ICS-CERT released a bulletin that stated that the imbedded malware was observed attempting to exploit a C2 channel (command and control) within some entities. The egress was detected through analysis of entity network logs. In coordination with ICS-CERT, the FBI announced to the sector the probability of malicious intent to disrupt the power grid. Entities continued to report severe conditions and reliability concerns through RCIS bulletins while coordinating with Regional Entities and authorities. Some failover and back-up systems were inoperable, which forced many entities to initiate manual operations. This process severely taxed resources of RCs, BAs and other Regional Entities. The scenario affected several key calculations and forced some utilities to abandon market activity. Other small utilities that failed to detect the C2 egress experienced intermittent outages in their regions. ICS-CERT, in coordination with the FBI, gathered a fly-away team to engage in further analysis and forensics. Entities also experienced issues with their corporate LAN and other supporting systems, as the malware appeared to have vectored to the corporate network. Network functions were sluggish and DNS resolution was unreliable. Outage management/GIS systems are compromised, corrupting distribution functions among some entities. To conclude Move Two, the ES-ISAC scheduled a sector coordination call to review impacts, provide guidance, and coordinate a response.

Move Three (T+72): Maintaining Reliability and Initiating Recovery

Move Three began with a media report, chronicling the coordinated attack, grid conditions and response activities. By the start of Move Three, the ES-ISAC, ICS-CERT, FBI, DOE, and FERC shared information frequently. ICS-CERT analyzed malware and published near-term identification and mitigation measures and the NCCIC continued to serve as a coordination point for government agency interaction and information sharing. Entities worked with their anti-virus and control system vendors to obtain patches. A NERC Alert was issued to provide malware information and eradication steps to the community to clean systems and restore functionality. At the conclusion of Move Three, fragile grid reliability was achieved, but with significant inefficiencies.

Appendix B: Areas for Future GridEx Improvements

GridEx participants completed After Action Questionnaires, which provided both substantive input on response activities and feedback on exercise mechanics, logistics, and support. While the success and strengths of the exercise were widely acknowledged by planners and players, NERC noted several areas for improvement for future grid security exercises. Below are key themes that emerged from the after action process:

- **Broader Representation from Industry:** While GridEx featured comprehensive participation from across the sub-sector, some entity counterparts were not engaged. This forced some participating utilities to simulate interactions, rather than exercise real-world communications paths. During the planning of future exercises, the NERC planning team, in coordination with participating entities, should target and recruit previously absent organizations (such as key Independent System Operators and Reliability Coordinators) to increase realism. More extensive participation of business units within entities would also strengthen GridEx engagements.

- **Enhanced Inject Distribution and Sequencing:** Players remained occupied with exercise injects throughout GridEx, but planners observed some distribution gaps. While some exercise periods featured a rapid succession of injects, others periods provided far fewer updates to players. A more consistent inject release process could steady the overall exercise battle rhythm. In addition, revisions to pre-established inject content or timing should be more clearly communicated to players in advance to alleviate confusion during exercise play.

- **More Secure Media Viewing:** The mock news reports provided realistic updates to the evolving scenario that enhanced player engagement, but video distribution mechanisms can be improved. Several organizations block YouTube Internet Protocol addresses, forcing planners to rely on the file transfer protocol (FTP) site to access the video. Although the FTP site was an effective alternative, download speeds were slow, and some players were delayed in viewing videos. A more secure host that can stream high-resolution video should be identified for future exercises.

- **Clearer "Rules of Engagement" for Player Conduct:** While the C/E Handbook provided planners a detailed understanding of GridEx, some participants were unclear on exercise

expectations and guidelines. For example, players did not know if they should file OE-417s, or if the filing was considered a notional activity. In the future, more straightforward guidance can be provided on expected player activities and actions. Additionally, more accurate assessments about anticipated time commitment for C/Es and players will assist participating organizations in proper resource allocation.

