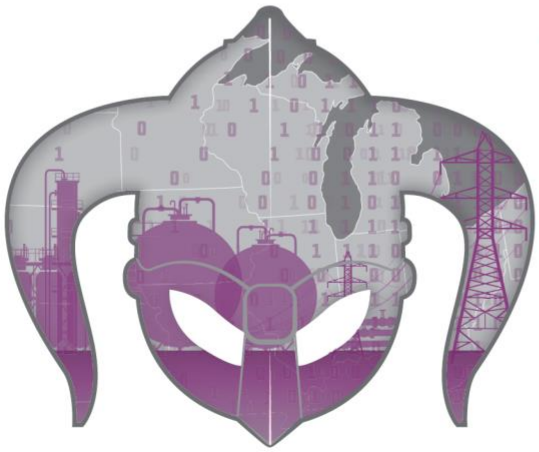
U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE



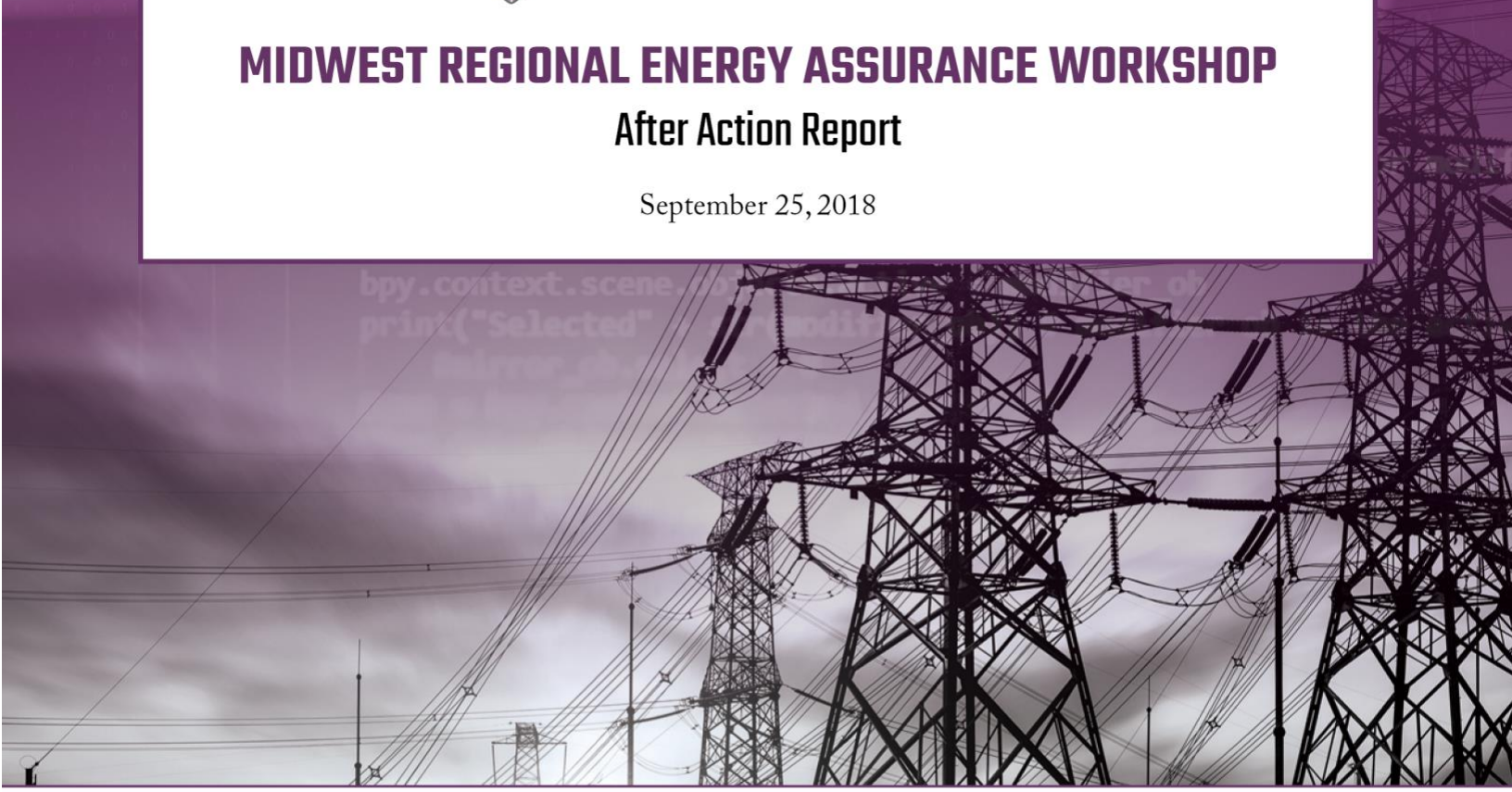
VIKING SHADOW

Energy Assurance Workshop

MIDWEST REGIONAL ENERGY ASSURANCE WORKSHOP

After Action Report

September 25, 2018



U.S. Department of Energy
Office of Cybersecurity, Energy Security, and Emergency Response
and National Association of State Energy Officials

HANDLING INSTRUCTIONS

1. The title of this document is "*Viking Shadow* Midwest Regional Energy Assurance Workshop After Action Report." The workshop overview, goals, and objectives in this report reflect the information that was distributed to participants in advance of and during *Viking Shadow.*

2. For more information about this workshop and proper handling procedures for the document, please consult the following point of contact:

