ANL/GSS-16/4

State Energy Resilience Framework

Global Security Sciences Division

About Argonne National Laboratory
Argonne is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC under contract DE-AC02-06CH11357. The Laboratory's main facility is outside Chicago, at 9700 South Cass Avenue, Argonne, Illinois 60439. For information about Argonne and its pioneering science and technology programs, see www.anl.gov.

ANL/GSS-16/4

State Energy Resilience Framework

prepared by
J. Phillips, M. Finster, J. Pillon, F. Petit, and J. Trail
Global Security Sciences Division, Argonne National Laboratory

December 2016

Contents

Figures

Tables

Acknowledgements

This document was prepared for Greg Singleton and Dr. Karen Wayland at the Department of Energy's Office of Energy Policy and Systems Analysis (EPSA). Argonne National Laboratory (Argonne) would like to thank a number of participants that donated their time and effort toward informing the results of this report, as well as the support of Mr. Singleton and Dr. Wayland for their encouragement and support throughout the process. Special thanks goes out to multiple subject matter experts, especially Mr. Duane Verner. Special thanks also to inputs from National Association of State Energy Officials, National Association of Regulatory Utility Commissioners, and the kind and knowledgeable employees of the State Energy Offices of New Jersey, Oregon, and Michigan.

Executive Summary

The energy sector infrastructure's high degree of interconnectedness with other critical infrastructure systems can lead to cascading and escalating failures that can strongly affect both economic and social activities. Large-scale disaster events, such as Superstorm Sandy in 2012 or the Northeast Blackout in 2003, have demonstrated the strong interconnections between lifeline network infrastructures (e.g., energy, communications, and transportation) and their influence on response and restoration mechanisms. The national importance of these energy systems has led to renewed efforts by Federal and State governments, as well as private-sector organizations and institutions, to ensure the resilience of our energy systems.

At the national and engineering systems level, resilience can be defined as the "ability of an entity—e.g., asset, organization, community, region—to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance."[1] In layman's terms, this translates to efforts to reduce the magnitude and duration of energy service disruptions. Resilience is an objective characteristic of energy infrastructure systems, which is developed from a precautionary perspective to limit disruptions even in the face of new or evolving hazards and threats. Resilience-enhancing measures generally fall within four broad categories: preparedness, mitigation, response, and recovery (as illustrated in Figure ES.1). A core resilience challenge for energy system owners and operators is to translate the definitions, objectives, and approaches for resilience into identifiable and implementable actions at the component and engineering levels.

Figure ES.1: Categories of Resilience-Enhancing Measures

The operational goal is to maintain energy availability for customers and consumers. For this body of work, a State Energy Resilience Framework in five steps is proposed. This framework, illustrated in Figure ES.2, enables State and local governments, in conjunction with energy utilities, to identify resilience concepts, challenges, and vulnerabilities so that they can implement cost-effective and proven resilience enhancement options. The framework comprises five steps that State and local governments can use to link broad resilience concepts to the implementation of actions tailored to their individual resilience needs and capabilities.

[1] Carlson, L., G. Basset, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitfield, 2012, *Resilience Theory and Applications*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1, Argonne, IL. Available at http://www.ipd.anl.gov/anlpubs/2012/02/72218.pdf.

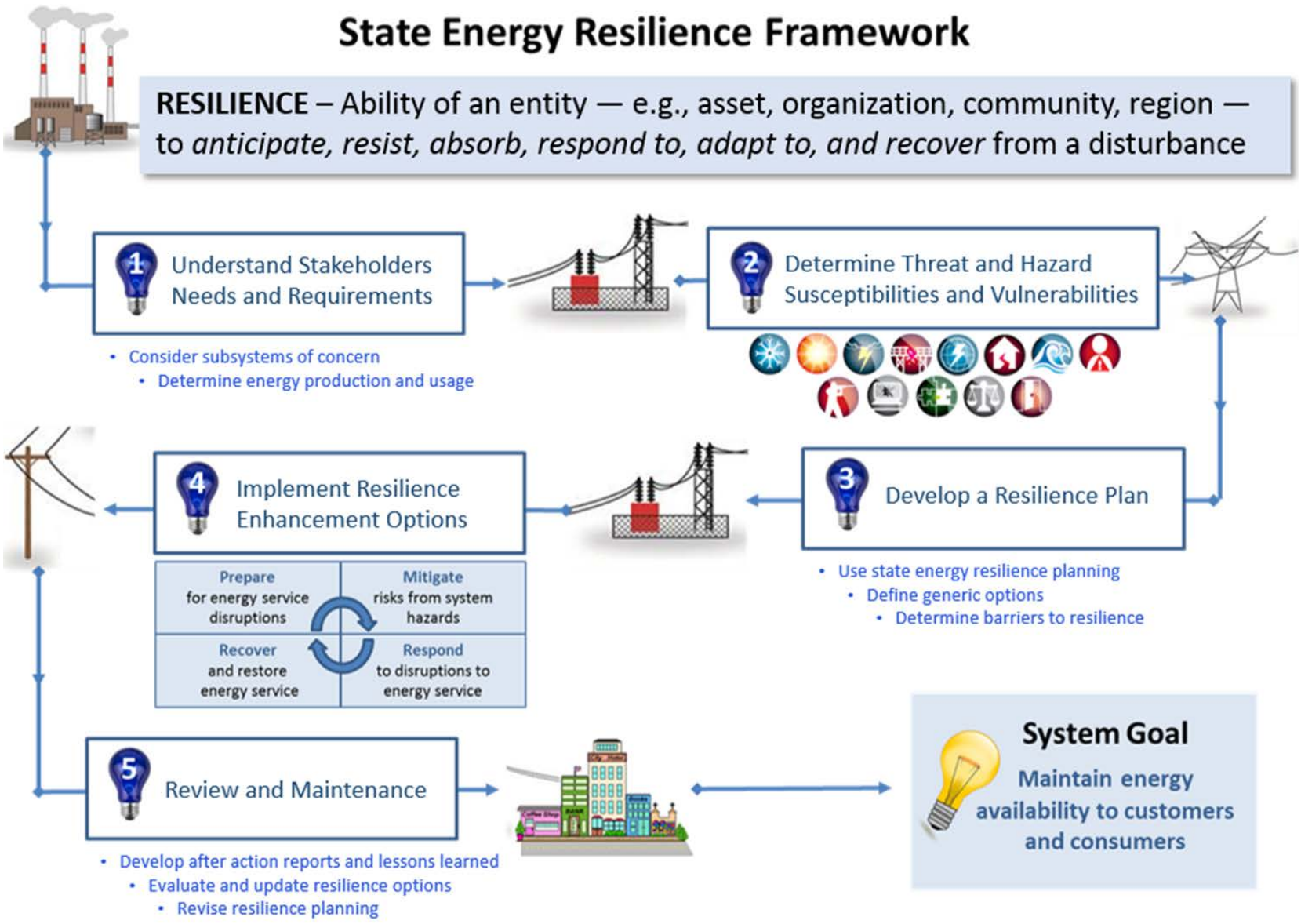

Figure ES.2: Proposed Five-Step State Energy Framework

Understand Stakeholders' Needs and Requirements

The resilience of a community and/or region is a function of the resilience of its subsystems, including its critical infrastructure (i.e., financial, utilities, law enforcement, and emergency shelters), economy, civil society, and governance (including emergency services). The number and complexity of these subsystems makes the measurement of resilience more challenging when moving from individual assets/facilities to the community/regional level (where critical infrastructure resilience is only one component).

Determine Threat and Hazard Susceptibilities and Vulnerabilities

Effective and efficient determination and implementation of resilience options requires a good understanding of the threats and hazards to which energy and other critical infrastructure are exposed. Some threats and hazards are universal (e.g., cyber), while others (e.g., natural disasters) vary by geographic location. Threats and hazards commonly take advantage of or affect a system as a result of specific vulnerabilities or points of weakness.

In addition to understanding threats, hazards, and vulnerabilities, it is also important to consider dependencies and interdependencies when analyzing resilience. They can constitute additional sources of vulnerability for critical infrastructure and lead to further consequences, as well as cascading and escalating failures.

Develop a Resilience Plan

Developing a plan includes considering energy stakeholders' needs and requirements, as well as the consequences potential hazards may have on the gap between the desired performance of the energy system and its performance following a disruptive event. Addressing the gaps allows State and local governments, in conjunction with energy utilities, to define generic options that can be implemented to enhance resilience. Several State initiatives integrate energy resilience considerations:

- State energy assurance planning
- State risk assessment capabilities
- State comprehensive strategic energy planning
- State-regulated utility planning

Resilience planning should also integrate possible barriers to resilience, for efforts to enhance resilience are often challenging for utilities. Resilience investments also can be expensive and require significant capital investment and time to implement. Some of the gaps that inhibit

resilience enhancement measures include: uncertainties in global climate change; development of State and local policies and regulations related to energy infrastructure resilience; and the incomplete understanding of the interactions between energy infrastructure and other systems of critical infrastructure.

