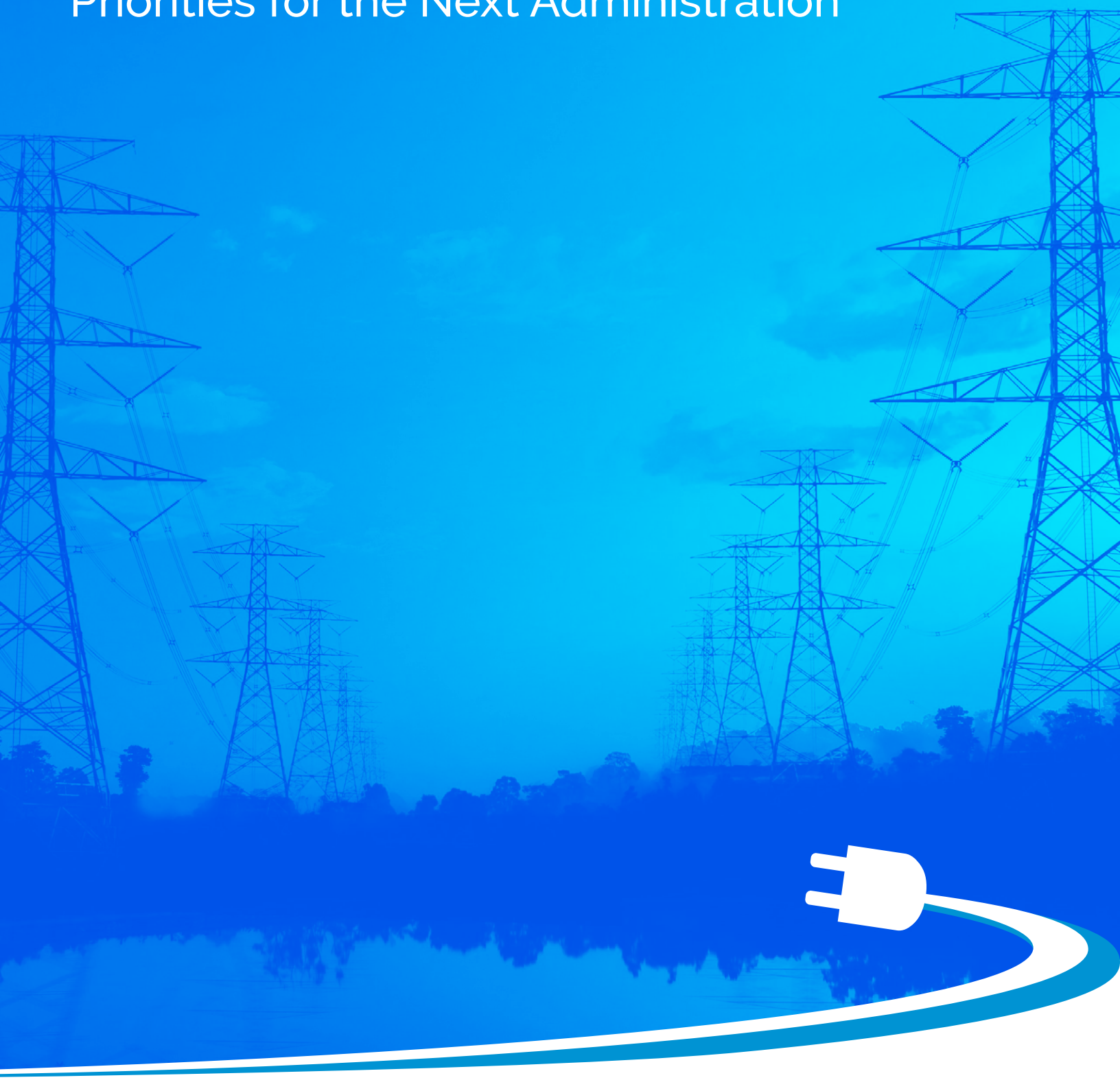
Grid Resilience:

Priorities for the Next Administration



www.gridresilience.org

NCGR
National Commission on Grid Resilience

Commissioners

Co-Chair General Wesley Clark (USA, ret.)
Co-Chair Congressman Darrell Issa (R-CA, 2001-2019)
Commissioner Norman Augustine
Commissioner General Paul Kern (USA, ret.)
Commissioner Kevin Knobloch
Commissioner Gueta Maria Mezzetti, Esq.
Commissioner Daniel Poneman

Special Advisor to the Commission

John Dodson, Thayer Energy

Research Team, AUI

Adam Cohen, Executive Director of the NCGR
Adam Reed
Peter Kelly-Detwiler
David Catarious
Matt Schaub
Kevin Doran

Subject Matter Experts

The Commission extends its gratitude to the following energy subject matter experts, who donated their time to be interviewed for this report. The opinions and recommendations of the Commission do not imply endorsement from any of the experts interviewed.

Morgan Bazilian, Colorado School of Mines
Gerry Cauley, Siemens Energy Business Advisory
Michael Coe, U.S. Department of Energy
Christopher Clack, Vibrant Clean Energy
Kenneth Davies, Birch Infrastructure
Jennifer DeCesaro, U.S. Department of Energy
Lindsey Geisler, Centrus Energy Corporation
William Hederman, University of Pennsylvania Energy Policy Center, CSIS-Maxwell School Joint Program
Bri-Mathias Hodge, University of Colorado Boulder and National Renewable Energy Laboratory
Eliza Hotchkiss, National Renewable Energy Laboratory
Cynthia Hsu, National Rural Electric Cooperative Association
Joshua Johnson, LSI
Hank Kenchington, U.S. Department of Energy (fmr.)
Jeffrey Logan, National Renewable Energy Laboratory
Richard Mignogna, Renewable & Alternative Energy Management
Edward T. (Tom) Morehouse, Executive Advisor to the National Renewable Energy Laboratory
Chris Nelder, Rocky Mountain Institute and The Energy Transition Show
Michael Pesin, U.S. Department of Energy
Adam Rousselle, Renewable Energy Aggregators
Stephen Volandt, Vice Chair, National Disaster Resilience Council, InfraGard

Table of Contents

Executive Summary

Our electricity grid's resilience—its ability to withstand shocks, attacks and damages from natural events, systemic failures, cyberattack or extreme electromagnetic events, both natural and man-made—has emerged as a major concern for U.S. national security and a stable civilian society. Rising international tensions have increased the risk of directed aggression against civilian populations, and the power grid is both highly vulnerable to attack and attractive to potential adversaries due to the dependence of all other critical infrastructures on it. A widespread power outage lasting weeks or months would have severe and staggeringly lethal consequences: imagine a pandemic-lockdown without telecommunications, water, food, refrigeration, or working fuel pumps.

The risks are not theoretical. In the past decade incidents have accelerated and attacks and probing have become increasingly sophisticated. We have witnessed a Russian cyberattack take down the eastern Ukrainian power grid in the dead of winter, a clandestine physical assault on a California substation threaten to cut power to Silicon Valley, and a space weather event of sufficient magnitude to permanently damage power grids at continental scales move straight through Earth's orbit, missing the planet by only a week. As these threats have revealed themselves, the nation's best scientific and business minds have dedicated considerable efforts toward understanding vulnerabilities and improving the grid's resilience, and, for some vulnerabilities, substantial progress has been made in a short time.

But more needs to be done, and in record time. Protecting the grid from the rapidly evolving threats examined in this report requires a multi-pronged approach. First, the nature of the threat requires rapid response and development of new technologies with a minimum of bureaucratic red tape. Second, the sheer scale of the transmission and distribution systems and the widening attack surface of grid-connected devices requires diverse sets of expertise: cybersecurity; industrial control systems; artificial intelligence; civil, electrical, and mechanical engineering; materials science; grid architecture; interdependent systems analysis for gas and telecommunications considerations; systems management; public policy design, and many others. Third, the need to not only react to emerging threats but to anticipate and regain the lead against potential adversaries requires the innovation and talent of the private technology sector in combination with forward thinking government planners.

This report presents a roadmap for those next steps. We aim to accelerate resilience investment in the grid and foster the development of the advanced technologies necessary to meet an evolving threat landscape, before it is too late. Government and industry must travel this road together: national security is a public concern, but most of the power grid is owned and operated by the private sector. While federal power authorities can and should be directed to provide early examples, most regulation is at state level jurisdiction, where reliability standards and mandates are rare. We therefore stress the importance of public-private partnerships as the engines of progress throughout the report. The federal government must provide the motivation, leadership, and resources for a resilience transformation, while the power industry must ultimately direct it, alongside its ongoing transition to sustainability. Our recommendations, explored in detail in Section (6) of the report, represent the bare minimum of what government and industry must undertake to meet the challenges and circumstances of the next two decades. They are as follows:

Recommendation 1:

Congress should direct the Department of Energy (DOE), Department of Homeland Security (DHS), and the Director of National Intelligence (DNI) to establish a central clearinghouse and decisional node for communicating full and accurate threat

information to bulk power system operators and electric utilities.

The clearinghouse should build upon and expand the capabilities of the industry-led Electricity Subsector Coordinating Council (ESCC) and the North American Electric Reliability Corporation's (NERC's) Energy Information and Analysis Center (E-ISAC) to provide: 1) Detailed and timely threat intelligence sharing with appropriate industry personnel; 2) Real time threat-information networks and action tools for control room operators; and 3) Expanded and continually-evolving red-team exercises to test defenses against evolving threats. The clearinghouse should also collaborate with the government to increase the number of security clearances available to electric utility industry personnel.

Recommendation 2:

Congress should establish a National Resilient Grid Authority (NRGA)—an independent agency staffed by rotating appointments of the country's most highly qualified energy, cybersecurity, and national defense experts from both the government and private sectors.

Congress should provide sufficient funding and charge the NRGA with developing a state-of-the-art grid scale experimentation program that identifies emerging threats and vulnerabilities via world-class red-teaming, invites the private sector, the Defense Advanced Research Projects Agency (DARPA), the Advanced Research Projects Agency-Energy (ARPA-E) and federal government labs to submit and judge innovative solutions, and tests those solutions against attackers in a competitive experiment environment. The NRGA's operations should be cyclical, with new threats identified and new solutions developed on an annual basis by an ever-changing cohort of the country's best technical and strategic talent. Based on the threats and technologies it works to solve, the NRGA should also identify potential policies and regulations for consideration by the Federal Energy Regulatory Commission (FERC), NERC, and the insurance industry. The NRGA should report its findings and recommendations to the National Security Council (NSC), which will then facilitate dissemination information to the relevant executive branch and Congressional stakeholders.

Recommendation 3:

Congress should direct the Department of Defense and the Department of Energy to establish a nationwide advanced resilience technology (ART) test bed network of long-duration, blackout survivable microgrids on military bases and other critical federally-owned facilities that are pre-determined to be safely sited on stable lands free from flooding, wildfires and other high impact disasters for the foreseeable future. These should be devoted to both immediate defensive capabilities and rapid development of advanced grid resilience technologies.

ART test beds should take the form of public private partnerships, where industry can host technologies for testing and commercial development at government facilities. Though managed by DOD and DOE at their respective facilities, the ART network should be integrated with and report to the National Resilient Grid Authority (NRGA) described in Recommendation 2. At least one ART test bed should be of sufficient scale to provide an integrated test site for combined transmission and distribution systems, so as to provide a laboratory for end-to-end security and resilience testing. Once designed, planners should aim to deploy a geographically diverse set of "Safe Haven" secure microgrids that could support their surrounding civilian communities with stability and critical functions (electric power, water, telecom, etc.) in the event of any state, regional or national emergency.

Recommendation 4:

The Federal Energy Regulatory Commission (FERC)—in consultation with appropriate expertise at the U.S. Department of Energy and the Department of Interior, states actively procuring offshore wind energy resources, and the relevant Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) responsible for the management of the onshore grid in their jurisdictions—should reform and strengthen interregional transmission planning, cost allocation, and competitive bidding processes

to better address the characteristics of widely dispersed renewable energy generation.

Regarding the emerging offshore energy industry, FERC should develop a robust, standards and systems-oriented planning process for new offshore transmission grids serving next-generation resources such as ocean-based, offshore wind turbines, wave and tidal energy, and transmission.

Recommendation 5:

Congress should direct the Department of Energy and the Department of Homeland Security to create a voluntary central repository of information regarding security and resilience investments in the electric power system.

Participating utilities and other stakeholders should be invited to submit annual reports of activities, which could form a basis for cost-recovery arguments to regulators by providing comparative data between utilities. In addition, NIST should examine the impacts of severe short-, mid- and long-term climate and weather predictions to ensure grid-related equipment is resilient to the challenges of tomorrow. In addition, NIST should examine the impacts of severe climate and weather predictions to ensure grid-related equipment is resilient to the challenges of tomorrow.

Recommendation 6:

Congress should pass a Resilience Investment Tax Credit (RITC) that incentivizes investments in cyber, physical, American-manufactured transmission components and equipment, and electro-magnetic pulse (EMP) security measures at both the distribution utility and bulk power system levels, and direct federal spending toward resilience and security investments in federally-owned electric utilities and end-use federal facility energy applications such as grid connected devices, electric vehicle fleets and charging infrastructure, and distributed energy resources.

State Public Utility Commissions should develop new methods of valuing resilience investments in the private sector so as to include such expenditures in the utility rate base calculation. In all cases, every advantage should be taken of opportunities for public-private partnerships to deepen investments in grid resilience.

Recommendation 7:

Congress should establish a bipartisan caucus on grid security that meets regularly to consider issues impacting the security and resilience of the U.S. electric grid. The National Security Council should lead a complementary interagency committee on grid security that acts as a liaison with the caucus.

Recommendation 8:

The Administration and Congress should establish a secure ongoing domestic supply chain, manufacturing capability and labor skills sets for all critical components and whole equipment essential to the operational security of the bulk electric grid, particularly prioritizing the largest and longest lead time transformers. Further, Congress should direct annual updates and briefings to the NSC and Congress to the DOE Reports "Large Power Transformers and the U.S. Electric Grid (2012)" and "Strategic Transformer Reserve Report (2017)."

While the domestic large transformer industry was re-established following the recommendations of the 2008 Defense Science Board Energy Security Task Force, foreign competition and pricing have severely diminished the U.S. manufacturing capacity and skills sets meant to ensure a reliable and secure domestic supply for national security and critical infrastructure.

Recommendation 9:

The President should issue a Presidential Decision Directive initiating climate impact modeling of a range of future scenarios to identify where it will be safe to site new and upgraded bulk electric transmission. These planning scenarios should take into account sites critical to national infrastructure, areas threatened by environmental impacts (including sea-level rise, extreme heat, and climate-driven population migration), impacts to the national economy, and enhancements that could be made by public-private partnerships.

This is an inherently government function and industry, while it largely owns the grid, does not have the assets to perform the complex national scale modeling required for reliable planning. The project should be managed from the NSC (for defense purposes) in coordination with the National Economic Council (NEC, for civilian infrastructure purposes) to assure all federal agency and state government consensus on models and necessities as we move through the process.

Introduction

In recent years, resilience of the electricity grid—its ability to withstand shocks, attacks and damages from natural events, systemic failures, cyberattack or extreme electromagnetic events, both natural and man-made—has emerged as a major concern for U.S. national security for both civilian infrastructure and military installations. As extreme weather events have intensified in frequency and severity, local governments have been among the first to face the challenges of superstorms, droughts, and wildfires, and to call for the need to develop resilient infrastructures that could better withstand and recover from such events.[1] Likewise, military leaders have shifted from considering energy, water, and land resources and infrastructures as "constraints" to "mission enablers," and sought to advance capabilities to "anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions."[2]

Resilience concerns do not stop with the weather. Rising international tensions and disruptive technologies have increased the risk of directed aggressions against critical infrastructure and civilian populations, through a variety of pernicious mechanisms, including cyberattacks, terrorism, and nuclear capabilities.[3] Among the most attractive and vulnerable targets for such attacks is our nation's power grid. Because of the dependency of nearly every other critical function on reliable supply of electricity—drinking and wastewater systems, food, transportation and fuel, health care, communications, and financial services—a long-duration, large-scale power outage caused by a cyber-physical attack or EMP event would cause "severe, widespread, and long-lasting" consequences, according to the National Infrastructure Advisory Council (NIAC).[4]

Moreover, decades of efficiency-enhancing investments in coupled cyber-physical systems and automation technologies have made the grid uniquely vulnerable.[5] The very things that have made our electricity both highly reliable and inexpensive have also opened a Pandora's box of risks—once thought too improbable for consideration—that now reveal themselves as far more worrisome. Incorporating new and advanced technologies into the grid also often incorporates brand new and unexpected avenues of attack. We have seen profound impacts to the power grid already in the form of natural hazards: Hurricane Katrina (2005) and Superstorm Sandy (2012), among others. But malicious and coordinated attacks against the grid by hostile state-actors pose risks that could dwarf most natural hazards in both the scale of impacts and the duration of outages.[6]

> *"Confronted with the ravages of a pandemic that many understood as an abstract possibility but failed to recognize as a real public health or economic threat, it is time to think differently about how we conceptualize and prepare for potentially catastrophic events."*

Confronted with the ravages of a pandemic that many understood as an abstract possibility but failed to recognize as a real public health or economic threat, it is time to think differently about how we conceptualize and prepare for potentially catastrophic events. The challenge is that the range of such events is limitless, but resources are not. Which risks call most urgently to us will be a matter of both policy and politics, and differences in culture, geography, and values will lead different people to different conclusions. But imagine, for a moment, the

horror of daily life in a long-duration power outage: dead refrigerators full of spoiled food; dry taps; supermarkets reduced to shelf-stable stocks, themselves quickly hoarded by panicked shoppers or looters; thousands desperately crowding bodies of water to avoid heat stroke or—alternately—burning trash to stay warm; exhausted motorists trudging away from their empty cars, passing gas stations that cannot pump fuel. The lucky ones make it to crowded shelters, encampments, or stadiums, where military and civil authorities squabble over access to a limited fleet of mobile diesel generators. Many more do not. Desperation and violence spread in lockstep, one reinforcing the other in a continuous feedback loop. Those communities already disadvantaged are hit hardest of all. It sounds like a Hollywood disaster movie, and yet the pandemic has shown us just how closely life can imitate—and sometimes tragically exceed—art.[i] No matter one's political leanings, the realities of a "black sky" event number among the most catastrophic disasters we can imagine, short only of a nuclear strike in its devastation. The difference is that we have developed sophisticated defenses against nuclear strikes, both technological and diplomatic. The same cannot be said of a massive cyberattack or EMP event targeting the bulk power system.

These risks can and must be addressed as a priority. Significant efforts have already been directed toward understanding and addressing power grid resilience to major disruptions. Investment, likewise, is ongoing: the American Recovery and Reinvestment Act of 2009 (ARRA) committed $4.5 billion toward grid modernization, and electric utilities in hurricane prone areas have experienced an average of $1.4 billion each in weather-related damages over the last two decades—much of it spent augmenting their grids to better withstand future events. But much remains to be done, especially in the enactment of robust federal and state government policy to support grid resilience and security efforts, to prepare for the consequences of malicious attacks, and to develop appropriate opportunities for public-private partnerships in some of these efforts.

In recognition of this need, the National Commission on Grid Resilience has produced this report with the goal of providing actionable, nonpartisan policy recommendations for grid resilience that can be adopted into legislative efforts and campaign platforms. Resilience is an emerging concept that is likely to shift considerably as it becomes operationalized in the grid by the largely private-sector actors that own and operate it.[7] But we know enough to enact policies now that can accelerate the transition to more resilient energy systems that support our lives and our economy and also protect us from potential catastrophe.