Kate Marks
Infrastructure Security and Energy Restoration (ISER) Division
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
U.S. Department of Energy
Phone: (202) 586-9842
Email: kate.marks@hq.doe.gov

TABLE OF CONTENTS

WORKSHOP OVERVIEW

Workshop Name	*Viking Shadow:* Midwest Regional Energy Assurance Workshop
Workshop Date	Monday, July 30 – Tuesday, July 31, 2018
Workshop Location	Minnesota History Center, St. Paul, Minnesota
Purpose	The U.S. Department of Energy (DOE) and the National Association of State Energy Officials (NASEO) hosted the *Viking Shadow* Midwest Regional Energy Assurance Workshop on July 30–31, 2018, in St. Paul, Minnesota, to assess 15 states' preparedness and response capabilities to a fuel disruption and a cyberattack impacting the electricity, petroleum, and natural gas sectors.
Scope	The workshop scenarios examined state, federal, and private-sector roles and procedures in response to an emergency fuel disruption and a cyberattack that was complicated by weather events affecting the Midwest. Participants focused on discovering gaps and solutions in existing state, federal, and private energy emergency response planning, policies, roles, and procedures. They also explored cybersecurity issues that states and the private sector should consider as they oversee energy system (regulated and unregulated) investments and modernize policies to reflect the growing cyber threat, and special planning and response considerations where cyber events and natural disasters occur in the same time period. See Appendix One for the workshop agenda.
Classification	UNCLASSIFIED
Core Capabilities	*Community Resilience* *Infrastructure Systems* *Logistics and Supply Chain Management* *Long-Term Vulnerability Reduction* *Planning* *Public Information and Warning* *Operational Coordination* *Operational Communication* *Risk and Disaster Resilience Assessment* *Situational Assessment*
Objectives	• Identify gaps in state energy assurance and response plans, specifically as they relate to cybersecurity, fuel coordination, and regional coordination. • Examine state and federal government roles and responsibilities, authorities, and actions that would be used during a regional event to validate procedures and identify gaps to be addressed.

	• Review the ability of existing state-level all hazards response plans to facilitate response and recovery from a cyber incident on the energy infrastructure in the Upper Midwest. • Examine state emergency fuel plans, policies, and procedures to facilitate response and recovery from a petroleum supply shortage or transportation disruption, as well as the impact of fuel shortages on the electric sector (e.g., blackstart capability, utility crew logistics, etc.). • 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 regional incident affecting energy infrastructure in the Midwest and Upper Midwest.
Scenario	*Viking Shadow* used several scenarios to help participants work through existing planning and response procedures and identify opportunities for improvement or gaps specific to cybersecurity threats. The first scenario focused on a disruption in fuel supply due to a winter storm and investigated measures for addressing shortages and communicating with the public, industry, and across state lines. The second scenario consisted of three modules, beginning with initial outages to the power sector and a suspected cyber threat and including a cyberattack that resulted in an extended outage lasting over 14 days. NASEO shared the scenario and background information on the energy infrastructure and supply chains in the region with participants in advance of the event through an infrastructure webinar on July 25, 2018. Educating participants before the workshop helped increase its value by facilitating greater engagement and understanding of the scenarios and issues.
Participating Organizations	Participants included representatives from state energy offices, state utility commissions, and other security-related state agencies; representatives from the petroleum, natural gas, and electricity industries; and experts from DOE and other key federal agencies. A list of participating organizations is in Appendix Two.

1. INTRODUCTION

The U.S. Department of Energy (DOE) and the National Association of State Energy Officials (NASEO) hosted the *Viking Shadow* Midwest Regional Energy Assurance Workshop on July 30–31, 2018 in St. Paul, Minnesota, to assess 15 states' preparedness and response capabilities to a cyberattack impacting the electricity, petroleum, and natural gas sectors. The workshop convened approximately 70 participants—including state energy officials, emergency managers, energy industry representatives from both the oil and natural gas and electricity subsectors, and federal government representatives—to examine planning and response procedures for energy disruptions and identify opportunities for improving energy assurance plans.

Viking Shadow examined two energy emergency scenarios: (1) a fuel supply disruption, and (2) a cyber event leading to a long-term outage. Prior to the workshop, participants received a detailed description of each scenario and background information on the associated energy infrastructure. NASEO also hosted a webinar for workshop participants on July 24, 2018, to review each scenario in detail and highlight the infrastructure impacts. This advanced preparation and engagement increased the value of the time spent by the participants at the workshop.

During the workshop, each scenario session began with "Setting the Stage" panels, which featured subject matter experts providing topical overviews of the associated energy infrastructure and their respective organization's emergency preparedness planning and operations, with a particular focus on cybersecurity considerations. An overview of the scenario and a facilitated discussion about how state and federal government and industry would respond to the emergency scenario followed the stage setting.

The workshop closed with a panel on Regional Coordination and Resources. This session focused on resources available to state governments for improving energy assurance, emergency preparedness and response, and communication and coordination across state boundaries.

This report provides a brief overview of the scenarios and the key findings and recommendations from the discussions and the action cards submitted by participants, which highlighted issues and how to address them.

2. SCENARIO DISCUSSIONS

Midwest Winter Storm Incident Scenario

A severe winter storm has moved swiftly into the Midwest, paralyzing the region with cold air and 18–24 inches of snowfall. Roads are icy and snow covered. Prior to the storm, propane inventory levels were already tight due to a record corn harvest—which increased propane demand for crop drying—as well as a steady increase in the demand for propane for home heating due to record low temperatures brought on by a polar vortex.

