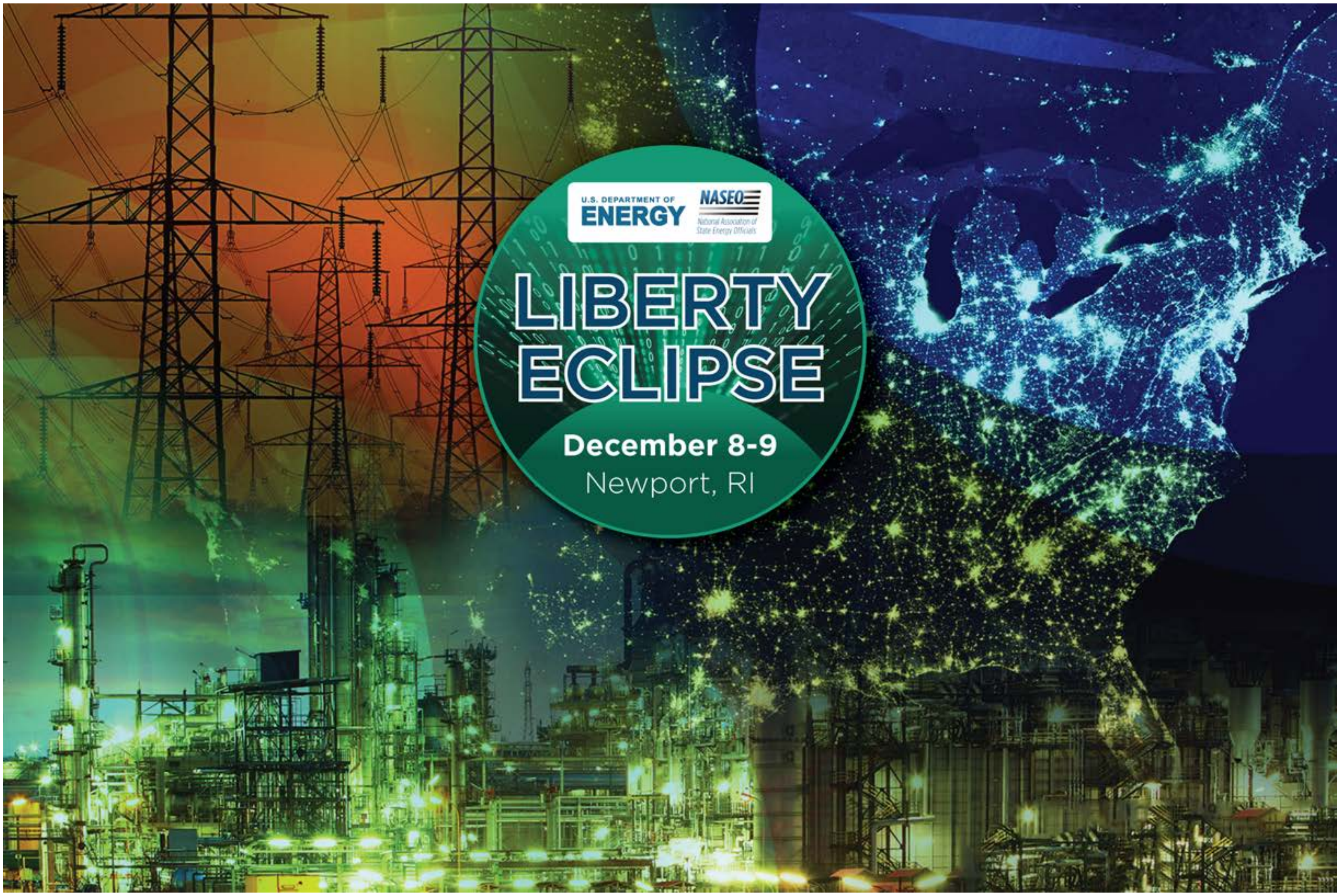
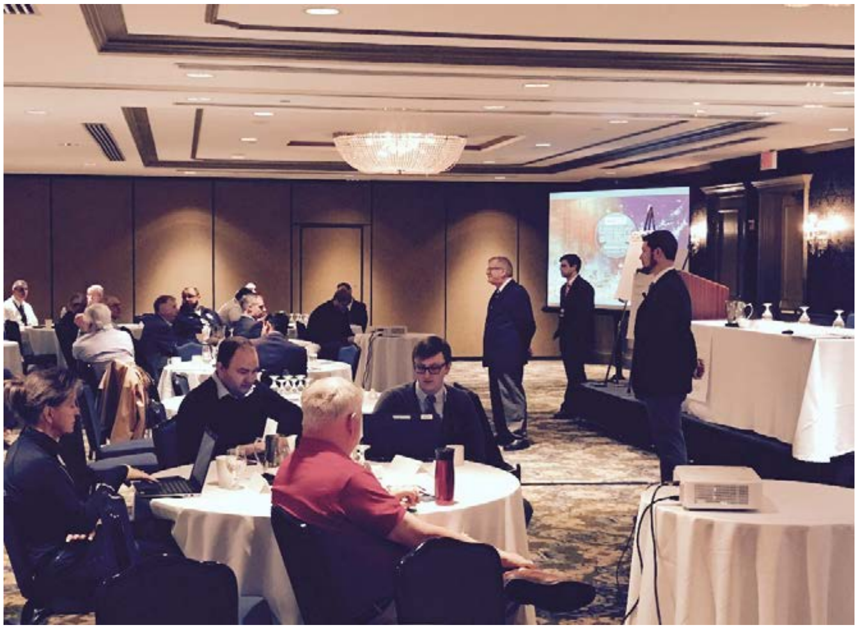