In Section (1), we provide an overview of the U.S. electric power sector and explain the complex governance systems and institutional heterogeneity that define the system, enable its innovative features, and—unavoidably—constrain the feasibility of directed interventions. We review the three major threats facing the grid from malicious actors in Sections (2) —cyberattack, (3) physical attack, and (4) EMP attack—and explore other threats and threat multipliers in Section (5). In Section (6), we examine a variety of investments, measures, strategies, and solutions to increase resilience to those threats, organized around specific policy recommendations that are intended as nonpartisan "plug-and-play" components for use in legislation, executive orders, and presidential and congressional campaign platforms. We conclude in Section (7) with a call to action.

i *The filmmakers of the critically and scientifically acclaimed Contagion (2011), for example, anticipated much of the tragedy and unrest associated with a global pandemic. Even so, they underestimated. Dr. Mark Smolinski, who consulted for the film, was shocked to see that "medical workers in developed nations would be dying of the virus because of a lack of personal protective equipment." C. Farr, "The medical advisors for the movie 'Contagion' saw a pandemic coming, but got this one big thing wrong," CNBC, Apr. 14, 2020.*

Section 1: State of the U.S. Electric Power System and Resilience Investments to Date

Overview: The Evolution of U.S. Electric Power System Operations and Governance Mechanisms

The fundamental challenge in addressing the grid's vulnerabilities is that the electric power system is profoundly heterogeneous in its technical structure, market organization, and regulation.[8] Solutions that enable the grid to avoid, plan for, cope with, and recover from attack will be diverse and highly varied according to local grid conditions. The U.S. grid is also largely privately owned and operated, and under constant evolution as new technologies emerge and gain momentum and others decline and eventually leave the system. Consequently, the ability of the government to direct action toward any particular outcome—such as security against catastrophic attack—is inherently limited. On the other hand, the decentralized and innovation-forward nature of the U.S. power system is itself an engine for developing emergent, context-appropriate solutions to resilience and security. Of course, this happens only if markets value such solutions, and then access and commercialize cutting edge R&D developed by national labs, universities, and the private sector. In this section, we will briefly review the evolution and current state of the U.S. electric power system as a baseline from which to explain its vulnerabilities as well as consider opportunities for security and resilience investments.

Over a century ago, the earliest electric power service was provided by private direct current (DC) generators serving only a few blocks and operated by property owners. As the industry evolved and the economies of scale of larger generators became apparent, it adopted the use of alternating current (AC), which could be stepped up to high voltages that allowed for efficient transmission over larger distances, and then stepped down to safer voltages for distribution systems and consumers. This decision transformed the electric industry from one based on equipment manufacture and sales to the provision of service to entire communities using networks, via the electric utility. For much of the 20th Century, electric utilities were vertically integrated monopolies regulated by state governments. Private, for-profit utility companies (and some publicly owned enterprises) owned and operated all or nearly all of the generation, transmission, and distribution assets in their service territory, and the utility was the only entity with the legal right to sell power in the service territory. Under the vertically integrated model, a disruption in one utility system would have little to no impact on another utility system.

Gradually, however, utilities began interconnecting their systems and trading power. A wholesale market developed wherein utilities bought and sold power across state lines, and thus outside of the jurisdiction of state regulators. An entirely new dimension of the electric industry was born: the bulk power system. Wholesale trade of energy provided new economic efficiencies to growing systems, but also increased the complexity of operations, as multiple entities then were responsible for maintaining the instantaneous match of supply with demand over larger regional areas. Unlike the retail market, where utilities provided service to end users at state regulated, cost-of-service rates, prices in the wholesale bulk power system were regulated under federal jurisdiction, first through the Federal Power Commission (FPC) in 1935, and then in its successor agency, the Federal Energy Regulatory Commission (FERC) in 1977. Initially charged with ensuring that wholesale power prices were fair and reasonable, FERC's mission shifted after the Energy Policy Act of 1992, which began a long process of liberalizing electricity markets towards greater competition and would result in the development of even greater regional system complexity.

Increasing complexities in the bulk power system have historically come with a tradeoff between economic benefits and risks of cascading system

failures. The first major incident that revealed this tradeoff was the northeast blackout of 1965, when a mis-programmed protective relay on a transmission line connected to a Canadian hydropower station tripped—due to a small power variation at a generating unit in New York—and disconnected from the system during a cold November evening when regional lines were already heavily loaded. The power flowing on the first tripped line instantly moved into the other regional lines and overloaded them, causing those lines to trip. The Canadian hydropower station, cut off from the western portions of the grid, then fed excess power onto still other lines to the East, into New York State, before tripping offline itself. Within minutes, the effects of further transmission line overloads and subsequent generator losses broke the grid into islands, leaving over 30 million people in an area of over 80,000 square miles without electricity for up to 13 hours on an exceptionally cold night.[9]

The 1965 blackout was understood as a profound failure of the power system to account for widespread blackout risks, and led to the creation of the North American Electric Reliability Corporation[ii] (NERC), formed by twelve regional and area power organizations in 1968 in order to address the risk of cascading failures through regional cooperation and planning. Within a decade, NERC had formed nine regional councils covering all of the U.S. and Canada. Another major blackout hit the Northeast in 2003, this time caused by an overloaded transmission line in Ohio that sagged into contact with an overgrown tree, tripped offline, and caused a cascading blackout that affected 10 million people in Ontario and 45 million people across 8 northeastern U.S. states for seven hours.[10] In response, the Energy Policy Act of 2005 deemed voluntary cooperation to be insufficient and called for the creation of an Electric Reliability Organization (ERO) with the power to enforce compliance with mandatory reliability standards in the U.S. Since 2006, NERC has served as the ERO for North America under grants of authority from both U.S. and Canadian regulatory agencies.[iii]

The bulk power system's evolution in the wake of the restructuring process that began in 1992 has been highly disruptive to vertically integrated utilities, and has provided fertile ground for innovation at every level of the grid. Today's power grid is highly interconnected across vast regional scales—a product of market participants seeking ever-greater economic efficiencies, "wheeling" power through multiple systems to reach customers. As wholesale generation markets were opened in the 1990s and 2000s to further competition from non-utility generators and independent transmission developers, the bulk power system grew to accommodate a vastly expanded group of entities. Many utilities, particularly in the Northeast, Midwest, Texas, and California, ceded control of transmission systems to non-profit market coordinators and system operators, variably called Independent System Operators (ISOs) or Regional Transmission Organizations (RTOs), which now operate the system on behalf of their expanded class of asset owners using sophisticated software, remote operations controls in both generation and transmission components, and a complex array of organized market auction mechanisms for scheduling power flows from minutes to days ahead of schedule.

In other parts of the country, such as the Intermountain West and Southeast, legacy utilities continue to own and operate large portions of the system, but also perform market operations[iv] to coordinate independent generators and distributed energy resources on their system as well as buy and sell power over vast

ii The original name was the "North American Electric Reliability Council."

iii NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which provides cyber and physical threat information to grid operators in coordination with intelligence agencies.

iv Market operations performed by incumbent utilities are subject to oversight by FERC to ensure fairness and prevent self-dealing.

distances to other regions of the bulk power interconnection. Still other enclaves exist, such as the Pacific Northwest, parts of the desert Southwest, and the Tennessee Valley, where the system is federally owned and operated by Power Marketing Administrations (PMAs) or federally owned corporations, a legacy of the New Deal's rural electrification efforts and hydropower infrastructure investments.

As the bulk power system's interconnections grow and as its generation mix changes, these sundry entities—private and public, for-profit and non-profit, regulated and unregulated—must coordinate the buildout of the transmission grid to move power efficiently from generation to loads. Transmission planning processes vary significantly from region to region within the U.S. power system (Figure 1), though all must comply with FERC Order 1000's directive to utilize regional transmission planning and cost-allocation procedures (Figure 1).[11] Though passed with high hopes of a renaissance in large scale transmission development, FERC Order 1000 has been criticized for failing to anticipate the need for transmission *between* regions over wide geographic areas.[12] Electric utility restructuring and deregulation has led to complex ownership of the grid, including, for example, one utility's non-contiguous ownership of bulk grid in 28 states. This construct further complicates reliability and security initiatives. Complicating matters further, states retain near total authority over siting and permitting of individual transmission lines, irrespective of where transmission planning processes may have identified the most attractive pathways for the bulk power system.

Meanwhile, states also retain their jurisdiction over the retail distribution systems of the grid and the interaction of utilities and other electricity providers with consumers. Those consumers are adding millions of internet-connected devices to the edge of the grid for a wide range of uses, from controlling thermostats in response to time-dependent pricing signals to charging electric vehicles to smart inverters for on-property solar panels. The proliferation of smart devices both on the system and behind customer meters constitutes a quantum of potential illicit entry points to the grid that is orders of magnitude higher than on the bulk power system.

These profound regional differences in ownership, market design, and regulatory practices, combined with the complexities of the federal/state jurisdictional split, make the U.S. power grid not only one of the largest machines on the planet, but also one of the most complicated institutional systems human beings have ever developed. As a comparison, consider the Chinese power grid: it consists of two major transmission companies running a single synchronized grid and five major state-owned generation companies, all of which are directed by the national government in a rigidly hierarchical system. The Chinese grid is the largest power system in the world, but it exhibits none of the institutional complexities of the U.S. grid.

A key takeaway for policymakers is that successful resilience and security policies for the U.S. grid must account for its complexity and heterogeneity, and work with the decentralized governance systems of the grid rather than against them. Top-down directives that would deploy identical investments or technology approaches throughout a hierarchical system like China's grid are fundamentally incompatible with the U.S. grid, just as they are incompatible with our governing philosophies and bedrock values. In the grid's century of development, markets have emerged as the preferred mechanism for guiding bulk power system development, and thus the grid's evolution is a complex, emergent phenomenon that occurs in the absence of a central authority. Any approach to spurring private sector investment in grid resilience and security against malicious attack should consider the incentives necessary to make such investments attractive, as well as the role of the industry's self-organizing governance systems (such as the NERC and its Regional Councils) in coordinating activity and developing feasible standards.

Where the government does make active investments in the grid ecosystem, it typically does so in order to "fill in" functions that commercial

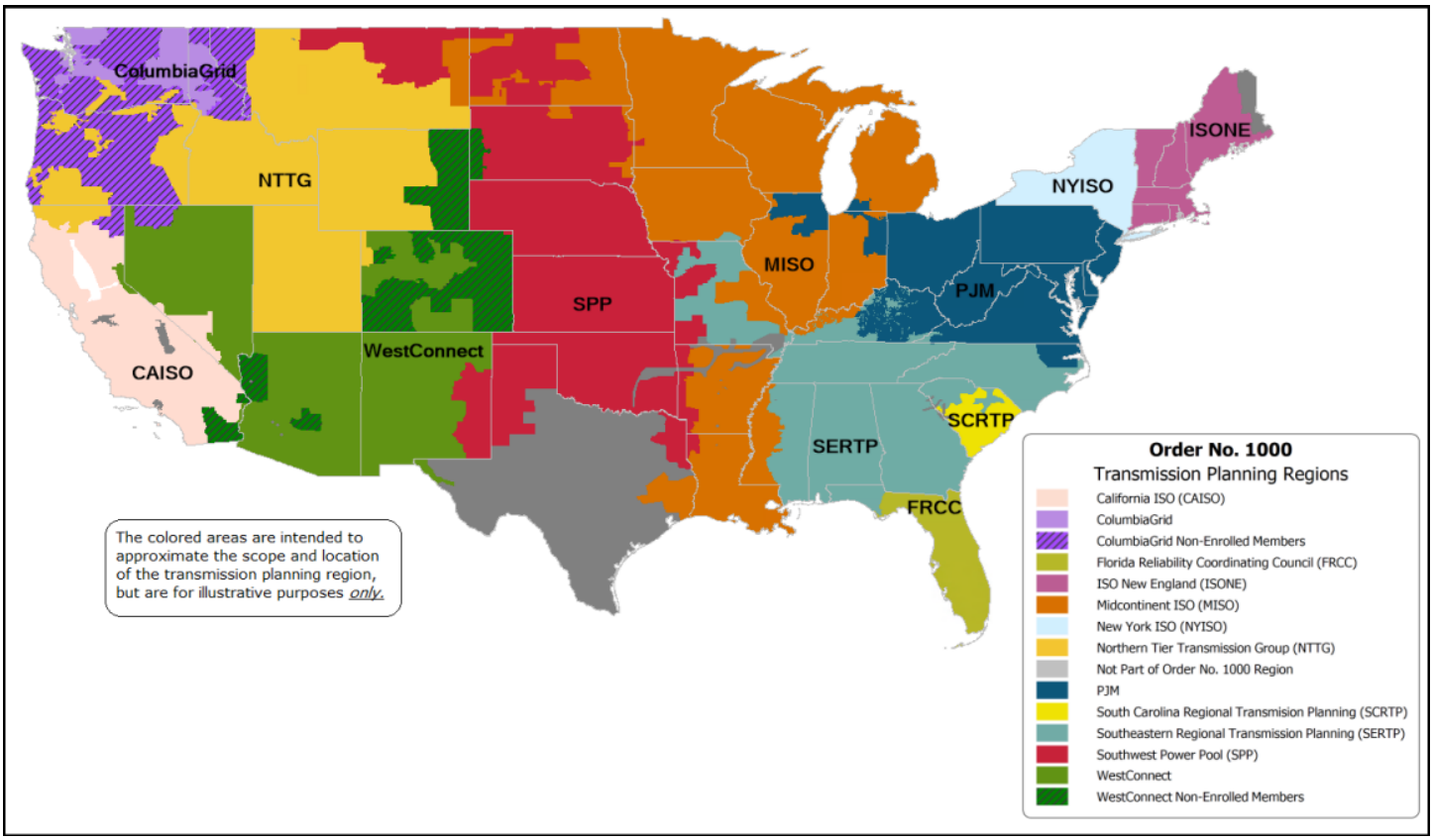


Figure 1 : Order No. 1000 Transmission Planning Regions (Source: FERC)

interests have not addressed, such as advanced or high-risk research and development and the creation of public infrastructure[v] where necessary. The government also takes responsibility for national defense, but determining who is—or ought to be—responsible for protecting the grid is surprisingly difficult. U.S. Cyber Command has no specific directive to protect the grid, and the provision of threat information to system operators and utilities falls under overlapping responsibilities of civilian agencies within both the Department of Homeland Security (DHS) and the Department of Energy (DOE) (*see* Annex II). Many of those responsibilities have been defined only in the last few years, and much ambiguity remains as to who is responsible for what. This ambiguity exists not only between government departments, but also between the public and private sectors. In the realm of malicious attacks and the ability to recover from them, some investments are the responsibility of the power sector, while others are the responsibility of the government under its national defense functions. But where to draw the line remains an open question. A clear and functional multi-agency structure to both guide private investment and strategy and respond to catastrophic attacks on the power grid is both critical and currently lacking, according to the most prestigious collection of infrastructure executives at the country's disposal.[13] As we explore throughout the report, there are also clear needs for direct governmental action in the interest of national defense of power systems that require more attention.

Progress to Date: Grid Resilience as an Emerging Focus of the Power Sector

v The Rural Electrification Act (1936), for example, created much of the transmission systems that serve rural electric cooperatives, and the government invested heavily in hydropower dams in the mid-20th Century to provide power to rural energy systems.

"These profound regional differences in ownership, market design, and regulatory practices, combined with the complexities of the federal/state jurisdictional split, make the U.S. power grid not only one of the largest machines on the planet, but also one of the most complicated institutional systems human beings have ever developed."

Grid resilience investments to date have typically been justified by either co-reliability benefits—improvements to the operational up-time of the grid given the usual, daily operating conditions of the system—or heuristic decision-making regarding events that can have large impacts on system operation when they occur: hurricanes, wildfires, earthquakes, and others.[14] Investments in the latter category tend to be made in the aftermath of particularly disruptive events, reflecting cognitive biases that interpret disruptive events we have recently experienced as inherently more likely or repeatable than events we have not yet experienced, irrespective of their objective probability.[15]

The potential impacts of natural and human threats to the grid are readily imagined, but there is far less agreement on how to define, measure, and value resilience investments themselves in a rigorous or universal way.[16] This is not for lack of effort or ingenuity from the research community or electric power industry, but a reflection of the inherent difficulty of both conceptualizing the challenge and measuring success in addressing it. There is no neat series of qualitative checkboxes or quantitative benchmarks to tick off in reaching the goal of grid resilience. The success of grid resilience is ultimately defined by what *does not* happen: a superstorm that does not take out the power; a cyberattack that fails to reach industrial control systems; a planned physical assault that is aborted because of robust security measures. Resilience investments are highly varied in form, intent, and cost, and uncertainty surrounds both the nature and probability of threats and the efficacy of proffered solutions.

The lack of common definitions and metrics for resilience investments makes rigorous and comprehensive tracking of efforts across the power sector very difficult.[vi] Nevertheless, the U.S. has made substantial progress on some issues toward a more resilient power grid over the past decade, primarily in response to the effects of extreme weather and, increasingly, in response to human threats. Following the devastation of Hurricane Katrina[vii] in 2005, The American Recovery and Reinvestment Act of 2009 (ARRA) allocated $4.5 billion for grid modernization efforts, and by early 2013 those funds had been used for the deployment of 343 advanced grid sensors, 3,000 digital upgrades to distribution systems, 6.2 million smart meters, and 16 energy storage projects. Subsequent analyses of grid

vi The U.S. Energy Information Administration (EIA) collects and curates massive amounts of data about the electric power system, and maintains sophisticated analytical tools for public use on its website. The challenge for resilience tracking is not, strictly speaking, a lack of data, but the lack of a universal conceptual framework that defines, for example, what is or is not a resilience investment, or how resilience investments relate to one another, or whether they are sufficient for the range of natural and human threats facing the system. Indeed, even comprehensive asset inventories themselves are rare and quickly become outdated. See National Academies of Sciences, Engineering, and Medicine (2020), Communications, Cyber Resilience, and the Future of the U.S. Electric Power System: Proceedings of A Workshop, Washington, DC: The National Academies Press. The Department of Energy's North American Energy Resilience Model (NAERM) is an early effort at providing such a framework, but it was only launched last year and remains in planning stages.

vii Hurricane Katrina made landfall on the Gulf Coast in August 2005 and ranks among the worst natural disasters in national history. The storm displaced an estimated 2 million people and killed approximately 1,200. It was immediately followed the next month by Hurricane Rita, which proved less lethal but prompted major shifts in preparedness strategy and efforts. See Congressional Research Service (2006), 2005 Gulf Coast Hurricanes: The Public Health and Medical Response, prepared by Sarah A. Lister.

"A key takeaway for policymakers is that successful resilience and security policies for the U.S. grid must account for its complexity and heterogeneity, and work with the decentralized governance systems of the grid rather than against them."

performance in the wake of Hurricane Irene[viii] and Superstorm Sandy[ix] found that the smart grid upgrades made with ARRA funds had significantly lessened the impact of the storm for hundreds of thousands of customers and provided utilities with disaster response capabilities—such as the ability to pinpoint outages without relying on customer telephone calls—that resulted in faster recovery.[17] Resilience investments are on the rise as utilities consider the growing costs associated with more extreme weather as well as climate hazards.[18] The average electric utility in hurricane-prone areas of the U.S., for example, has experienced $1.4 billion in hurricane-related costs over the past two decades, and greater damage is expected in the future.[19] 2019 saw 14 separate billion-dollar weather and climate disasters.[20]

The first half of 2020 alone saw 10 such billion-dollar disasters (Figure 2). In March 2019, Standard and Poors issued a report in response to California wildfires being sparked by an antiquated electric grid, advising that not only PG&E but also other CA utilities run the risks of credit downratings and potentially bankruptcy due to changing climate impacts and liability constructs.[21] Utility investments to date have varied substantially, both in the type of investments made and in utilities' willingness to describe their plans in detail.[22]

Recent examples include:

- Pacific Gas & Electric (PG&E) is formally considering the high costs of undergrounding lines against the high costs and associated legal liability of wildfires, and has planned for 73 microgrids on its system by the end of 2020, both parts of a resilience planning effort ordered by state regulators.
- San Diego Gas & Electric (SDG&E) developed California's first renewable-energy based microgrid in Borrego Springs, which had previously suffered frequent outages because it was located at the end of a single transmission line.
- The Sacramento Municipal Utility District (SMUD) has developed emergency action plans for grid resilience.
- The Tennessee Valley Authority (TVA) has developed its own resilience tool to consider risk and response capabilities, and has made transmission and distribution system hardware investments throughout its system based on the tool's calculations.
- New York's Consolidated Edison (ConEd), in the wake of Superstorm Sandy, installed pumps to remove water from substations and surrounded them with walls, invested in stronger poles and wiring, and deployed smart switches for better control of distribution systems during disasters. It has also developed a resilience management framework in collaboration with Columbia University, while recognizing the need for better resilience valuation to drive "a broader suite of adaptation strategies."

viii Hurricane Irene made landfall at Cape Lookout, North Carolina on August 27th, 2011 before moving northeasterly to Atlantic City, New Jersey. The blackout affected 6.5 million people, and resulted in damages of $15.8 billion. Executive Office of the President (EOP) (2013), Economic Benefits of Increasing Electric Grid Resilience to Weather Outages.

ix Superstorm Sandy made landfall in New Jersey on October 29th, 2012 before continuing northwesterly over Delaware and Pennsylvania and surging record flooding into New York and New Jersey. Floods in lower Manhattan reached as high as 11 feet, and ten counties in New Jersey saw flooding of 2 to 9 feet. The blackout affected 8.5 million customers and caused an estimated $65 billion in damages. Ibid.

