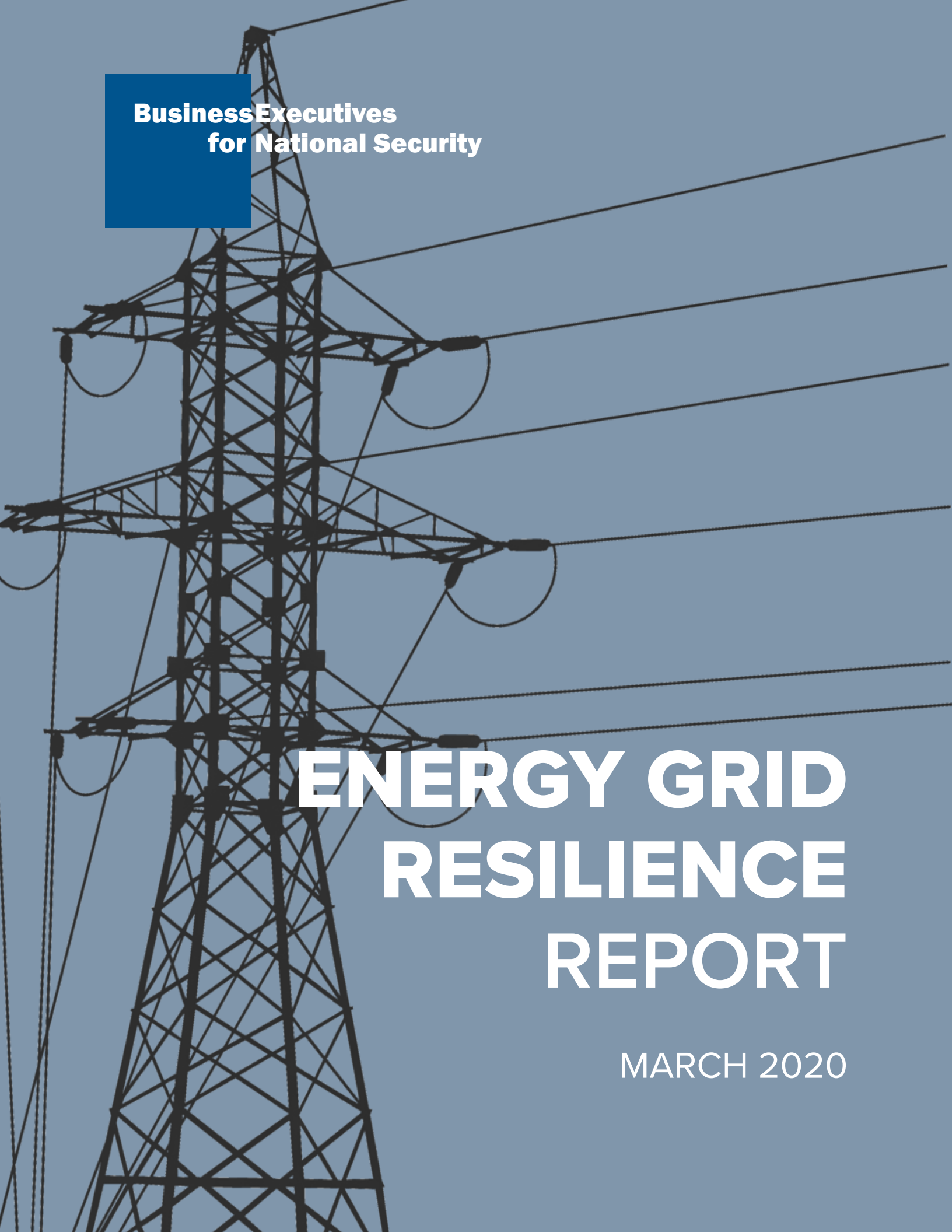


Business Executives for National Security

ENERGY GRID RESILIENCE REPORT

MARCH 2020

Executive Summary

U.S. national security and commerce depend on the uninterrupted flow of electricity delivered through the electric grid (the grid). The grid is a highly complex, interconnected network that produces and delivers power to all sectors of society, including homes, businesses, and critical infrastructure sectors such as first responders, airports, and military installations.

This essential function of the grid is under increasing risk from man-made and natural threats, including cyber and physical attacks, natural disasters, and electromagnetic pulse/geomagnetic disturbance. States and utility companies are at the front lines of ensuring grid resilience against these threats. The growing complexity and interconnectedness of the electric grid, the emerging risk landscape, and the practical limitations of private companies to address certain risks, however, underscore for the public and the private sectors the need to collaborate to ensure overall grid resiliency. These actions will ultimately be needed to ensure the grid is safe and resilient, which is critical to safeguard U.S. national security.

In this context, key grid stakeholders have illustrated the important roles public-private partnerships can play to secure the grid. In the course of assessing the increasing risk to the U.S. grid from man-made and natural threats, the Business Executives for National Security's (BENS) Energy Council[1] determined that it would be wise to examine how state-level public-private partnerships are structured to secure the grid and maximize enhanced grid resiliency and security. States are often at the nexus of grid resilience efforts because: 1.) they regulate or manage utilities that operate at the state and local level; 2.) they implement regulations and guidance from federal and supranational bodies; and 3.) they are a logical point of connection for private sector actors. The several states highlighted – California, Florida, Illinois, Maryland, New Jersey, New York, and Texas – illustrate forward leaning approaches that address/enhance grid security.