Implement Resilience Enhancements Options

Some States have already taken steps to increase the resilience of their energy infrastructure through legislation as well as regulatory and planning efforts. Many critical infrastructure sectors, including the energy sector, utilize resilience enhancements options as part of normal operations. Select examples are provided in Table 1.

Table 1: Example Resilience Enhancement Options Already Being Utilized

Prepare	Mitigate
• Coordinating communications between responders • Development of continuity, contingency, and strategic plans • Training and exercising of plans	• Fences • Hardening/strengthening/retrofitting • Automation and smart monitoring • Backup generators • Onsite fuel storage • Cogeneration plants • System redundancies
Respond	**Recover**
• Mobile incident management and command center • Mutual aid agreements Coordinating agreements between energy system assets & emergency response	• Material provider priority plans • Access to critical equipment • Memorandum of understanding/ memorandum of agreement activation (e.g., with material providers or outside contractors) • After-action reporting and lessons learned

Review and Maintenance

Resilience assessment is an iterative process that requires regular reviews and updates of existing resilience gaps and potential resilience enhancement options. These reviews should integrate after-action reports and lessons learned following disruptive events.

This page left intentionally blank.

1 The Resilience Mission

Resilience has become a household word across the nation, from local communities to State governments to the national level. Of particular concern is the resilience of energy infrastructure such as that related to electricity, natural gas, and petroleum. The energy sector infrastructure's high degree of interconnectedness with other critical infrastructure systems can lead to cascading and escalating failures that can propagate across several jurisdictions and strongly affect both economic and social activities.

In February 2013, the president released a policy directive[2] addressing the need to strengthen the resilience and protection of critical infrastructure. However, most critical infrastructure, especially energy infrastructure, is owned and operated by the private sector or local governments. Since energy infrastructure crosses State lines, a combined effort between the private sector, the regulators, and the local and State governments is necessary to promote resilience of this infrastructure. Nonetheless the nature of the relationship between these different entities, as well as their varying goals, can make a cooperative effort difficult to navigate. The framework developed in this report can help State and local policymakers identify energy infrastructure resilience issues, resilience barriers, and enhancement options. Through discussion of resilience factors, resilience strategies and approaches, and case studies of State resilience improvements, this document will also assist State and local policymakers in understanding, developing, and improving infrastructure resilience measures.

[2] The White House, 2013, *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD-21, Office of the Press Secretary, February 12. Available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

2 Resilience Considerations

2.1 Resilience Principles

Resilience is, fundamentally, part of an entity's broader risk management strategy. Ultimately, the goal of assessing system and asset properties, such as vulnerabilities, resilience, consequence, and so forth, is to enable decisionmakers to make informed choices that will result in cost-effective reductions in the risks associated with the range of natural hazards and man-made threats entities face. Considering resilience allows these entities to adapt to uncertainty—and potentially to develop the ability to react to hazards that have never occurred, but that would have devastating impacts if they did occur. Viewed from this perspective, resilience is a necessary element of a comprehensive approach to risk management.[3]

Resilience for energy systems can be defined as the ability of an energy system to minimize disruptions to energy service by anticipating, resisting, absorbing, responding to, adapting to, and recovering from a disturbance.[4] Figure 1 illustrates the relationship between the different components of resilience and the occurrence of an adverse event. In layman's terms, this translates into efforts to reduce the magnitude and duration of disruptions to energy service. Resilience enhancing measures fall within four broad categories: preparedness, mitigation,

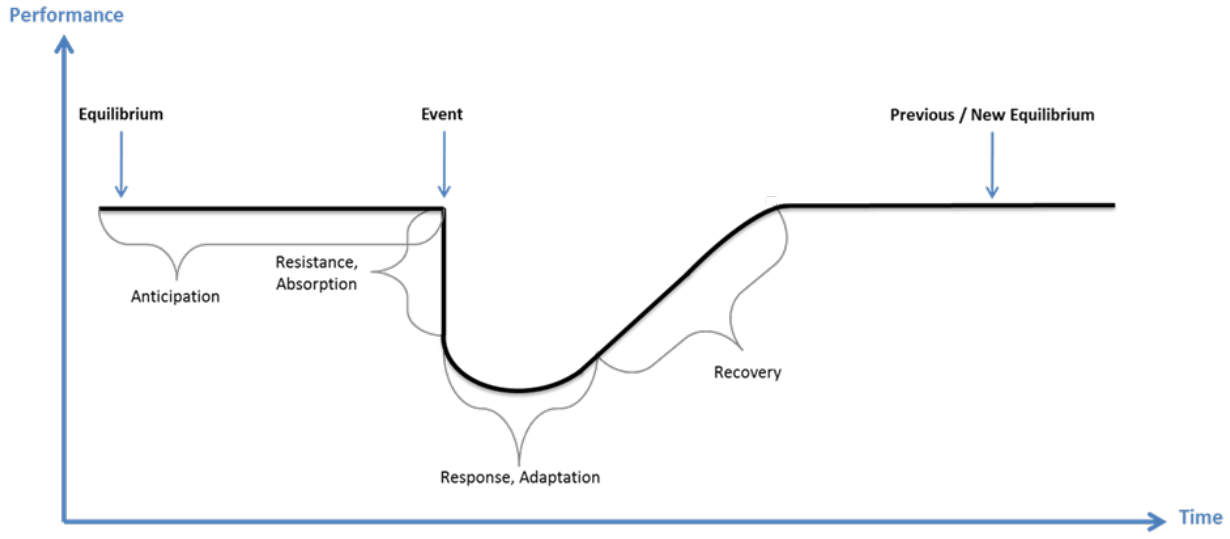

Figure 1: Components of Resilience and the Timing of an Adverse Event[5]

[3] Carlson, L., G. Basset, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitfield, 2012, *Resilience Theory and Applications*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1, Argonne, IL.. Available at http://www.ipd.anl.gov/anlpubs/2012/02/72218.pdf.

[4] Definition adapted from: Carlson, L., G. Basset, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitfield, 2012, *Resilience Theory and Applications*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1, Argonne, IL. Available at http://www.ipd.anl.gov/anlpubs/2012/02/72218.pdf.

[5] Carlson, L., G. Basset, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitfield, 2012, *Resilience Theory and Applications*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1, Argonne, IL. Available at http://www.ipd.anl.gov/anlpubs/2012/02/72218.pdf.

response, and recovery. Table 2 illustrates how the six components that define resilience are connected to the actions that enhance the capacity of an entity to be resilient.

Resilience enhancement measures are generally applied to achieve at least one of three primary goals: (1) prevent or minimize damage to help avoid or reduce adverse events; (2) expand alternatives and enable systems to continue operating despite damage; and/or (3) promote a rapid return to normal operations when a disruption does occur (i.e., speed the rate of recovery).

Table 2: Relationship between Components of Resilience and Resilience-Enhancing Measures[6]

Resilience-Enhancing Measures	Components of Resilience	Definition
Preparedness	Anticipate	Activities taken by an entity to define the hazard environment to which it is subject
Mitigation	Resist	Activities taken prior to an event to reduce the risk by reducing consequences, vulnerabilities, and threats/hazard
	Absorb	
Response	Respond	Immediate and ongoing activities, tasks, programs, and systems that have been undertaken or developed to manage the adverse effects of an event
	Adapt	
Recovery	Recover	Activities and programs designed to effectively and efficiently return conditions to a level that is acceptable to the entity

2.2 State Considerations for Resilience

Because risk-management principles are multifaceted and complex, considerations for resilience are likewise complex. State officials must consider resilience within a risk-management framework. Such a framework involves consideration of the types of threats and hazards the systems face, vulnerabilities, the implications of possible disruptions including cascading and escalating disruptions due to dependencies and interdependencies, the costs associated with enhancing resilience, and the amount of risk the utilities and the State are willing to accept when making decisions about resilience enhancement options.

2.2.1 Key Threats and Hazards

To effectively and efficiently determine and incorporate resilience options, it is necessary to have a good understanding of the threats and hazards to which energy and other critical infrastructure are exposed. In general, these can be viewed as anything that can disrupt or affect energy systems. Some threats and hazards are universal (e.g., cyber), while others (e.g., natural

[6] Ibid.

disasters) vary by geographic location. Threats and hazards commonly take advantage of or affect a system as a result of specific vulnerabilities or points of weakness. Threats and hazards to the Energy Sector include natural hazards and manmade threats, as depicted in Figure 2. Figure 2 also includes other types of threats or hazards that have yet to happen, or are emergent (and thus their effects are not yet known), and related vulnerabilities.

Figure 2: Threats, Hazards, and Vulnerabilities Faced by the Energy Sector

2.2.2 Vulnerabilities

Different components of energy systems are more or less susceptible to specific hazards. These vulnerabilities are driven not only by the functional nature of equipment but also by the local conditions within which the infrastructure operate. For example, energy infrastructure located on the coast will be more susceptible to the impacts of hurricanes (i.e., high winds, storm surge, and flooding) than those inland. Infrastructure in the northern part of the United States will be susceptible to intense winter storms, compared to the infrastructure in the southern part of the United States. Energy companies can implement different measures to attempt to protect vulnerabilities (i.e., to protect substations from flooding or lines from icing) and/or implement measures to ensure the system recovers rapidly from exploitation of its vulnerabilities. The route taken is often driven by cost factors, local regulatory considerations, frequency of occurrence, and amount of impact caused by the hazard in question.