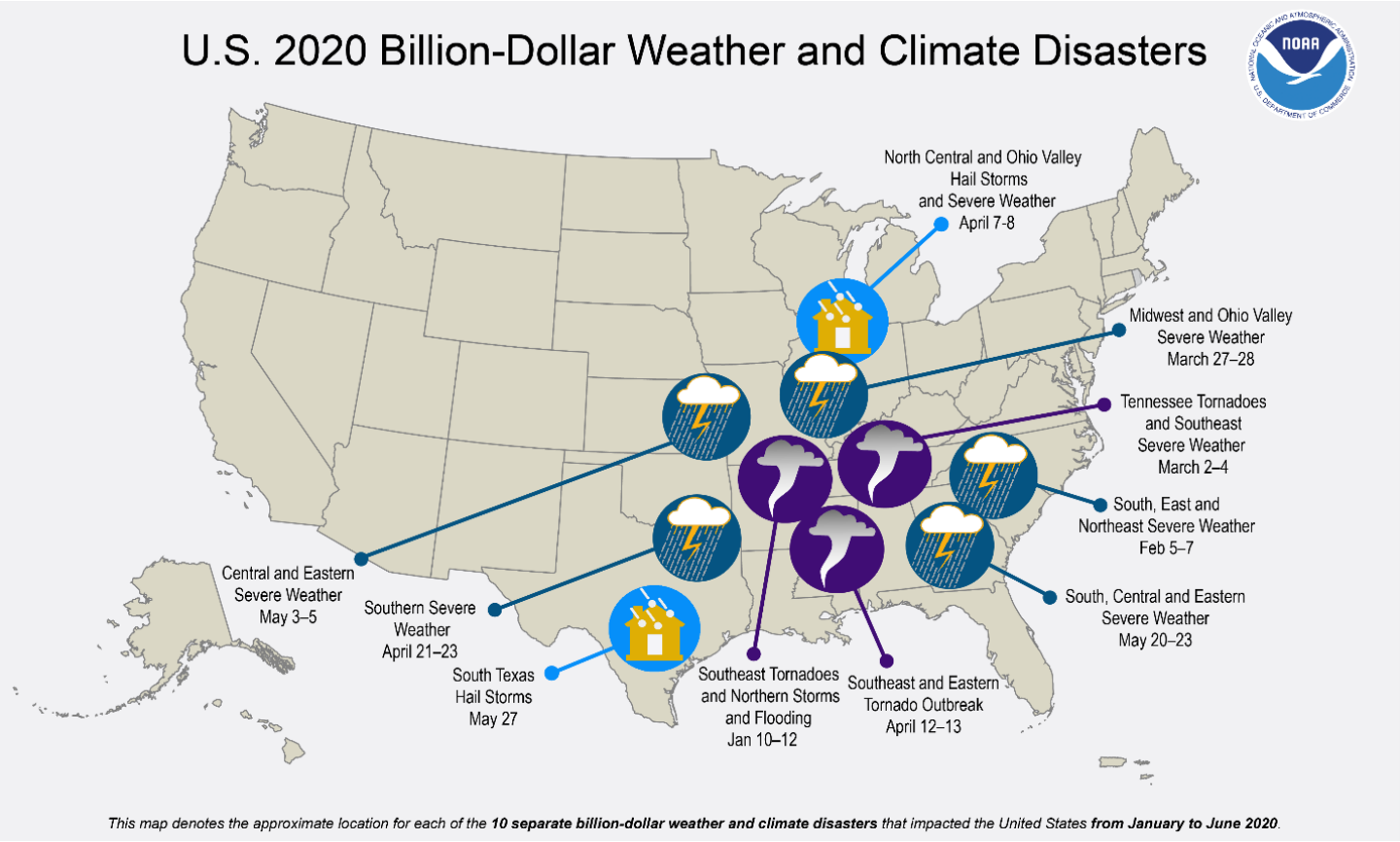


Figure 2: U.S. 2020 Billion-Dollar Weather and Climate Disasters[23]

- Xcel Energy, which operates both transmission and distribution systems across 8 states, has developed "robust plans" for resilience and reliability based on the guidelines of the National Infrastructure Advisory Council's 2018 report.

Though individual analyses and frameworks vary in the details, experts generally agree that resilience investments can be conceptualized according to a disruptive event spectrum, from early warning of an event through disruption, response, and recovery.[24] However, since the useful life of grid equipment investments typically exceeds 30 years, modeling that looks ahead to regional heat, flood, climate conditions and population migrations is highly advisable for mid to long term planning. Different types of resilience investments and measures are effective for different points along the disruption spectrum, and overlap in many instances with operations to ensure the power system's day-to-day reliability.[x] A sample (but not definitive, as the field is still maturing) division of the spectrum might look like the following:

- **Hardening and Security.** Preventative measures or investments that aim to ensure that threats do not reach the grid. Includes front-line cybersecurity measures, emerging non-programmable industrial control systems for secure national security sites and microgrids, tougher physical infrastructure, air-gapping of critical operational technology (OT) systems from information technology (IT) systems, EMP shielding, etc.

x Regarding malicious attacks, investments along the resilience spectrum can also contribute to layered deterrence strategies by helping to "deny benefits" to attackers by decreasing the likelihood that the attack will succeed or have the desired effect, and by erecting multiple barriers to mission success for adversaries, as described in the Report of the Cyberspace Solarium Commission. U.S. Cyberspace Solarium Commission (CSC), A. King, and M. Gallagher (2020), Cyberspace Solarium Commission Final Report.

- **Inherent Technical Resilience.** Preventative measures or investments that allow the grid to ride through the disruption without the need for active response outside normal operating procedures. Includes availability of operating reserves and frequency/voltage regulation operations, improved asset health monitoring, applications for energy storage assets, use of rotational inertia in wind generation for grid-stability functions, etc. In the future, it might include adaptive AI software that can detect malware attacks to IT or OT systems and take immediate corrective action.
- **Response / Adaptation.** Emergency preparedness investments and measures that allow the grid to respond to major disruptions. Includes microgrid islanding, grid parallel operations, and grid support capabilities, as well as emergency cybersecurity protocols for enhanced-threat environments.
- **Recovery.** Emergency preparedness investments and measures to enable recovery from a catastrophic failure. Includes blackstart capacity and pathways, adequate large transformer reserves and protected spares, protections for gas and communications networks critical to successful re-start, and effective training, playbooks, and federal/state agency planning that determine who is in charge and what they need to be doing in the event of a major incident.

We can also classify the wide range of existing and potential grid resilience investments according to traditional divisions of power system operation: generation, transmission, distribution, and end-use or distributed energy resource (DER) connection (Tables 1, 2).

Such classifications can be useful in considering how resilience investments can reinforce one another, and how different actors within the system have different roles to play. But enormous questions remain regarding how regulators can properly value resilience investments against their costs, which are ultimately borne by ratepayers.

New methods and metrics are needed to fully incorporate resilience investments into utility planning processes, and there is substantial disagreement in the industry, regulatory, and research communities regarding how to do so. The National Renewable Energy Laboratory's (NREL) March 2020 study is instructive of the challenges, and serves as a critical *caveat* to the pace of current efforts. NREL's study conceptualized resilience from a variety of different perspectives, from generation operators to transmission system control rooms, load centers, and system planners, and even to the perspective of individual homeowners in a long duration blackout during cold weather.[25] Among the report's most relevant findings: (a) "one-size-fits-all" metrics are not appropriate for informing system modeling efforts for implementation, (b) understandings of what customers are willing to pay to avoid long-duration outages are highly limited and may not be quantifiable, and (c) accurate quantification of how particular resilience investments might lead to performance improvements requires better understandings of relationships between threats, their impacts, and their subsequent consequences.

> *"...the grid faces a multitude of threats that appear to be evolving faster than resilience efforts are expanding."*

Thus, while utilities are indeed making significant resilience investments at multiple levels of the grid, the sector has many challenges to overcome before it is able to comprehensively plan, implement, and assess resilience improvements in a rigorous way, much less justify such investments at scale to its regulators, ratepayers, and shareholders. As with transitions of the energy system toward more environmentally sustainable sources, the full transition of the power grid toward a secure, resilient design across both the bulk power and distribution levels will likely require many decades of coordinated effort. In the meantime, the grid faces a multitude of threats that appear to be evolving faster

Table 1: Grid Resilience Measures by Asset Type: Bulk Power System

Generation	Transmission System
• Improved coordination and security regarding interdependencies between fuel supply, telecommunications, and power generation infrastructures • IT/OT cybersecurity improvements and standards • Physical security improvements for power plants • Rotational inertia capabilities for ancillary services and provision of reserves • Dispatchability solutions for intermittent generation • Improve ride-through of solar and wind resources during voltage drops or frequency excursions via smart inverters. • Improve asset health monitoring • On-site fuel storage • Nuclear plants (which can operate for long periods between refueling operations) • Diverse fuel mix	• Visioning, planning, and operations processes to improve technical resilience and recovery performance through continual learning and improvement • Probabilistic Risk Models • Technologies that enable "graceful degradation" of transmission system by selective closing of busses ("load shedding") when power is insufficient to serve all loads. • IT/OT cybersecurity improvements and standards • Advanced cyber situational awareness for system operators • Advanced visualization and situation awareness systems for system operators • Expanded information sharing arrangements and decision-systems between system operators and intelligence agencies • Expanded high-impact event simulation exercises • Vegetation management • Improved design and construction standards for physical assets • Adaptive wide-area protection and control schemes • Adaptive islanding, where critical sub-systems are designed to maintain critical functions in the event of an islanding event. • Underground HVDC lines • Grid-scale energy storage • Large transformer reserve and sharing programs • Substation physical security improvements • Substation elevation • Improve asset health monitoring • Redundant transmission routes • Dynamic line ratings • Power electronics for power-flow control

Table 2: Grid Resilience Measures by Asset Type: Distribution Systems and End Users

Distribution Systems	End-Use and Distributed Energy Resources
• Undergrounding of power lines • Design and construction standards, such as steel or concrete distribution poles • Smart grid advancements and improved Supervisory Control and Data Acquisition (SCADA) capabilities and defenses • Information Technology (IT) / Operational Technology (OT) cybersecurity requirements and standards (state-level)	• Private-sector microgrids • Controllable/Aggregated DER • Local energy storage • Backup generators • Secure military microgrids • Community resilience hubs with on-site, secure generation capabilities • Vendor cybersecurity requirements for grid-connected consumer devices • Improve thermal resilience of residential building stock • Improve ride-through of solar/other DER during voltage drops or frequency excursions via smart inverters.

than resilience efforts are expanding.[xi, 26] And paradoxically, many of the cyber investments we have made to drive economic efficiencies through automation and improve grid resilience and response to natural hazards have simultaneously opened new vulnerabilities to attack from human hazards. As we explore *infra*, recent years have seen a coordinated physical assault on bulk power system transformers in California, unknown-origin drone surveillance activities on French nuclear plants, and the first successful use of entirely remote cyber-attack capabilities to cause physical damage and an hours-long blackout in the dead of winter in Ukraine. Ever-present as well are the risks of electromagnetic pulse or geomagnetic disturbance events—triggered, respectively, by atmospheric nuclear strikes or naturally occurring solar coronal mass ejections—which could permanently disable large bulk power systems in mere moments. As geopolitical systems shift toward a less cooperative and more unstable era, the possibility of state-sponsored or terroristic attacks on civilian infrastructure increases, including attacks that could be opportunistically coordinated to coincide with natural disasters or other disruptive events.[xii]

An early consequence of these changing circumstances has been the development of a variety of national exercises and simulations for critical infrastructure. NERC's E-ISAC, in collaboration with DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), conducts its Grid Security Exercise (GridEx) every two years to provide grid operators with opportunities to respond to simulated cyber

xi An important consideration in the assessment of malicious threats to the grid is the lack of publicly available information on their quantum and severity. There are strategic reasons for this, not least of which that intelligence agencies are often reticent to disclose information about where attacks might be occurring and how often, as it informs adversaries of what we know.

xii Russia, for example, has targeted COVID-19 vaccine development efforts in the US, UK, and Canada with cyberattacks. W. Booth, A. Taylor, and E. Nakashima (2020), "U.S., Britain and Canada say Russian cyberspies are trying to steal coronavirus vaccine research," The Washington Post, July 16th, 2020.

and physical attacks. CESER also conducts a "Liberty Eclipse" exercise focused around state energy agencies and emergency management agency responses to cyber incidents affecting energy infrastructure.

The latest GridEx occurred in November 2019 and involved over 7,000 actors from 526 organizations, including 277 electric, 72 natural gas and 13 water utilities, as well as three telecommunications companies, representatives of various critical federal government agencies, as well as a limited number of vendors.[27] The exercise simulated a coordinated cyber and physical attack on multiple transmission and generation facilities, as well as natural gas transmission assets, resulting in a widespread power outage across New York and Southern Ontario. Among the key recommendations in the after-action summary were that response and restoration plans should account for the complexity of national security issues and specify coordination between agencies, and that they should further take into account inter-dependencies with other sectors (such as gas supply). Also emphasized were the criticality of communications, potential liability issues, and critical supply chain elements. The report also recommended an expansion of the cyber mutual assistance program, as well as strengthened coordination with Canada.

On the Department of Defense side, the Defense Advanced Research Projects Agency (DARPA) conducts secretive cyber war games exercises every six months on a deserted island in Long Island Sound, where grid operators and cybersecurity defenders try to jump-start a dead grid against a "red team" of hackers trying to thwart them. Grid exercises like these recognize that investments in infrastructure, devices, and cyber capabilities are only part of a successful resilience approach. Continual effort is required to improve the capabilities of machines and humans, across multiple institutions, and create effective approaches for coordinated responses. Well-trained soldiers and athletes, for example, function effectively because when critical moments arrive, they have a playbook, training, and know-how of what to do and how to do it.

As innovative early actors and gaming exercises inform the development of best practices for both investment and response, the foundation of resilience is the development of standards that can be applied throughout the sector. NERC has promulgated Critical Infrastructure Protection (CIP) standards that serve as a minimum baseline for cybersecurity on the bulk power grid, and the Trump Administration has signed Executive Orders on both the coordination of national responses to EMP and supply-chain security rules for bulk power system components.[28] Because they apply to all stakeholders, standards and rules must account for differences in the capabilities of the entities they regulate, and thus tend toward minimum requirements rather than reflecting industry-leading best practices. In the expert community, standards are thought necessary for closing the most obvious and critical vulnerabilities in areas of the grid that suffer from underinvestment, but are considered insufficient for developing a fully vigilant approach to security. In some cases, standards can even pose a risk of perverse incentives for security initiatives: when IT personnel are more afraid of auditors than they are of adversaries, cybersecurity operations can become complacent and performative, a series of box-ticking exercises rather than the vigilant defense of systems against motivated and clever adversaries.[29] In such cases, collaborative approaches to standards as tools to improve coordination and best practices—the model used by the National Institute for Standards and Technology (NIST), which promulgates voluntary standards through consensus-based processes—can be a preferable approach. DOE's Cyber Risk Information Sharing Program (CRISP) follows this approach as well, but its high participation costs have thus far precluded many smaller utilities from joining the effort.

Progress to date on resilience within the power sector, when considered in light of the industry's heterogeneous infrastructures, markets, and governance systems, reveals another key strategic consideration. While progress on grid resilience and security must continue and accelerate on an industry-wide scale, it will be a long time before the macro-grid transitions to a sufficiently

resilient architecture and operational culture to address the startling pace of emerging threats to the system. We posit, as a recommendation of our report explored in Section (6), that a "bridge" strategy to a more resilient grid is necessary as both a strategic stopgap as well as a test bed for the rapid development and deployment of advanced and innovative technologies. Military installations, public infrastructure, and public-private partnerships operating at the edge of the bulk power system have already shown progress toward such roles by investing in advanced microgrids, distributed and renewable energy, energy storage, and advanced nuclear technologies.[30] But expanding such efforts into a programmatic vision that aligns civilian and military security needs with the complexity of the grid requires understanding the nature of the threats in greater detail. We turn now to those threats.

Section 2: Cyber Threats

The Wake-Up Call from Ukraine

In late 2015, a cyberattack was launched on the Ukrainian power distribution grid, cutting power to over 200,000 people for up to six hours in the dead of winter. This assault was widely seen among utility professionals and industry insiders as a wake-up call, the first demonstration of what determined cyber-assailants could do to an electric grid. A 2016 follow-on attack on Ukraine's transmission grid (dubbed CRASHOVERRIDE) garnered far less attention, in part because its physical effect was more limited: only one transformer was affected for approximately one hour. It was nonetheless almost immediately pointed to by security experts as more disturbing, as it utilized a sophisticated and modular array of tools with the capability of being both automated and scalable. It was also focused on transmission-level equipment.

A later re-appraisal and analysis of the code involved suggested that the attackers likely possessed the specific intent to destroy critical equipment, with disruption of power operations just the first step in an attack on the transmission system, "with disabling protective gear as a final attack phase to introduce possible physical destruction via cyber means."[31] Perhaps the most unsettling element of the CRASHOVERRIDE attack hinges on this fact: the assailants targeted the protective relays after breakers were opened and operators' situational awareness was compromised, knowing—based on the 2015 experience—that Ukrainian operators would likely resort to manual restoration mode, without knowing the relays were out of service. This could have put operators at risk, while creating extensive damage to the transmission system.

Cyber Threats to U.S. Transmission and Distribution Grids

The available "surface" of the U.S. grid that is susceptible to such attacks is continually expanding. In recent decades, our power grid has evolved from a centralized one-way delivery system to a bidirectional cyber-physical system that is highly complex and increasingly distributed. Several decades ago, a typical utility might have managed a few hundred assets via its manual or semi-automated supervisory control and data acquisition (SCADA) systems.

However, in recent years, significant changes have occurred at both the bulk power system and distribution utility levels. An examination of any grid operator's generator interconnection queue will reveal that instead of a handful of large assets generally well in excess of 100 megawatts (MWs), there are now hundreds of smaller assets.[32]

In addition, much of the grid has migrated from the vertically integrated utility approach of the past to a more complex relationship between generators, transmission owners, distribution utilities and retail providers, overseen by regional grid operators. Physical failures now also have the potential to create dispatch and market-related consequences that would not have existed in the

old utility environment, and create the potential for additional problems across broader regions.

At the distribution utility level, the deployment scale of devices is even more profound, as distributed and "smart devices," ranging from advanced automation, local solar arrays with smart inverters to batteries, programmable electric vehicle chargers, air conditioners, and water heaters proliferate across the system. In 2020 alone, it is estimated that up to 50,000 new residential battery systems will be installed in California,[33] a state that already has over 1 million rooftop solar installations.[34] Likewise, 53 utilities nationwide had control of nearly 600 MW of hot water heater capacity for demand response in 2018: operated in the aggregate, small variations in the load profiles of these consumer-side devices added up to the equivalent of a substantial power plant.[35] In the future, it is anticipated that utilities or associated vendors could be controlling millions of smart devices, with little ability to control the access conditions of the devices themselves or enforce uniform cybersecurity standards.