Gasoline supply also is an issue. The Flint Hill Resources Pine Bend Refinery in Rosemount, Minnesota, was idled for unscheduled maintenance. The refinery estimates that repairs will take about 30 days. In addition, the Magellan refined product pipeline network is operating at reduced flows in some areas as personnel are unable to reach pump stations to monitor and service issues caused by the storm. The winter storm impacted the railways, which have either ceased operating or have reduced their capacity and shortened trains from 100 to 50 cars. This has reduced propane shipments to the Upper Midwest. Customers unable to procure extra propane supply have been contacting various local government offices, requesting assistance. Additionally, the BP Whiting Refinery in Whiting, Indiana, which can normally process 413,500 barrels per day, has reportedly reduced crude oil runs by 50% due to routine maintenance scheduled for the next 30 days. This is expected to reduce refined product shipments north into Wisconsin on the Badger Pipeline and east into Michigan.

Facilitated Discussion

Following the presentation of the Midwest Winter Storm Scenario, participants engaged in a facilitated discussion on the following key issues:

- Practices for public information coordination and management
- How to identify critical fuel shortages and establish priorities
- Communication between responding government agencies and fuel providers
- Where to find and how to compile weather forecast and impact assessments
- Cascading impacts down the fuel supply chain for propane and gasoline.

State agency participants explained that major activities following the incident would include developing an understanding of fuel inventories and the fuel supply and distribution infrastructure in their states. They would assess power outages and the status of fuel supply and fuel distribution channels. To help with this assessment, states need strong energy profiles for their states. This requires collecting and synthesizing data from multiple resources, such as the U.S. Energy Information Administration (EIA). Many participants noted that they were not aware of the best resources for obtaining this data. In this scenario, states recognized that they should communicate with neighboring states to collect information and develop a common operating picture of the emergency situation to avoid conflicting public messages from emergency authorities. For example, encouraging customers to top off their tanks in one state can create price spikes or shortages throughout the region.

Industry participants indicated that an outage at multiple power substations that disrupts reliable power for pipeline operations would need to be addressed quickly. In the Midwest region, participants said that oil and natural gas infrastructures have redundancies and workarounds that

would keep a scenario such as this from causing major long-term problems. However, alternative methods for moving fuel would need to be implemented. Moving fuel via trucks would not be a sufficient alternative as there may not be enough trucks in the region to move the fuel that would be required under the scenario.

Fuel allocation is a function of the contracts that customers hold. Large fuel customers, first responder groups, and others that require a steady flow of fuel need to understand the terms and conditions of their fuel supply contracts.

States would request waivers, stand up call centers, and initiate coordinated public messaging to avoid a spike in fuel demand. States and industry would also begin to monitor social media for misinformation that may cause public panic or other problems. Additional information on waivers would be useful to states. It was noted that the National Governor's Association recently issued report, *Executive Authorities During Energy Emergencies*, and the NASEO *Guidance for States on Petroleum Shortage Response Planning* document would both provide useful information to states and the industry. In addition, the Infrastructure Security and Energy Restoration Division (ISER) created a Waiver Library on its website to compile available waivers and provide guidance on how to request them when needed.

Participants identified several recommendations regarding regional coordination, public messaging, energy assurance planning, and other areas that are further described in Section 3: Key Findings and Recommendations.

Cyber Scenario and Extended Outage Scenario

The Midwest Cyber Incident included three modules with increasing severity, moving from the potential of a cyber event to an actual cyber event and an extended electricity outage. The background for Module One was a state-sponsored cyber and physical attack similar to one on a European nation's electrical grid six months prior. Three months later, electric utilities in Minnesota and Wisconsin detected breaches and removed malware. While public concern was heightened temporarily, it quickly waned when no severe outages occurred. Three months later, on July 30, a combination of a physical attack at a substation and weather-related outages left 1.5 million people without power in the region. This is shortly followed by overloaded transmission lines failing in rapid succession, which left about 4.6 million customers—or 80% of customers in Minnesota and Wisconsin—without power. This complicated restoration and amplified concerns of a cyberattack.

Module Two began one day later on July 31, with information being released that state-sponsored hackers successfully gained control of 100 strategically located power generators servicing utility distributors across the region. The hackers installed malware capable of directly controlling components of the electric system. The damaged power grid has begun to overload, causing electrical failures to cascade throughout the region. Phone and cellular systems have begun to switch to back-up generators; internet and data are slow. Most gasoline stations cannot pump fuel. Refineries in the region are also idled or running at reduced runs due to lack of power and lack of crude supply. The public is becoming increasingly anxious and unrest is a concern.

Module Three begins in mid-August—two weeks after the July 30 attack. Power has been restored to isolated areas, but a majority of customers remain without power. Damage to the power system has been severe and critical components need to be replaced. Shelters have been

stood-up. Banks in the region are closed. The lack of power has left railways, ports, and other crucial supply chain modes unable to operate.

Facilitated Discussion:

Even though Module One of the Midwest Cyber Incident Scenario simulated hazard-agnostic events with no cyberattack confirmed, all participants explained that they would be responding to the situation as if it were a cyber threat. States agencies would be contacting utilities to gather information on any suspicious activity. Information would be shared through Fusion Centers. In this situation, unified and clear public messaging would be used to avoid panic and instead make sure the public takes appropriate precautions.

During Module Two, which confirmed a cyberattack, participants further expressed the importance of improving coordinated preparedness for cyber events.