2.2.3 Dependencies and Interdependencies

Dependencies and interdependencies are important to consider when analyzing resilience. They can constitute additional sources of vulnerability for critical infrastructure and lead to further consequences and cascading and escalating failures. A dependency is a "linkage or connection between two assets, by which the state of one asset influences or is reliant upon the state of the other."[7] An interdependency is a "bidirectional relationship between two assets in which the state

[7] Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly, 2001, *Complex Networks, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, IEEE Control Systems Magazine, December, pp. 11–25. Available at http://user.it.uu.se/~bc/Art.pdf.

of each asset influences or is reliant upon the state of the other."[8] Figure 3 presents an example of the complexities of interdependencies between lifeline networks.

States have done much already to start increasing energy resilience. Figure 3 identifies the many interdependencies among lifeline networks, but the existence of an interdependency alone is not itself a cause for concern. Many of these interdependencies exist due to efficiencies and operational improvements available during the course of normal operations through tight cross-system integration. In many cases, risk from interdependencies and dependencies can be mitigated through physical redundancy, alternative options, manual intervention, or other resilience approaches. In addition to identifying a potential interdependency or dependency, it is important to understand which ones are active vulnerabilities and which ones have been successfully managed. Table 3 presents a selection of the different activities States have engaged in to support energy infrastructure resilience. More information can be found in Appendix A.

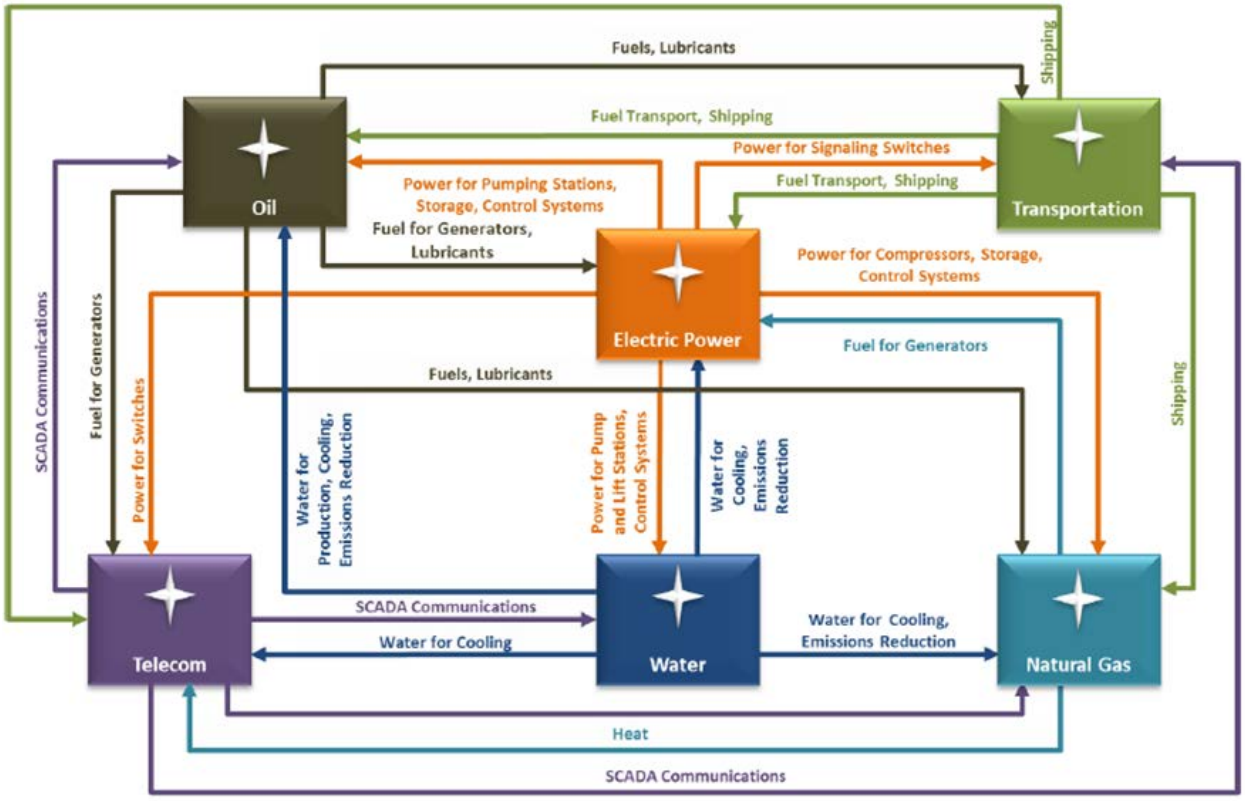

Figure 3: Example of Interdependencies between Lifeline Networks[9]

[8] Ibid.

[9] NIST, 2015, *Community Resilience Planning Guide for Buildings and Infrastructure Systems*, National Institute of Standards and Technology Special Publication 1190, 258 p. Available at http://www.nist.gov/el/resilience/upload/NIST-SP-1190v2.pdf. Figure adapted from Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly, 2001, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, December.

Table 3: State Energy Resilience Initiatives

Activity	Description
State Energy Assurance Planning	Between 2009 and 2010, grants awarded by the DOE were made available to States and local governments to support a State Energy Assurance Planning (EAP) initiative. Funds were used to improve energy emergency preparedness plans and to enable quick recovery and restoration from any energy supply disruption.
State Risk Assessment Capabilities	The DOE supported the development of State and Regional Energy Risk Profiles that examine the relative magnitude of risks at regional and State levels, highlighting energy infrastructure trends and impacts. The profiles present both natural and man-made hazards that have the potential to disrupt the electric, petroleum, and natural gas infrastructures.
State Comprehensive Strategic Energy Plan	The strategic plans identify options for meeting future energy needs in a way that provides multiple social benefits, including risk reductions, enhanced resiliency and reliability, improved efficiency and energy cost savings, job creation and economic development opportunities, and improvements in environmental quality.
State Regulated Utility Planning	On the regulatory side, State Public Utility Commissions (PUCs) also work to address costs, reliability, resiliency, rates, and environmental impacts. In recent years there has been an increased focus on cybersecurity and the risk it poses to the power grid. This has resulted in a number of regulatory actions that encouraged resiliency, security, and reliability through a variety of regulatory approaches including cost recovery.

2.2.4 Risk Acceptance or Nature of Risk

Because utilities and State decisionmakers do not have limitless time or budgets to implement resilience options, the decision on what to implement is largely driven by the amount of risk they are willing to accept. Much of this risk acceptance might be inherited from the risk postures of the utilities themselves, since most of the infrastructure is privately owned and operated. The amount of risk acceptance often boils down to a cost-benefit analysis, where measures are implemented as long as the benefits outweigh the costs. One of the challenges with resilience enhancements is that it is often difficult to quantify the benefits and competitive project prioritization for funds within a company or entity. For example, if training is established and implemented for emergency plans, what is the accompanying benefit from that training? How can that benefit be measured? This often drives decisionmaking for resilience enhancement options toward the options that result in more tangible measures of resilience, such as hardening or installing backup generators even if they are less cost-effective.

State energy officials must balance several factors when considering resilience enhancement options. For one, they are obligated to be responsible stewards of taxpayer funds. The difficulty of tangibly demonstrating resilience options can make public buy-in equally difficult. Second, most of the energy infrastructure is owned by private owners and operators. A third challenge is determining what can be done with limited resources and competition among other State entities that also require funds for infrastructure resilience, such as the State department of transportation.

3 Resilience Enhancement Approaches

Some States have already taken steps to increase the resilience of their energy infrastructure through legislation as well as regulatory and planning efforts. Many critical infrastructure sectors, including the energy sector, utilize resilience enhancements options as part of normal operations. Items such as backup generators, emergency plans, and relationships with local emergency service providers are examples of common resilience options. Given the considerations explained in the previous section, it can be difficult to choose which options to use to enhance resilience. Often a prioritization scheme is developed to assist in deciding which options are most feasible. This prioritization scheme should stem from goals the States are trying to achieve with respect to energy infrastructure resilience. The development of common criteria upon which to evaluate different resilience options can help in objectively comparing options in a transparent, repeatable, and consistent manner. Some criteria that could be considered for resilience enhancement options are lifecycle cost, longevity, and regulatory concerns. The criteria should have a measureable aspect, so as to maintain consistency when evaluating the different options.

Separating the concept of resilience into four components (see Table 1) helps break down a complex idea into smaller, easier to understand parts. Those interested in resilience can then focus on resilience enhancing options within each of these components, which can assist decisionmakers in prioritizing efforts and allocating limited resources to enhance resilience. Appendix B provides further types of resilience enhancement options within each of the four categories.

3.1 Preparedness

Preparedness refers to *activities undertaken by an entity in anticipation of the threats/hazards*, or "pre-event." The creation of Energy Assurance Plans and Strategic Energy Plans is an example of a preparedness action.[10] A component of preparedness that is often overlooked is the communication, coordination, training, and exercising of plans, as well as regular reviews and updates of those plans.