In all of these cases, the implications for security are profound. Every new connected device represents a new potential attack surface for cyber assailants. At the bulk power level, that implies more opportunities for hackers to bridge across the IT environment into the critical OT environment controlling the critical assets and their operation. As these assets rapidly proliferate at the distribution utility level, at some future point it may not even be necessary to "attack the fortress" of protected centralized grid assets at all. Instead, the ability to hack into vendor systems controlling various distributed devices may be sufficient to destabilize and even take down parts of the power grid. Recent attention has been paid to the rapidly growing electric vehicle charging infrastructure, for example, where hackers could theoretically hack into charger networks, and manipulate them to cause grid instability and potential blackouts.[xiii, 36] The fastest chargers in the U.S. now deliver up to 350 kW of instantaneous demand, equivalent to that required by a large grocery store.

"...the ability to hack into vendor systems controlling various distributed devices may be sufficient to destabilize and even take down parts of the power grid."

In a 2020 sector report, the cybersecurity firm Dragos characterized the utility industry as a "valuable target," with disruptions that can occur across multiple components, including operational systems necessary for situational awareness and facilitating energy trading, enterprise environments and associated IT systems, or cyber-digital assets within the OT environment.[37] Recent attacks in the OT and industrial controls space (with implications for utility controls systems) have included a 2013 Iranian cyber-attack on the SCADA system of the small Bowman flood control dam in Rye, New York,[38] a 2014 attack on an unidentified steel plant in Germany,[39] and the potentially disastrous but fortuitously unsuccessful "Triton" attack on a Saudi oil and gas facility that sabotaged the plant's industrial controls systems.[40]

The Triton attack type, aimed at compromising industrial control safety systems, may become even more effective through the use of artificial intelligence (AI), which can help attackers better blend in with the operational environment and thus avoid detection. One cybersecurity company that deploys AI in defensive strategies

xiii The overall impact of electric vehicles (EVs) and electric vehicle chargers on grid resilience once the industry fully scales is as yet unknown. Obviously, having vehicles dependent on the grid means that extended blackouts would have cascading impacts to mobility, though this is also true for gasoline-based vehicles as stations rely on electricity to operate pumps and most do not have backup generators. On the other hand, the development of technologies and regulations that allow EVs to provide services to the power grid could provide resilience and recovery benefits if EVs could be used in aggregate as a simulated power plant. C. Nelder, J. Newcomb, and G. Fitzgerald (2016), Electric Vehicles as Distributed Energy Resources, Rocky Mountain Institute, *Electricity Innovation Lab.*

indicates that it "has already discovered attacks that leverage basic machine learning techniques to understand how an infected device normally communicates and therefore when and how it should be active to appear as similar as possible."[41] It goes on to state, "In the future, a highly effective use of machine learning will be to train malware in optimal decision-making . . . Supervised machine learning can transfer the skills of the best malware operators directly into the malware itself." Such developments could magnify the damage that could be achieved with little to no human intervention, and would necessitate a significant investment in future defensive AI capabilities.

We have every reason to anticipate that attackers and their supporting nations or organizations will continue to invest more money and research into cyberattacks. Of the 11 activity groups actively monitored by Dragos, seven are looking at utilities in North America, with "the threat landscape focusing on electric utilities . . . expansive and increasing, led by numerous intrusions into ICS networks for reconnaissance and research purposes and ICS activity groups demonstrating new interest the electric sector."[42] Indeed, activity within the last year has been significant, with one Chinese hacker group, known as APT10, believed to have targeted at least 17 U.S. utilities in 2019 with phishing emails intended to infect employee computers with a remote access program called LookBack. At least three active groups show intent or capability to affect and disrupt generating facilities, while two groups—including the one responsible for the Ukraine attacks—are focused on the transmission sector, possibly utilizing the Ukrainian experience as "a blueprint . . . to disrupt operations and cause the greatest possible damage." In addition, the same actors going after the transmission networks could deploy similar tools in attacking distribution-level facilities.[xiv]

Supply chains are also at risk. Original equipment manufacturers (OEMs), telecommunications providers, and third-party vendors are targets in their own right, as each presents opportunities for infiltration by malware that can lie in wait for years before activation by malicious actors, who might use them to cripple critical communications or control networks for restoring power in a coordinated fashion. This is a challenging, time-consuming, and costly issue to address. One Connecticut utility reported over 200 suppliers that required scrutiny in 2019, with the need to hire more personnel to oversee that process.[43]

A recent Executive Order addresses the issue of OEMs in the electric industry and the need to "protect the security, integrity, and reliability of bulk-power system electric equipment used in the United States,"[44] prohibiting acquisition and installation of any bulk power equipment that may have been supplied by an adversary of the United States. Further guidance is expected from the Department of Energy as to the specific ambit of the rule. In addition to the Executive Order, NERC will soon institute CIP-013, a new cyber standard addressing utility supply chains affecting

xiv Connecticut's experience with distribution-system infiltration is eye-opening. As reported by the state's Chief Cybersecurity Risk Officer: "[a]ggression against Connecticut utilities grew during the past year, with an increased number of threat actors, larger volume of attempted penetrations and introduction of new, more sophisticated attack weaponry. Nation states remain active, with most threats coming from the same four nations previously reported: Russia, China, Iran and North Korea. One utility recorded threat attempts from more than 1,000 distinct actors (which may include sources using multiple identities) . . . By all accounts, the volume, sophistication, creativity and persistence in efforts to penetrate and gain control of U.S. utilities and their services all were greater in 2019 than in the past." The report also notes the advent of "machine-to-machine threats, met by concurrent machine-to-machine defenses," and excursions of implantations beyond communications into management systems for generation and transmission activities. Indicative of a fundamental problem in institutional response, the report notes that "national security officials insist that utility executives and many players with high-level security clearances are not aware of the extent of ongoing operations penetration and implantation," thus work in the area "will necessarily be incomplete until intelligence sharing reflects partnership at levels not currently in place." Astonishingly, Connecticut utilities themselves have reported no evidence of security breaches, nor have they been informed of any specific intrusions. The report concludes ". . . if those utilities, despite arduous, serious, good-faith efforts to detect and eliminate threats do not find evidence of penetration, they need and deserve U.S. Government timely and detailed information sharing." A. H. House (2019), Connecticut Critical Infrastructure 2019 Annual Report, *Office of the Chief Cybersecurity Risk Officer, State of Connecticut.*

medium and high-risk bulk power system assets, by October 2020. CIP-013 is intended to address software, vendor remote access, information system planning, and vendor risk management.

Cyber Threats to the Vulnerable Grid Edge

Supply chain and vendor management issues have grown with the rapid growth of the "smart grid" and other industry trends, in which a rapidly proliferating number of actors is creating multiple dynamic solutions and deploying a host of interactive technologies at the so-called "grid edge," both behind the meter at the customer level on distribution systems and at the end of transmission lines for wholesale energy consumers, such as civilian critical infrastructure and military bases. Many of these customer-sited solutions are specifically designed to interact with the distribution grid or with the bulk power grid. Some assets are simply designed to curtail consumption—such as water heaters that only warm water during specific hours. However, an increasing population of devices—ranging from solar panels to batteries and vehicle-to-grid capabilities—is now injecting energy into the grid, creating increasingly large bi-directional power flows.

Today, for example, 56,000 single family homes on the Hawaiian Island of Oahu boast rooftop solar arrays,[45] with most of those exporting electricity to the grid during mid-day sunshine. The local utility, Hawaiian Electric, recently signed a contract with global solar installer SunRun to install 1,000 residential battery systems that can be aggregated as a resource.[46] Hawaii may represent an extreme case today, but it demonstrates emerging trends as solar costs decline and installed battery costs have fallen by 50% in the past two years.[47]

The risks here are twofold: First, the devices are connected and aggregated, which means that they could be controlled *en masse* by the wrong entity, creating an increasing risk of instability to the power grid—especially at the distribution level. Second, many of the companies active in this space are start-ups, which generally implies that they are under-investing in robust cybersecurity solutions.

A critical piece of this new ecosystem is the smart inverter – the device that connects the DC-level device to the AC-level power grid, provides operating instructions, and communicates with the grid to autonomously manage voltage through the use of internet-connected software. If malware were able to control a significant population of smart inverters and adjust voltages in the wrong direction, it could create significant instability and even potential blackouts.[48] There is growing industry recognition of this issue, and an effort to establish cyber security protocols as an industry, but remote firmware upgrades remain a major vulnerability. In fact, inverter manufacturer Enphase unintentionally highlighted the potential scope of the problem in a 2015 blog highlighting its efficiency in undertaking a remote firmware upgrade to 800,000 devices.[xv] This is good news if the person undertaking the upgrade is sitting in Enphase's backroom. The news is not quite so sanguine if that operator happens to be sitting in Russia, China, North Korea, or Iran, with other designs in mind.

xv *"So the other day someone in a backroom in Enphase HQ quietly pressed the enter button and changed the settings on 800,000 inverters across 51,000 homes. No truck rolls. No field calls. No dogs to navigate. No chatty retired engineers to talk to."* A. Konkar (2015), *"'Something Astounding Just Happened': Enphase's Grid-Stabilizing Collaboration with Hawaiian Electric,"* Enphase Stories, *Mar. 11, 2015.*

Transmission System Vulnerabilities

A coordinated attack on a limited number of critical assets, such as high-voltage transformers or large power plants, could render parts of the grid inoperable for months. While no attack of this nature has occurred to date, there have been some disturbing indicators that suggest both the future possibility of such an event and the lack of physical security in place to prevent it.

An attack on a California substation in the middle of the night on April 16, 2013 highlighted the potential vulnerabilities. An unknown number of individuals approached the Pacific Gas & Electric (PG&E) Metcalf substation in San Jose, California and cut the fiber optic communications lines to the station. In an attack taking less than 20 minutes, they then fired over 100 rounds of ammunition into 17 transformers, rendering the equipment inoperable. PG&E was, fortunately, able to re-route power around the damage, avoiding any major outages to Silicon Valley. But doing so was challenging and neighborhoods lost power temporarily, the utility reported. The attack resulted in $15 million in damages and a pledge from the utility to spend an additional $100 million improving facility security through measures such as armor plating for large electronics, infrared cameras, audio sensors, and seismic recorders. FERC ordered development of mandatory physical security standards in the aftermath of the attack. Later assessments from DHS indicated that the attack may have been an "inside job" perpetrated by disgruntled employees.[49] Though the attack was unsuccessful, what is disturbing about physical attacks is the ease with which they can be executed, and the difficulty of tracing responsibility. In less than half an hour, a small group of people with cable cutters and rifles caused more damage to the U.S. grid than any state-funded team of OT cyber-hackers from across the ocean with top talent and million-dollar budgets. No one has ever been arrested or charged in connection with the Metcalf station sniper attack.

Such a localized attack may pose significant problems, but is not existential. By contrast, a coordinated attack on a combination of some of the most critical high-voltage transformers could pose a far greater problem. The National Research Council reports:

- Substations and the large high-voltage transformers they contain are especially vulnerable, as are some transmission lines where the destruction of a small number of towers could bring down many kilometers of line. Terrorist attacks on multiple-line transmission corridors could cause cascading blackouts.[50]

This vulnerability exists because a large volume of energy—as much as 60-70% of annual electricity demand—travels over a relatively small number of high-voltage transformers, about 3% of the U.S. transformers overall.[51] These larger transformers are enormous, in some cases weighing over 400 tons, so replacements are not easy to move into place. Furthermore, they are often custom-built, not interchangeable across the system, and take a long time – typically between five and 16 months—to manufacture.[52] Also troubling is that most of these transformers have been imported from abroad in recent years,[53] and the U.S. lacks domestic manufacturing capacity, down to the specialized steel[xvi] required for the cores, to produce them.[54] A blackout caused by a sufficient failure of high voltage transformers could thus last for weeks, if not months.

xvi The U.S. Commerce Department launched an investigation in May 2020 into whether imports of foreign transformer parts pose a threat to national security. S. Eaton (2020), "Trump administration to prove whether imported transformer parts threaten Cleveland Cliffs subsidiary AK steel," Cleveland.com, May 4, 2020.

There has been some effort to address this vulnerability, but in a patchwork fashion. For example, three large energy companies[xvii] launched Grid Assurance– a private company that provides a geographically dispersed stockpile of transformers warehoused in confidential locations close to transportation access points.[55] In addition to Grid Assurance, the Edison Electric Institute (EEI) maintains the Spare Transformer Equipment Program (STEP) under a mutual aid approach that currently includes 56 utilities.[56] EEI also coordinates SpareConnect, a mutual assurance effort to help utilities with equipment in the event of events not related to terrorism. Finally, there are a handful of other programs across the country including Wattstock—which offers a Transformer Recovery Program that maintains an inventory of spare transformers—and RESTORE—an initiative of largely southern utilities created in response to DOE's 2017 Strategic Transformer Reserve Report.[57]

The fundamental drawback to these approaches is that mutual assurance approaches may fail when widespread events happen, putting simultaneous stress on systems and finite resources when multiple parties need assistance at the same time. Further, a determined adversary could not only target the physical equipment, but also the vulnerabilities in the related infrastructure (*e.g.*, bridges and rail lines) that would need to be traversed in order to bring in replacement equipment. It is also critically important that the IT networks of these various replacement programs be protected at the highest level.

Vulnerability of Generating Facilities

Transformers are perhaps the most vulnerable element in the system to physical attack, but large power plants are not immune, and past events have shown that they may be targets as well. The loss of several major generating stations could pose a potential threat to grid stability, although many grids may have sufficient generating resources in their reserve margins to address that issue. Of particular concern is the radioactive risk posed by a targeted attack on a nuclear facility.

Although nuclear facilities possess high levels of security, assailants may be probing defenses for weaknesses. French nuclear plant operator EDF reported at least six flights of unidentified and unauthorized drones over seven of its nuclear plants during a two-week period in October of 2014, with four of those flights taking place at widely separated sites on the same day.[58] A later report highlighted additional flights, bringing the total to 15 over nine nuclear facilities.[59]

Though initially dismissed as a stunt by anti-nuclear environmental groups, later intelligence established that the aircraft used were not the typical hobbyist equipment, but helicopter-like drones with more extensive tactical capabilities.[60] The French Prime Minister's General Secretariat for Defense and National Security characterized the flights as "being carried out in a repeated and simultaneous manner over certain nuclear sites in our country...The objective apparently sought by this type of organized provocation is to disrupt the chain of surveillance and protection at these sites." France's interior minister indicated publicly at the time that the government had ways to neutralize the drones, but would not comment further.[61] Activist group Greenpeace has made it a point to focus on potential vulnerabilities in this area, and in January 2019 succeeded in dropping a distress flare canister onto a French nuclear fuel processing facility from an octocopter drone to demonstrate that facilities are not adequately protected.[62]

xvii The companies involved include Berkshire Hathaway, American Electric Power, and FirstEnergy.

Section 4: Electro-Magnetic Pulse Threats

Electro-Magnetic Pulse Attacks

Electromagnetic Pulses (EMP) constitute another existential threat. The potentially devastating impact of EMP[xviii] to power grids first became known in 1962, when the U.S. military exploded a high-altitude 1.4 megaton nuclear device 240 miles about the earth and 900 miles distant from Hawaii. The resulting EMP proved sufficiently disruptive to the power grid to blow out streetlights, and also resulted in radio and telephone disruption. It should be noted that today's electrical systems are miniaturized compared to those in 1962, and thus far more vulnerable to electromagnetic pulse damage. Such a pulse can immediately damage utility computer and SCADA (supervisory control and data acquisition) systems that govern the grid.

While the military subsequently made some efforts to harden its infrastructure,[xix, 63] the same cannot be said for civil society, which has been left largely unprotected. In the early 2000s, this glaring weakness came to the attention of Congress, which commissioned an initial report delivered in 2004. A more detailed assessment—Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack—followed in 2008. That seminal document summarized the danger to society as follows:

- A single EMP attack may seriously degrade or shut down a large part of the electric power grid in the geographic area of EMP exposure effective instantaneously. There is also the possibility of functional collapse of grids beyond the exposed one, as electrical effects propagate from one region to another . . . Should significant parts of the electric power infrastructure be lost for any substantial period of time, the Commission believes that the consequences are likely to be catastrophic, and many people may ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities.[64]

A late 2019 North America Electric Reliability Corporation (NERC) report on the topic comments that the entire span of the electric system would likely be affected (NERC, 2019).[65]

It is estimated that an EMP explosion 30 miles above the earth would affect a radius of nearly 500 miles, while a detonation at 300 miles (potentially delivered by missile or satellite) would have an estimated radius of 1,500 radius, effectively covering most of North America. The potential threat actors with clear ballistic missile capabilities include not just Russia and China, but also Iran and North Korean, which has articulated the goal of delivering a "super powerful EMP attack" as a strategic goal (AFPC, 2018).[66]

Despite the magnitude of the potential threat, the level of effort to respond to it has been relatively minimal to date. Both the Department of Homeland Security (DHS) and the Federal Energy

xviii The International Electrotechnical Commission (IEC) defines three EMP hazard fields based on distinct characteristics and time scales: 1) The early time component (E1 EMP) consists of an intense, short-duration electromagnetic pulse characterized by a rise time of 2.5 nanoseconds and amplitude on the order of tens of kV/m (up to 50 kV/m at the most severe location on the ground). 2) The intermediate time component (E2 EMP) is considered an extension of E1 EMP and has an electric field pulse amplitude on the order of 0.1 kV/m and duration of one microsecond to approximately ten milliseconds. 3) The late time component (E3 EMP) is a very low frequency (below 1 Hz) pulse with amplitude on the order of tens of V/km with duration of one second to hundreds of seconds. E3 EMP is often compared with severe geomagnetic disturbance (GMD) events; however, the intensity of E3 EMP can be orders of magnitude more severe, and E3 EMP is much shorter in duration than GMD events, which can last for several days. Electric Power Research Institute (2019), High-Altitude Electromagnetic Pulse and the Bulk Power System: Potential Impacts and Mitigation Strategies.

xix E.g., the North American Aerospace Command (NORAD) and U.S. Northern Command announced plans to move resources including communications equipment to the EMP-hardened Cheyenne Mountain complex. American Foreign Policy Council (2018), Strategic Primer: Electromagnetic Threats: Current Capabilities and Emerging Threats.

Regulatory Commission (FERC) have established some limited guidance for addressing the threat of EMPs. However, the NERC document specifically addressing EMPs and offering recommendation provides insight into the current insufficient level both of understanding and preparation. The three policy recommendations are as follows:

- **Policy Recommendation #1:** Establishing BPS (Bulk Power System) performance expectations for a pre-defined EMP event
- **Policy Recommendation #2:** Providing industry and public education on EMPs
- **Policy Recommendation #3:** Coordination with other Critical Infrastructure sectors on EMP matters

These recommendations make it abundantly clear that the current state of preparation is far from adequate. That impression is further reinforced by the 'policy matters' the report highlights as influencing the electric sector's response to the threat:

- **Policy Matter #1:** The high costs of EMP mitigations and the lack of cost recovery mechanisms
- **Policy Matter #2:** Access to classified information on EMP threats and impact
- **Policy Matter #3:** Declassification of information for industry use

In other words, the industry currently lacks information that could help define the threat, the costs to address the issue will be high, and there is no clearly defined mechanism to pay for the necessary investments, especially since the public utility sector is compensated through state-defined ratemaking and reimbursement policies that do not address this type of consideration.

The report recommends that guidelines should be developed for the industry in order to mitigate impacts on assets such as control rooms, substations, and power plants. It also notes that to create capabilities for response and recovery, the electric reliability enterprises (NERC and its regional entities) "should consider partnering with the appropriate agencies to develop a real-time national notification system for the electric sector to System Operators and Plant Operators pertaining to an EMP event and its parameters."

In March of 2019, the Trump Administration issued a long-overdue Executive Order on Coordinating National Resilience to Electromagnetic Pulses that directed various agencies to address the issue of both human-induced and naturally occurring EMPs. Among other tasks, it directed the Secretary of Energy "to conduct early-stage R&D, develop pilot programs, and partner with other agencies and the private sector, as appropriate, to characterize sources of EMPs and their couplings to the electric power grid and its subcomponents, understand associated potential failure modes for the energy sector, and coordinate preparedness and mitigation measures with energy sector partners." It further directed DHS to "use the results of risk assessments to better understand and enhance resilience to the effects of EMPs across all critical infrastructure sectors, including coordinating the identification of national critical functions and the prioritization of associated critical infrastructure at greatest risk to the effects of EMPs."