This assessment identified four state-level approaches that are important for grid resiliency, and if practiced across the country would lead to a more resilient national grid:

1. **Identify threats/info-sharing:** Examine trends to identify emerging threats to the energy grid and participate with industry to facilitate timely mutual sharing of threat information to protect critical infrastructure and key resources;

2. **Funding/key technologies:** Identify available funding mechanisms at the local, state, and federal levels, leverage private investment for infrastructure development, and accelerate the development of key commercial technologies that mitigate those risks and modernize the grid;

3. **Preparedness planning:** Develop emergency preparedness and crisis management plans, regularly exercise and plan/test for multiple scenarios, and ensure coordination between government and utilities by integrating staff within emergency response centers; and

4. **Cybersecurity strategy:** Develop a formalized strategy to prepare for and respond to cyber-attacks and system intrusions and work with government partners on supply chain challenges. Train a cybersecurity workforce to operate effectively within the cyber threat environment, and require cyber workshops and exercises for key personnel to advance collective awareness of cyber vulnerabilities.

Table of Contents

Introduction

On July 13, 2019, a power failure plunged a stretch of the West Side of Manhattan into darkness, trapping people in subway cars and elevators across boroughs for extended periods of time. Failed traffic signals left drivers to fend for themselves at intersections and challenged emergency response personnel to respond to calls for assistance.[2]

This was not the first nor the most severe blackout to hit NYC; another affected the entire city on the same date in 1977, and yet another struck in the summer of 2003. The causes vary: a transformer fire caused the 2019 outage; the 1977 event resulted from a series of lightning strikes; and a remote software error caused the blackout in 2003.

Such disruptions are not unique to New York City and its particular electric grid. In 2018, Hurricane Michael's 155 mile per hour winds hit the Florida panhandle, knocking out power to approximately 2.5 million customers across the southeast United States.[3] A March 2019 digital attack interfered with electrical grid operations of a utility company that serves parts of California, Utah, and Wyoming.[4]

The uninterrupted delivery of electricity is a pillar of U.S. national security. Disruptions to the electricity system carry security, health and safety, and economic consequences at an estimated annual cost to the United States of $18-70 billion. Severe weather-related outages are primary cost drivers.[5] The U.S. government forecasts that the number of future outages will increase. Changing weather patterns and the increasing frequency of severe weather events are the leading causes. Other factors include deferred maintenance, increased demand, and threats from hostile actors that may seek to damage grid operations through cyber, physical, or electromagnetic pulse (EMP) attacks.[6]

Background and Context

The de-centralized character of the electric grid, with public and private owners/operators, government regulators at the local, state, and federal levels, and supply chain vendors, requires collaboration among key grid stakeholders to maximize grid resiliency. This cooperation can often take the form of a public-private partnership, where public and private sector entities/ stakeholders pool resources, expertise, and/or personnel for specific projects with public benefit. The U.S. National Electric Grid Security and Resilience Action Plan recognizes the role of public private partnerships in enhancing grid resilience. It notes the federal government will work through such partnerships to address grid vulnerabilities.[7] The cases examined in this study illustrate how state-level public and private grid stakeholders have cooperated to help share information, leverage resources, and coordinate action to strengthen and protect the U.S. electric grid.

No single pathway exists to address current and future grid vulnerabilities because the threats are diverse. Moreover, the grid cannot be made invulnerable to all threats. The U.S. government's emphasis on resiliency stems from a recognition that not all risks can be avoided. Electricity delivery must continue despite events that will inevitably damage the grid.

This diverse set of threats has led utilities to take a risk management approach to determine where to invest their resources to secure the grid. Such risk management involves weighing the likelihood of events occurring, the scale of their consequences, and the value of investments made to enhance resilience. High-likelihood, high-consequence risks, such as severe weather events, have been the key drivers for investments and stringent regulatory standards.[8] Utilities have also developed standard practices to respond and recover from "routine," or high-likelihood low-consequence events. Low-probability high-consequence events such as an EMP from a nuclear weapon are difficult to factor into risk management strategies. There are few, or no, examples from which to draw lessons. There is no way to anticipate them. So it is challenging to determine what resources to allocate to address them. For these reasons, such risks are often handled through an "all-hazards" approach to security and resiliency where steps are taken that can help avoid or mitigate damage from a range of events.[9]

Specific initiatives in seven states – California, Florida, Illinois, Maryland, New Jersey, New York, and Texas – provide examples of forward leaning efforts of public and private sector cooperation for grid resilience. Each state-based case exhibits forward leaning approaches to maximize grid resiliency, including advanced grid planning, investment in distributed energy, strengthening cyber standards, workforce development, emergency exercises, and establishing formalized information sharing architectures. In combination, their efforts demonstrate smart approaches available to utilities and other key stakeholders to enhance overall grid security.