Examples of Preparedness Activities

- Coordinating communications between responders
- Development of continuity, contingency, and strategic plans
- Training and exercising of plans

3.2 Mitigation Measures

Mitigation measures characterize the capabilities to *resist a threat/hazard or to absorb the consequences* from the threat/hazard. Mitigation

Examples of Mitigation Measures

- Fences
- Intrusion detection systems
- Closed circuit television
- Hardening, strengthening and retrofitting
- Automation and smart monitoring investments
- Backup generators

[10] Other types of plans to increase resilience include response/emergency action planning, continuity of operations plans, cyber security plans and preventative maintenance.

measures are usually implemented before an event occurs; however, their benefits can be realized before, during, and after an event.

3.3 Response

Response capabilities are a function of immediate and ongoing activities, tasks, programs, and systems that have been undertaken or developed *to respond and adapt to the adverse effects* of an event. These capabilities are typically associated with actions taken immediately following the event. Response capabilities are a mix of components that can be provided from both the public sector and the private sector.

Examples of Response Activities

- Mobile incident management and command center
- Mutual aid agreements
- Coordinating agreements between energy system assets and emergency response entities

3.4 Recovery

Recovery mechanisms include activities and programs designed to be effective and efficient in *returning operating conditions to a level that is acceptable to the entity*. Recovery measures usually consist of longer-term remediation measures.

Examples of Recovery Activities

- Critical material provider priority plans
- Access to critical equipment
- Memorandum of understanding/ memorandum of agreement activation (e.g., with material providers or outside contractors)
- After-action reporting and lessons learned

3.5 Common Barriers to Resilience

There are barriers that inhibit resilience enhancement measures. These include uncertainties in global climate change, development of State and local policies and regulations regarding energy infrastructure resilience, and incomplete understanding of the interactions between energy infrastructure and other critical infrastructure. In some cases, there has not been much research or planning for changes in some of the lifeline infrastructure. Common issues include the lack of actionable predictive modeling for natural hazards and uncertainty regarding terrorist or insider threats; coordination and collaboration activities between State and local governments, as well as the private-sector entities that own the infrastructure; and the uncertainty surrounding what the future operational environment will be due to climate change impacts and global political unrest.

4 Case Studies and Examples

Since 1980, the United States has sustained 144 weather disasters whose damage costs reached or exceeded $1 billion. Seven of the 10 costliest storms in U.S. history occurred between 2004 and 2012.[11] The current efforts to address risk from these naturally occurring hazards or incidents, in addition to risk from deliberate attacks or accidents, stem from Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (PPD-21).[12] States have roles to support the public and private partnerships, which work to enhance the resilience of their energy infrastructure because it is clearly in their public interest to do so. The loss or failure of critical energy infrastructure can have enormous economic and human consequences, as we have historically seen. This section presents a series of case studies in which States have implemented some type of resilience enhancement, usually following a major disaster. Recent events have often revealed significant, and costly, information on the resilience of our energy infrastructure.

4.1 New York—Fuel NY: Strategic Gasoline Reserve and Gas Station Backup Generation Initiatives

The Northeast suffered devastating impacts when Superstorm Sandy made landfall on October 29, 2012. Although much of New England was affected, New York and New Jersey sustained the brunt of the most severe and devastating damage.[13] Subsequently, New York has emerged as a leader in energy infrastructure reform in response to lessons learned from Sandy. According to the Superstorm Sandy After-Action Report (AAR)[14] completed by New York City officials in May 2013, the storm caused one of the most serious

Figure 4: Gas Lines in the Wake of Superstorm Sandy[15]

[11] The White House, 2013, *The Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, Council of Economic Advisers and the U.S. Department of Energy, August 12. Available at http://energy.gov/articles/white-house-council-economic-advisers-and-energy-department-release-new-report-resiliency.

[12] The White House, 2013, *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD-21, Office of the Press Secretary, February 12. Available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[13] U.S. Department of Commerce, Economics and Statistics Administration,2013, *Economic Impact of Hurricane Sandy Potential Economic Activity Lost and Gained in New Jersey and New York*, Office of the Chief Economist, September. Available at http://www.esa.doc.gov/sites/default/files/sandyfinal101713.pdf. Accessed 13 Jan 2016.

[14] Gibbs, L., and Holloway, C., 2013, *Hurricane Sandy After Action Report and Recommendations to Mayor Michael R. Bloomberg*. Available at http://www.nyc.gov/html/recovery/downloads/pdf/sandy_aar_5.2.13.pdf.

shortages of fuel the city had ever experienced. Figure 4[15] illustrates the length of lines to get gasoline in the wake of Superstorm Sandy. This was primarily a result of regional damage to the energy infrastructure, which led to difficulties in obtaining fuel for the critical vehicles needed to support recovery efforts. In immediate response to the fuel shortage, the New York National Guard and several Federal agencies set up a temporary fueling point for City vehicles, as well those used by critical personnel. Additional complications to the fuel supply issue were associated with the lack of electricity and/or product flow to local gas stations, which were critical to support citizens as they returned to work and their everyday lives.

Post-Sandy analysis led the AAR to recommend the creation of a fuel plan to preemptively plan for shortages that may arise due to severe weather or other emergencies. In response to these recommendations, the Governor's Office of New York started a program called "Fuel NY." There are two major parts to this program. The first part created a strategic gasoline reserve on Long Island, as announced by Governor Cuomo in October 2013. This $10 million pilot uses the capacity of the Northville Industries to create a reserve of approximately 3 million gallons of fuel, which will be available for emergency use when there is a declared emergency.[16]

The second part of Fuel NY established a backup generation program for critical gas stations.[17,18] Although some gas stations were physically damaged due to storm surge, the disruptions in the supply chain, as well as the lack of power, prevented numerous other gas stations from providing gasoline, even if they had it available onsite. The legislation that Governor Cuomo passed in May of 2013 outlined the following criteria for participation:[19]

1) All gas stations within a half-mile of highway exits and hurricane evacuation routes will be required to have a transfer switch prewired by April 1, 2014.
2) These gas stations will be required to deploy and install a generator within 24 hours of losing electric power during a fuel shortage.
3) All gas stations that are part of a chain must have transfer switches installed at 30% of their stations by August 1, 2015.

The State of New York has committed approximately $17 million in support of the Fuel NY program, which include grants of up to $13,000 per gas station to assist with required upgrades.[20]

---

[15] DeLong, K., 2012, *After Sandy, Gas Lines Stretch for Miles in New York, New Jersey*, Fox6Now, November 1. Available at http://fox6now.com/2012/11/01/after-sandy-gas-lines-stretch-for-miles-in-new-york-new-jersey/.

[16] State of New York, 2013, *Office of the Governor: Press Release on Strategic Gasoline Reserve to Prevent Supply Gaps During Emergencies*. October 26. Available at http://www.governor.ny.gov/news/governor-cuomo-launches-first-ever-strategic-gasoline-reserve-prevent-supply-gaps-during.

[17] State of New York, 2013, *Office of the Governor: Press Release on Gas Station Backup Generation Legislation*, February 20. Available at https://www.governor.ny.gov/news/governor-cuomo-proposes-legislation-protect-new-yorkers-gas-shortages-natural-disasters.

[18] New York State, 2013, *Article 16 of the Agriculture and Markets Law Weights and Measures, Section 192-h. Alternate generated power source at retail gasoline outlets*. May 30. Available at http://stormrecovery.ny.gov/sites/default/files/documents/Article-16-192-h.pdf.

[19] Ibid.

[20] Governor's Office of Storm Recovery (GOSR), 2016, *Fuel NY Initiative*, Website. Available at http://stormrecovery.ny.gov/fuel-ny.

There was little open-source information available on the progress or current status of these initiatives. According to an article posted by the New York State Energy Research and Development Authority (NYSERDA) under the Office of the Governor, on July 14, 2014, the State strategic gasoline reserve is operational.[21] Though it will take another declared emergency to fully realize the impacts, these initiatives look to reduce the impacts experienced by New York in the event of another major disaster. The actions New York has taken illustrate the resilience principles of preparedness (policies, planning), mitigation (backup generators), and response (strategic gasoline reserve).

4.2 California—Physical Security

Pacific Gas and Electric (PG&E) suffered two major physical security incidents at their Metcalf Transmission Substation located in San Jose, California. This substation is a critical node that assists in in supplying electric power to the Silicon Valley, headquarters to some of the largest technological corporations in the world (e.g., Intel, Google, Facebook, and SanDisc, to name a few). An extended power outage to this area could lead to wide-ranging economic consequences.