Both the NERC report and the Executive Order highlight an uncomfortable reality: the country is unprepared to deal with this contingency at this time: any real planning at a regional or national level for such an EMP contingency—or any meaningful investment to coordinate activities to mitigate against it—has yet to occur.

An oft-deployed counterargument to the threat of an EMP attack of this nature is game theoretic. Such an attack would most likely be launched by another nation-state and be clearly attributable, and thus the U.S. has sufficient military response capability to deter an adversary from considering such an option. Surely, such arguments postulate, the doctrine of mutual assured destruction familiar from the Cold War may still hold sway in this instance. No one can ultimately know such

things until the moment at which it is too late to matter. What we can know, however, is that the Sun has no such strategic considerations, and that it may pose a naturally occurring threat that obviates such debates.

Geomagnetic Disturbances

Naturally occurring geomagnetic disturbances (GMD, often referred to as "solar flares," "solar weather," or the more technical "coronal mass ejections") create similar effects as those from an EMP event, but affect longer power lines operating at transmission voltage levels and large power apparatus, and thus may not be as widespread across the system but may affect its critical components at an even wider geographic span.[67] The logical question to be asked, then, is just how powerful and widespread a worst-case event might actually be. The most recent event of this type was the 1989 solar storm that centered in the province of Quebec. That geomagnetic disturbance, amplified by transmission lines hundreds of miles long, almost immediately blacked out Hydro-Quebec's grid, with a province-wide outage lasting nine hours.[xx]

Over the subsequent 24 hours, additional and significant impacts were felt further south in the U.S., putting other power grids at risk. Indeed, a subsequent NERC analysis highlighted 211 "Reported Events" from utilities across the country, some of which were quite severe.[68] For example, a 1,000 MVA transformer connected to the 500-kV transmission grid at New Jersey's Salem Nuclear Plant was completely destroyed. One report on the topic commissioned by Oak Ridge National Laboratory indicated that the damage was widespread, though in some cases not immediately visible. For example, within two years of the 1989 event, 11 nuclear plants observed failures of large transformers that were likely linked to the event.[69]

The 1989 event resulted in significant damage, but it is by no means the most powerful solar storm possible. The August 1859 "Carrington Event" gives us some sense of what a more powerful storm could be like. In that instance, many telegraph lines around the world were rendered unusable, and some even caught on fire.[70] That storm is estimated to have had a Disturbance Storm-Time (Dst)[xxi] index between -800 and -1750 nano-teslas (nT), while the Quebec storm measured -589 nT.

Recent events indicate that GMDs are no relic of the past, and are in fact much more likely than most realize. In July 2012, NASA reported that the Earth experienced a near miss from a solar flare on the same level as the Carrington Event, registering a Dst index in the neighborhood of -1200 nT. In that instance, the powerful solar flare moved straight through the Earth's orbit, but fortunately the planet was elsewhere on its trajectory and it only just happened to hit a solar observatory satellite. A week earlier, and the world would have been severely impacted. Thanks to that serendipitous hit on the satellite, NASA scientists estimate the odds of a Carrington-class solar storm hitting the Earth in the next ten years at a sobering 12%.[71]

"Thanks to that serendipitous hit on the satellite, NASA scientists estimate the odds of a Carrington-class solar storm hitting the Earth in the next ten years at a sobering 12%

xx As Hydro-Quebec described the event: "On March 10, a strong wind left the Sun, heading for Earth. On March 12, the first voltage fluctuations were being seen on the Hydro-Québec transmission grid. The System Control Centre was doing what it could to maintain stability. However, on March 13 at 2:44 a.m., the Earth's magnetic field was fluctuating violently. The grid's protection system was triggered, and a blackout occurred in less than a minute! The province was submerged in darkness for more than nine hours."

xxi The Dst index measures magnetic activity derived from equatorially-proximate geomagnetic observatories, which measure the intensity of disruptions to the "ring current," a globally symmetrical equatorial electrojet.

Section 5: Other Threats and Threat Multipliers

To the three major existential threat categories—focused and coordinated physical attacks on critical infrastructure, human-induced or natural electro-magnetic disturbances, and cyberattacks—one might add a fourth, at least in some areas of the country. That would be a large-scale seismic event, such as might occur in California, the Pacific Northwest, or the Midwestern United States. The New Madrid Seismic Zone, for example, produced a 7.7 magnitude earthquake in the country's mid-section over 200 years ago. Should a similar event occur today, it would likely damage or destroy hundreds of critical assets over many states in the region impacting as many as 150 million Americans.[72]

Major hurricanes were the original impetus for much of the resilience spending in the grid to date, and their continuing intensification will amplify the background impacts to the grid against which lower-frequency events occur. Each event is significant enough in its own right, but in some instances, each could be made worse, magnified by the existence of some other event or situation, such as the pandemic we are currently experiencing. For example, hackers could launch an attack immediately on the heels of a widespread regional weather event, such as a hurricane or blizzard, where resources are stretched thin and the population is already vulnerable. From an adversary's point of view, such an event might be a desirable time to stage an attack, since the potential impacts could be highly magnified and response times significantly delayed.

In addition, a multi-pronged and systematic attack must also be considered, since that type of worst-case scenario would bring about the highest level of confusion and lethality. Planning exercises should not shy away from these types of scenarios, simply because they are unimaginable. As the 911 report commented, "The 9/11 attacks were a shock, but they should not have come as a surprise." It went on to state, "We believe the 9/11 attacks revealed four kinds of failures: in imagination, policy, capabilities, and management."[73] Every potentially hostile activity to date, whether testing of a rocket or the implantation of malware, should be read for what it could turn out to be: a signal of hostile intent in a prolonged geopolitical struggle where the battlefield is no longer clearly defined, nor the rules of engagement definitively proscribed. As the natural world that supports human civilization becomes increasingly unstable, nations, populations and independent actors will likely become desperate, thus increasing the risk of taking increasingly desperate measures.

COVID-19 is a similar "unimagined" phenomenon in that respect. SARS, MERS, repeated Ebola outbreaks – they all signaled to us that this has always been a real and distinct possibility. Yet even as we watched the February videos of Chinese governments spraying whole cities with disinfectant in a desperate attempt to fight the virus, and the first cases had likely already invaded our shores, our stock markets were soaring to record heights and Americans took no meaningful precautions. That an invisible plague would shut down most of our economy and destroy over 30 million jobs within two months was simply not within our ability to comprehend.

We must develop the imagination to do so, and in doing so we must consider the future direction of the grid itself, and how new capabilities as well as vulnerabilities may emerge within it. Most of the U.S. population resides near the oceans and other large bodies of water. Offshore wind energy in the United States gained its first commercial operation in 2016: the 30 MW Block Island Wind Farm off the coast of Rhode Island. Many more are slated to follow: seven states on the U.S.'s east coast have committed to build up to 29,768 MW of wind power offshore by 2035,[74] and the Department of the Interior's Bureau of Ocean Energy Management has already executed fifteen active leases for development.[75] The National Offshore Wind Strategy developed by the U.S. Department of Energy and Department of Interior envisions 86 GW of offshore wind by 2050.[76] Not only do

these developments necessitate the development of massive oceanic power infrastructure for the collection and transmission of wind energy (and potentially other marine energy sources, such as wave and tidal power) to coastal load centers, but the terrestrial grids they connect to must be overhauled to be able to accept such large influxes of power. That need presents a tremendous opportunity for coastal grids that is unavailable to more established portions of the bulk power system: the ability to plan them for resilience and security from the ground up, both to protect offshore assets from natural and human threats, and to provide grid resilience benefits and black start capacity to the terrestrial grid. Indeed, as land use management and stability become increasingly difficult to predict and unstable due to flood, hurricanes, fire, droughts, erosion, and the like, it may be simpler and faster to site major transmission underwater. Ample precedent exists in undersea cables.

Bays, lakes and coves also present underwater transmission opportunities. For example, where concentrated populations and attendant power demand resides on one side of a large bay, and ample solar siting opportunities exist on the opposite side, underwater transmission can simplify and hasten the outcome. Some bayside communities, such as Sausalito, California, a community facing east on steep hillsides with little solar radiation, are evaluating docked and bay anchored solar barges in combination with battery and electric vehicles to supplement land sited solar powered microgrids. Local planners see that as sea level rises, the barges rise and transmission is not interrupted.

Section 6: Recommendations

Recommendation 1:
Provide Full and Accurate Threat Information to Grid Operators.

Congress should direct the Department of Energy, Department of Homeland Security, and the Director of National Intelligence to establish a central clearinghouse and decisional node for communicating full and accurate threat information to bulk power system operators and electric utilities. The clearinghouse should build upon and expand the capabilities of the industry-led Electricity Subsector Coordinating Council (ESCC) and the North American Electric Reliability Corporation's Energy Information and Analysis Center (E-ISAC) to provide: 1) Detailed and timely threat intelligence sharing with appropriate industry personnel; 2) Real time threat-information networks and action tools for control room operators; and 3) Expanded and continually-evolving red-team exercises to test defenses against evolving threats. The clearinghouse should also collaborate with the government to increase the number of security clearances available to electric utility industry personnel.

Officials have been aware of threats to our electricity grid for some time. We know that a well-resourced, determined, and sufficiently trained adversary would be capable of taking down significant parts of the grid for potentially extended timeframes. And yet the response, both in countering the networks that target us and in preparing for the aftermath of a successful attack, has not kept pace with the threat. The reasons for this are manifold: a tangle of agencies with poorly coordinated responsibilities and conflicting departmental priorities, heterogeneous and increasingly decentralized private ownership of

power sector assets, and a continually expanding attack surface through the proliferation of smart devices both within and at the edge of the system, among many others.

None of these realities are easily or quickly addressed. Our government cannot command and control a largely privately-owned power grid, or the many private companies that provide services and devices for use on it, from generation to end-use. The agencies involved—housed throughout the Department of Energy (DOE), Department of Homeland Security (DHS), and Department of Defense (DOD)—all have legitimate interests in the problem and perspectives that connect but do not precisely align, and for the foreseeable future must continue to work together with one another and with industry.

That collaboration, albeit imperfect, must be radically empowered to act with unprecedented speed and agility in response to real-time threat intelligence information via a central clearinghouse and decisional node. Placing that node within any one of the relevant agencies is likely to exacerbate interagency seams rather than resolve them, and would do little to encourage private sector participation and buy-in. Accordingly, we recommend an approach that leverages existing self-governance mechanisms within the industry: the powers of the Electricity Subsector Coordinating Council[xxii] (ESCC) and NERC's Electricity Information Sharing and Analysis Center (E-ISAC) should be substantially expanded to serve as such a node, just as the NERC was empowered to manage reliability after the 2003 Northeast Blackout. The expanded ESCC/E-ISAC node should be charged with ensuring, through a public-private partnership arrangement:

- Detailed and timely threat intelligence sharing with appropriate industry personnel, the NSC, and federal agencies charged with cyber defense of governmental and military networks;
- Mechanisms—such as real-time information sharing networks and action tools that reach directly into system control rooms—to enable utilities, system operators, and federal agencies to act on threat intelligence in a timely and effective manner; and
- Expanded and continually evolving red-team exercises[xxiii] in coordination with efforts at DOE, DHS, and DOD that test utility sector defenses and resilience plans against evolving threats, and that create cultures of vigilance and proactive defense rather than "check-the-box" approaches to security.

The single most important factor for empowering both the private sector and the government to act on resilience and security at the systems level is the first of the clearinghouse's responsibilities: full, accurate, and timely information about the nature and quantum of the threats facing the grid. In interview after interview with subject matter experts, the bottleneck of information between intelligence agencies and system operators emerged as a recurring frustration. The dearth of meaningful details in threat alerts has prevented the industry from appropriately responding to them or justifying investment in security measures to regulators. On the other hand, the sensitive nature of threat information presents a countervailing consideration for secrecy that has stymied attempts to share it. We recommend a three-pronged approach to navigate the impasse.

First, the clearinghouse should be empowered to publicly "name and shame" hostile and malicious actions to our nation's civilian infrastructure and reveal the frequency of intrusions, while maintaining appropriate secrecy regarding

xxii The industry CEO-led ESCC is the principal liaison for national-level disaster preparation and response between the electric power industry and the federal government.

xxiii DARPA has pioneered this approach with its Plum Island exercises. B. Christofaro (2019), "The Pentagon has its own island off New York where nobody can go that it's using to run war games for a giant cyberattack on power grid," Business Insider, May 25, 2019.

specifics. Second, the government should grant security clearances, at least at the SECRET level, to more Congressional leadership and committee staff with energy responsibilities, and to more partners in the private sector. Currently, it is common that only the senior-most personnel in the utility sector are granted clearances, and this prevents them from sharing detailed information with appropriate staff needed to actually address vulnerabilities. Third, coordinating agencies for critical infrastructure should be permitted to speed up sharing of tear-line data, a key component in allowing system owners and operators to implement protective measures as quickly as possible to stem malicious activity and intrusions. In all of these goals, the clearinghouse should work to leverage and augment the pioneering work done by DOE's voluntary Cybersecurity Risk Informational Sharing Program (CRISP), which was significantly expanded in 2018.

The slow pace of current intelligence sharing negatively affects power system resilience, but goes beyond just the power sector. For example, the Chinese Ministry of State Security coordinated attacks on managed service providers (MSPs)—who provide IT services to partner organizations—starting in May 2016 with malware called PLUGX and REDLEAVES, implanted by a hacker team known as APT10. Public guidances were not issued by UK and U.S. intelligence agencies until April 2017 (with the U.S. guidance issued 3 weeks after the UK guidance).[77] Full reports were not released until December 2018: a year and a half after it was well-known that the hackers had targeted UK and U.S. businesses, and over two and half years since the initial attack occurred. Still, mainstream U.S. news media did not report on APT10 at all until August 2019,[78] when the group's LookBack malware attacks on the U.S. utilities sector—implanted by spear phishing[xxiv] efforts wherein APT10 hackers impersonated engineering licensing boards—were reported by Proofpoint, a private sector security firm.[79] If it is indicative of standard procedure, the extended information release timelines related to the REDLEAVES attack and the silence of agencies on LookBack indicates a systematic failure of the government to communicate threat information to critical infrastructure owners and operators in a timely manner.

The argument, generally, for such "run silent, run deep" procedures is that intelligence agencies are loath to publicly disclose to adversaries what we know about their activities. But it strains credulity to believe that our competitors, who have devoted massive state resources to developing top-talent cyberespionage groups—whose elite workforce does not, as in our country, have the opportunity to earn lucrative Silicon Valley stock options instead of working for the government—would be unaware of our ability to see them. Certainly, the lack of public disclosures about their successful intrusions has not dissuaded them from further activity. Perhaps, in some cases, sunlight is the best disinfectant: more threat intelligence information might simply be declassified.

In any case, a serious reappraisal of the balance of information between the intelligence and critical infrastructure communities is warranted. We deride the "Great Firewall" of China for shielding its citizens from the alleged decadence of Western culture. But how much longer can we shield ours from the realities of the autocratic forces that would remake the world in our absence, and who actively seek ways to neutralize us?

Recommendation 2:
Establish an Independent National Resilient Grid Authority to Develop a State-of-the-Art Grid Scale Experimentation Program.

Congress should establish a National Resilient Grid Authority (NRGA)—an independent agency staffed by rotating appointments of the country's most highly qualified energy, cybersecurity, and national defense experts from both the government and private sectors. Congress should provide sufficient funding and charge the

xxiv "Spear phishing" refers to personalized hacking attempts targeted to specific individuals in an organization based on publicly-available information about the target. Proofpoint (2020), *Spear Phishing Attacks*.

NRGA with developing a state-of-the-art grid scale experimentation program that identifies emerging threats and vulnerabilities via world-class red-teaming, invites the private sector, DARPA, ARPA-E and federal government labs to submit and judge innovative solutions, and tests those solutions against attackers in a competitive experiment environment. The NRGA's operations should be cyclical, with new threats identified and new solutions developed on an annual basis by an ever-changing cohort of the country's best technical and strategic talent. Based on the threats and technologies it works to solve, the NRGA should also identify potential policies and regulations for consideration by FERC, NERC, and the insurance industry. The NRGA should report its findings and recommendations to the National Security Council (NSC), which will then facilitate dissemination information to the relevant executive branch and Congressional stakeholders.

On October 4th, 1957, the Soviet Union launched its first satellite, *Sputnik I*, and a shocked America realized suddenly that it was losing the space race. In less than a year, Congress created the National Aeronautics and Space Administration (NASA) from the National Advisory Committee for Aeronautics, and pulled top talent from other government agencies and the private aerospace sector to address the critical need for American space supremacy. Eleven years later, NASA put Neil Armstrong on the moon. The story of NASA demonstrates what can be done when the nation's best and brightest are given the resources to solve big problems and the autonomy to attack those problems with boldness and speed. Independent agencies have proven to be indispensable organizational structures for doing both.[xxv]

Independent federally funded research and development centers (FFRDCs) have also contributed rapid advances to critical needs, often yielding ancillary benefits well beyond the original objective. For example, in response to the Air Defense Systems Engineering Committee's (1950) finding that the country was unprepared to repel air attacks, the government created the Lincoln Laboratory at the Massachusetts Institute of Technology (MIT) in 1951 to improve air defense systems through advanced electronics.[80] Within five years, the Lincoln Laboratory had created the Semi-Automatic Ground Environment (SAGE), the network of computers that could coordinate data from many radar sites and aggregate a unified image of wide-area airspace. But the critical technology that made SAGE work would have even broader ramifications: Jay Forrester's development of magnetic core memory, which formed the basis for computer hard drives.[81]

More recently, government-sponsored organizations that operate in the private sector have demonstrated innovative means of fostering talent and technologies outside of government and academic systems: particularly cyber technologies. In the late 1990s, the intelligence community recognized the need for vastly improved collection and analysis of information—capabilities that were already being developed in the private sector, which had attracted the top talent in the field to Silicon Valley and elsewhere. But the frenetic pace of the tech sector made for a poor interface with slower moving government agencies. The solution was a private, not-for-profit strategic investment firm to accelerate information technology developments for national security agencies: In-Q-Tel, known informally as the "venture capital arm of the CIA."[82] In-Q-Tel has since invested in over 170 known startup companies, including Keyhole, which Google acquired in 2004 in order to build Google Earth.

Protecting the grid from the rapidly evolving threats examined in this report requires a hybrid approach of the three types of independent agencies described above, for three connected reasons. First, the nature of the threat requires rapid response and development of new technologies with a minimum of bureaucratic red

xxv Indeed, a year after the moon landing, Congress established another independent agency—the Environmental Protection Agency (EPA)—to address the air and water pollution crisis. Today, criteria and precursor pollutants are 77% lower than they were in 1970 (EPA, 2020a). U.S. Environmental Protection Agency (2020), Our Nation's Air 2020.

tape. Second, the sheer scale of the transmission and distribution systems and the widening attack surface of grid-connected devices requires diverse sets of expertise: cybersecurity; industrial control systems; artificial intelligence; civil, electrical, and mechanical engineering; materials science; grid architecture; interdependent systems analysis for gas and telecommunications considerations; and many others. Third, the need to not only react to emerging threats but to anticipate and regain the lead against potential adversaries requires the innovation and talent of the private technology sector.

Accordingly, we recommend that Congress create a National Resilient Grid Authority (NRGA) consisting of the operational capabilities of an independent agency, the research breadth and access to facilities and academic resources of an FFRDC, and the connection to private sector innovation of an In-Q-Tel style organization. NRGA's primary mission should be the testing and demonstration of critical technologies associated with providing grid security and resilience capabilities through a fully functional integrated transmission and distribution system test bed, focused on continuous and iterative threat and vulnerability identification and solutions development and testing.

The agency should follow a rotating staffing procedure that ensures the influx of new talent and new ideas on a regular basis, while preserving senior technical staff to assure institutional memory, mentoring of new recruits, and preservation of lessons learned, and position itself so as to attract the country's most qualified and promising minds from both the private and public sectors.