Cyber events, threats, and terminology need to be better understood by state, local, and tribal entities. Better processes and guidelines are needed for sharing information in a secure and protected manner during a cyber event. Cyber events need to be exercised more frequently so that the sector becomes more accustomed to preparedness and response procedures, such as they are with hurricanes and other natural disasters. Future exercises and training should include third-party vendors, as they can be gaps in cybersecurity preparedness.

Smaller utilities (e.g., some rural electric cooperatives) will need greater assistance in addressing cyber events from their national associations or the state or federal government, as they do not have the same resources as large investor-owned utilities, larger cooperatives, or larger public power entities.

During the session on Module Three, which focused on regional extended outages, much of the discussion focused on interdependencies, workforce concerns, greater coordination with other sectors such as finance and telecommunications, and coordination with nonprofit organizations such as the American Red Cross. Utilities need to exercise and train on operating systems in manual mode so that they can be protected from additional cyber threats until the situation is resolved. Another important concern is inventories of equipment needed for repair, stockpiles of fuel, spare parts, and other resources. Just-in-time inventory practices create a problem when trying to execute large-scale restoration activities.

Other concerns raised by state participants included the need for more awareness of the utilities' process for prioritizing restoration. Participants noted that the recovery process would be different with a cybersecurity emergency than with natural disasters. In the event of natural disasters, for example, evacuations may be required and homes may not be habitable. Following a cyber event, homes may be habitable, but they may not have power or communication and water if those utilities are also impacted. The response may not need to have as much of a focus on finding shelter, but instead communities may need places to charge batteries or obtain ice and water.

Preparedness at the family and individual levels is very important. The public needs to be educated on how to prepare for an extended outage so that they do not take actions that may further stress themselves or others. During an extended outage, the American public would likely be very eager to lend a helping hand, as they are during severe disasters. To be most useful though, volunteer assistance needs to be directed to where there is a real need. Planning should include identifying productive tasks that volunteers can perform during an extended outage.

One participant noted that while mutual aid would likely be used during restoration, every crew coming into the region puts more strain (housing, meals, supplies, fuel, etc.) on a relief system that is already incapable of providing basic services.

Participants identified several recommendations regarding establishing procedures for sharing and protecting information, training staff, developing public messaging, conducting energy assurance planning, and more. These recommendations are listed in Section 3: Key Findings and Recommendations.

3. KEY FINDINGS AND RECOMMENDATIONS

The discussions during *Viking Shadow* led to a number of findings and recommendations from participants, which are summarized below. In addition, an improvement plan for addressing the recommendations is shown in Exhibit 1.

Exhibit 1 - Improvement Plan

Key Finding	Action	Lead Organization
1. **Education and Training:** There is a continuous need for educating and training staff on energy assurance planning and how to integrate cyber threats into planning and response.	*State associations such as NASEO, along with ISER will conduct and assess training opportunities for state energy officials, especially those new to their positions. The State, Local, Tribal, and Territorial (SLTT) program will also begin to identify modules for trainings and build a foundation for a future training platform. Opportunities for information sharing will be explored.*	NASEO, ISER
2. **Update Energy Assurance Plans (EAPs):** EAPs have become useful tools and should be updated to include an energy profile of the state, information to help orient new energy assurance coordinators, information pertaining to cybersecurity, and other content to improve their quality. Consideration should be given to making the plans more operational.	*ISER will coordinate with NASEO to develop guidelines for EAP updates and provide a listing of available resources for states to use. ISER, NASEO and states will coordinate to create a series of actionable playbooks to provide a more consistent and adaptable approach to energy incident preparedness and response.*	ISER, NASEO, States
3. **Conduct Regional Workshops and Exercises:** These are an excellent means of testing EAPs, identifying gaps, educating new staff on preparedness and response, and establishing contacts in other organizations. Regional workshops improve communication across states and are more cost effective for energy sector companies.	*NASEO and ISER will host multistate exercises for state energy officials, emergency managers, and responders in the western half of the country. The SLTT program will evaluate gaps and assess solutions that can be applied across more states and regions.*	ISER, NASEO, NARUC
4. **Coordinate Preparedness and Response Efforts and Unity of Message:** Public messaging continues to be important to ensure communication is unified among states within a region and between government and industry.	*NASEO will integrate public messaging components into future energy assurance exercises. The SLTT program will review existing communication strategies that may be beneficial for states and will work with NASEO and the other state organizations to develop communications and public messaging checklists.*	NASEO and ISER
5. **Develop Resilient Communication Methods and Effective Social Media:** Back-up communication methods will be needed in the event of a	*Industry and State government should identify resilient means for communicating with the public; develop methods for combating misinformation on social media;*	States, Industry, Emergency Management Agencies

long-term outage impacting communications infrastructure, including the internet. Increasing use of social media requires increased focus to combat misinformation and to ensure the public has the accurate, up-to-date information they need.	*and integrate communications with the public during a long-term outage in future exercises. They should coordinate with FEMA and local emergency management agencies to leverage existing tools and resources which may already be in use or planned.*	
6. Reduce Vulnerability to Fuel and Propane Supply Disruptions: States and customers need a better understanding of the supply infrastructure, supply contracts, and methods to have supply on hand if disruptions occur.	*Develop educational materials on the storage and distribution infrastructure for propane and fuel, and on terms and conditions of supply contracts so that customers can better plan.*	ISER, NASEO, Industry

1. Improve Opportunities for Education, Training, and Workforce Development

Key Finding: There is a continuous need for energy emergency and cybersecurity training. States emphasized that the absence of formal energy emergency and cybersecurity training can slow response and increase system risks. All workshop participants noted the limited availability of an energy-focused cybersecurity workforce.