On the morning of April 16, 2013, the Metcalf substation was attacked by gunfire. According to an article released through the *Wall Street Journal,*[22] cross-checked with a security brief from the California Public Utility Commission (CPUC),[23] right before 1 a.m., six AT&T communication fiber-optic lines were cut in an underground vault adjacent to the substation. Approximately half an hour later, security cameras detected muzzle flashes and sparks hitting various high-voltage transformers throughout the yard (see Figure 5[24]). Although fencing and cameras were on site, the cameras were not pointed outside the perimeter of the substation; this enabled the shooter(s) to remain out of sight. The gunshots caused the 17 transformers to discharge approximately 52,000 gallons of

Figure 5: Gunfire Attack Captured on Metcalf Substation Security Camera[24]

[21] New York State Energy Research and Development Authority (NYSERDA), 2014, *NYSERDA Launches New Portable Emergency Generator Program ad State Strategic Gasoline Reserve for Declared Emergencies*, July 14. Available at http://www.nyserda.ny.gov/About/Newsroom/2014-Announcements/2014-07-14-NYSERDA-Launches-New-Portable-Emergency-Generator-Program.

[22] Smith, R.,2014, *Assault on California Power Station Raises Alarm on Potential for Terrorism*, Wall Street Journal, February 5. Available at http://www.wsj.com/articles/SB10001424052702304851104579359141941621778.

[23] Fugere, R., *PG&E Metcalf Incident and Substation Security*, briefing by CPUC Safety and Enforcement Division. Available at http://www.cpuc.ca.gov/uploadedFiles/CPUC_Website/Content/Safety/Presentations_for_Commission_Meeting/SafteySlidesfromPowerPointforthe22714Meeting3331.pdf.

[24] Fernandez, L., 2013, *Surveillance Video Release from Sabotaged PG&E Substation*, NBC Bay Area, June 5. Available at http://www.nbcbayarea.com/news/local/Surveillance-Video-Release-From-Vandalised-PGE-Substation-210248291.html.

oil, which caused the transformers to overheat and shut down. Although power was successfully rerouted around the substation and no customers lost power in the adjacent Silicon Valley area, it cost an estimated $15.4 million to repair the damage.

Slightly over a year later, in the late hours of August 26 into the early hours of August 27, 2014, the Metcalf Substation Construction Yard was burglarized. The suspects cut through the fence and stole approximately $40,000 of construction equipment. Although PG&E was actively working on upgrading security to select substations, including Metcalf, as a result of the April 2013 shootings, there were still several gaps in security and procedures that allowed this burglary to happen. An investigation by the CPUC Security and Enforcement Division (SED)[25] revealed that personnel failed to respond properly to alarms, which were turned off after the completion of a preliminary camera check revealed nothing. The SED acknowledged that although improved physical security measures were place, deficiencies in the security management procedures facilitated the burglary. The following list summarizes the deficiencies discovered in the investigation:[26]

- Lack of accountable training procedure to verify security staff training;
- Lack of a proper preventative maintenance plan for security equipment;
- Insufficient security equipment and monitoring system;
- Absent supervising staff at critical substations (to manage constant patrols);
- Absent security staff inside the substation; and
- Breakdown of communication between on-site officers and control center staff.

In response to the 2013 gunshot incident, PG&E initially invested $100 million toward increasing physical security measures at key substations, one of which was the Metcalf substation. Physical security enhancements included privacy fencing or solid walls and equipment shielding, as well as installation of thermal cameras with enhanced detection analytics, public address systems, improved lighting, and gunshot detection technology.[27] Following the August 2014 burglary incident, PG&E invested another $100 million to provide additional enhancements to critical substations, including additional lighting, more cameras with improved monitoring technology, and enhanced on-site patrols. In 2015, the CPUC required PG&E to submit a revised security management plan that addressed the deficiencies identified in the SED report. PG&E plans to include these costs in their future Transmission Owner rate cases.[28]

[25] California Public Utilities Commission, 2015, *SED Incident Investigation Report on Metcalf Burglary*, Safety and Enforcement Division, August 26. Available at http://www.cpuc.ca.gov/uploadedFiles/CPUC_Public_Website/Content/Safety/Electric_Safety_and_Reliability/Facility_Safety/Citations/Enclosure%201%20-%20SED%20Report%20Redacted.pdf.

[26] Note that some of the deficiencies are vague or omitted due to the nature of the redacted report.

[27] PG&E, 2015, *Citation for Violation of the Public Utilities Code Issued Pursuant to Decision 14-12-001, Enclosure 5 - PG&E Data Response 2 Supplement*, March 20. Available at http://www.cpuc.ca.gov/uploadedFiles/CPUC_Public_Website/Content/Safety/Electric_Safety_and_Reliability/Facility_Safety/Citations/Enclosure%205%20-%20Response%202%20Supplement%20Redacted.pdf.

[28] Ibid.

In addition, the CPUC issued an order instituting rulemaking (OIR) in June 2015[29] to establish policies, procedures, and rules for the regulation of physical security risks to the electric supply facilities of electrical corporations, down to the distribution level. The resulting requirements would build upon the North American Electric Reliability Corporation (NERC) physical security standard for transmission level substations, and could require utilities to consider such measures as hardened perimeters, security guards, intrusion detection, and optimal lighting systems.[30] The actions taken in response to the shooting incident link to the preparedness (procedures and training) and mitigation measures (physical security) principles of resilience.

4.3 Oregon—Earthquake

A Cascadia Subduction Zone earthquake would pose a serious threat to the Pacific Northwest and would have a devastating impacts on Oregon (see Figure 6). As a point of comparison, a 9.0-magnitude subduction zone earthquake occurred in Japan in March 2011. The Japan 2011 earthquake, combined with an associated tsunami, aftershocks, and ground failure, resulted in nearly 22,000 missing or dead people, approximately 4.4 million homes experiencing power outages, and extensive physical damage to the electric infrastructure that took months (or longer) to recover from.[31]

Research indicates that a similar event in Oregon would result in thousands of deaths, damage across critical infrastructure sectors (e.g., transportation, energy, telecommunications, and water/wastewater systems), and economic losses in excess of $30 billion.[32,33] Buildings and lifeline infrastructure systems would be damaged so severely that it could take 3 months to a year to restore full service in the western valleys, more than a year in the hardest-hit coastal areas, and several years in the coastal communities inundated by a resulting tsunami.

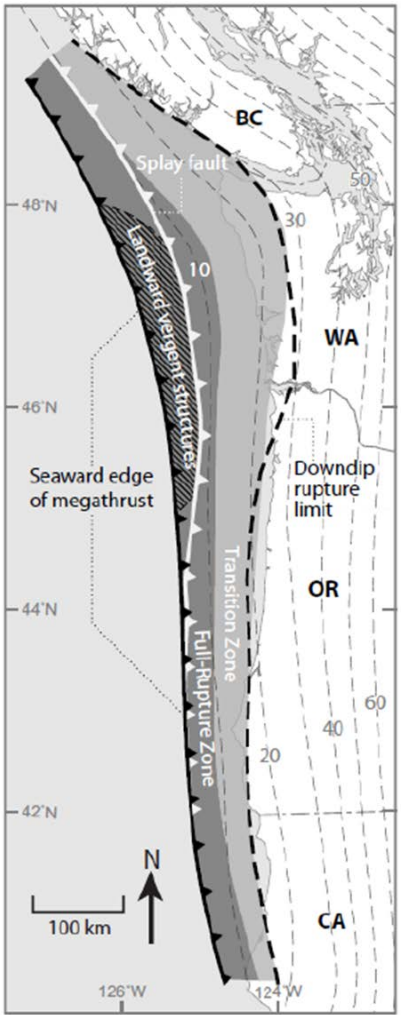

Figure 6: Cascadia Subduction Zone (located between the black dashed line and the white line with triangles)

[29] California Public Utilities Commission, 2015, *Order Instituting Rulemaking to Fulfill the Requirements of Public Utilities Code Sections 364 and 768.6*, June 22. Available at http://docs.cpuc.ca.gov/SearchRes.aspx?docformat=ALL&DocID=152877601.

[30] Ibid.

[31] Kazamaa, M., and T. Noda, 2012, *Damage statistics (Summary of the 2011 off the Pacific Coast of Tohoku Earthquake damage)*, Soils and Foundations 52(5):780–792.

[32] Wang, Y., S.F. Bartlett, and S.B. Miles, 2012, *Earthquake Risk Study for Oregon's Critical Energy Infrastructure Hub*, prepared for Oregon Department of Energy and Oregon Public Utility Commission, August.

[33] OSSPAC (Oregon Seismic Safety Policy Advisory Commission), 2013, *The Oregon Resilience Plan: Reducing Risk and Improving Recovery for the Next Cascadia Earthquake and Tsunami*, Report to the 77th Legislative Assembly, February.

Experience from past disasters has shown that businesses will move or fail if services cannot be restored in 1 month, and Oregon faces a very real threat of permanent population loss and long-term economic decline.

Oregon has undertaken considerable work to address the need for greater resiliency. This has included risk and vulnerability assessments, development of an Energy Assurance Plan (August 2012),[34] and creation of a State Resilience Plan (February 2013).[35] More recently, in 2015, Oregon established a State Resilience Officer position in the Governor's Office. This person is tasked to coordinate and oversee seismic safety and resilience planning and preparation by State agencies. These efforts have laid a strong foundation for the consideration of resiliency in future plans, programs, and initiatives to improve the energy sector.