Key Takeaways & Case Studies

1 **Identify threats/info-sharing:** Examine trends to identify emerging threats to the energy grid and participate in industry collaboration to facilitate timely, mutual sharing of threat information to protect critical infrastructure and key resources. **New York and Texas**

EXAMINE TRENDS, ASSESS RISK, SHARE INFORMATION

Assessing the nature of threats facing the grid, and how vulnerable grid systems are to them, is an important first step for all stakeholders. Owners/operators are responsible, and uniquely positioned, to manage risk to their operations and assets. They must make making risk-informed decisions about where to allocate resources to enhance resilience and security. Strengthening grid security and resilience depends upon them.[10] Assessing risk, which includes analyzing costs, value, and related benefits, is an ongoing task. It must be performed regularly. Situational awareness of the conditions of grid assets and the threats facing them, in real time, can be vital for understanding and addressing vulnerabilities before damage can occur.

"Situational awareness of the conditions of grid assets and the threats facing them, in real time, can be vital for understanding and addressing vulnerabilities before damage can occur."

A strong threat information sharing architecture is also required for maintaining overall grid resiliency. The multi-stakeholder system of grid maintenance, operations, and regulations means that owners and operators are joined by many others receiving information regarding threats. Collaborative efforts between the public and private sectors, as well as subject matter experts in academia and/or national laboratories, can be helpful in ensuring all stakeholders have a better picture of the range of threats, including the probability and consequences of occurrence. Such information sharing may require formalized agreements, or legislative structures, to allow for such a two-way flow of information. For example, most states have exempted information on critical energy infrastructure from certain open government laws, ensuring such information remains protected even while it is shared between industry and government. Federal agencies can also share declassified intelligence regarding threats to the grid or provide classified briefings to cleared individuals in the public and private energy sectors.

New York | Integrated Smart Operations Center (iSOC)

New York State's Integrated Smart Operations Center (iSOC) involves the state's public power utility partnering with a private company to develop technology contributing to grid resilience.

New York launched the iSOC in 2017 to analyze the performance of power generation assets and the statewide network of transmission lines. This real time data monitoring system is meant to identify grid-related problems before they occur, prevent potential service outages, and reduce repair and replacement costs. The New York Power Authority (NYPA) established this system through a long-term agreement with a private sector partner, which developed and provided predictive, diagnostic software that analyzes data gathered from roughly 24,000 sensors throughout state's power grid. The software assesses the real time performance of equipment and compares it to an idealized performance model generated from the manufacturer's performance claims. Anomalies raised by the analysis are flagged for specialists staffing the iSOC, which then determine whether the issue merits follow up with the asset owner. NYPA intends to continue to build on the sensor network in phases, with the first phase completed at a cost of roughly $9 million. A second phase began in 2018 to expand the sensor network beyond power generation and transmission assets, and a third phase is intended to deploy advanced sensors using technology still being developed. The total program cost is estimated at $100 million.

The effort has been part of NYPA's plans to become the world's first "fully digital utility," a central feature of which is the collection and analysis of large amounts of data in real time. Such digitization is expected to become the norm for efforts to modernize grid operations across the industry. This digitization, however, can increase vulnerabilities to hostile cyber actors. While the iSOC's digital systems are restricted to monitoring functions and cannot be used to affect grid operations, the data collected is still sensitive and must be protected. To address cyber threats, the iSOC houses cybersecurity personnel as part of its monitoring functions.

Texas | Grid Resilience Working Group

The Texas Grid Resilience Working Group is an example of a state-level body formed with representatives from public and private grid stakeholders to evaluate and share information regarding threats to the grid.

The Electric Reliability Council of Texas (ERCOT)[11] established the working group in 2016 to assess and share information regarding low probability, high consequence risks to the grid. The working group was formed specifically to address the issues raised in a 2010 report by the North American Electric Reliability Corporation (NERC)[12] that identified pandemic illness, coordinated cyber and/or physical attacks, EMP from a high altitude nuclear weapon detonation, and geomagnetic disturbances as low probability occurrences that could have major cascading effects on the U.S. power grid.[13] Low-probability, high-consequence events are difficult to prepare for and can impact multiple utilities, sectors, and regions over a long period of time. As the NERC report details, industry is "heavily reliant" on information from the public sector for these types of risks, making formalized information sharing mechanisms such as the working group important for evaluating risks and prioritizing mitigation strategies.[14]

Participation in the working group includes a mix of public and private grid stakeholders, including industry, consumers, and state government representatives. While the meetings are open to anyone, they include closed sessions for more sensitive topics such as specific mitigation measures and receiving threat briefings from government agencies. Meetings are held on a periodic basis as determined by the chair, an ERCOT representative.