U.S. DEPARTMENT OF ENERGY
NASEO National Association of State Energy Officials
LIBERTY ECLIPSE
December 8-9
Newport, RI

U.S. DEPARTMENT OF ENERGY | Infrastructure Security & Energy Restoration

Liberty Eclipse Energy – Energy Assurance Exercise & Event

December 8–9, 2016

Exercise Summary Report



E-ISAC
Staff Organization
RESILIENCY | RELIABILITY | SECURITY

HANDLING INSTRUCTIONS

1. The title of this document is *Liberty Eclipse Energy-Energy Assurance Exercise & Event* (*Liberty Eclipse*) Exercise Summary Report. The exercise overview, goals, and objectives in this manual reflect the information that was discussed by participants at *Liberty Eclipse*.
2. For more information on this exercise, please consult the following point of contact:

Matthew D. Duncan

State, Local, Tribal, and Territorial Energy Assurance Program Manager

Infrastructure Security and Energy Restoration

Office of Electricity Delivery and Energy Reliability

United States Department of Energy

Phone: (202) 586-8828

Email: matthew.d.duncan@hq.doe.gov

TABLE OF CONTENTS

EXERCISE OVERVIEW

Exercise Name	Liberty Eclipse Energy-Cyber Incident Exercise
Exercise Date	December 8–9, 2016
Exercise Location	Newport, Rhode Island
Purpose	Through education and facilitated discussion, *Liberty Eclipse* sought to better inform state energy and emergency management agencies of how to revise plans, policies, and procedures in the response to and recovery from a cyber incident affecting the energy infrastructure of the Northeast and Mid-Atlantic regions. To ensure a thorough informational perspective, the exercise involved key partners in the response and recovery of the energy infrastructure, including energy suppliers, trade associations, and federal agencies.
Scope	This exercise stretched across one and a half days. The first day included a morning session of informational briefs on topics related to the exercise. This was followed in the afternoon by the initial presentation of the scenario and a plenary facilitated discussion of the consequences and responses relative to Days 1–4 of the event. The exercise play moved forward in time to the period covering Days 5–14. Three breakout sessions based on Federal Emergency Management Agency (FEMA) Regions I, II, and III were conducted to enable more in-depth discussions based on the consequences and on the differences between the regions. Day 2 of the exercise established an additional set of conditions that would be used for Day 15 and beyond into the Recovery phase. It continued with additional breakout sessions for the three FEMA regions, and concluded with a plenary session to discuss lessons learned and action items for further improvements to planning and response activities. Overall, the exercise explored specific components of the energy sector's incident response to a cyber incident, one causing long term power outages and having a cascading impact resulting in a significant petroleum product shortage.
Classification	UNCLASSIFIED

Objectives	• Objective 1: Review the ability of current *"all hazards"* response plans to facilitate response and recovery from a cyber incident on the energy infrastructure in the Northeast and Mid-Atlantic regions. • Objective 2: Identify gaps in current state energy assurance plans' cybersecurity, response, and recovery frameworks. • Objective 3: Examine state and federal government roles and responsibilities, authorities, and actions that would be used during a cyber incident to validate procedures and identify gaps to be addressed. • Objective 4: Explore the ability of states, federal agencies, and the private sector to coordinate in support of the needs of businesses and citizens in the aftermath of a cyber incident on energy infrastructure. • Objective 5: Review the ability of communications procedures outlined under the Energy Emergency Assurance Coordinators program, as well as other relevant reporting mechanisms, in response to a cyber incident on the energy infrastructure in the Northeast and Mid-Atlantic regions.
Scenario	A cyber incident caused a major power outage affecting 16.7 million customers in Massachusetts, New York, Rhode Island, Connecticut, New Jersey, Pennsylvania, and Delaware—impacting a total population of 37 million people. Power was restored to some areas, only to go out again at unpredictable intervals. There are concerns that this disruption could spread to other parts of the country. The power outage shut down refineries in Delaware, New Jersey, and eastern Pennsylvania, and 975,000 barrels per day of petroleum fuel production capacity was lost (equal to about 22 million gallons of gasoline and 17 million gallons of distillate and jet fuel per day). Other critical infrastructure, such as telecommunications and water/wastewater, was also affected.
Participating Organizations	Stakeholders from federal, state, and local governments; electricity subsector; oil and natural gas subsector; and key domestic partners participated in *Liberty Eclipse*. Please see Appendix A for a complete list of exercise participants.

General Information

Introduction

This *Liberty Eclipse* After Action Report provides observations of the conduct of the exercise and recommendations for the energy sector, both government and industry, to improve policies, plans, and procedures for energy emergencies. This report was prepared by the National Association of State Energy Officials (NASEO) and the Infrastructure Security and Energy Restoration (ISER) Division of the U.S. Department of Energy's (DOE's) Office of Electricity Delivery and Energy Reliability.