An Oregon Resilience Task Force was established in 2013 by Senate Bill 33[36] to oversee the implementation of the Oregon Resiliency Plan. In October 2014, the task force presented a report[37] that made recommendations on implementation of the Oregon Resilience Plan to the State Legislative Assembly. For the energy sector, the task force recommended the following:

1. "The OPUC [Oregon Public Utility Commission] require energy providers it regulates conduct seismic assessments of its regulated facilities. Furthermore, we recommend the OPUC allow cost recovery for prudent investments related to assessments and mitigation of vulnerabilities identified during those assessments.

2. "In order to further reduce vulnerability, the State establish a public-private partnership to mitigate and evaluate diversification of locations for storing liquid fuels, and identification of new liquid fuel energy corridors."

This first recommendation provided further support of action by the OPUC, which since 2012 has held regular executive sessions with the OPUC Commissioners and all investor-owned utilities to discuss their progress on seismic vulnerability assessments and mitigation achievements. Actions resulting from the second recommendation were not immediately known. The actions that the State of Oregon has taken to address the potential impacts of a Cascadia Subduction Zone incident reflect the resilience principles of preparedness (planning) and recovery (public-private partnerships allowing for diversification of storage and transportation of liquid fuels).

---

[34] State of Oregon, 2012, *Oregon State Energy Assurance Plan*, Oregon Department of Energy (ODOE) and Oregon Public Utility Commission, August. Available at https://www.oregon.gov/energy/docs/Oregon%20State%20Energy%20Assurance%20Plan%202012.pdf.

[35] Oregon Seismic Safety Policy Advisory Commission (OSSPAC), 2013, *The Oregon Resilience Plan: Reducing Risk and Improving Recovery for the Next Cascadia Earthquake and Tsunami*, Report to the 77th Legislative Assembly, February. Available at http://www.oregon.gov/OMD/OEM/osspac/docs/Oregon_Resilience_Plan_Final.pdf.

[36] 77th Oregon Legislative Assembly, 2013, *Senate Bill 33*. Available at http://www.oregon.gov/OMD/OEM/docs/resilience_tf/SB33.pdf.

[37] Governor's Task Force on Resilience Plan Implementation, 2014, *Senate Bill 33, Implementation of the Oregon Resilience Plan, Report to the 77th Legislative Assembly*, October 1. Available at http://www.oregon.gov/OMD/OEM/docs/resilience_tf/2014%2009%2029%20ORTF%20Report.pdf.

5 Framework for State Energy Resilience

5.1 Concept

Building on the ideas presented in Sections 1 through 4 of this report, this section will discuss the development of a framework for how State and local officials can think about the nature of State energy resilience. A State Energy Resilience Framework is proposed to assist the States in understanding and meeting the primary goals for energy infrastructure: to maintain energy availability to customers and consumers. This framework, illustrated in Figure 7, enables State and local governments, in conjunction with energy utilities, to identify potential vulnerabilities and implement cost-effective and proven resilience enhancement options. It comprises five steps that State and local governments can use and tailor to their individual resilience needs and capabilities.

5.1.1 Step 1: Understand Stakeholders' Needs and Requirements

The resilience of a community and/or region is a function of the resilience of its subsystems, including its critical infrastructures (i.e., financial, utilities, law enforcement, and emergency shelters), economy, civil society, and governance (including emergency services). The number and complexity of these subsystems makes the measurement of resilience more challenging when moving from individual assets/facilities to the community/regional level (where critical infrastructure resilience is only one component). Understanding resilience holistically involves considering all stakeholder needs and requirements when creating policies and regulations for critical infrastructure.

5.1.2 Determine Threat and Hazard Susceptibilities and Vulnerabilities

As stated previously, effective and efficient determination and implementation of resilience options requires a good understanding of the threats, hazards, and vulnerabilities to which energy and other critical infrastructure are exposed. In addition, it is also essential to consider dependencies and interdependencies when analyzing resilience because they can constitute additional sources of vulnerability for critical infrastructure and lead to further consequences, as well as cascading and escalating failures.

Over time, the priorities upon which the different threats and hazards are addressed may change. As processes and procedures mature in relation to a certain threat or hazard (e.g., vegetation management), priorities in resilience enhancement options may shift to emerging or escalating threats and hazards that may cause greater hardship and consequence if they are not addressed.

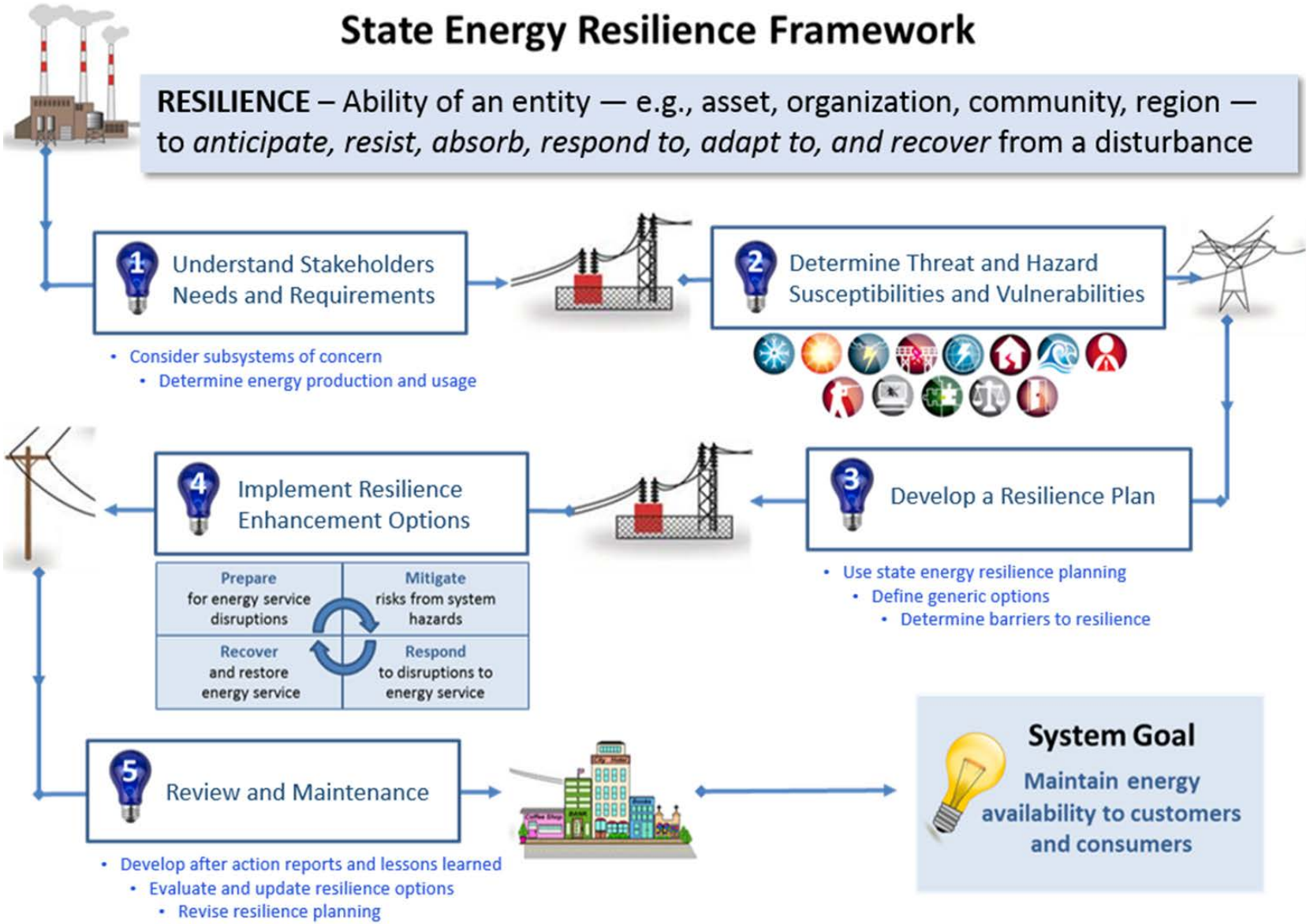

Figure 7: Proposed Five Step State Energy Framework

5.1.3 Develop a Resilience Plan

Developing a plan includes considering energy stakeholders' needs and requirements, as well as the consequences potential hazards may have on the gap between the desired performance of the energy system and its performance following a disruptive event. Addressing the gaps allows State and local governments, in conjunction with energy utilities, to define the generic options that can be implemented to enhance resilience. The following are several State initiatives to integrate energy resilience considerations:

- State energy assurance planning
- State Risk assessment capabilities
- State comprehensive strategic energy plan
- State-regulated utility planning

Resilience planning should also address possible barriers to resilience. Efforts to enhance resilience are often challenging for utilities. Resilience investments can be expensive, and they can require significant capital investment and time to implement. There are also gaps that inhibit resilience enhancement measures, which include uncertainties in global climate change, development of State and local policies and regulations regarding energy infrastructure resilience, and incomplete understanding of the interactions between energy infrastructure and other systems of critical infrastructure.