The working group determined that its initial focus would be the threat from an EMP because the NERC has not promulgated standards to protect grid elements from such an event, as it has for geomagnetic disturbances. As noted above, the EMP threat is an example of a low-likelihood high-consequence event that can be difficult to factor into risk management strategies. In addition to learning more about the nature of the threat, the working group was tasked with examining current practices to harden equipment from an EMP, feasibility of additional protective measures, and recovery plans. The group sought input from national authorities such as the Federal Bureau of Investigation (FBI) on the nature of the threat, as well as the Electric Power Research Institute (EPRI), which undertook a major technical study with the support of U.S. national labs assessing the potential impact of a high-altitude EMP. The results of that study, released in April 2019, determined that such an EMP attack would have severe regional effect on the bulk power system but "because damage to large power-transformers is expected to be minimal, recovery times following a (high altitude EMP)-induced blackout would be expected to be commensurate with historical large-scale blackouts."[15]

2 **Funding/technology:** Identify available funding mechanisms at the local, state, and federal levels, leverage private investment for infrastructure development, and accelerate the development of key commercial technologies that mitigate those risks and modernize the grid. **New Jersey, Florida, and Maryland**

IDENTIFY FUNDING & INVEST IN TECHNOLOGIES FOR MITIGATION AND RESILIENCE

Efforts to modernize and build resilience into the grid can be capital-intensive, including future operations and maintenance costs. Grid stakeholders need to account for how the cost of grid upgrades are structured. California, Illinois, and Maryland state regulators have denied requests from their respective utilities to modernize grid operations or develop microgrids[16] due to concerns over costs (including plans to recoup those costs from consumers), and/or the possibility of decreasing overall market competitiveness. Developing models that leverage public and private funds for modernization and construction, including for advanced grid planning such as microgrids, has been an alternative and preferred approach for some state officials, utility owner/operators, and the private sector to address concerns in leveraging private funding for public benefit. Sources of capital through special funding and grants generally provide only partial funding for modernization projects. The public and private sectors will need to work together to determine how private capital can support grid modernization efforts, including how the costs of grid modernization efforts are structured and absorbed by ratepayers.

When appropriate funding mechanisms are identified, grid modernization efforts can assist in building grid resiliency through faster responses to outages and/or providing alternative sources of electricity generation during grid failure. Grid modernization efforts have typically involved two types of technologies: smart grid technology and microgrids.

New Jersey | Energy Resilience Bank

The New Jersey Energy Resilience Bank was the first public bank in the country devoted to funding energy resilience. New Jersey established the Energy Resilience Bank in 2014 in the wake of its experience with Hurricane Sandy in 2012. The bank offered $200 million in grants and loans to develop resilient energy generating capabilities, including Distributed Energy Resources (DERs)[17] and microgrids that serve critical facilities such as hospitals and water treatment facilities. The $200 million was drawn from a federal Housing and Urban Development (HUD) grant the state received to recover from Hurricane Sandy and develop long-term energy resilience against future storms. Projects eligible for funding had to apply to facilities that were directly or indirectly affected by Hurricane Sandy or any of the nationally-declared disasters dating back from December 2010.

"New Jersey established the Energy Resilience Bank in 2014 in the wake of its experience with Hurricane Sandy in 2012."

The bank faced several challenges during its first year of operations, which prevented proposals from being agreed upon and approved. To address these challenges, the bank took steps to streamline its operations in 2015. It loosened some of its proposal criteria in 2016, including opening up to private utilities and businesses that did not meet Small Business Association (SBA) criteria for a small business, expanding its focus beyond water treatment and supply facilities, and providing 100 percent of unmet need funding for projects by non-for-profit and public applicants. These changes allowed an initial round of $65 million to fund projects at two hospitals and two water treatment plants. A second round of funding begun in 2016 saw several hospital projects selected to receive up to $135 million in funds.

SMART GRID DEPLOYMENT

Florida | Energy Smart Florida Project

Energy Smart Florida is a case of a private utility whose plans for modernizing the grid were accelerated and bolstered by federal funding directed towards grid modernization projects. This led to the deployment of one of the first comprehensive smart grids in the country.

Energy Smart Florida was a four-year, $800 million project by Florida Power & Light (FPL) to deploy advanced smart meters and monitoring equipment throughout the utility's transmission system. It was completed in 2013. Smart grid technology comprises digital communications, sensing, metering, and control equipment that provide utilities with more accurate real-time information regarding electricity delivery and consumption. It also includes automated response capabilities for equipment damage and outages. The effort leveraged nearly $200 million in federal Department of Energy (DOE) grant funding for smart grid development, with the remaining funds covered by FPL. Prior to receiving federal funding, FPL had a more limited plan to incrementally install smart grid technology, focusing on smart meter installation for customers. With funding from the DOE smart grid grant, FPL revised its plans to

take a more holistic approach to phasing in smart technologies for a broader set of functions, including communications infrastructure deployment, and diagnostic center development.