Recommendations:

- States should have a designated lead for energy assurance planning and coordination. Job functions should be clearly outlined, and an example Energy Assurance position description should be developed.
- DOE should develop energy emergency and cybersecurity training materials to orient new staff and energy assurance designees. Training and educational materials should focus on state roles and responsibilities, as well as development of Emergency Support Function #12-related transition plans. Training materials should also describe the energy infrastructure and the supply chain to help state agency staff better understand the sector.
- Best practices, updated contact lists, available resources, and standard operating procedures should be developed by state agencies.
- Trainings should include greater consideration of the risks of combined natural disaster and cyberattack scenarios and potential cyberattacks involving infrastructure interdependencies on the energy sector (e.g., telecommunications, water, etc.).
- Methods to develop a cybersecurity workforce that can work in the energy sector, state government, and other areas relevant to infrastructure security should be investigated. States should engage colleges and universities in cyber workforce development initiatives.
- States and DOE should move toward more operationally focused "playbooks" for state and local energy emergency planning and response guidance. This will provide a more consistent and adaptable approach to energy incident preparedness and response. Playbooks will identify specific tools, resources, and procedures. They should describe lines of communications and points of contact; address procedures for sharing

information in a protected manner during a cyber incident; and include resources, tutorials, and other information states can access.
- State, Local, Tribal, and Territorial partners raised the need for a clear, defined process for long-term power restoration scenarios. This includes an examination of fuel requirements for blackstart electric generating units and the consideration of cybersecurity planning and response related to mission critical customer energy resources (e.g., blackstart capable combined heat and power units used for hospital operation or backup). These plans and discussions must occur prior to an event.

2. Update Energy Assurance Plans (EAPs)

Key Finding: When maintained, EAPs are useful tools for helping states monitor their energy infrastructure and develop procedures for mitigating and responding to energy supply disruptions. Plans should be updated to include a state energy profile, information to help orient new energy assurance coordinators, and information to help address cybersecurity issues.

Recommendations:

- Develop a comprehensive energy profile for the state using available data (e.g., EIA-782C, etc.). The profile can include information such as supply and demand data; production, storage, and supply routes; microgrids; key points of contact; and data needed in an energy emergency.
- Provide ongoing clarification about the roles of states, federal government, and industry in cyberattack response.
- Clarify the responsibilities of energy assurance coordinators or other state staff with responsibilities in energy assurance.
- Address training curricula and schedules for regular training of staff.
- Address considerations that may not have been fully included in the first round of development, such as regional coordination and communication, cybersecurity, and information sharing or crisis communication protocols.
- Include a method for understanding when refineries or other assets will be down for routine or unplanned repairs, as well as potential implications should a supply disruption occur during that time.
- Include methods and resources for conducting vulnerability assessments and risk assessments (national labs may be useful resources).
- Build upon best practices and lessons learned from other states.
- Share and exercise EAPs with industry stakeholders and relevant state and local agencies to improve coordination.
- Improve and expand cooperation between state and local officials to include energy sector companies, such as utilities. Already existing Local Emergency Planning Committees could provide venues for collaboration and to pre-identify current capabilities. These committees are part of the Emergency Operations Centers that report to the government.
- Establish a schedule for updating and maintaining EAPs.
- Consider establishing a cross-agency team focused on cybersecurity.

- Create mechanisms for volunteers to get involved in a constructive way after an event so that public altruism is targeted to the real need rather than being ad hoc.

3. Conduct Additional Regional Energy Assurance Workshops to Improve Communication and Coordination

Key Finding: If not coordinated properly, actions taken by states in response to an energy supply disruption could have adverse impacts on other states in the region. Regional workshops and exercises are an excellent means of testing EAPs, identifying gaps and how they can be addressed, educating new staff on preparedness and response, and establishing contacts in other organizations. States should be familiar with EAPs of other states in their region as should relevant local governments and industry stakeholders. Regional workshops are also more cost effective for energy sector companies because they allow them to participate with multiple states in one exercise.

Recommendations:

- Conduct energy assurance workshops in other regions of the United States.
- Include additional sectors as workshop participants, such as terminal operators, to discuss fuel distribution; nongovernmental organizations such as the American Red Cross to discuss response during extended outages; and third-party vendors to discuss cyber-related events and emergency response protocols. Third-party vendors can discuss replacement methods for compromised components of Industrial Control Systems and Supervisory Control and Data Acquisition systems and how they fit into the larger recovery and mitigation discussion.
- Include interdependent sectors in future workshops and exercises, such as finance, communications, water, and wastewater treatment. Involve other parts of the supply chain in future cyber-related exercises, such as terminal operators and rail operators.
- Include relevant organizations such as Information Sharing and Analysis Centers and the Federal Bureau of Investigation in future workshops and exercises.
- Continue to address cybersecurity in future exercises and workshops to help educate states. Consider involving national labs and other resources available to states for performing risk assessments.

4. Improve Coordination of Preparedness and Response Efforts

Key Finding: States want to better coordinate preparedness and response efforts with local governments and the private sector. Cooperation between state and local government officials is improving in this area but needs greater focus and standardized procedures. It should also include advanced planning with utilities, fuel providers, and other relevant energy industry representatives.