We recommend that NRGA's approach to solutions development follow a format pioneered by the U.S. Army for developing advanced communications and interoperability and known as the Army Expeditionary Warrior Experiment (AEWE).[xxvi] The NRGA, in partnership with DOE and DHS, should host an annual competitive "experiment" to test private-sector technologies that could enhance grid resilience in specific scenarios and circumstances. Such an experiment would establish the scenario, provide a venue, and invite vendors to apply and then demonstrate in a competitive format the effectiveness of their technologies.

This could include a wide variety of technologies, from new cyber hardware/software combinations to ultra high speed disconnects and switching technologies to advancements in quantum computing and quantum communications. These experiments would then serve as a basis for upgrading basic standards, inviting procurement, and guiding Federal funding and other incentives across the grid.

Thankfully, there are valuable prior efforts for the NRGA to incorporate and build upon. NERC E-ISAC's GridEx Event and the DOE's Infrastructure Security & Energy Restoration Office (ISER) conduct tabletop exercises for industry and government officials related to power outages and integrated response and recovery efforts (*see* Annex I). The Pentagon's weeklong Plum Island Exercises have gone a step further and provided an isolated physical simulation environment for an OT-focused cyberattack that trips breakers in low-voltage sub-stations to cause a blackout, and then tasks participants with bringing the power grid back up while red teams try to thwart them (Newman, 2018).[83]

xxvi The AEWE invites technology vendors to submit their technologies for testing in field-conditions experiments. It provides vendors with testing conditions they could not fund themselves, while also providing visibility for promising technologies that can lead to procurements. U.S. Army Fort Benning and the Maneuver Center of Excellence (2020), U.S. Army Maneuver Battle Lab Army Expeditionary Warrior Experiment (AEWE).

The NRGA experiment should seek to build upon and augment these efforts, toward an annual cycle that tests power systems in real conditions via dedicated world-class red teams. The process is circular, driven by a recurring cycle of threat identification and response. It would resemble the following (Figure 3):

Figure 3 - NRGA Experiment Cycle

1. **Threat Identification**. NRGA red teams are given access to the latest threat intelligence information, and spend months finding vulnerabilities and developing plans of attack on the system. Unlike prior exercises and simulations, the nature of the attacks are not be pre-determined. Instead, red teams are tasked with rooting out new vulnerabilities and exploiting those vulnerabilities in innovative ways.
2. **Testing Environment Design**. Based on their findings, these red-team groups define threats for the year's experiment, and an isolated, scale-model facility hosts the testing environment according to the identified threats for a given year. Critically, the facility must be of appropriate scale to test an integrated system with multiple components and both transmission and distribution level equipment.
3. **Requirements Development**. Threats identified by the red teams then drive a requirements development phase by NRGA blue teams, with requirements defined according to the contemplated threats.
4. **Vendor Invitation**. Those requirements are then released to vendors, who are invited to submit technologies for testing in the experiment.
5. **Testing and Training**. The NRGA invites grid operators to the testing environment, both to assess the submitted technologies and to derive additional training that they can take back to their respective systems.
6. **Post-Experiment Analysis and Refinement**. Results from the experiment are used to refine the next year's threat recognition process.

Successful technologies would be submitted to DOD and DOE facilities for implementation in other functional microgrid test beds at military bases and national laboratories (described in Recommendation 3), as well as for the civilian power sector, where they can be incentivized through cost assistance programs (described in Recommendation 6).

In addition to identifying new technology pathways to meet grid resilience goals, the NRGA should also identify potential new policies and regulatory actions derived from technology advances that can be considered by FERC, NERC, and the insurance industry in order to accelerate the adoption and deployment of secure and resilient technologies.

Recommendation 3:
Establish Test Beds for Advanced Resilience Technologies

Congress should direct the Department of Defense and the Department of Energy to establish a nationwide advanced resilience technology (ART) test bed network of long-duration, blackout survivable microgrids on military bases and other critical federally-owned facilities that are pre-determined to be safely sited on stable lands free from flooding, wildfires and other high impact disasters for the foreseeable future. These should be devoted to both immediate defensive capabilities and rapid development of advanced grid resilience technologies. ART test beds should take the form of public private partnerships, where industry can host technologies for testing and commercial development at government facilities. Though managed by DOD and DOE at their respective facilities, the ART network should be integrated with and report to the National Resilient Grid Authority (NRGA) described in Recommendation 2. At least one ART test bed should be of sufficient scale to provide an integrated test site for combined transmission and distribution systems, so as to provide a laboratory for end-to-end security and resilience testing.

Once designed, planners should aim to deploy a geographically diverse set of "Safe Haven" secure microgrids that could support their surrounding civilian communities with stability and critical functions (electric power, water, telecom, etc.) in the event of any state, regional or national emergency.

At least one completely safe all-inclusive critical infrastructure site in each state expands the concept of Continuity of Government Operations to a wider government (federal, state and local levels) and critical industry audience. The national security community should prioritize the identification of Safe Havens in parallel to developing ART test bed networks to assure access to land in the public interest. Disaster modeling has become a business, and the government must assure access to develop these lands for Safe Havens ahead of the private real estate industry, which is beginning to model climate scenarios for private investment purposes.

As explored throughout the report, the macro-grid is constantly evolving, but does so gradually due to its size and complexity. In parallel, alternative paradigms and technologies for more localized power systems demonstrate the potential for more rapid development, with resilience and security against both natural and human hazards built-in rather than added-on: features to be leveraged instead of bugs to be fixed. It is our view that these technologies and models have not received the same level of attention as the grid itself has in high-level resilience reports, and that significant opportunities exist to leverage public-private partnerships and emerging technologies to create rapid-action test beds that can provide substantial resilience and national defense capabilities at significantly shorter time-scales than the macro-grid's slower-moving efforts. Such test beds could also coordinate with the NRGA experiments discussed in Recommendation 2, as demonstration and commercialization sites for successful technologies.

Microgrids are defined by DOE as "a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island mode."[84] A microgrid can—if designed and operated in particular ways—provide resilience benefits on two fronts: maintaining critical localized loads that can remain islanded and operational in the event of a grid-scale blackout, as well as enhancing integration of distributed and renewable energy, providing ancillary services, and assisting in black-start for the macro-grid.

If development of microgrids proves sufficiently dense, microgrids of the future could even be connected by EMP-proof buried high-voltage DC (HVDC) lines. Though very expensive today, with technology advances and cost reductions such solutions could eventually evolve into a meso-

scale "grid of grids," providing superior security for critical loads that may deem such resilience beneficial and worth additional cost: military bases, hospitals, port authorities, first responders, water and sewage infrastructure, communications, and other civilian infrastructures that have public responsibilities or partial public ownership.[xxvii]

An important historical lesson of the power system is that no pathway of development is set in stone. When we imagine the shape of the power system in 2050, it is helpful to remember that we are as far from 2050 today as we were from our present moment in 1990. No future vision of the grid in 1990 bears much resemblance to how our system operates today, and the impossibility of deterministic forecasting has been an enduring quality of the power system throughout its history.[85] To wit: microgrids reflect a return of the original vision of Thomas Edison of hyper localized loads and generation managed through direct current, a vision that was discarded in the War of the Currents when George Westinghouse's alternating current systems won out due to their massive economies of scale and the ability to serve territories of greater size.

Whether Edison's vision will ultimately return from the past to revolutionize the grid of the future is, of course, impossible to know. Most likely, the grid of the future will utilize microgrids and other emergent technologies in configurations that we have not yet imagined. But it can only do so if microgrids and the technologies that enable them have the opportunity to develop in an environment where their unique resilience benefits are valued.

We propose the establishment of Advanced Resilience Technology (ART) test beds focused on the development of resilience-specific microgrids[xxviii] and other enabling technologies and directed toward the goal of accelerated maturation toward commercial scale feasibility. Such test beds, which should take the form of public private partnerships, can also provide near-term resilience benefits to critical facilities. The earliest sites should leverage existing momentum for DOD resilient energy system installations on military bases (Figure 4),[86] and develop test beds around key structural requirements to be defined by the Department of Defense according to installation-specific needs. Department of Energy facilities, which often have substantial continual power needs due to the use of supercomputers and already host a number of microgrid R&D test beds, are also likely candidates for focused resilience efforts. Due to the imminent threats facing the grid from hostile actors, the ART test bed program should focus on rapid development, and aim to produce deployable resilient microgrid technology solutions within 5 years.

In the near-term, the ARTs would provide a much needed accelerant to designing and building resilient microgrid-based test beds across the country. In the longer-term, they could be the first seeds of a grid-of-grids that would provide secure power to military installations as well as to critical public needs in the event of natural or man-made disasters. By aggregating demand for micro-grids

xxvii The military has long recognized the need for on base secure power for critical operations; beginning in the 1940s and 50s, with 50 year statutory contracting authority to develop coal plants on military bases, and in the 1970s with the development of China Lake's world class geothermal resources, which provide secure power to the base, while excess over demand is sold to the LA grid, thus producing revenue the Navy allocates for the development of additional energy projects. A group led by Commission advisor John Dodson has also worked to pioneer and lay the groundwork for this high-concept approach—dubbed the "Guardian Grid"—for over two decades. There has been ongoing work on this concept within the DOE National Laboratories over the past 20 years, and it has been a topic of discussion between senior leaders in DOE and DOD over at least the past decade.

xxviii DOD and DOE both host multiple existing test beds for microgrids. The bulk of work at these R&D sites focuses on "niche application needs, such as the needs for meeting peak load reduction, renewable energy mandates and directives, and energy surety and reliability at some critical facilities including military installations." D.T. Ton and M.A. Smith (2012), "The U.S. Department of Energy's Microgrid Initiative," The Electricity Journal 25: 84-94. ART test beds would utilize similar technologies to these efforts, but emphasize different goals, focused instead on system resilience to extended blackouts and critical security functions against cyberwarfare and EMP/GMD events.

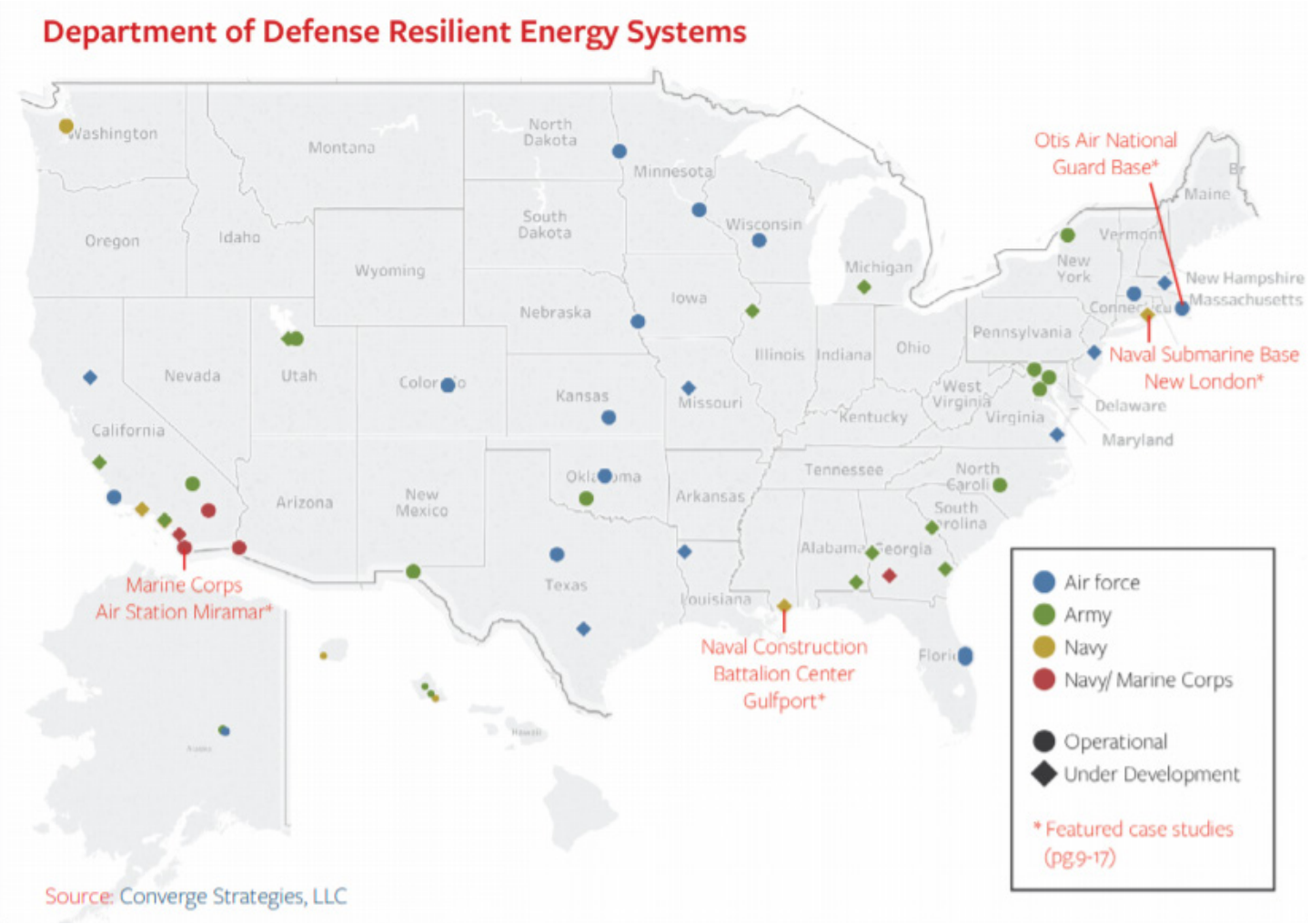


Figure 4: Department of Defense Resilient Energy Systems (Rickerson, et al., 2018)

and continuing to act as an "anchor customer/ first adopter", the government can accelerate the capability of the fledgling micro-grid industry (and utilities opting to participate) to scale up so the industry actually has the capacity to serve national security objectives with national-scale supply that can meet national-scale demand.

ART test bed structural requirements should differ according to the facilities or installations in question. Forward operating bases, remote operating bases, and expeditionary forces, for example, may require higher levels of dispatchable power and greater levels of redundancy than renewable energy sources alone can provide.[87]

Civilian research facilities or domestic bases, on the other hand, may find microgrids with higher penetrations of renewable energy and batteries sufficient to meet many needs. At least one ART test bed should be of sufficient scale to provide an integrated test site for combined transmission and distribution systems, so as to provide a laboratory for end-to-end security and resilience testing. Specifically, we recommend the DOE Idaho National Laboratory and DOE Savannah River Site as promising sites for such a test bed, due to their size.

ART test beds should be operated jointly by facility owners (DOD or DOE, respectively) and the

private sector in a public-private partnership.[xxix] Designing these test beds as public-private partnerships offers the opportunity to leverage the speed, effectiveness, and efficiency of private sector construction and operation with the appropriate oversight and coordination of the government. Such an investment model could attract private sector utilities and technology firms to join the expertise of military, civilian agencies, and federally-sponsored laboratories. Participating facilities should receive public funding for their test beds via the budget of the National Resilient Grid Authority (NRGA) proposed in Recommendation 2, and such funding should be conditional upon reporting requirements to NRGA and integration with NRGA initiatives.[xxx]

Privately-owned ART test beds should also be encouraged and integrated into NRGA initiatives, with the opportunity to apply for public funding through a potential parallel program. ART test beds should form a symbiotic relationship with the NRGA experiment mission, and serve as demonstration sites for technologies that excel in NRGA experiments. Data regarding technology performance at ART sites should, in turn, inform development of future threat scenarios for the NRGA. Interagency agreements are never easy, but we feel this strikes the appropriate balance between facility control by hosting agencies and the autonomy and integrated mission of the proposed NRGA, with appropriate incentives on both sides to encourage coordination and collaboration. Indeed, ART test beds themselves could serve as feeders for the rotating expert staff of the NRGA.

In any case—and irrespective of whether the proposed NRGA is created—ART test beds should prioritize two major challenges for resilient microgrid expansion at scale that, while differing from installation to installation, are likely pivotal for all of them. The first is that current microgrids are typically bespoke installations, designed from the ground up by specialized engineering firms for the particular characteristics of each facility. This adds considerable cost and makes maintenance and repair of the microgrid by facility personnel nearly impossible. Microgrid developers typically sell lifetime service contracts with their installations, as on-site mechanics and engineers do not have the requisite expertise to keep the systems running.

The Lincoln Laboratory at the Massachusetts Institute of Technology (MIT) has designed a Tactical Microgrid Standard (TMS) to define self-sufficient power systems that can be configured for thousands of unique sites and be owned and operated directly by the warfighter,[88] and the Army in spring 2020 announced its intent to standardize microgrid requirements for its installations. Such "plug and play" designs would allow for components to be sourced from a variety of vendors and integrated by onsite personnel and would avoid the risk of vendor lock-in to bespoke systems.

The second challenge for resilient microgrids is the need for dispatchable power. While the bulk power system enjoys the benefit of aggregation of generation and load over millions of customers and hundreds to thousands of miles, microgrids must match local generation to fluctuating loads in a more precise fashion when they operate in their island mode. Renewable generation over small geographic areas exhibits much higher variability than when it is spread over vast regions.[89]

xxix One of the forerunners of the emerging public-private partnership model for microgrids is the Highland Falls-West Point Muni-Grid, which was designed in the aftermath of Superstorm Sandy. The West Point Muni-Grid aims to provide energy resiliency to the Village of Highland Falls, the Town of Highland, and the West Point Garrison by pairing DERs and energy storage with microgrids to provide localized power. R. Horner (2015), *"Microgrid Solutions: From Building to Regions," Conference Presentation for BuildingEnergy NYC, Oct. 15, 2015.*

xxx Such initiatives might include, e.g., EMP-proof underground HVDC lines between ART microgrids, which could lead to a growing network of black sky survivable microgrids.

Declining costs in batteries, which can store energy from renewables or other sources during periods of high production and release it during periods of high demand, has allowed more utilities to incorporate more energy storage into grid operations, but costs remain prohibitive for batteries designed to operate longer than a few hours.[90] For a microgrid with high renewable energy penetration, reserves must last substantially longer than that to meet loads continuously through the night or over multiple cloudy days.[xxxi]

The solution to date for continuous power generation on microgrids has been to pair renewable generation and batteries with natural gas or diesel generation. Besides being a source of greenhouse gas (GHG) emissions, gas and diesel generators present a specific security and resilience risk to the microgrid system: dependence on regular fuel deliveries, typically via truck for diesel and via pipeline or tanker for natural gas. The risks are twofold. First, the vulnerable interdependencies of natural gas pipelines, electric power systems, and communications infrastructures mean that even if the microgrid can island itself from the grid in the event of an outage, its gas generators still require delivery of fuel from a pipeline network[xxxii] that itself may experience an outage due to the blackout. Second, increased demand for natural gas deliveries to microgrids in a high-microgrid-deployment future could, depending on specific gas-electric architectures, exacerbate shortages on pipeline networks during a blackout and thus contribute to macro-grid system instability rather than providing the intended resilience effect. Gas-electric interdependencies and risks remain poorly understood,[91] so guarding against this outcome is difficult. For this reason, DOD and DOE have both expressed considerable interest in the development of small modular nuclear reactors (SMRs) and very small modular nuclear reactors (vSMRs)[xxxiii] as sources of dispatchable power for microgrids, tactical microgrids, mobile power plants, and other applications.[92]

The Commission endorses the deployment of SMRs and vSMRs at the earliest practical date. We feel that the potential value of SMR technology to U.S. grid resilience efforts make SMRs a vital component of the nation's energy secure future. Nuclear technology is also a critical component for the nation to meet emissions and climate goals. Because SMRs can be designed to carry all of their fuel and store all of their waste within the footprint of the device, they offer the possibility of a dispatchable power source that is entirely decoupled from fuel supply lines. That capability could allow microgrids to feasibly island for much longer periods of time—possibly months—and could transform military logistics from one limited by energy scarcity (and its consequent needs for water, munitions, fuel, and spare parts) to one defined by an abundance of power "constrained only by the output capacity of the reactor and not logistics."[93] Indeed, such abundance may soon become a necessity, as it is anticipated that high-energy weapons for competition with near-peer competitors such as "lasers, high-powered

xxxi Of course, this presumes that the system has disconnected from the macro-grid and is operating in island mode for an extended period of time. Most microgrids are not designed to do this, and use their islanding capabilities over much shorter time periods. Providing resilience to long duration blackouts or serving as a primary source of power in the field thus requires very different design requirements than most microgrids operating today exhibit, which is why we argue for the importance of ART test beds as a need distinct from microgrid test beds to date.

xxxii An alternative to this is on-site storage of fuel, but site-specific conditions will differ from facility to facility and thus impact the extent and feasibility of fuel storage available, and storage of natural gas on-site at generators is generally considered impractical (Apt et al., 2018). Following 9/11, the military considered and cast aside the idea of expanding its capacity to site more diesel storage on base for backup generators, which turned out to be a weighty investment, especially given the emergence of new energy technologies.

xxxiii vSMRs are typically designed to produce less than 10 MWe. Defense Science Board (2016), Task Force on Energy Systems for Forward/Remote Operating Bases Final Report.