While one of the primary benefits from smart grid technology is the cost savings from tying power distribution closer to actual demand through automated demand response systems, smart grids also improve equipment monitoring capabilities, allowing the detection of equipment problems prior to costly equipment failures and associated outages. According to the DOE, the upgrades have helped to prevent outages by allowing the utility to isolate specific defective equipment and divert energy to customers from fully functional systems.[18]

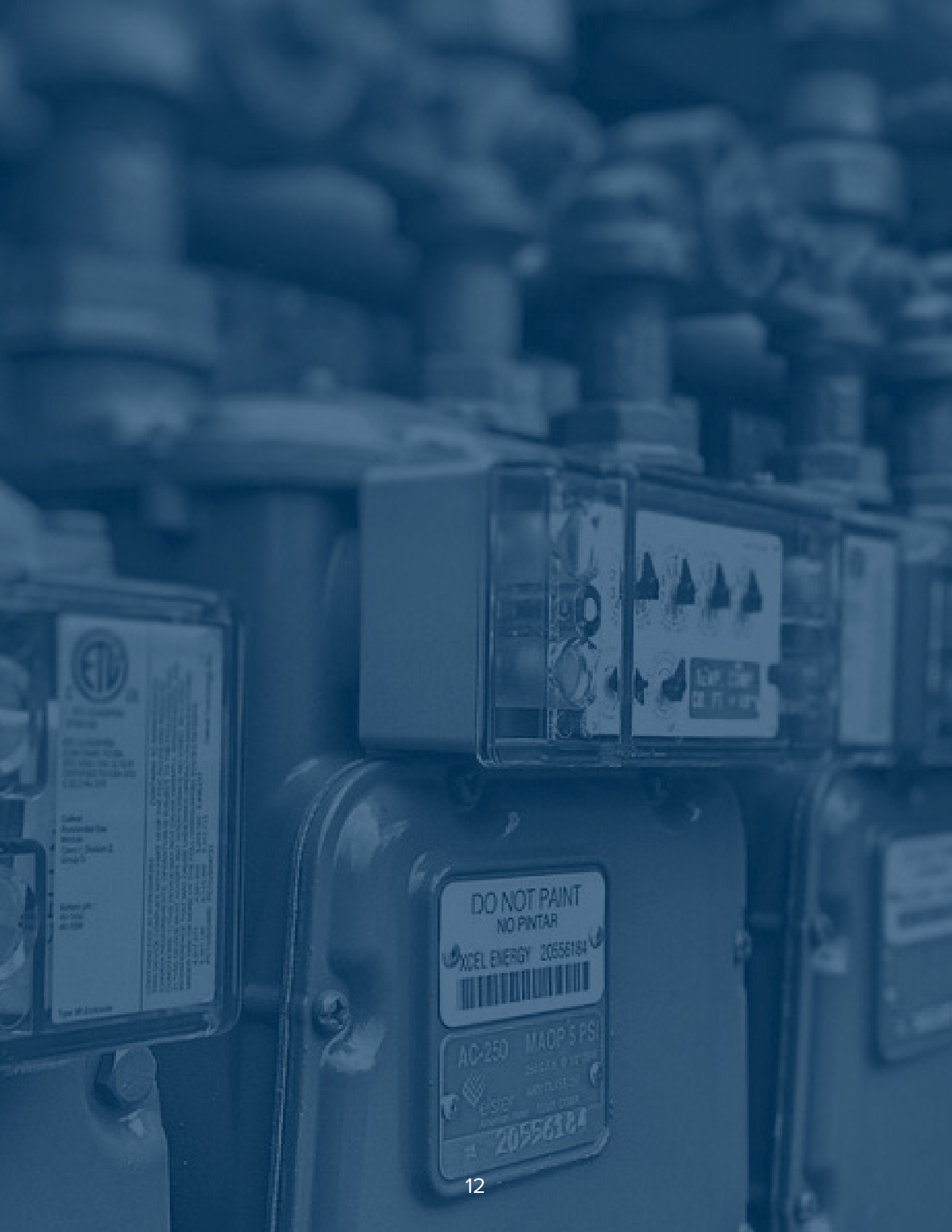
MICROGRID DEPLOYMENT

Maryland | Public Purpose Microgrids

Maryland's public purpose microgrids are an example of a state partnering with private energy firms to construct microgrids providing energy resiliency for critical public facilities. The effort came as the state promoted such public purpose microgrid development but struggled to approve proposals by utilities which sought to recoup costs through rate increases.

The Maryland Energy Administration (MEA) completed two microgrids in 2018 serving the Public Safety Headquarters and a correctional facility in Montgomery County. In both cases, the microgrids had to be "islandable." They could be disconnected from the main grid in the event of outages to continue providing electricity. Both microgrids also generate power using solar energy. The microgrids are funded through "microgrid-as-a-service" partnerships between the county and private companies where the companies own and operate equipment and receive regular payments from the county for the cost of energy generated.

The two microgrids were constructed following a 2014 MEA report on microgrids and resiliency that recommended the state pursue public purpose microgrids in the near-term for critical facilities, commercial hubs, and community centers. However, even though the report supported utility development and ownership of such microgrids, the state regulator rejected a 2016 proposal from Baltimore Gas and Electric to build two microgrids due to the utility's intention to recoup costs from ratepayers and the lack of other funding sources. The Montgomery County public-private partnerships funding structure avoided these concerns, allowing those projects to move forward.


DO NOT PAINT
NO PINTAR
XCEL ENERGY
AC-250
MAOP 5 PSI

3 **Preparedness planning:** Develop emergency preparedness and crisis management plans, regularly exercise and plan/test for multiple scenarios, and ensure coordination between government and utilities by integrating staff within emergency response centers. **Illinois**

Once an event occurs that damages the grid and its operations, it is already too late to begin considering how to measure the damage, communicate to consumers estimated recovery forecasts, and repair damage and resume operations. Successful crisis management requires that key grid stakeholders have crisis management and associated response processes in place. Response plans should define staff roles, methods for assessing damage, and response coordination efforts with other public and private stakeholders. Emergency response plans also should be tested and updated through regular exercises, which can be live or table-top simulations, or a combination of the two.