5.1.4 Implement Resilience Enhancement Options

Some States have already taken steps to increase the resilience of their energy infrastructure through legislation, and through regulatory and planning efforts. Many critical infrastructure sectors, including the energy sector, utilize resilience enhancements options as part of normal operations. Implementing resilience enhancement requires cooperation and buy-in from all players, from energy customers, to utilities, to State and local governments. These options can take significant time and capital investment, the impact of which may not immediately be realized. It is critical that State officials and regulatory bodies be aware of these properties of resilience enhancement options and work with utilities to identify mechanisms to implement appropriate options. Together, these entities will have to develop criteria upon which to evaluate different resilience alternatives, so that those alternatives can be compared and contrasted in a consistent, repeatable, and transparent manner. Criteria development can be challenging, because different entities typically have different, sometimes conflicting, goals. It is helpful if an outside party can assist the vested entities in identifying different goals, as well as common criteria upon which to capture success in meeting those goals and by which to measure alternatives.

5.1.5 Review and Maintenance

Resilience assessment is an iterative process (Figure 8) that requires existing resilience gaps and potential resilience enhancement options to be regularly reviewed and updated. Commonly, AARs are generated after disruptive events or exercises. The lessons learned in these AARs can

inform future iterations of the resilience plan. It is critical to maintain and exercise the plan regularly to ensure all entities are prepared for incidents and have the ability to bring the system back online as soon as possible.

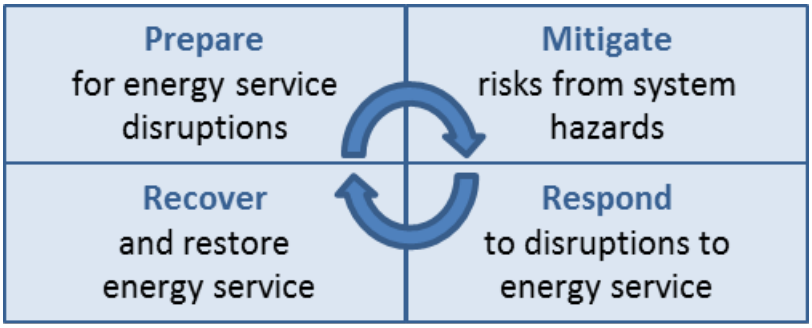

Figure 8: Resilience as an Iterative Process

The proposed framework outlined in this report provides State officials a mechanism upon which to begin or enhance discussions with energy infrastructure owners and operators within their State.

6 Conclusions

The increasing frequency of severe weather events; uncertainty in changes to the climate and their implications; and the possibility of energy infrastructure interruptions due to malicious actors have highlighted the need for increasingly resilient energy infrastructure. Aspects of what resilience enhancements to implement and how to implement them be confusing and conflicting for stakeholders. In addition, resilience options can be expensive, can take a long time to incorporate, and can have difficult-to-quantify benefits. States have started to implement measures for energy resilience such as creating State energy assurance plans and State strategic energy plans. State regulatory entities have begun working with States and utilities to implement regulatory structures that are favorable to resilience enhancements. The case studies provided in this document point toward only few of the different resilience options that are available. National organizations and associations such as National Association of State Energy Officials (NASEO), National Association of Regulatory Utility Commissioners (NARUC), National Governors Association (NGA), National Conference of State Legislatures (NSCL), and National Electrical Manufacturers Association (NEMA) have dedicated significant time and effort to establishing programs, workshops, exercises, webinars, training, model plans, guidance, and other technical assistances for States. State resilience framework will provide State officials with a better understanding of the energy infrastructure within the State, the hazards these infrastructures are susceptible to, and a method for addressing and implementing the wide variety of available resilience enhancement options.

Appendix A—States' Progress in Energy Resilience Planning

Since 1980, the United States has sustained 144 weather disasters whose damage costs reached or exceeded $1 billion. Seven of the 10 costliest storms in U.S. history occurred between 2004 and 2012.[38] Current efforts to address risk from these naturally occurring hazards or incidents, in addition to risk from deliberate attacks or accidents, stem from Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (PPD-21),[39] signed in February 2013. This order states in part:

> *It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT [State, local, Tribal, and territorial] entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.*

States have roles in supporting the public and private partnerships that work to enhance the resilience of their energy infrastructure; it is clearly in the public interest to do so. The loss or failure of critical energy infrastructure can have enormous economic and human consequences, as we have seen historically. For example, on August 14, 2003, 50 million people lost power for up to 2 days in the biggest blackout in North American history. The event contributed to at least 11 deaths and cost an estimated $6 billion.[40]

A.1 State Energy Assurance Planning

A major effort began when funding from the U.S. Department of Energy (DOE), Office of Electricity Delivery and Energy Reliability (OE) was made available to States and local governments to support a State Energy Assurance Planning (EAP) initiative. Grants awarded under this initiative totaled $38 million and were issued in 2009 and 2010 to 48 States, 2 territories, and 43 cities. The grants were used over a 3- to 4-year period to improve energy emergency preparedness plans and to enable quick recovery and restoration from any energy supply disruption. States also used the funds to address energy supply disruption risks and

[38] The White House, 2013, *The Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, Council of Economic Advisers and the U.S. Department of Energy, August 12. Available at http://energy.gov/articles/white-house-council-economic-advisers-and-energy-department-release-new-report-resiliency.

[39] The White House, 2013, *Presidential Policy Directive – Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD-21, Office of the Press Secretary, February 12. Available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[40] Minkel, J.R., 2008, *The 2003 Northeast Blackout--Five Years Later*, Scientific American, August 13. Available at http://www.scientificamerican.com/article/2003-blackout-five-years-later/

vulnerabilities, with the aim of mitigating the devastating impacts that such incidents can have on the economy and on public health and safety.

State energy agencies typically had a lead role for this work, which included State Energy Offices and Public Utility Commissions. The EAP initiative also required that they coordinate with the State emergency management and Homeland Security agencies so the plans complemented the overall State disaster plans and plans for protecting critical infrastructure.

Each State under the EAP initiative was required to track energy emergencies, to assess the restoration and recovery times of any supply disruptions, to train appropriate personnel on energy infrastructure and supply systems, and to participate in State and regional energy emergency exercises that were used to evaluate the effectiveness of their energy assurance plans. States were also required to address cybersecurity concerns and to prepare for the challenges of integrating smart-grid technologies and renewable energy sources into their plans. As a result of the initiative, nearly all States, territories, and select local governments have in place EAPs that have improved the speed and quality of their response capabilities and led to investments that have made the energy sector more resilient. A review of the State EAP was recommended (by NASEO) to occur every 2 to 3 years, and to date some States have undertaken update efforts.[41]

A.2 State Risk Assessment Capabilities

The DOE's Office of Electricity Delivery, Energy Reliability, Energy Infrastructure Modeling and Analysis Division established a State Energy Risk Assessment Working Group comprised of representatives from 19 State energy agencies. This group has been working since December of 2014 to define needs and capabilities to improve States' ability to quantify risk. One of the products of this effort was the developments of State and Regional Energy Risk Profiles that examine the relative magnitude of risks at a regional and State level, highlighting energy infrastructure trends and impacts. The profiles present both natural and man-made threats and hazards with the potential to disrupt the electric, petroleum, and natural gas infrastructures. A second product currently under development is a web-based Energy Risk Resource Library that will provide a comprehensive listing of data, analysis, tools, models, and studies on energy sector risk analysis. This analysis is an important planning tool that will allow States, in conjunction with energy utilities, to more clearly understand, and quantify where possible, the risk reductions that can result from resiliency investments.

A.3 State Comprehensive Strategic Energy Plan

EAPs are not the only way States have worked to achieve resilience. Nearly all States have at some point developed or updated a longer-term State comprehensive strategic energy plan. These plans look at current and future energy needs, emerging trends, and the changing economics of

[41] National Association of State Energy Officials (NASEO), 2009, *State Energy Assurance Guidelines*, v3.1, December. Available at https://www.naseo.org/data/sites/1/documents/publications/State_Energy_Assurance_Guidelines_Version_3.1.pdf

technologies. The strategic plans identify options for meeting future energy needs in ways that provide multiple social benefits, including risk reductions, enhanced resiliency, enhanced reliability, improved efficiency and energy cost savings, job creation, economic development opportunities, and improvements in environmental quality. These plans have brought about legislative changes, and generated new programs, policies, and initiatives that have spurred innovations and accelerated the adoption of new technologies and practices to the benefits of the State and nation.[42] Some of these plans may be focused on a single objective function such as environmental or economic benefit, but actions taken can contribute to resiliency even when that is not the principal objective.

A.4 State Regulated Utility Planning

On the regulatory side, State Public Utility Commissions (PUCs) work to address costs, reliability, resiliency, rates, and environmental impacts. In recent years, there has been an increased focus on cybersecurity and the risk cyber threats pose to the power grid. As a result, a number of regulatory actions have encouraged resiliency, security, and reliability through a variety of approaches including cost recovery. In recent years, a number of States began or resumed work on utility Integrated Resource Plans (IRPs). These plans use an approach that considers risk and scenario analysis to examine the comparative effects of different decision outcomes. This risk analysis helps to quantify consequences and vulnerabilities under a range of threats and hazards and then measures the combined total cost of the future plan against the benefits. The mission of PUCs can generally be described as ensuring the establishment and maintenance of utility services as required by State law, and ensuring that these services are provided at rates and conditions that are fair, reasonable, and nondiscriminatory for all customers.[43]

As shown in these examples, States have a strong and inherent self interest in addressing energy sector risks and have, in many instances, taken actions to reduce these risk and build resiliency. Section 4 of this report provides more concrete examples of how this work has been undertaken by some State governments.