Figure 5: Rendering of a NuScale Power Plant (Source: NuScale Power)

microwaves, and electromagnetic rail guns" will likely require energy dense nuclear reactors to function (Gilbert *et al.*, 2020).[94]

In regard to SMRs, there is much activity about which to be excited. For example, U.S.-based NuScale Power is co-funded through a public-private partnership with DOE and has recently completed an Advanced Safety Evaluation under the Nuclear Regulatory Commission (NRC), which NuScale CEO John Hopkins described to Congress as "a major milestone as it signifies near-completion of the technical review." It intends to publish its Design Certification by the end of 2020. That certification will lead to the company's first deployment project, the Utah Associated Municipal Power Systems (UAMPS) Carbon Free Power Project, sited at DOE's Idaho National Laboratory (INL) (Figure 5).[95] The plant will consist of 12 SMRs—all constructed offsite and shipped to the facility, and each with 60 MW of capacity—working in a shared pool. One unit will be dedicated to research applications for INL.

In addition, R&D for SMRs goes beyond light water-cooled technologies. DOE is funding R&D on Generation IV technologies through its Advanced Reactor Development program that includes designs utilizing non-light water coolants such as a gas, liquid metal, or molten salt. These new designs can offer significant security and nonproliferation benefits, and the Commission endorses their continued focus as a priority area of R&D for Congress and the Executive Branch.

In regard to vSMRs, the Commission is also intrigued by recent advances and investments by the federal government. Project Pele is a project of the DOD's Strategic Capabilities Office (SCO) aimed at design, construction, and demonstration of a prototype mobile nuclear vSMR reactor within 5 years.[96] The object is to create a nuclear microreactor that can be forward deployed with forces outside the country and would have capacities of 1-5 MWe. In March of this year, the Pentagon awarded contracts to BWX Technologies, Westinghouse, and X-energy for a 2-year design competition with support from

DOE at INL. Following the design period, one of the companies may be selected to build and demonstrate a prototype.

Attempts to create modular reactors go back to the mid-1950s and have had a poor track record compared to larger civilian nuclear plants, which benefitted from economies of scale that small reactors cannot leverage.[97] Logistical challenges and risks associated with kinetic attacks, flooding, and seismic events are real and potentially serious, as discussed in an otherwise positive report from the Army Chief of Staff[98] as well as reports by INL[99] on the Mega-Power concept developed by Los Alamos National Laboratory.
However, while SMRs still need to overcome significant challenges, the Commission remains enthusiastic about their inclusion in the nation's future grid. There are, of course, risks to such efforts, as with any high-risk technology endeavor. But if we abandon SMR research now, we leave potential gains to our adversaries, ones that we will not readily remedy. For this reason, we recommend SMR development and integration into resilience microgrids be considered a major component of ART test beds. We did not become the most powerful nation in the world by shying away from high-risk, high-reward scenarios, and we should not do so now.

Recommendation 4:
Build Resilience into Future Power Grids

The Federal Energy Regulatory Commission (FERC)—in consultation with appropriate expertise at the U.S. Department of Energy and the Department of Interior, states actively procuring offshore wind energy resources, and the relevant Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) responsible for the management of the onshore grid in their jurisdictions—should reform and strengthen interregional transmission planning, cost allocation, and competitive bidding processes to better address

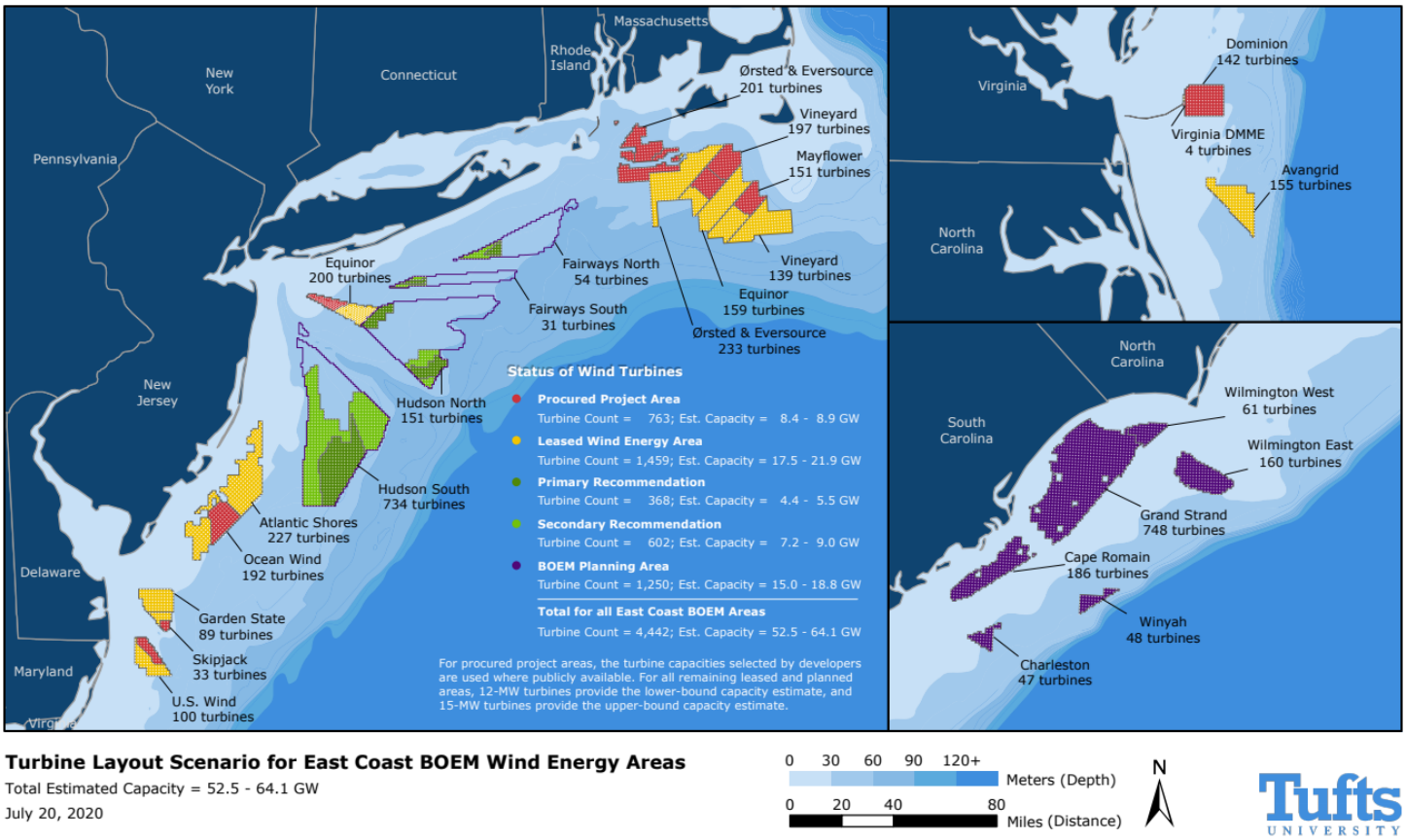


Figure 6: Turbine Layout Scenario for East Coast Bureau of Ocean Management Wind Energy Areas (Source: Tufts University)

the characteristics of widely dispersed renewable energy generation.

Regarding the emerging offshore energy industry, FERC should develop a robust, standards and systems-oriented planning process for new offshore transmission grids serving next-generation resources such as ocean-based, offshore wind turbines, wave and tidal energy, and transmission.

The other area of future grid development where it is readily possible to build resilience in from the ground (or seabed) up is in the massive infrastructure buildout that will accompany the development of offshore wind power and other forms of marine energy, such as wave and tidal energy, in decades to come. Nearly 80% of the country's electricity demand is located in coastal states, and the technical potential for offshore wind power is roughly double that of all current electricity demand.[100] With the launch of the Block Island Wind Farm in 2016 and seven states committed to 29,768 MW by 2035,[101] the race is on for an entirely new mega-component of the macro-grid, one that could provide up to 64 GW from the existing and anticipated Federal offshore wind leases, with significantly more generation available with additional lease areas and the advent of floating turbine technology (Figure 6).

Like microgrids, offshore and marine energy offers that rarest of opportunities in the bulk power sector: a blank slate. The opportunity to build offshore wind systems from the ground up for resilience and security is a boon for both the industry and the onshore grid, to which it will interconnect and could provide a host of benefits: ancillary services, backup power, a hedge against fuel price risk, and potentially even black start capabilities for dispatchable power plants. But while much attention has been paid to the development of generation capacity in offshore wind,[xxxiv] there has been very little consideration of the optimization and planning of offshore energy collection and delivery systems from a systems perspective. In the race to develop the resource, developers seek the fastest and cheapest way to connect new wind farms to the mainland, maximizing profitability for the project but sowing a lack of resilience and redundancy in the system that will only become fully apparent decades hence. Current transmission planning processes, organized under FERC Order 1000, are not optimized for offshore development. FERC's recent announcement of a technical conference in October to explore grid integration of offshore wind energy suggests an interest in taking a strong leadership role in the planning of future grids to support marine renewables.[102]

A robust, systems-oriented planning process for offshore grids and their interconnection to mainland grids is required, and resilience and redundancy should be core design criteria for such processes. The planning process should closely work with and leverage the expertise and technology development efforts of the U.S. Department of Energy's Transmission, Permitting and Technical Assistance Program (Office of Electricity) and Wind Energy Technologies Office (Office of Energy Efficiency and Renewable Energy), the U.S. Department of Interior's Bureau of Ocean Energy Management (BOEM), states actively procuring offshore wind energy resources, and the relevant Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs). DOE has lead policy and technology development responsibility for the integrity and reliability of the nation's electric grid and BOEM has lead authority for identifying and leasing Wind Energy Areas in the open ocean and permitting energy infrastructure, including offshore wind towers and associated transmission infrastructure, in Federal waters. In addition to procuring offshore wind energy, states have jurisdiction over

xxxiv Though we do not make specific recommendations on device design in this report, there is much work to be done in the resilience of individual turbines. Current IEC design criteria for offshore wind turbines are not intended for tropical storm environments and "do not encompass extreme wind speeds and directional shifts of hurricanes stronger than category 2." R.P. Worsnop, et al. (2017) "Gusts and shear within hurricane eyewalls can exceed offshore wind turbine design standards," Geophysical Research Letters 44: 6413-6420.

the first three nautical miles from shore, from which point Federal jurisdiction begins. The ISOs and RTOs are responsible for the management of the onshore grid in their jurisdictions and adapting and upgrading the onshore electric grid to cost-effectively accommodate the anticipated large injections of offshore wind energy. An additional key resource is the newly-created National Offshore Wind Research and Development Consortium (NOWRDC), a partnership of DOE and the New York State Energy Research and Development Authority (NYSERDA). Specifically, we recommend that offshore grid planning prioritize capabilities to consolidate and connect large collector platforms[103] to create redundancy, and emphasize the use of DC transmission lines. While AC lines are cheaper in the short run, they offer few resilience benefits. DC lines, by contrast, can carry three times the power over the same length of cable, suffer fewer energy line losses, and can provide black start capacity to onshore power plants. Additionally, because many mainland connection points for offshore grids may not match levels of offshore generation with equivalent amounts of local load, planning processes should emphasize the importance of energy storage technologies at strategic offload points to minimize curtailments.

Onshore power grids face similar challenges regarding the need to move increasing amounts of weather driven renewable energy from far flung locations to load centers. Unlike the offshore environment, solutions are complicated by existing infrastructure and stakeholders and planning processes. FERC Order 1000 requires transmission planning processes to utilize regional transmission planning and cost-allocation procedures. But critics of FERC Order 1000 point out that despite high hopes when it was promulgated a decade ago, it has not delivered on its promise to drive a renaissance in regional transmission buildout. In the PJM Interconnection, which serves 65 million people across 13 states, the vast majority of new transmission projects in recent years have been for smaller "supplemental," "immediate need," and "end of life replacement" projects that undergo minimal review and are exempt from regional planning process.[104] Order 1000 also failed to anticipate the need for *inter*-regional transmission over larger geographic scales between multiple grid regions in the wake of rising penetrations of renewable energy, according to former FERC commissioners[xxxv] Tony Clark and Jon Wellinghoff.[105]

Transmission buildout is critical to resilience as it can relieve line overloading—or "congestion" in industry jargon—on the existing system, lessening the compounding risks that come with a strained grid that could then be tested by an extreme weather event or an attack incident. Moreover, by enabling further development of renewable energy resources over wider geographic areas, well-planned transmission expansion can make targeted attacks on the grid more difficult to plan and carry out. We agree with calls for reform, and specifically recommend that FERC strengthen requirements for interregional transmission planning, encourage longer term thinking about the value of larger lines (including HVDC lines) and advanced technologies such as power flow controls and dynamic line ratings, and require RTOs/ISOs to assert leadership in planning processes and represent the public interest in doing so.

Recommendation 5:
Improve Standards and Reporting

Congress should direct the Department of Energy and the Department of Homeland Security to create a voluntary central repository of information regarding security and resilience investments in the electric power system. Participating utilities and other stakeholders should be invited to submit annual reports of activities, which could form a basis for cost-recovery arguments to regulators by providing comparative data between utilities. In addition,

xxxv Current FERC commissioner Cheryl LaFleur has partially concurred in Clark and Wellinghoff's critiques, but with the reservation that many benefits of Order 1000's process may not be fully recognized for years to come, and thus some critiques may be premature.

NIST should examine the impacts of severe short-, mid- and long-term climate and weather predictions to ensure grid-related equipment is resilient to the challenges of tomorrow. In addition, NIST should examine the impacts of severe climate and weather predictions to ensure grid-related equipment is resilient to the challenges of tomorrow.

Any series of programs at the private or public level to improve resilience necessitates a means of measuring progress and assessing the successfulness of efforts. Resilience investments will come with costs, to both the power system itself and to society at large. Determining the value of such investments both *ex ante* and *ex post* requires the development of metrics and assessment standards. Numerous efforts are underway in the field, but a consensus view of how to define, measure, and value resilience has not yet emerged.[106] It is likely that multiple definitions and metrics will be needed to address different types of resilience in different parts of the energy system. As those definitions and metrics are created, we expect that NERC will continue to develop standards related to security and resilience through collaborative processes.

In the meantime, however, the lack of mature standards and metrics for resilience should not preclude the power sector from reporting its investments and measures related to resilience in a more comprehensive way. At present, there is no publicly available resource that indicates with any specificity or uniformity how the sector is investing in resilience or security. Such reporting marks the beginning of taking a problem seriously, not a distant future goal to be attained.[xxxvi] Utility investments in resilience should, at a minimum, be reasonably classifiable as such and reportable to a central repository managed in the interest of national security. Even if such efforts were to begin with modest efforts such as voluntary filing of annual reports, it would provide a baseline for measuring progress and a potential documentation trail that utilities could use in arguing for cost recovery from regulators. Future data collection could also be pulled from tax return filings for the resilience investment tax credit we discuss in Recommendation 6.

Logical homes for such a database would include DHS's Cybersecurity and Infrastructure Security Agency (CISA), DOE's Cybersecurity, Energy Security, and Emergency Response (CESER) Office, or the expanded and empowered ESCC / E-ISAC clearinghouse and decisional node cognized *supra* in Recommendation 1. Wherever it is housed, resilience investment data should feed into the ongoing development of the DOE's North American Energy Resilience Model (NAERM) and Multiyear Plan for Energy Sector Cybersecurity.

Likewise, improved disclosure to the insurance sector of the risks of system compromise due to cyber and physical attacks, and sabotage of critical equipment in manufacturing overseas will lead to better valuation of resilience and security investments, as utilities can point to those investments as limiting catastrophic exposure and thus reducing premiums. Such savings serve as quantifiable justifications for resilience investments to shareholders, regulators, and ratepayers alike. Because it is uniquely incentivized to do so through its core business model, the insurance industry has already led the way in monetizing climate change risks throughout the economy. Provided it has access to meaningful data, we expect that it is capable of doing the same with respect to the escalating risk of malicious attacks and other existential threats to the power system. Crucial to this development, however, is the transformation in information sharing from the intelligence community to the power sector that

---

xxxvi For example, developing plans to address greenhouse gas emissions from the power sector began with requiring utilities to report the emissions associated with their portion of the grid to the Environmental Protection Agency's (EPA) Emissions & Generation Resource Integrated Database (eGRID) Program. U.S. Environmental Protection Agency (EPA) (2020), Emissions & Generation Resource Integrated Database (eGRID): eGRID2018. Likewise, developing competitive wholesale markets for bulk power through industry restructuring began with requiring reporting of hourly marginal cost data from all electric balancing authority areas to FERC under the Commission's Form 714 reporting requirement.

we have recommended in Recommendation 1. The insurance industry cannot create actuarial models related to, for example, cyberattacks launched by foreign adversaries if it cannot access reliable data about the nature and severity of the threat as evidenced by distinct events.

The U.S. financial investment rating agencies are also considering a wider range than traditional criteria in measures taken to both reduce cyber and overseas manufacturing vulnerabilities in grid equipment, and projected climate conditions, including the risks that could lead to utility bankruptcy. Moody's has stated that compliance with Executive Order 13920, which restricts transformer imports from adversarial nations, is "credit positive", implying that non-compliance with the EO is credit negative. Blackstone has published a working paper[107] evaluating risk of electricity generation from climate, stating that their evaluation of grid transmission risk to climate impacts was infeasible due to the difficulty in obtaining geolocation of the grid. Standard and Poors published in 2019[108] that California utilities run the risk of credit down ratings and potentially bankruptcy in the future given projections of drought laden, dying forests and wildfire risk combined with liability constructs.

Finally, given the predictions of increased temperatures and natural disasters (specifically hurricanes, wildfires, and sea level rise), we urge NIST to study how these impacts could affect the resilience of grid- and generation-related technologies and propose associated changes in industry standards. Equipment added to the nation's grid today will still be in place 30 and 50 years from now, and we must ensure that private and public sector dollars in this equipment is spent wisely. As such, we must ensure that our energy backbone has the resilience to endure the predicted environmental changes and challenges.

Recommendation 6:
Provide Incentives and Direct Federal Spending

Congress should pass a Resilience Investment Tax Credit (RITC) that incentivizes investments in cyber, physical, American-manufactured transmission components and equipment, and EMP security measures at both the distribution utility and bulk power system levels, and direct federal spending toward resilience and security investments in federally-owned electric utilities and end-use federal facility energy applications such as grid connected devices, electric vehicle fleets and charging infrastructure, and distributed energy resources. State Public Utility Commissions should develop new methods of valuing resilience investments in the private sector so as to include such expenditures in the utility rate base calculation. In all cases, every advantage should be taken of opportunities for public-private partnerships to deepen investments in grid resilience.

While standards and reporting continue to develop, opportunities also exist to make near term resilience investments more attractive to the private sector through the use of tax credits, akin to the wind Production Tax Credit (PTC) and solar Investment Tax Credit (ITC) that were pivotal in driving early investment in carbon-free generation sources in the 1990s and 2000s. For example, since the enactment of the ITC in 2006, which originally provided for a tax credit of 30% of cost of any residential or commercial solar installation, the solar industry has grown by over 10,000%, and continues to expand even as the size of the tax credit has declined in recent years.[109]

Accordingly, we recommend that Congress pass a grid Resilience Investment Tax Credit (RITC) program that defines and supports cyber, physical, transmission equipment, and EMP security investments at 30% of investment cost, as the solar ITC did at its inception. The cost differential of imported vis-a-vis U.S. sourced and manufactured transformers, for example, is informally estimated by U.S. manufacturers at 25 to 30%. Related tax return filings could also form the basis of the resilience data repository discussed in Recommendation 5.