Illinois | Operation Power Play

Illinois' Operation Power Play is the only state-wide emergency response exercise organized by a private utility.[19]

Starting in 2013, ComEd, the state's largest electric utility, has coordinated the statewide Operation Power Play exercise every two years to test cooperation between the public and private sectors in several areas, including critical logistics and resource management operations, interoperable communications, and restoration of critical services. Since its inception, dozens of private sector entities, federal, state, and local government agencies, national labs, and academic institutions have participated, with more joining with each iteration. The most recent exercise held in May 2019 involved more than 50 entities. The Illinois Institute of Technology served as the host and participants conducted a tabletop exercise there and used it as a base to coordinate the state-wide emergency response drills. In the exercises since 2013, ComEd has incorporated community leaders to provide input into what facilities and community services would be priorities for power restoration at the local level.

"ComEd...has coordinated the statewide Operation Power Play exercise...to test cooperation between the public and private sectors in several areas, including critical logistics and resource management operations, interoperable communications, and restoration of critical services."

The exercise is meant to test statewide emergency response capabilities addressing threats and hazards affecting multiple grid functions and other critical services around the state. Most of the scenarios involve responding to extreme weather events, such as state-wide flooding or tornadoes. Some elements have involved hazardous material leaks, a simulated plane crash into a critical facility, and cyberattacks. Not every scenario simulated in the exercises involve damage to the grid's operations. The exercises are intended to be multidisciplinary in testing whether response capabilities can address unrelated emergencies in the context of events that lead to major power outages.

At the exercises' endpoint, participants gather to assess performance, discuss lessons learned, and exchange ideas for response improvement.

4 **Cybersecurity strategy:** Develop a formalized strategy to prepare for and respond to cyber-attacks and system intrusions and work with government partners on supply chain challenges. Train a cybersecurity workforce to operate effectively within the cyber threat environment, and require cyber workshops and exercises for key personnel to advance collective awareness of cyber vulnerabilities. **California**

The March 2019 cyberattack that caused periodic "blind spots" for grid operators in the western United States is the first and only known incidence of a cyberattack affecting the U.S. grid. The attack followed a DoE report to Congress in September 2018 stating that the U.S. energy infrastructure "has become a primary target for hostile cyber actors," and the "frequency, scale, and sophistication of cyber threats have increased."[20]

To address this threat, grid stakeholders first need to have in place a cybersecurity strategy outlining how the organization monitors for, defends against, and responds to hostile cyber activities. This strategy should address grid operations and security supply chain for equipment connected to the grid. This strategy should also entail developing a skilled workforce that understands both cybersecurity and power generating systems.[21]

California | California Energy Systems for the 21st Century

The California Energy Systems for the 21st Century (CES-21) program is a public-private partnership between Lawrence Livermore National Laboratory (LLNL) and California's three investor-owned utilities aimed at developing automated cybersecurity capabilities for next generation grid industrial control systems.

Established in 2012 by the state's Public Utilities Commission (PUC), CES-21 involves a collaborative research and development agreement between LLNL, Pacific Gas and Electric, Southern California Edison and San Diego Gas and Electric. The program initially included a price tag of $152 million authorized by the PUC and a research plan encompassing cybersecurity for the entire energy sector.[22] In 2013 the state Senate reduced this funding to $35 million, however, and focused the program's research to address cybersecurity for the electric grid.[23]

Within the program, technical experts from each organization form an R&D team. Given the limited time available to respond to a cyber attack before it affects grid operations, the team is tasked with developing a system that can automatically detect, immediately respond to, and mitigate cyberattacks prior to critical infrastructure damage. Using the supercomputing power available at LLNL, this effort included creating a virtual simulation of California's grid to determine safely the impact of cyber attacks and the performance of mitigation technologies, at scale.[24] The researchers also use a physical testbed with substation equipment for testing threats and response. Due to the sensitivity of the program's work, its results are largely classified. This creates challenges for effective oversight because few PUC members and staff have the necessary security clearances to access the work.[25] The effort also produced, however, four software applications for industrial control system communications. The PUC authorized these applications for open source licensing, determining that doing so would aid other utilities' efforts to enhance grid resiliency.

Conclusion

State-level actors are at the nexus of decision-making and actions needed to continue to build the resiliency of the U.S. electricity grid. Effective grid resilience efforts depend on coordination and cooperation between public and private state-level actors, including through public-private partnerships, which can pool resources and expertise. New technologies, demands, and designs bring opportunities and challenges to strengthening grid resiliency, alongside changes in the type, nature, and severity of threats from cyber, physical, natural disaster, or electromagnetic pulse/geomagnetic disturbances, and more. Efforts at the state-level to take advantage of these opportunities and address corresponding challenges should be bolstered through a national-level impetus to enhance grid resilience across the country. This will ensure the grid remains a backbone for our country's security.