Exercise Overview

The *Liberty Eclipse* Northeast and Mid-Atlantic Regional Energy Assurance Exercise was held December 8–9, 2016, in Newport, Rhode Island. *Liberty Eclipse* was conducted by ISER and NASEO. The National Governors Association, National Association of Regulatory Utility Commissioners (NARUC), and National Emergency Management Association supported the event. This exercise was a critical component of DOE's efforts to strengthen regional cooperation between government and industry on emergency response in order to better facilitate the restoration of energy services in the case of a catastrophic incident.

The exercise consisted of a scenario that involved a widespread power outage caused by a cyber incident. The time to restore power was originally estimated to be 3 weeks due to the need to manually restart and to test systems' operations. Reoccurring power outages also took place in some areas that previously had power restored. The cause of the power outage and restoration timeline was initially unknown to participants. The electric utility industry would have reported the outages to the Regional Transmission Operators, Federal Energy Regulatory Commission, Electricity Information Sharing and Analysis Center (ISAC), DOE, and state public utility commissions (PUCs). Local emergency management agencies and first responders would have contacted their state's emergency management agencies to report outages in their jurisdictions as well.

In addition, the event would have impacted other critical infrastructure elements, which would need to be restored following the power outage. Battery backup power for radio/some commercial cellular providers would probably have been depleted within the first few hours, making communications more difficult. Water/wastewater utilities with emergency backup power might have required additional fuel within the first 24 hours, or they would need to safely shut down operations to avoid releasing chemicals or raw sewage into public waterways. Residents would also have had difficulty accessing safe water and grocery stores; those without backup generators would have faced increased cold-weather health risks—increasing the likelihood of self-evacuation to areas with power and fuel.

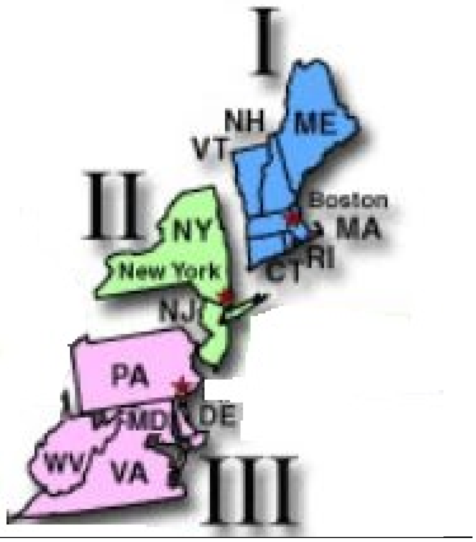
Most refineries cannot operate without utility power. An unanticipated shutdown caused by a power outage as postulated in the scenario would have required equipment testing and a sequential restart of refinery components once power was restored. This process would have taken as long as 7 to 10 days, assuming no equipment was damaged when it went offline. The loss of nearly all of the East Coast refining capacity and the loss of power to retail gas stations, petroleum jobbers, and terminals would have resulted in a major fuel shortage compounded by motorists topping off fuel tanks in areas where the power was still on.

Summary of Exercise

The first day of the exercise was structured in two parts. The morning session comprised informational briefings on select topics to provide additional background and context for participants. This information ensured that participants had a common understanding of the issues, allowing them to address the scenario in greater depth during the exercise play. The exercise began in the afternoon with the presentation of the scenario, allowing for an examination of the coordination of regional response operations among federal, state, and local governments and the electricity and oil and natural gas subsectors. The impacts on the telecommunication and water sectors were also considered. The exercise continued into the second day of the program and concluded with a plenary session to discuss lessons learned and action items.

- **Day 1:** Exercise activities on this day were divided into an examination of two time periods:
  - Days 1–4 after the initial event: This discussion addressed initial assessment and response actions, which included incident notification, alerts, and activation. It examined the initial response processes of relevant stakeholder organizations in the immediate aftermath of a widespread power outage from Maine to Virginia. This discussion took place in a plenary session.
  - Days 5–14: This discussion examined actions taken in response to cascading interdependencies and impacts on electric power and petroleum supplies. This discussion took place in three breakout sessions organized around Federal Emergency Management Agency (FEMA) Regions I, II, and III.
- **Day 2**: Exercise activities on this day covered one additional time frame:
  - Days 15+ following the initial event: This discussion was covered during the breakout sessions and explored the transition from response into recovery; the state and federal response; and coordination with the electricity and oil and natural gas subsectors. The discussion also began to identify actions that could be taken to mitigate the consequences of such an event. During the concluding plenary session, the three FEMA-region breakout groups provided individual reports, followed by a discussion of the overall exercise. Lessons learned, corrective actions, and means to improve information sharing and communications were the final topics of discussion.

FEMA Regions



Key Findings and Proposed Actions

Liberty Eclipse was the first major multi-state regional energy assurance exercise held for the Northeast and Mid-Atlantic since the *Amber Borealis* in June 2011, and was indicative of DOE's renewed commitment to state and local energy resilience. The exercise brought stakeholders together from across the energy assurance spectrum to confront a fictitious significant cyber incident that cascaded into the physical sector, and to discuss the challenges of restoring electric and fuel systems. *Liberty Eclipse* reinforced the interest and attention both government and industry place on improving cyber resilience, while also highlighting the many gaps in both capability and perception that exist with the cyber incident hazard.