Recommendations:

- Increase engagement with states to work with local governments (particularly larger or remote jurisdictions) in coordinating energy emergency planning and response activities.
- Establish regional battle rhythms with synched messages, possibly pre-scripted, to help ensure consistent communication between entities and to the public.
- Investigate Local Emergency Planning Committees—part of the Emergency Operations Center function—as a venue for collaboration and identify their current capabilities.
- State participants said that State Energy Program (SEP) funding is supporting energy emergency coordination with local governments and rural engagement with utilities and fuel providers in an increasing number of states. DOE can assist in collecting information on how states are approaching SEP work and identify best practices for broader adoption.

5. Develop Resilient Means of Communication, Improve Unity of Message, and Utilize Social Media Effectively

Key Finding: Changes in the delivery of information to include decentralized outlets, such as social media, have substantially increased the risk of the public receiving misinformation and added to confusion about the appropriate steps to take during an emergency. States recognized the pervasiveness of social media and the benefits and problems it can present. It can be a useful tool in public messaging, but it can also be a source of misinformation. Moreover, back-up, resilient communications media need to be identified in the event communications technologies, including the internet, become unavailable during a long-term outage.

Recommendations:

- Coordinate messaging through public-private cooperation (state, local, federal, and industry) to ensure consistent messaging across the entire affected region.
- Use messaging to help families and individuals prepare for long-term outages and become more self-sufficient.
- Review the upcoming Electricity Subsector Coordinating Council communications strategy as a possible model for other sectors and states.
- Identify, and integrate into planning, back-up means of communication in the event internet and other telecommunications are unavailable. Make the public aware of back-up communication methods.
- Encourage State, Local, Tribal, and Territorial entities to develop plans to use social media to distribute critical information.
- Develop plans to monitor social media for misinformation and methods to combat that misinformation immediately.
- Include communications strategies/components as part of future exercises.

6. Continue to Address Vulnerabilities and Sector Interdependencies Associated with Propane and Fuel Supply

Key Finding: While the Midwest states are familiar with the planning and response measures necessary to manage petroleum and fuel supply disruptions, states highlighted particular issues

of regional concern with regard to fuel and propane supply disruptions, as well as rising interest in understanding cybersecurity threats in this sector.

Recommendations:

- Include information on the interconnectedness of the petroleum and propane sectors as part of education and training (see Key Finding #1).
- Assess the cyber vulnerability of the fuel storage and distribution infrastructure (i.e., pipelines, rail, terminals, and secondary storage).
- Include information on fuel supply contracts as part of education and training (see Key Finding #1), as this drives prioritization among suppliers.
- Investigate use of, or templates for, contingent contracts to deal with shortages and disruptions.
- Improve coordination and communication with rail companies involved in fuel delivery.
- Look for methods to address national truck driver shortages.

APPENDIX A – WORKSHOP AGENDA

Midwest Energy Assurance Workshop

Minnesota History Center

345 W Kellogg Boulevard, St. Paul, MN 55102

Agenda

Workshop Goal and Objectives:

Through education and facilitated discussion, the Midwest Regional Energy Assurance Workshop will better inform energy and emergency management agencies in the revision of plans, policies, and procedures related to state-level regional, fuel, and cyber coordination to events regardless of cause. Workshop objectives include the following:

- Identify gaps in current state energy assurance and response plans, specifically as they relate to cybersecurity, fuel coordination, and regional coordination.
- Examine state and federal government roles and responsibilities, authorities, and actions that would be used during a regional event to validate procedures and identify gaps to be addressed.
- Review the ability of current state-level all hazards response plans to facilitate response and recovery from a cyber incident on the energy infrastructure in the Upper Midwest.
- Examine state emergency fuel plans, policies, and procedures to facilitate response and recovery from a petroleum supply shortage or transportation disruption.
- 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 regional incident affecting energy infrastructure in the Midwest and Upper Midwest.

Day One – Monday, July 30, 2018

7:00 am – 8:00 am *(Heffelfinger Room, First Floor)*

Registration and Continental Breakfast

8:00 am – 8:30 am *(Heffelfinger Room, First Floor)*

Welcome and Opening Remarks

- *Kate Marks, Senior Advisor, Infrastructure Security and Energy Restoration Division, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy*

- *David Terry, Executive Director, National Association of State Energy Officials*
- *Jessica Burdette, State Energy Manager, Energy Efficiency, Assurance, and Operations, Division of Energy Resources, Minnesota Department of Commerce*

8:30 am – 8:45 am *(Heffelfinger Room, First Floor)*

Workshop Overview and Rules of Engagement

- *Ken Green, Chief Operating Officer, BCS, LLC (Workshop Facilitator)*

8:45 am – 9:45 am *(Heffelfinger Room, First Floor)*

Setting the Stage: State and Industry Perspectives on Fuel Incident Coordination and Communications

- *Megan Levy, Energy Programs Manager, Wisconsin Office of Energy Innovation; Co-Chair, National Association of State Energy Officials Energy Security Committee*
- *Drew Werner, Planning Specialist for Critical Infrastructure, Wisconsin Emergency Management*
- *Nate Schoenkin, Emergency Support and Security Specialist, Oil Spill Preparedness and Emergency Support Division, Office of Pipeline Safety, Pipeline and Hazardous Materials Safety Administration, U.S. Department of Transportation*
- *Drew Combs, Vice President of Propane, CHS Inc.*
- *Art Haskins, Emergency Response Coordinator, Enbridge*
- *Bruce Heine, Vice President Government and Media Affairs, Magellan Midstream Partners*