The types of programs and policies executed in the California, Florida, Illinois, Maryland, New Jersey, New York, and Texas case-studies provide a straightforward grid resiliency checklist. As many states as possible should make all four areas standard practice:

(1) **Identify Threats/Info-sharing:** identify emerging threats and share threat information;

(2) **Funding/Technology:** identify and leverage both public and private funding mechanisms and invest in technologies for resilience;

(3) **Preparedness Planning:** develop emergency preparedness plans and test them through exercises; and

(4) **Cybersecurity Strategy:** develop a cyber strategy and train a cybersecurity workforce.

Endnotes

1 BENS Councils leverage BENS members' experience and substantive expertise. The Councils serve as BENS' research and development laboratories.

[2] James Barron and Mihir Zaveri, "Power Restored to Manhattan's West Side After Major Blackout," The New York Times, July 13, 2019, https://www.nytimes.com/2019/07/13/nyregion/nyc-power-outage.html.

[3] Electric companies mobilized more than 35,000 workers from at least 27 states and Canada to restore power across the southeast. Alyssa Danigelis, "Hurricane Michael Causes Widespread Power Outages, Damage in Southeast," Energy Manager Today, October 15, 2018, https://www.energymanagertoday.com/hurricane-michael-outages-damage-0179581/.

[4] A review of the incident by the North American Electric Reliability Corporation (NERC) indicated that while the attack resulted in the brief loss of communications between a "low-impact" operations center and multiple "low-impact" power generation sites, it had no effect on power generation and did not lead to power outages. The attack took advantage of a known firewall vulnerability at those sites that was addressed by firmware released by the vendor prior to the incident. However, the unnamed operator had not yet updated its firmware because it was undergoing a process to standardize how it carries out such updates. The incident was resolved once the firmware was upgraded. See North American Electric Corporation, Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities, Sept. 4, 2019, https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf.

[5] Executive Office of the President, Economic Benefits of Increasing Electric Grid Resilience to Weather Outages (Washington, DC: President's Council of Economic Advisers, U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability, with assistance from the White House Office of Science and Technology, 2013). Available at http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

[6] Argonne National Laboratory, "Frontline Resilience Perspectives: The Electric Grid," November 2016, pg. xiii, Available at https://www.energy.gov/sites/prod/files/2017/01/f34/Front-Line%20Resilience%20Perspectives%20The%20Electric%20Grid.pdf.

[7] Executive Office of the President, National Electric Grid Security And Resilience Action Plan, December 2016, pg. 11, available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/images/National_Electric_Grid_Action_Plan_06Dec2016.pdf.

[8] Office of Energy Policy and Systems Analysis, Department of Energy, "Resilience of the U.S. Electricity System: A Multi-Hazard Perspective," August 18, 2016, pgs. 6-7, Available at https://www.energy.gov/sites/prod/files/2017/01/f34/Resilience%20of%20the%20U.S.%20Electricity%20System%20A%20Multi-Hazard%20Perspective.pdf.

[9] Argonne National Laboratory, "Frontline Perspectives," pg.23.

[10] Department of Homeland Security. National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure and Resilience. (January 8, 2014, pg. 1-3). Available at: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

[11] The Electric Reliability Council of Texas is a nonprofit entity that manages electric power distribution for the Texas grid and is subject to oversight by the Public Utilities Commission of Texas.

[12] The NERC is a nonprofit regulatory body formed in 2006 by the electricity utility industry to "ensure the reliability of the North American bulk power system." It works with grid stakeholders to develop and enforce legally mandated standards for grid operations across the United States, Canada, and parts of Mexico. In the United States, its enforcement authority is designated by the Federal Energy Regulatory Commission (FERC). For more information, see the NERC's website: https://www.nerc.com.

[13] See North American Electric Reliability Corporation, *High-Impact Low-Frequency Event Risk to the North American Bulk Power System*, June 2010, available at: https://www.energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

[14] Ibid. see pg. 9.

[15] Electric Power Research Institute, "High-Altitude Electromagnetic Pulse and the Bulk Power System: Potential Impacts and Mitigation Solutions," April 29, 2019, Available at https://www.epri.com/#/pages/product/3002014979/.

[16] The Department of Energy defines a microgrid as a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously.

[17] The Department of Energy defines distributed energy resources (DER) as small, modular, energy generation and storage technologies that provide electric capacity or energy where it is needed. DER systems may be either connected to the local electric power grid or isolated from the electric grid in stand-alone applications. DER technologies include wind turbines, photovoltaics (PV), fuel cells etc.

[18] Department of Energy Smart Grid Case Study, 2012, available at: https://www.smartgrid.gov/files/FPLcase-study.pdf.

[19] "Statewide Emergency Exercise Prepares Agencies for Severe Weather and Other Events" Business Wire, May 22, 2019, available at: https://www.businesswire.com/news/home/20190522005573/en/.

[20] U.S. Congress, House, Committee on Energy and Commerce, *Hearing on DOE Modernization: The Office of Cybersecurity, Energy Security, and Emergency Response*, Sept. 27, 2018, 115th Cong. (testimony of Assistant Secretary Karen Evans), available at: https://docs.house.gov/meetings/IF/IF03/20180927/108725/HHRG-115-IF03-Wstate-EvansK-20180927.pdf.