Building off of the success of the *Clear Path* series (DOE's flagship annual energy sector exercise), the planning of *Liberty Eclipse* relied on participation from national associations of state officials and industry representatives. The planning team developed an event that was educational and that would accurately review the state of the energy sector's cyber-incident coordination. Participants' familiarity with the envisioned cyber hazard ranged from general awareness of the threat to recognized subject-matter-expertise at both the technical and policy levels, which led to a great deal of peer-to-peer learning. Even those with cyber expertise found value in the event, as they were exposed to differing viewpoints on cyber matters and encountered expertise in other areas such as regulation, systems' operation, and emergency response doctrine. The diversity of participants promoted far-ranging discussions that deepened relationships and professional networks critical to response and revealed that the energy assurance community needs to address many key questions if they wish to achieve greater cyber resilience.

The conduct of *Liberty Eclipse* took the form of educational workshops and briefings on the morning of the first day, followed by a guided discussion of the cyber incident scenario through the rest of the afternoon and into the morning of the second day. Discussions occurred in both plenary sessions and in smaller breakout groups, organized by FEMA regions, that encouraged cross-talk between government and industry. As recommended by a number of the participants, a list of acronyms is provided in Appendix B.

Cyber Incident Coordination Policy Findings

Key Finding #1 – The cyber incident coordination frameworks at both the state and federal levels need to be further defined and synchronized with industry.

Proposed Actions:

- Energy assurance plans should provide more detailed plans and approaches for dealing with cyber incidents, and they should include roles and responsibilities of all the state agencies that could be involved in the responses and public messaging. States should be prepared to identify what planning, policy, and regulatory actions have already taken place, and align them with Presidential Policy Directive (PPD)-41.[1]

[1] For example, see: National Association of State Energy Officials' *NASEO State Energy Cybersecurity Model Analysis: Michigan Cybersecurity Structures and Programs Profile*, http://naseo.org/Data/Sites/1/michigan-cyber-profile-12-29-15-final-draft.pdf.

- States should work with the energy sector on their energy assurance plans and response efforts to provide better coordination between the public and private sectors. Meetings at a state level on this subject, if not already underway, should be considered.

- DOE should identify opportunities to best align and communicate coordination procedures with states and industry for cyber incidents in the energy sector.

- DOE, the U.S. Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI) should coordinate to identify legal restrictions on sharing cybersecurity information gathered during an FBI law enforcement action.

- FBI, DHS, the Office of the Director of National Intelligence, and DOE should more clearly define their roles and responsibilities in cyber incident coordination in the energy sector than what is currently outlined in PPD-41. They should also communicate thresholds and expectations more clearly to states and industry.

- Federal cybersecurity advisories to infrastructure owners and operators relating to cyber threats should be coordinated between the FBI, DHS, and the relevant sector-specific agencies.

- States and electric utilities should be prepared to understand the implications of the rules enacted in the event that the President should declare a Grid Security Emergency, as well as the Secretary of Energy’s authority under this declaration. State and electric utilities emergency response plans should include consideration for the Grid Security Emergency authority.

Key Finding #2 – The public will face a great deal of uncertainty following a significant cyber incident that causes physical damage (such as a long-term power outage or petroleum disruption), creating a considerable challenge for public information and expectation management, particularly around restoration times.

<u>Proposed Actions</u>:

- Public information programs should be part of energy emergency response plans. Public and private Public Information Officers (PIOs) should review existing plans and identify improvements to address a long-term power outage or incident that may create considerable public concern.

- Social media is an important communications mechanism that can reduce misinformation and provide the public with information on response and recovery efforts. It can also provide the public with actions that they can take to ensure their safety and the safety of their family and neighbors.

- PIOs should be invited to participate in future exercises so that this can be more fully addressed.

Key Finding #3 – The evolving nature of cybersecurity threats makes it difficult for PUCs to accurately quantify the cost of cybersecurity investments for rate recovery.

<u>Proposed Actions</u>:

- DOE/OE should support state PUCs’ understanding of cybersecurity capabilities and the costs of investments, and should work with NARUC to explore cost recovery mechanisms for cyber incidents. PUCs could consider reviewing their utilities’ cybersecurity plans on a regular basis (e.g., every 3–5 years or more often), and could help identify gaps and determine how to address the gaps. Care should be taken when reviewing sensitive information to avoid disclosing it to unauthorized parties who may use it to disrupt utility operations.

- PUCs could consider how to track electric utility spending on cybersecurity over time to help measure the ongoing efforts to maintain an appropriate level of cybersecurity. This is a complex problem.

Key Finding #4 – While the consequence management activities for the physical impacts caused by a cyber incident are largely the same as they would be for any other hazard—including the potential use of the Stafford Act—the unique conditions of a cyber incident pose additional challenges that necessitate new capabilities and the use of new authorities.

Proposed Actions:

- The electricity subsector should continue its efforts to develop and further refine the mutual assistance framework for responding to cyber incidents that is being led by the Electricity Subsector Coordinating Council (ESCC).
- DOE and FEMA should investigate the jurisdiction and cost recovery potential of the Stafford Act for recovery from significant cyber incidents.

Key Finding #5 –Information sharing and the ability to communicate remain prime concerns in an energy emergency—regardless of the cause.