9:45 am – 10:00 am *(Heffelfinger Room, First Floor)*

Fuel Scenario Overview and Presentation

- *Ken Green, Chief Operating Officer, BCS, LLC (Workshop Facilitator)*

10:00 am – 10:15 am *(Heffelfinger Room, First Floor)*

Networking Break

10:15 am – 11:15 am *(Deluxe I and II Rooms, Second Floor)*

Fuel Scenario Facilitated Breakout Discussions

- *Matthew Duncan, Program Manager, Infrastructure Security and Energy Restoration Division, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy*
- *Jeffrey Pillon, Director of Energy Assurance, National Association of State Energy Officials*

11:15 am – 11:45 am *(Heffelfinger Room, First Floor)*

Fuel Scenario Recap and Large Group Discussion

- *Ken Green, Chief Operating Officer, BCS, LLC (Workshop Facilitator)*

12:00 pm – 12:45 pm *(Great Hall, Third Floor)*

Networking Lunch

1:00 pm – 2:00 pm *(Heffelfinger Room, First Floor)*

Setting the Stage: State and Industry Perspectives on Cybersecurity Incident Coordination and Communications

- *Alex Morese, Manager, Energy Security, Michigan Agency for Energy*
- *Robert Jagusch, Director of Engineering and Policy Analysis, Minnesota Municipal Utilities Association*
- *Dawn Philaya, Director, Enterprise Resilience, Enterprise Security Services, Xcel Energy*

2:00 pm – 3:15 pm *(Heffelfinger Room, First Floor)*

Cybersecurity Scenario Presentation and Discussion (Module One)

- *Ken Green, Chief Operating Officer, BCS, LLC (Workshop Facilitator)*

3:15 pm – 3:30 pm *(Heffelfinger Room, First Floor)*

Networking Break

3:30 pm – 4:30 pm *(Heffelfinger Room, First Floor)*

Cybersecurity Scenario Presentation and Discussion (Module Two)

- *Matthew Duncan, Program Manager, Infrastructure Security and Energy Restoration Division, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy*
- *Jeffrey Pillon, Director of Energy Assurance, National Association of State Energy Officials*
- *Ken Green, Chief Operating Officer, BCS, LLC (Workshop Facilitator)*

4:30 pm – 5:15 pm *(Heffelfinger Room, First Floor)*

Day One Wrap-Up Discussion

- *Ken Green, Chief Operating Officer, BCS, LLC (Workshop Facilitator)*

5:15 pm – 6:15 pm *(Great Hall, Third Floor)*

Networking Reception

Day Two – Tuesday, July 31, 2018

7:00 am – 8:00 am *(Heffelfinger Room, First Floor)*

Continental Breakfast

8:00 am – 8:30 am *(Heffelfinger Room, First Floor)*

Brief Recap of Day One and Day Two Introduction

- *Ken Green, Chief Operating Officer, BCS, LLC (Workshop Facilitator)*

8:30 am – 9:30 am *(Heffelfinger Room, First Floor)*

Long Term Restoration and Recovery Scenario Facilitated Discussion (Module Three)

- *Matthew Duncan, Program Manager, Infrastructure Security and Energy Restoration Division, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy*
- *Ken Green, Chief Operating Officer, BCS, LLC (Workshop Facilitator)*

9:30 am – 9:45 am *(Heffelfinger Room, First Floor)*

Networking Break

9:45 am – 11:15 am *(Heffelfinger Room, First Floor)*

Resources and Regional Coordination Facilitated Discussion

- *Megan Levy, Energy Programs Manager, Wisconsin Office of Energy Innovation; Co-Chair, National Association of State Energy Officials Energy Security Committee*
- *Jeffrey Pillon, Director of Energy Assurance, National Association of State Energy Officials*
- *David Batz, Senior Director, Cyber and Infrastructure Security, Edison Electric Institute*
- *Gustav Wulfkuhle, Operational Planning Branch Chief, Federal Emergency Management Agency Region V*
- *Walter Yamben, ESF-12 Regional Coordinator, U.S. Department of Energy*
- *Raja Thappetaobula, Manager, Reliability Coordination and Engineering – Northern Region, Midcontinent Independent System Operator, Inc.*

11:15 am – 11:45 am *(Heffelfinger Room, First Floor)*

Workshop Wrap-Up and Defining the Path Forward

- *Ken Green, Chief Operating Officer, BCS, LLC (Workshop Facilitator)*

11:45 am – 12:00 pm *(Heffelfinger Room, First Floor)*

Closing Remarks

- *Kate Marks, Senior Advisor, Infrastructure Security and Energy Restoration Division, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy*
- *David Terry, Executive Director, National Association of State Energy Officials*

APPENDIX B – PARTICIPATING ORGANIZATIONS

Matthew Acho
Program Officer
National Association of Regulatory Utility Commissioners

Troy Allen
Inspector
Michigan State Police

Lindsay Anderson
Minnesota Department of Commerce

Anne Armstrong Cusack
Executive Director
Michigan Agency for Energy

David Batz
Senior Director, Cyber and Infrastructure Security
Edison Electric Institute

Matt Beaudry
Section Manager
Utah Public Private Partnership

Rick Bender
Executive Director
Kentucky Office of Energy Policy

Robert Benedict
Director, Infrastructure and Transportation
American Fuel and Petrochemical Manufacturers

Amy Black
Emergency Management Liaison
Xcel Energy

Rick Bondy
Emergency Response Supervisor
Magellan Midstream Partners

Jessica Burdette
State Energy Office Manager, Energy Efficiency and Operations
Minnesota Department of Commerce

Chris Bush
Assistant Division Commander, Management and Homeland Security Division
Michigan State Police Emergency

Mike Christianson
U.S. Department of Homeland Security

Drew Combs
Vice President of Propane
CHS Inc.