A.5 Support from National Organizations and Associations

At a national level, there has been strong historical support for State energy assurance efforts, including energy emergency response and resiliency enhancements to reduce the risk from all hazards. Support and leadership, from the DOE's Office of Electricity Delivery, Energy Reliability, Infrastructure Security and Energy Restoration (ISER) Division, have been consistent and sustained for well over 10 years. During this time, ISER has provided resources to the National Association of State Energy Officials (NASEO), National Association of Regulatory

[42] National Association of State Energy Officials (NASEO), 2013, *An Overview of Statewide Comprehensive Energy Plans from 2002-2001*, July. Available at https://www.naseo.org/Data/Sites/1/naseo_39_state_final_7-19-13.pdf.

[43] National Association of Regulatory Utility Commissioners, 2016, *About NARUC*, Website. Available at https://www.naruc.org/about-naruc/about-naruc/

Utility Commissioners (NARUC), National Governors Association (NGA), National Conference of State legislators (NCSL), and more recently, the National Emergency Management Association (NEMA) in support of energy assurance efforts at the State level. Working together in a coordinated and complementary way, these organizations have undertaken numerous initiatives over many years that have helped build and sustain States' capabilities, thus reducing the human and economic impacts of energy supply disruptions.

NASEO, NARUC, NGA, and NCSL have conducted a number of programs, workshops, exercises, webinars, and training, and have provided model plans, guidance, and other technical assistance for States over many years.[44] These efforts have resulted in better response plans, greater understanding of risks, and increased the ability to assess the scope, duration, and consequences of energy disruption. This support has also resulted in longer-range State energy plans, policies, legislation, incentives, and programs that have increased the resiliency of the States' and nation's energy infrastructure.

These associations have also helped to identify needs and set priorities for the energy sector though various committee and working groups. For instance, since its inception in 1989, NASEO has had an Energy Security Committee that provides a forum for discussing energy data collection and analysis issues and energy assurance.[45] Following the September 11, 2001, terrorist attacks, NARUC established a permanent Committee on Critical Infrastructure, which provides State regulators a forum to analyze solutions to utility infrastructure security and delivery concerns.[46] In addition, NASEO and NARUC serve on the Government Coordination Council (GCC), which meets with the Electric and Oil and Gas Sector Coordinating Councils, as established under the National Infrastructure Production Plan (NIPP). NGA includes the Governors Homeland Security Advisors Council, which provides organizational structure through which the homeland security advisors can discuss issues, share information and expertise, and keep governors informed of the issues affecting homeland security policies in various States.[47] NGA also includes the Governors' Energy Advisors Policy Institute, which provides an opportunity for governors' State energy advisors to examine a comprehensive suite

[44] For additional information on these activities, see: State Energy Assurance Guidelines (available at http://www.naseo.org/eaguidelines); National Petroleum Council Enhancing Emergency Preparedness for Natural Disasters Government and Oil and Natural Gas Industry Actions to Prepare, Respond, and Recover, Appendix C: After-Action Report Summary (available at http://www.npc.org/reports/2014-Emergency_Preparedness-lr.pdf); Resilience in Regulated Utilities (available at http://pubs.naruc.org/pub/536F07E4-2354-D714-5153-7A80198A436D); Resilience for Black Sky Days (available at http://pubs.naruc.org/pub/536F42EE-2354-D714-518F-EC79033665CD); and Regional Mutual Assistance Groups – A Primer (available at http://pubs.naruc.org/pub/536E475E-2354-D714-5130-C13478337428).

[45] National Association of State Energy Officials, 2016, *Energy Security Committee*, Website. Available at http://www.naseo.org/committee-energy-security.

[46] National Association of Regulatory Utility Commissioners, 2016, *Committee on Critical Infrastructure*, Website. Available at http://members.naruc.org/4DCGI/committees/committeeroles.html?Action=naruc&naruc_Activity=CommitteeandRole&CommCode=NARUC109.

[47] Nationals Governors Association, 2016, *Governors Homeland Security Advisors Council*, Website. Available at http://www.nga.org/cms/ghsac.

of energy policy best practices with State peers, as well as private sector and Federal experts.[48] NCSL has published numerous reports highlighting State legislative efforts on energy risk and assurance. It has also developed webinars and hosted several meetings designed to educate and inform State legislators, so they can make informed policy decisions that improve resiliency. Furthermore, the associations have regularly coordinated conference calls to discuss current efforts and initiatives in support of energy assurance. As a result of all of these different groups, the level of expertise that can be leveraged to address energy assurance issues, combined with the links to the association's membership base, provides significant support to State actions and functions as a major component of the State resiliency framework.

[48] Nationals Governors Association, 2016, *Governors' Energy Advisors Policy Institute*, May 31. http://www.nga.org/cms/home/nga-center-for-best-practices/meeting--webcast-materials/page-eet-meetings-webcasts/col2-content/main-content-list/governors-energy-advisors.html.

Appendix B—Further Resilience Enhancement Options

This appendix expands upon different resilience options for each of the four subcategories presented in Section 2 of this report. This list is not exhaustive, but some of these options are applicable for all energy infrastructure, and some for all critical infrastructure.

B.1 Preparedness—Awareness and Planning

B.1.1 Awareness

- Information Sharing
- Communication and Notification
- Coordination
- Collaboration

B.1.2 Planning

- State Energy Assurance Planning and Preparedness
- Business Continuity Planning (BCP)
- Business Resilience Strategy Planning (BRSP)
- Continuity of Operations
- Continuity of Government (COG) Essential Operations
- Enterprise Risk Management (ERM)
- Emergency Operations/Emergency Action Planning
- Supply Chain Resilience Planning
- Cybersecurity and Resilience
- Supply Management
- Resource Management
- Procurement Procedures/Agreements
- Preventive Maintenance Plans (e.g., scheduled, condition based, site inspection, routine data collection and analysis)
- Evacuation Exemptions
- Regularly Scheduled Plan Reviews and Updates

There are crucial components of planning, which include training, updating, and exercising of the plans. A few options are described below.

- Workforce Development
  - Training to Maintain the Institutional Knowledge
  - Personnel Education and Training
  - Cybersecurity and Social Engineering Awareness

- Exercise and Simulations
  - Exercises and Simulations to Test Plans (e.g., tabletop, drill)
  - Bring Stakeholders Together
  - Sustaining Capabilities
  - Intra-State and Multi-State Regional Exercises
  - Exercise After-Action Reports

B.2 Mitigation Measures

- Cyber- and Physical Security
  - Barriers and Fences (e.g., bullet-proof walls, reinforced buildings)
  - Intrusion Detection
  - IT System Backup and Disaster Recovery
- Electronic Security
  - Detection and Deterrence Measures (e.g., cameras, sensors)
  - Role-Based Access Controls and Policies
- Hardening, Strengthening, and Retrofitting Measures
  - Wind Protection
  - Flood Protection
- Robustness and Reliability Measures
  - Backup Capabilities
  - Redundant Systems (e.g., communications)
  - Supply Chain Resiliency
- Technology
  - Supervisory Control and Data Acquisition (SCADA) Systems
  - Substation Automation
  - Automated Mapping and Facilities Management
  - Geographic Information Systems (GIS)
  - Distributed/Cogeneration Generation Systems

B.3 Response

B.3.1 Activities

- Incident Management and Command Center (deployable)
- Situational and Consequence Assessment Capabilities and Tools
- Emergency Operations Center

B.3.2 Equipment

- Systems Supporting Response
  - SCADA Systems
  - Distribution Management System(s) (DMS)
  - Outage Management Systems
- Backup and Alternative
  - Backup/Alternate Control Center
  - Portable Generators
  - Mobile Options

B.3.3 Agreements

- Service Level and Supply Dependency Agreements
  - Emergency Fuel Contracts
- First Preventers/Responders Agreements (including public works department)
  - Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA)
  - Interoperable Communication
  - Participation in Mutual Assistance Groups
- Contractual Arrangements to Receive/Share Equipment and Crews
- Mutual Aid Approach for Potential Cyber Attack

B.4 Recovery

B.4.1 Activities

- Participation in Provider Priority Plan For Restoration

B.4.2 Equipment

- Access to Specialized Materials (e.g., large power transformers)
- Strategic Transformers Reserves
- Cyber Security and Resilience (e.g., disaster recovery capabilities—hot swap servers remote storage of system images and data backup, etc., for critical information technology systems)

Global Security Sciences Division
9700 South Cass Avenue, Bldg. 221
Argonne, IL 60439-4854

www.anl.gov

Argonne National Laboratory is a U.S. Department of Energy
laboratory managed by UChicago Argonne, LLC