Proposed Actions:

- DOE/OE, states, and the energy sector need to maintain, on an annual basis, a list of federal, state, and energy sector contacts to be used in an emergency event.
- Public and private sector emergency contacts need to maintain ongoing communications and information sharing. This can best be done through regular communication during nonemergency times. For example, the states in the Northeast hold regular conference calls with the energy sector and federal partners over the winter months to assess electric, petroleum, and natural gas supply and demand conditions. States in the West have used a similar approach. Other regions should consider similar approaches in the spring and fall to assess the outlooks for summer and winter.
- States should update their Energy Emergency Assurance Coordinator (EEAC) contacts annually and when any significant reorganization occurs that may change individuals' roles and responsibilities for responding to energy emergencies. States should also share information on events within their states that may affect energy supplies and any actions that they may take in response. They should also make aware states that are in their region and who are within their energy supply chain, as provided for in the "Agreement for Enhanced Federal and State Energy Emergency Coordination, Communications, and Information Sharing."[2] DOE/OE should coordinate with the energy sector ISACs to determine what kind of information, and under what restrictions, the ISACs can share information with state energy offices and PUCs.

[2] For more information on the EEAC MOU and training, please visit the http://www.naseo.org/eeac .

- State EEACs and other officials should consider applying for Government Emergency Telecommunications Services (GETS) Cards and the Wireless Priority System (WPS) to ensure connectivity during high call volume events.

Key Finding #6 – There is a need to improve state petroleum response plans to make them more operational and detailed and provide for greater consistency across multi-state regions.

Proposed Actions:

- DOE and NASEO should consult with petroleum suppliers to develop model petroleum shortage response plans, also called "Fuel Plans." States could then adopt them when they update their energy assurance plans. These "Fuels Plans" should address the roles and responsibilities for implementation and operations, and they should include draft executive orders accompanied by press releases to notify the public of their implementation.[3]

- As a precursor to the development of model plans, a webinar should be held to present and discuss select state petroleum or fuels plans that have been developed in greater detail.

- States should review their energy assurance plans and work with the oil and natural gas subsector within their states to update those plans, as well as develop more operation fuel plans.

- Additional guidance should be developed for states on the use of the waivers for gasoline fuel specification from the Environmental Protection Agency, and regarding Jones Act waivers for allowing foreign-flagged tankers to make marine fuel shipments.

Key Finding #7 – Emergency response stakeholders need to have a good understanding of the energy sector supply chains and interdependencies to plan for, and respond to, energy emergencies.

Proposed Actions:

- Exercise participants and those responsible for energy assurance and preparedness need to understand the energy infrastructure and its capacity, flows, and operations. If there is a gap in their knowledge base, they should take advantage of the many resources available to achieve such an understanding. These are listed in Appendix C – References and Appendix D – Resources.

- PUCs can work with utilities to understand what their networks and infrastructure look like and to develop or identify visualizations such as maps, which are very helpful to workers providing aid in emergency situations. PUCs should also work with utilities to have a common understanding of what assets and systems should be the priority during restoration.

[3] For additional guidance of the details that should be included in these plans see NASEO's *State Energy Assurance Guidelines and the Planning Framework*: http://www.naseo.org/eaguidelines; and NASEO's *Petroleum Shortage Supply Management Options for States*: http://naseo.org/data/sites/1/documents/publications/Petroleum_Shortage_Supply_Management.pdf.

- State energy offices and PUCs should develop robust workforce training and development programs to ensure appropriate levels of preparedness, so workers can address events such as those contemplated in the exercise and other related energy emergency exercises.

Key Finding #8 – There are substantial resources available to support efforts that would enhance cybersecurity. These resources, and their applicability, are not always well known at the state and local levels by some of the organizations within the energy supply chain.

Proposed Actions:

- DOE should prepare a document which catalogs cybersecurity resources from federal agencies, energy sector entities, and other organizations. Example resources include the Cybersecurity Capability Maturity Model for the electricity and oil and natural gas subsectors, cybersecurity threat briefings from Energy Sector, the Cybersecurity Risk Information Sharing Program, and others.
- DOE and DHS should work with state energy offices and PUCs to develop best practices for state-level cyber incident coordination in the energy sector.
- DOE should work with energy sector ISACs to clarify information-sharing procedures, the types of information being shared, and information-sharing mechanisms for stakeholders.

Exercise Design Findings

Key Finding #9 – The quality of the exercise, the ability to identify planning gaps, and action items are affected by the composition of the individuals and organizations that participate in the exercise.

Proposed Actions:

- Leverage the Energy Government Coordinating Council, ESCC, and the Oil and Natural Gas Subsector Coordinating Council to ensure that appropriate attendees are invited to and attend future DOE energy emergency exercises.

Key Finding #10 – Participants felt that the exercise should have been a more focused set of events targeting a smaller geographic region to allow for more in-depth discussions.

Proposed Actions:

- DOE should consider hosting smaller-scale, more focused energy sector exercises across smaller geographic areas to better test and drill-down on state and industry plans.
- Encourage states to participate in industry exercises to test coordination mechanisms, and encourage industry to develop useful play for state or local participants.

CONCLUSION AND RECOMMENDATIONS

Liberty Eclipse provided the energy assurance community with its first opportunity to confront a large-scale, multi-region significant cyber incident that created physical world consequences. As expected, many planning and communications gaps were revealed concerning the cyber incident. However, the exercise also demonstrated the tight cooperation and coordination that already exists on consequence management for standard hazards.