Jeremy Comeau
Assistant General Council
Indiana Utility Regulatory Commission

Dan Cook
Detective Sergeant
Michigan State Police

Tracy Cowan
Contingency Planning Specialist
Andeavor

Samuel Cramer
Program Manager
National Association of State Energy Officials

Daniel Dahler
Energy Specialist III, Division of Energy
Missouri Department of Economic Development

Campbell Delahoyde
Research Associate
BCS, LLC

Matt Duncan
Program Manager, Sector Specific Agency Activities (Acting) and State, Local, Tribal, and Territorial Energy Assurance
U.S. Department of Energy

Zachary Ellison
Iowa Department of Homeland Security and Emergency Management

Gene Felchner
Emergency Coordinator
Illinois Department of Transportation

Colin Frazier
Policy Advisor
American Petroleum Institute

Deborah Fulk
Senior Planner
Federal Emergency Management Agency

Stephen Goss
Program Manager
National Association of State Energy Officials

Peter Grandgeorge
Berkshire Hathaway Energy

Ken Green
Chief Operating Officer
BCS, LLC

Susan Grissom
Chief Industry Analyst
American Fuel and Petrochemical Manufacturers

Jeff Gunnulfsen
Director, Security and Risk Management Issues
American Fuel and Petrochemical Manufacturers

Jake Hamlin
Director, State Government Affairs
CHS, Inc.

Darin Hanson
Critical Infrastructure Program and Security Manager
North Dakota Department of Emergency Services

Brenna Hartner
Planning Analyst, Emergency Management and Homeland Security Division
Michigan State Police

Art Haskins
Supervisor Emergency Response
Enbridge

Bruce Heine
Vice President, Government and Media Affairs
Magellan Midstream Partners

Ed Holbrook
Federal Aid Administrator III
Nebraska Energy Office

Robert Jagusch
Director of Engineering and Policy Analysis
Minnesota Municipal Utilities Association

Doris Jansky
Statistical Analyst
Nebraska Energy Office

Chris Kelenske
Deputy State Director/Commander, Emergency Management and Homeland Security Division
Michigan State Police

Ryan Kelley
CHS Inc.

Don Kern
Facilities Manager
Flint Hill Resources

Marinko Kimmer
Senior Security Consultant
Phillips 66

Brian Kroshus
Commissioner
North Dakota Public Service Commission

Blake Larsen
Vice President, Information Technology
Andeavor

Nicholas Larson
Berkshire Hathaway Energy

Megan Levy
Local Energy Programs Manager
Wisconsin Office of Energy Innovation

Dan Lloyd
Section Supervisor
Montana Energy Office

Brian Marko
Energy Sector Exercises
U.S. Department of Energy

Kate Marks
Senior Policy Advisor
U.S. Department of Energy

Hitesh Mohan
Vice President
INTEK Inc.

Alexander Morese
Manager, Energy Security
Michigan Agency for Energy

Paul Ovrom
Iowa Department of Agriculture and Land Stewardship

Stephen Pepper
Director, Crisis Management
Phillips 66

Shelly Peterson
Iowa Economic Development Authority

Jeffrey Petrash
Vice President and General Counsel
National Propane Gas Association

Dawn Philaya
Director Enterprise Resilience
Xcel Energy

Jeffrey Pillon
Director of Energy Assurance
National Association of State Energy Officials

Jake Reint
Managing Director, Public Affairs
Koch

Douglas Renier
Principal Planner
Minnesota Department of Commerce

Lynn Retz
Energy Program Director, Energy Division
Kansas Corporation Commission

Michael Rush
Critical Infrastructure Security Engineer
Missouri Public Service Commission

Glenn Sanders
Protective Security Advisor
U.S. Department of Homeland Security

David Sayles
Business Resiliency Manager
Tri-State Generation and Transmission

Annie Schneider
Emergency Management and Alternative Transportation Specialist
Utah Governor's Office of Energy Development

Nathan Schoenkin
Emergency Support and Security Specialist
U.S. Department of Transportation

Thomas Simchak
Senior Policy Analyst
National Governors Association

Shemika Spencer
Director, Contracts and Grants Administration
National Association of State Energy Officials

Jeremy Sroka
Critical Infrastructure Protection Coordinator
Iowa Department of Homeland Security and Emergency Management

Dan Strachan
Director
American Fuel and Petrochemical Manufacturers

Jillian Sulley
Emergency Manager, U.S. Operations
Devon Energy

David Terry
Executive Director
National Association of State Energy Officials

Raja Thappetaobula
Manager, Reliability Coordination and Engineering – Northern Region
Midcontinent Independent System Operator

Thomas Weber
Planning Manager
Michigan State Police

Drew Werner
Planning Specialist, Critical Infrastructure
Wisconsin Emergency Management

Ethan Williams
Planning Supervisor
Colorado Division of Homeland Security and Emergency Management

Gus Wulfkuhle
Operational Planning Branch Chief, Region V
Federal Emergency Management Agency

Walter Yamben
ESF-12 Regional Coordinator
U.S. Department of Energy