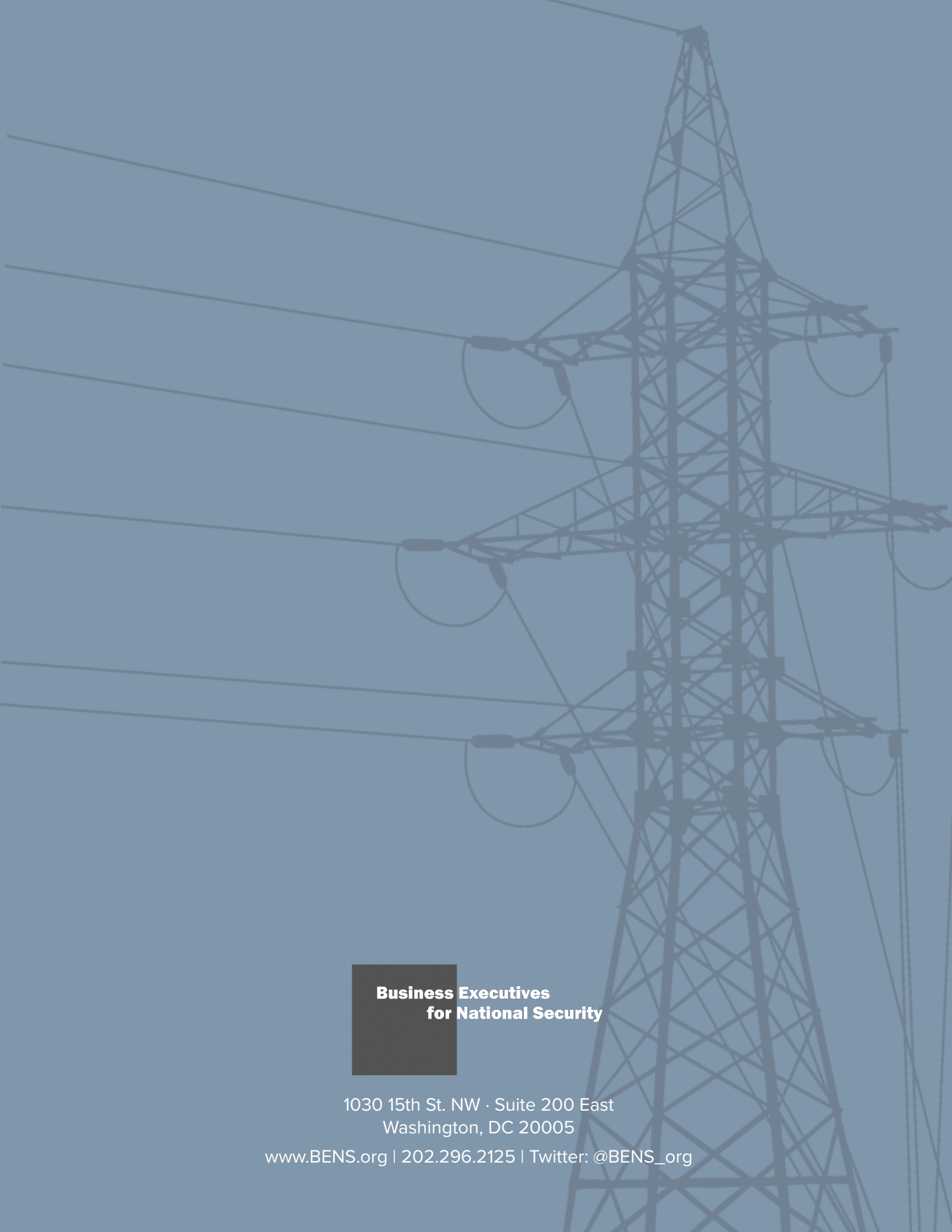
[21] NextGrid: Illinois Utility of the Future Study. *NextGrid Working Group 3: Reliability, Resiliency, and Security – Chapter Report*. Page 15. University of Illinois. Springfield, Illinois. Available at: https://nextgrid.illinois.gov/index.html.

[22] Mark James et al., *Improving the Cybersecurity of the Electric Distribution Grid*, Institute for Energy and the Environment, Vermont School of Law, April 2019, pgs 14-15, available at: https://www.vermontlaw.edu/sites/default/files/2019-04/VLS_IEE_Electricity_Distribution_Grid_Cybersecurity_Phase_1%20Report%5B1%5D.pdf.

[23] California Senate Bill (SB) 96, Chapter 396, Statues of 2013, §§ 44-45, available at: http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0051-0100/sb_96_bill_20130926_chaptered.html.

[24] Lawrence Livermore National Laboratory, CES-21: *California Energy Systems for the 21st Century*, [Fact Sheet], available at: https://www-gs.llnl.gov/content/assets/docs/energy/CES21.

[25] James et al,, *Improving the Cybersecurity of the Electric Distribution Grid, pg 16*.



Business Executives for National Security

1030 15th St. NW · Suite 200 East
Washington, DC 20005
www.BENS.org | 202.296.2125 | Twitter: @BENS_org