- **Improved Player Directory:** The Player Directory served as the key resource for enabling exercise coordination and information sharing during GridEx. Despite efforts to capture all player details prior to exercise play, some contact information was not initially available. An enhanced directory tool, potentially available online, could allow real-time additions and revisions to the player directory.

- **Arrange for training credit:** Some exercises, like GridEx, award training credits for full participation. Training credit serves as an incentive for active participation among players and satisfies organizational commitments. Planners should ensure the credit requirements are clear, and necessary preparation is undertaken in advance of the exercise.

Appendix C: GridEx Terminology

- **2500 Inject:** Injects that do not have a discrete time release designation. They are transmitted as needed based on actual exercise play, and are often sent when players are not responding appropriately to previous injects.

- **Controller/Evaluators**: C/Es observe and record key actions and interactions within their organization. They also plan and manage exercise play. C/Es provide key data to players and may prompt or initiate certain player actions to ensure exercise continuity. Any changes that impact the scenario or affect other areas of play must be coordinated through the C/E, who will coordinate with the Exercise Control (ExCon). All C/Es will be accountable to the ExCon. They also evaluate and provide feedback on a designated functional area of the exercise. C/Es assess and document participants' performance against established industry crisis response plans and exercise evaluation criteria, in accordance with Homeland Security Exercise and Evaluation Program (HSEEP) standards. They have a passive role in the exercise and only note the actions of players; they do not interfere with the flow of the exercise.

- **ENDEX:** Official end of exercise (1300 EST Thursday, 17 November, 2011).

- **Exercise:** An instrument to train for, assess, practice, and improve performance in prevention, protection, response, and recovery capabilities in a risk-free environment; can be used for: testing and validating policies, plans, procedures, training, and interagency agreements; training personnel; improving interagency coordination and communications; identifying gaps; and identifying opportunities for improvement.

- **Exercise Control:** ExCon is responsible for conducting the exercise. They will send injects to the C/Es. ExCon can be reached out to at any point during the exercise. ExCon is also to be copied on all outgoing mail during the exercise.

- **Hotwash:** Report findings and lessons learned to C/Es and/or Lead Planners as applicable.

- **Inject:** The information that the player actually receives from ExCon; could be a phone call, email, screenshot, error message, etc.; an observable event of the larger exercise scenario.

- **Monitor/Respond Player:** Monitor Responder players view selected segments of the exercise. They do not play in the exercise, and do not perform any control or evaluation functions. Monitor Responders can receive injects, exercise internal processes, and participate in coordination calls.

- **Players**: Players are participants who have an active role in responding to the simulated cyber attack and perform their regular roles and responsibilities during the exercise.

Players will fully engage in the exercise, responding to all injects and participating in coordination calls.

- **Planning Team:** Exercise support staff includes individuals who are assigned administrative and logistical support tasks during the exercise.

- **STARTEX:** Official start of exercise (0930 EST Wednesday, 16 November, 2011).

Appendix D: Acronym List

- **ACE** - Area Control Error
- **AGC** - Automatic Generation Control
- **C2** - Command and Control
- **CCA** - Critical Cyber Assets
- **ED** - Economic Dispatch
- **EMS** - Energy Management System
- **ES-ISAC** - Electricity Sector Information Sharing and Analysis Center
- **FEP** - Front End Processor
- **FTP** - File Transfer Protocol
- **GIS** - Geographic Information System
- **ICS-CERT** - Industrial Control Systems Cyber Emergency Response Team
- **IDS** - Intrusion Detection System
- **IP Address** - Internet Protocol Address
- **LAN** - Local Area Network
- **LFC** - Load Frequency Control
- **MS-ISAC** - Multi-State Information Sharing and Analysis Center
- **NCCIC** - National Cyber and Communications Integration Center
- **OE-417** - Electric Emergency Incident and Disturbance Report

For more information please contact:

Brian M. Harrell, CPP

Manager of CIP Standards, Training and Awareness

brian.harrell@nerc.net

(609) 651-0671