The event and exercise was designed to build mutual understanding of how systems could break, what the resulting consequences might be, and to reinforce the importance of collective effort not only within the energy sector, but also between the public and private sectors in rebuilding them. Universally cited in the participant feedback forms, the greatest value of the exercise was the bringing together of state, federal, and industry participants from different parts of the energy assurance community. *Liberty Eclipse* participants walked away from the event with critical new contacts and knowledge of the devastating potential of a significant cyber incident. They also left Newport, Rhode Island, with a sense that more work needs to be done to ensure cyber resilience.

To that end, this After Action Report captures those lessons and identifies the action items that can help us all be better prepared and to ensure that our plans can provide for a rapid and effective response to events that can disrupt energy supplies. DOE will continue to work in collaboration with government and industry partners to ensure that the lessons learned in *Liberty Eclipse* are considered and implemented.

Continued efforts of both government and industry officials to improve the ability of the sector to prepare for, respond to, and recover from catastrophic incidents should be guided by the following Recommendations:

1. DOE should support federal, state, local, tribal, and territorial (SLTT) governments and industry partners to improve communication and information sharing consistent with forthcoming cyber-incident coordination mechanisms, and strengthen procedures to facilitate energy restoration. Particular attention needs to be paid to public communication and expectation-setting during significant cyber incidents.

2. The federal government needs to better define its roles and responsibilities for a significant cyber incident and communicate those roles clearly to SLTT partners and industry.

3. DOE should continue its work with SLTT partners, other federal agencies, and the private sector to ensure that appropriate resources and capabilities are available to reduce the risks to the energy sector from a cybersecurity threat. DOE, DHS, and industry should also work together to ensure that measures are in place for the recovery of critical information technology systems to ensure a more rapid system restoration and to minimize impacts.

4. DOE should facilitate further dialogue between governments at all levels and industry on developing fuel-shortage response plans, and to evaluate these plans in future regional exercises that focused on the oil and natural gas subsector.

5. DOE should maintain and expand its energy assurance program to encourage and support planning and preparedness, through regular education, training, and exercises for SLTT partners, with the goal of promoting a better understanding of energy sector supply-chain interdependencies. These efforts should culminate in updated energy assurance plans at all levels.

APPENDIX A – PARTICIPATING ORGANIZATIONS

Federal Government
Federal Bureau of Investigation Boston
Federal Emergency Management Agency (FEMA)
FEMA Region I
FEMA Region II
FEMA Region III
North American Electric Reliability Corporation
U.S. Army North
U.S. Department of Energy
U.S. Department of Homeland Security
U.S. Department of Transportation
United States Cyber Command
State Government
Connecticut Department of Administrative Services
Connecticut Department of Energy and Environmental Protection
Delaware Division of Clean Energy and Climate
Delaware Emergency Management Agency
District Department of Energy and Environment
Kentucky Department for Energy Development and Independence
Maryland Energy Administration
Massachusetts Department of Energy Resources
Massachusetts Emergency Management Agency
New Hampshire Office of Energy and Planning
New Hampshire Public Utilities Commission
New Jersey Board of Public Utilities
New York State Energy Research and Development Authority
North Carolina Department of Environment and Natural Resources
Pennsylvania Department of Environmental Protection
Pennsylvania Public Utility Commission
Rhode Island Division of Public Utilities and Carriers
Rhode Island Emergency Management Agency
Rhode Island State Police Joint Cyber Task Force
South Carolina Office of Regulatory Staff
South Carolina Public Service Commission

Vermont Department of Public Service
West Virginia Army National Guard
West Virginia Division of Energy
Wisconsin Office of Energy Innovation
Local Government
City of Newark
Plymouth County Public Health Coalition
Energy Sector
Con Edison
Edison Electric Institute
Eversource Energy
Exelon
National Grid
New York Power Authority
Philadelphia Energy Solutions Refinery
Phillips 66
Phillips 66 – Bayway Refinery
Associations
American Fuel and Petrochemical Manufacturers
American Gas Association
American Public Power Association
National Association of Regulatory Utility Commissioners
National Association of State Energy Officials
National Governors Association
National Petroleum Council
Others
ICF International
Johns Hopkins University Applied Physics Laboratory
Powered for Patients
Wildan

Appendix B – Acronyms

Acronyms

(Note – Per the request of exercise participants, this acronym lists includes more than the acronymns found in this document. They include a number of common acronyms found in energy emergency response and may be used as a future reference.)

AAR	After Action Report
AMI	Advanced Metering Infrastructure
b/d	Barrels per day
BBL	Barrel(s)
Bcf	Billion cubic feet
Bcf/d	Billion cubic feet per day
Bcm	Billion cubic meters
CIP	Critical Infrastructure Protection
CIO	Chief Information Officer
CIPAC	DHS Critical Infrastructure Partnership Advisory Council
COG	Continuity of Government
COOP	Continuity of Operations Plan
CRG	Cyber Response Group
CRISP	Cyber Risk Information Sharing Program
DDOS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DOD	U.S. Department of Defense
DOT	U.S. Department of Transportation

EAC	Electricity Advisory Committee
EAD	Energy Assurance Daily
EAP	Energy Assurance Plan
EEAC	Energy Emergency Assurance Coordinator
EIA	U.S. Energy Information Administration
EIMC	Emergency and Incident Management Council
EMA	Emergency Management Agency
EMS	Energy Management System
EnergySec	Energy Sector Security Consortium, Inc.
EO	Executive Order
EOC	Emergency Operations Center
EPA	U.S. Environmental Protection Agency
ERO	Emergency Response Organization
ERO	Electricity Reliability Organization
EEAC	Energy Emergency Assurance Coordinator
ESCC	Electricity Subsector Coordinating Council
ESF	Energy Support Function
E-ISAC	Electricity Information Sharing and Analysis Center
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	U.S. Federal Energy Regulatory Commission
FHWA	Federal Highway Administration
FMA	Federal Maritime Administration

FMCA	Federal Motor Carrier Administration
GCC	Government Coordinating Council
GW	Gigawatt
HOS	Hours-of-service
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISER	Infrastructure Security and Energy Restoration
ISO	Independent System Operator
IT	Information Technology
KF	Key Findings
kV	Kilovolts
LNG	Liquefied Natural Gas
LPG	Liquefied Petroleum Gas
LPT	Large Power Transformer
MMb/d	Million barrels per day
MMBtu	Million British Thermal Units
MMcf/d	Million cubic feet per day
MMgal/year	Million gallons per year
MW	Megawatts
MWh	Megawatt-hour
NCCIC	National Cybersecurity and Communications Integration Center

NERC	North American Electric Reliability Corporation
NESCO	National Electric Sector Cybersecurity Organization
NESCOR	National Electric Sector Cybersecurity Organization Resource
NETL	National Energy Technology Laboratory
NGL	Natural Gas Liquid
NIAC	National Infrastructure Advisory Council
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NRC	U.S. Nuclear Regulatory Commission
NRCC	National Response Coordination Center
NRF	National Response Framework
NSC	National Security Council
NSTB	National SCADA Test Bed
NTSB	National Transportation Safety Board
NARUC	National Association of Regulatory Utility Commissioners
OE	Office of Electricity Delivery and Energy Reliability
PIO	Public Information Officer
PPD	Presidential Policy Directive
PSA	Protective Security Advisor
PUC	Public Utility Commission
RISI	Repository of Industrial Security Incidents
RTO	Regional Transmission Operator

SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SEO	State Energy Office
SEOC	State Emergency Operations Center
SERO	Senior Energy Response Official
SLTT	State, Local, Tribal, and Territorial
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
TCF	Trillion cubic feet
TTX	Tabletop Exercise
UCG	Unified Coordination Group
UCS	Unified Coordination Structure
USGC	U.S. Coast Guard

Appendix C – References

Edison Electric Institute. *Understanding the Electric Power Industry's Response and Restoration Process*. Washington, DC: Edison Electric Institute, October 2016. http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf.

Electric Information Sharing and Analysis Center (E-ISAC). "E-ISAC Home Page." Electric Information Sharing and Analysis Center (E-ISAC). Accessed December 28, 2016. https://www.esisac.com/.

Federal Register Notice. "Proposed rulemaking and request for comment: *Grid Security Emergency Orders: Procedures for Issuance*, 10 CFR Part 205, RIN 1901–AB40." Federal Register Notice, Vol. 81, No. 235. December 7, 2016. https://www.gpo.gov/fdsys/pkg/FR-2016-12-07/pdf/2016-28974.pdf.

Keogh, Miles, and Sharon Thomas. *Regional Mutual Assistance Groups: A Primer*. Washington, DC: National Association or Regulatory Utility Commissioners, November 2015. https://pubs.naruc.org/pub/536E475E-2354-D714-5130-C13478337428.

National Association of State Energy Officials. *Guidance for States on Relief from Federal Motor Carrier Safety Regulations in an Energy Emergency*. Arlington, VA: National Association of State Energy Officials, November 2014. http://naseo.org/Data/Sites/1/fmcsa-regulations-relief-guidance-11-03-2014.pdf.

National Association of State Energy Officials. *NASEO State Energy Cybersecurity Model Analysis: Michigan Cybersecurity Structures and Programs Profile*. Washington, DC: National Association of State Energy Officials, December 2015. http://naseo.org/Data/Sites/1/michigan-cyber-profile-12-29-15-final-draft.pdf.

National Association of State Energy Officials. "The Role of Energy Emergency Assurance Coordinators (EEAC) State Energy Emergency Assurance Coordinators (EEAC)." National Association of State Energy Officials. Accessed January 28, 2017. http://naseo.org/eeac.

National Petroleum Council. *Enhancing Emergency Preparedness for Natural Disasters*. Washington, DC: National Petroleum Council, December 18, 2014. http://www.npc.org/reports/NPC_EmPrep_Report_2014-12-18.pdf.

Schremp, Gordon. "Jones Act Waivers Presentation." Presented at the Western Fuels Emergency Coordination Meeting, Sponsored by the California Energy Commission and National Association of State Energy Officials, Sacramento, CA, September 2016. https://www.naseo.org/Data/Sites/1/schremp-3.pdf.

U.S. Department of Energy. *Electric Emergency Incident and Disturbance Report (OE-417).* U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability. Last modified July 2012. https://www.oe.netl.doe.gov/oe417.aspx.

U.S. Department of Energy. "Environment for Analysis of Geo-Located Energy Information (EAGLE-I)." U.S. Department of Energy. https://eagle-i.doe.gov/Default.aspx.

U.S. Department of Energy. "Northeast Gasoline Supply Reserve (NGSR)." U.S. Department of Energy, Office of Fossil Energy. January 8, 2017. https://www.energy.gov/fe/services/petroleum-reserves/northeast-regional-refined-petroleum-product-reserve.

U.S. Department of Energy. "Northeast Home Heating Oil Reserve (NEHHOR)." U.S. Department of Energy, Office of Fossil Energy. January 8, 2017. https://www.energy.gov/fe/services/petroleum-reserves/heating-oil-reserve.

U.S. Department of Homeland Security. "Government Emergency Telecommunication Service (GETS)." U.S. Department of Homeland Security. Last modified October 23, 2015. https://www.dhs.gov/government-emergency-telecommunications-service-gets.

U.S. Department of Homeland Security. "Wireless Priority Service (WPS)." U.S. Department of Homeland Security. Last modified October 23, 2015. https://www.dhs.gov/wireless-priority-service-wps.

U.S. Environmental Protection Agency. "Frequent Questions: Fuel Waivers." U.S. Environmental Protection Agency. January 8, 2017. https://compliancegov.zendesk.com/hc/en-us/sections/202349537.

Appendix D – Resources

Energy Infrastructure:

A. Energy Information Administration. "Energy Explained – Your Guide to Understanding Energy." Energy Information Administration. Accessed February 17, 2017. http://www.eia.gov/energyexplained/.

B. Energy Information Administration. "State Profiles and Energy Estimates." Energy Infrastructure Administration. Accessed February 17, 2017. http://www.eia.gov/state/.

C. National Petroleum Council. "Appendix G: Hydrocarbon Liquids Supply Chain." In *Enhancing Emergency Preparedness for Natural Disasters Government and Oil and Natural Gas Industry Actions to Prepare, Respond, and Recover*. Washington, DC: National Petroleum Council, December 18, 2014. http://www.npc.org/reports/npc_emprep_report_2014-12-18.pdf.

D. National Petroleum Council. "Appendix H: Natural Gas and Natural Gas Liquids Supply Chains." In *Enhancing Emergency Preparedness for Natural Disasters Government and Oil and Natural Gas Industry Actions to Prepare, Respond, and Recover*. Washington, DC: National Petroleum Council, December 18, 2014. http://www.npc.org/reports/npc_emprep_report_2014-12-18.pdf.

E. U.S. Department of Energy. *United States Electricity Industry Primer*. Washington, DC: U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, July 2015. https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf

F. Federal Energy Regulatory Commission. *Energy Primer: A Handbook of Energy Market Basics.* Washington, DC: Federal Energy Regulatory Commission, November 2015, http://www.ferc.gov/market-oversight/guide/energy-primer.pdf.

G. American Petroleum Institute. *Oil and Natural Gas Industry Preparedness Handbook*. Washington, DC: American Petroleum Institute, April 2016. http://www.api.org/~/media/files/policy/safety/ong-industry-preparedness-handbook-v2.pdf.

Planning

A. National Association of State Energy Officials. *State Energy Assurance Guidelines*, version 3.1. Arlington, VA: National Association of State Energy Officials, December 2009. http://www.naseo.org/Data/Sites/1/documents/energyassurance/eaguidelines/State_Energy_Assurance_Guidelines_Version_3.1.pdf.

B. National Association of State Energy Officials. *State Energy Assurance Frameworks.* Arlington, VA: National Association of State Energy Officials, April 2010. http://www.naseo.org/Data/Sites/1/documents/energyassurance/eaguidelines/State_Energy_Assurance_Guidelines_Version_3.1.pdf.

C. National Association of State Energy Officials. *Petroleum Shortage Supply Management Options for States*, version 3.1. Arlington, VA: National Association of State Energy Officials, September 2012. http://naseo.org/data/sites/1/documents/publications/Petroleum_Shortage_Supply_Management.pdf.

D. Public Technology Institute. *Local Government Energy Assurance Guidelines*, version 2.0. Alexandria, VA: Public Technology Institute, 2011. https://dl.dropboxusercontent.com/u/14265518/leap/PTI_Energy_Guidelines.correx.v2.pdf.

E. Developing and Maintaining State, Territorial, Tribal, and Local Government Emergency Plans, FEMA Comprehensive Preparedness Guide, November 2010, https://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf.

Cybersecurity Resources

A. U.S. Department of Energy. "The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)." U.S. Department of Energy, Office of Electricity Delivery and Renewable Energy. Accessed February 17, 2017. https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity.

B. U.S. Department of Energy. "The Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)." U.S. Department of Energy, Office of Electricity Delivery and Renewable Energy. Accessed February 17, 2017. https://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/oil-and-natural-gas-subsector-cybersecurity.

C. U.S. Department of Homeland Security. "Critical Infrastructure Cyber Community C³ Voluntary Program." U.S. Department of Homeland Security. Last modified October 14, 2015. https://www.dhs.gov/ccubedvp.

D. U.S. Department of Energy. *Energy Sector Cybersecurity Framework Implementation Guidance*. Washington, DC: U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, January 2015. https://energy.gov/oe/downloads/energy-sector-cybersecurity-framework-implementation-guidance.

E. Energy Sector Control Systems Working Group. *Cybersecurity Procurement Language for Energy Delivery Systems*. Washington, DC: Energy Sector Control Systems Working Group, April 2014. https://energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014.

F. U.S. Department of Energy. *Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline*. Washington, DC: U.S. Department of Energy, May 2012. https://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.