Tax related support for the energy sector was $17.8 billion in 2017 (CRS, 2019) for a large

variety of energy sources, from fossil to nuclear to renewables.[xxxvii] The largest component of this spending is for renewable energy, which accounted for 65.2% of tax related support for energy at $11.6 billion, followed by fossil fuels at $4.6 billion (25.8%), and nuclear, energy efficiency, and alternative technology vehicles at $1.3 billion (8%). Given the market failure in the case of resilience, we recommend reserving a portion of that budget to protect the underlying system that allows those sources to reach their customers and enables modern life as we know it. For purposes of illustration: if we were to target 5% of 2017 federal spending for tax related energy sector support for grid security, that would amount to a budget of just under $1 billion. Presuming a 30% credit, such expenditure could spur approximately $3.3 billion worth of resilience spending; that is 73% of ARRA's $4.5 billion in spending on grid modernization in 2009, but at a fraction of the cost—a policy that punches above its weight class and delivers preventative benefits that, while perhaps difficult to quantify, are no less real at the moment we need them.

Admittedly, energy related tax credit performance is difficult to predict, and an RITC runs the risk of underestimating or overestimating the impact of the credit on uptake. Tax credits also have a tendency to develop inertia that can outlive their necessity, providing government largess to technologies that have long since reached commercial viability. For both of these reasons, an RITC should be seen as only a first stage of spurring investment in grid security, and should have a hard sundown date of 10 years. Because security investments are so diverse in type and are undertaken directly by utilities rather than by project developers, there is a lower risk of lingering resistance to tax credit retirement. This is because future cost-recovery allowances for resilience investments in state regulatory proceedings are considerably more attractive to utilities than tax credits, and such processes would partially disallow cost-recovery for federally subsidized expenses.

In parallel to tax credits for the private sector, it is worth reflecting on the role of the government in correcting for market failures through the use of direct spending. Federal acquisition powers can be a strong driver of demand, and we strongly recommend that Congress create a program to enable adoption of grid security measures for end use / behind-the-meter energy devices at federally owned facilities and military bases, including but not limited to grid connected devices, electric vehicle fleets and charging infrastructure, and onsite distributed energy resources. Such a program could mirror DOE's Federal Energy Management Program (FEMP), which enables federal agencies to achieve energy goals and set best practices. Likewise, we urge federally-owned electric utilities to take the lead in demonstrating grid resilience and security investments so as to provide a benchmark for the private sector.

These special entities include the Tennessee Valley Authority (TVA), the Bonneville Power Administration (BPA), the Western Area Power Administration (WAPA), the Southeastern Power Administration (SEPA), and the Southwestern Power Administration (SWPA). These systems provide wholesale power to municipal electric systems and rural electric cooperatives, and thus resilience investments can provide downstream benefits and inspire action in publicly-owned distribution systems.

The lowest hanging fruit for federal spending toward grid resilience is in recovery efforts following major weather disasters, when federal dollars have already been committed to work led by the Federal Emergency Management Agency (FEMA) and Housing and Urban Development (HUD). Much of that spending goes to distribution grid and end-use energy concerns, but until recently the DOE has not been adequately involved in providing energy-specific expertise to guide investment. DOE's newly-launched Resilience and Recovery initiative aims to bridge this gap

xxxvii For this reason, we present the RITC as solely focused on distribution and transmission system security investments, not for generation resources, which are already subsidized by existing programs.

and provide coordination between subject matter experts at DOE and the national labs and disaster recovery operations, in order to leverage recovery spending toward future resilience co-benefits in disaster-prone areas.

Island power systems in particular present ripe opportunities for such efforts, because they are often government-owned. Puerto Rico,[xxxviii] for example, has benefitted from a number of public-private partnerships (P3s) to rebuild or expand infrastructure with augmented resilience attributes. These civil infrastructure P3s[110] are of a different type than the federal research and development P3s we have described elsewhere in the report, as the private partner is typically the main source of capital for the infrastructure project, and recoups its costs through fees or tariffs throughout the operative life of the investment.[111] For state and municipal budgets under stress, infrastructure P3s can provide critical "breathing room" for public investment by providing a mechanism for infrastructure financing that leverages private capital.[112] In the power resilience context, P3s can provide government-owned power systems with the capital needed to harden distribution and transmission assets, and can also develop alternatives to the grid, such as microgrids. Thanks to microgrids built in Puerto Rico after the devastation of Hurricane Maria, many residents maintained access to power when the island was hit by a grid-wrecking 6.4 magnitude earthquake on January 7th, 2020, and a 5.9 magnitude quake four days later.[113]

The ultimate goal of both incentives and federal spending is to provide a growing body of evidence for the private sector and state regulators as well as municipal systems and rural electric cooperatives toward better understanding of the value and characteristics of grid resilience investments, and to nurture technologies and approaches across the notorious "Valley of Death." Defining those values allows for costs to be fully integrated into the rate base (or public budget) as part of the expected operation of a system that is both efficient and resilient. We are encouraged that the track record for such approaches is strong. The same strategy has taken renewable energy, a marginal source 30 years ago, to the fastest growing segment of the power grid today. We hope resilience efforts can enjoy a similar success story, and believe that it is possible for our future power grid to be as secure as it is clean.

Recommendation 7:
Create a Congressional Caucus for Grid Resilience and Security

Congress should establish a bipartisan caucus on grid security that meets regularly to consider issues impacting the security and resilience of the U.S. electric grid. The National Security Council should lead a complementary interagency committee on grid security that acts as a liaison with the caucus.

Due to the span of grid resilience and security topics, no existing congressional caucus covers its full breadth from threat detection and system defense through response and recovery (Annex II). Caucuses allow for regular and informal engagement between lawmakers and industry around specific problems, and can encourage candor and collaborative problem-solving that are less forthcoming in contentious public committee hearings. We recommend that Congress establish a bipartisan caucus on grid security that meets regularly to consider issues impacting the security and resilience of the U.S. electric grid. This caucus would facilitate continued focus by the Congressional branch on the evolving threat

xxxviii Hurricane Maria devastated Puerto Rico in September 2017, causing an estimated $90 billion in damages (AP, 2017) *and a death toll in the thousands (with the actual number disputed), though the direct death toll was only 64.* AP (2017), "*Hurricane death toll in Puerto Rico more than doubles to 34, governor says*," The Guardian, Oct. 3, 2017; A. Florido (2019), "*2 Years After Hurricane Maria Hit Puerto Rico, the Exact Death Toll Remains Unknown*," *All Things Considered*, National Public Radio, Sept. 24, 2019. *The proximate cause of that staggering death toll discrepancy was the 11 month power outage that followed the storm, in which thousands of people died from lack of access to power.* A.F. Campbell (2018), "*It took 11 months to restore power to Puerto Rico after Hurricane Maria. A similar crisis could happen again*," Vox, Aug. 15, 2018.

landscape, foster bipartisan legislative initiatives, and elevate the profile of these exceptionally important issues. The caucus could also help break down the silos between Congressional Committees, helping to ensure that Congress approaches grid security from a strategic perspective, including but not limited to climate impact and infrastructure planning.

As a complement to the caucus, we also recommend that the National Security Council (NSC) lead an executive branch interagency committee on grid security. An interagency committee can help ensure visibility in the Administration as well as in Congress, and serve as a point of liaison between branches. Currently, grid security issues may fall between the cracks of the NSC's committees that focus on domestic resilience and cyber responses. In addition, the NSC's current structure means that grid security issues are handled by the same group that examines every other cyber threat to the nation, potentially diluting the significance of the threat landscape. In addition, creating a new committee would allow broader participation by the types of subject matter experts in the agencies and departments that have exquisite knowledge of energy-specific topics, including industrial control systems and grid architecture security.

Throughout this report, we advise that the NSC be deeply involved in directing grid security and planning-related matters; as such, we believe the creation of this committee is warranted to focus specifically on these activities. Going further, our government experts and the national security community have experienced that too little has been actually accomplished to secure and plan for a resilient grid without specific direction from the NSC. Given the well-documented threats and vulnerabilities, the trend toward intensified risk, the complexity of the tasks outlined here, the current legal and regulatory framework, the complexity of split federal agency and state jurisdiction, and the fact that the private sector largely owns the grid, strong and ongoing leadership, as well as oversight by the nation's most serious leaders is essential.

Recommendation 8:
Secure the Supply Chain, Specifically for Large Transformers

The Administration and Congress should establish a secure ongoing domestic supply chain, manufacturing capability and labor skills sets for all critical components and whole equipment essential to the operational security of the bulk electric grid, particularly prioritizing the largest and longest lead time transformers. Further, we recommend that Congress should direct annual updates and briefings to the NSC and Congress to the DOE Reports "Large Power Transformers and the U.S. Electric Grid (2012)" and "Strategic Transformer Reserve Report (2017)."

As noted above, the Administration released an Executive Order to protect the critical equipment in the nation's bulk power system from foreign adversaries. NERC is also focused on improving the security of utility supply chains. We endorse these efforts.

While the domestic large transformer industry was re-established following the recommendations of the 2008 Defense Science Board Energy Security Task Force, foreign competition and pricing have severely diminished the U.S. manufacturing capacity and skills sets meant to ensure a reliable and secure domestic supply for national security and critical infrastructure. As part of this endeavor, we urge the NSC, the NEC, Congress, DHS and DOE to focus on the feasibility of establishing a large transformer reserve and secure spare repository to enable the nation to recover quickly from an impactful man-made or natural disaster on the nation's bulk power system. Such a reserve is potentially costly but should be considered in light of avoided cost, insurance cost and cost/benefit analysis. The Nation has learned quickly through the COVID-19 pandemic the value of being prepared for surprises that can devastate our economy and way of life. The national security community has long understood that strategic losses of our key largest transformers and thus the electricity that enables national security and societal stability would overshadow by orders of magnitude the pandemic's effects. Investment

in upfront costs does not obviate the need for such a reserve or excuse our public officials from identifying or pursuing a resilient solution.

Recommendation 9:
Ensure Strategic Siting of Grid Investments

The President should issue a Presidential Decision Directive initiating climate impact modeling of a range of future scenarios to identify where it will be safe to site new and upgraded bulk electric transmission. These planning scenarios should take into account sites critical to national infrastructure, areas threatened by environmental impacts (including sea-level rise, extreme heat, and climate-driven population migration), impacts to the national economy, and enhancements that could be made by public-private partnerships.

This is an inherently government function and industry, while it largely owns the grid, does not have the assets to perform the complex national scale modeling required for reliable planning. The project should be managed from the NSC (for defense purposes) in coordination with the National Economic Council (for civilian infrastructure purposes) to assure all federal agency and state government consensus on models and necessities as we move through the process. The risk of population migrations and the need to plan for it is recognized by the Government Accounting Office (GAO), most recently in July 2020, and has long been recognized by Pentagon analysists as it applies to both U.S. communities and geopolitical risks.

Section 7: Conclusions

The recommendations provided in this report are presented as severable, but are intended as a unified strategy that works best when considered together. In building off of the diligent and comprehensive work of massive prior efforts from experts at the National Academies of Sciences, Engineering, and Medicine, the National Infrastructure Advisory Council, the Department of Energy, the Defense Science Board, the National Labs, industry organizations, and many others, we have had the luxury of focusing on a targeted set of recommendations that aim to do more than repeat the accepted wisdom that has informed them, but that identify where progress has been made and where attention is still required. In doing so, we have deliberately hewed toward bold, visionary, and aspirational solutions rather than succumb to paralysis in the face of a vast challenge. While these solutions are nonpartisan, they are—we think the reader will agree—not timid.

In the preceding pages, we have called for (1) a profound overhaul of the communication of classified threat information to utilities; (2) a new federal agency dedicated to regaining the upper hand against potential adversaries and developing and testing cutting edge technologies and strategies against both current and emerging threats; (3) a nationwide network of resilience-focused microgrid test beds to advance game-changing emergent technologies to deployment feasibility within half a decade; (4) a reformation of transmission planning for both terrestrial and offshore power grids; (5) & (6) major improvements to standards and reporting practices and ramp-ups of federal spending on resilience investments; (7) a new congressional focus on the topic of grid resilience that prioritizes the issue across the partisan divide; (8) a strategic reserve for our most essential grid transformers and investing in U.S. manufacturers to supply these most precious assets; and (9) an investment in modeling and in electric infrastructure—both bulk and secure

microgrids/Safe Havens—in locations where they will be safe from harm.

We have chosen this approach both because we have vigorously debated these recommendations and believe they are the right solutions, and also because we value the importance of inspiring further debate and new ideas. We fully anticipate that these recommendations will be critiqued, corrected, improved, and instantiated in new and better ideas as the field of power grid resilience evolves. What is important is that the momentum that this topic has developed in government, academia, and the private sector continues to build, and becomes a matter of national concern at the highest levels, irrespective of the outcome of November's elections.

The power grid is the foundation of our economy and way of life. Ronald Reagan built the household recognition that would later propel him to the presidency through his televised work for General Electric. Reagan was an advocate for electric power as the right and privilege of all Americans: the common scaffolding from which we would build a society that would become the envy of the entire world. It was a vision he shared, across decades and the partisan divide, with Franklin D. Roosevelt, who would ensure that even the most remote communities in the country would have access to electric power through the Rural Electrification Act. Over more than a century of development, the modern power grid has realized that dream, and stands as a marvel of efficiency and reliability. But the same innovations that have made the grid so efficient—coupled cyber-physical systems, a proliferation of smart computing devices, and complex operational interdependencies—have also unwittingly opened it to attack and vulnerabilities of changing climate conditions. We must act swiftly to both close those vulnerabilities and prepare to confront rapidly evolving threats to the grid, both human and natural. And we must prevail over them. We believe the recommendations we have outlined here provide an ambitious but actionable plan to do that.

We urge the current Presidential campaigns as well as House and Senate campaigns to consider these recommendations and develop policy platforms to secure our power grid for the benefit of all Americans.

References

[1] 100 Resilient Cities (2019). Resilient Cities, Resilient Lives: Learning from the 100RC Network.

[2] U.S. Army (2015). Energy Security & Sustainability (ES²) Strategy.

[3] Coats, D. (2019). Worldwide Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence.

[4] National Infrastructure Advisory Council (NIAC) (2018). Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation. U.S. Department of Homeland Security.

[5] National Academies of Sciences, Engineering, and Medicine (NAS) (2017). Enhancing the Resilience of the Nation's Electricity System. Washington, DC: The National Academies Press.

[6] Congressional Research Service (CRS) (2016). "Testimony – Blackout! Are we Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?" Remarks of Richard Campbell to Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management.

[7] Murphy, C., et al. (2020). Adapting Existing Energy Planning, Simulation, and Operational Models for Resilience Analysis. National Renewable Energy Laboratory. Technical Report NREL/TP-6A20-74241.

[8] NAS, 2017, supra n5.

[9] Federal Power Commission (1965). Report to the President on the Power Failure in the Northeastern United States and the Province of Ontario on November 9-10, 1965.

[10] U.S.-Canada Power System Outage Task Force (2004). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations.

[11] Eto, J.H. and G. Gallo (2017). Regional Transmission Planning: A Review of Practices Following FERC Order Nos. 890 and 1000. Lawrence Berkeley National Laboratory. LBNL-2001079.

[12] Clark, T. (2018). Order No. 1000 at the Crossroads: Reflections on the Rule and its Future. Wilkinson Barker Knauer.

[13] NIAC, 2018, supra n4.

[14] NAS, 2017, supra n5.

[15] Kahneman, D. (2011). Thinking, Fast and Slow. New York: Farrar, Straus and Giroux.

[16] See e.g., Murphy et al., 2020, supra n7; U.S. Department of Energy Office of Electricity (DOE) (2019). North American Energy Resilience Model; Taft, J.D. (2018). Electric Grid Resilience and Reliability for Grid Architecture. Pacific Northwest National Laboratory. PNNL-26623; NAS, 2017, supra n5.

[17] Executive Office of the President (EOP) (2013). Economic Benefits of Increasing Electric Grid Resilience to Weather Outages.

[18] Moody's (2020). Research Announcement: Moody's US regulated electric utilities face varied exposure to climate hazards. Moody's Investors Service, Inc.

[19] Perera, A.T.D., et al. (2020). "Quantifying the impacts of climate change and extreme climate events on energy systems." Nature Energy 5, 150-159; Brody, S., M. Rogers, and G. Siccardo (2019). "Investing in grid resilience." McKinsey Quarterly. November 2019;

[20] Smart Electric Power Alliance (SEPA) (2018). 2018 Utility Demand Response Market Snapshot.

[21] Standard and Poors (February 2019). "Will California Still Have An Investment-Grade Investor-Owned Electric Utility?"

[22] Penrod, E. (2020). "California utilities, regulators aim to hasten microgrid deployment ahead of wildfire season." Utility Dive. June 15, 2020; Trabish, H.K. (2020). "As extreme weather spurs billions in utility resilience spending, regulators struggle to value investments." Utility Dive. April 25, 2020.

[23] National Oceanic and Atmospheric Administration (NOAA) National Centers for Environmental Information (2020). U.S. Billion-Dollar Weather and Climate Disasters.

[24] See e.g., DOE, 2019, supra n16; Taft, 2018, supra n16; NAS, 2017, supra n5; Arghandeh, R. et al. (2016). "On the definition of cyber-physical resilience in power systems." 58 Renewable and Sustainable Energy Reviews 1060.

[25] Murphy et al., 2020, supra n7.

[26] See e.g., Dragos (2020). North American Electric Cyber Threat Perspective; Coats, 2019, supra n3; Defense Science Board (2017). Task Force on Cyber Deterrence. U.S. Department of Defense Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; Onyeji, I., M. Bazilian, and C. Bronk (2014). "Cyber Security and Critical Energy Infrastructure." The Electricity Journal 27, 52-60.

[27] NIAC, 2018, supra n4.

[28] Trump, D.J. (2019). Executive Order on Coordinating National Resilience to Electromagnetic Pulses. Exec. Order 13865; Trump, D.J. (2020). Executive Order on Securing the United States Bulk-Power System. Exec. Order 13920.

[29] NAS, 2017, supra n5.

[30] Gilbert, A., M. Bazilian, and J. Nesheiwat (2020). "The Complex Policy Questions Raised by Nuclear Energy's Role in the Future of Warfare." Just Security. March 16, 2020; Nutall, W.J., C. Samaras, and M. Bazilian (2020). Energy and the Military: Convergence of Security, Economic, and Environmental Decision-Making. Energy Policy Research Group Working Paper 1717, Cambridge Working Paper in Economics 1752. University of Cambridge.

[31] Slowik, J. (2019). CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. Dragos, Inc.

[32] New York Independent System Operator (NYISO) (2020). Interconnection Process.

[33] Bloomberg New Energy Finance (2020). "California Household Battery Sales to Quadruple in 2020." BloombergNEF. Feb. 20, 2020.

[34] California Solar and Storage Association (CALSSA) (2019). "California Celebrates Reaching One Million Solar Roofs Milestone; New Focus on 'One Million Solar Batteries' Goal." CALSSA Press Release. Dec. 12, 2019.

[35] SEPA, 2018, supra n20.

[36] Vasquez, C. (2020). "'Major vulnerability': EV hacks could threaten power grid." E&E News. June 17, 2020.

[37] Dragos, 2020, supra n26.

[38] U.S. Attorney's Office, Southern District of New York (2016). "Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyberattacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities." Press Release. March 24, 2016.

[39] Zetter, K. (2015). "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever." Wired. Jan. 8, 2015.

[40] Bing, C. (2018). "Trisis has the security world spooked, stumped and searching for answers." Cyberscoop. Jan. 16, 2018.

[41] Darktrace Industrial (2019). Triton 2.0 & The Future of OT Cyber-Attacks.

[42] Dragos, 2020, supra n26.

[43] House, A. H. (2019). Connecticut Critical Infrastructure 2019 Annual Report. Office of the Chief Cybersecurity Risk Officer, State of Connecticut.

[44] Trump, 2020, supra n28.

[45] Hawaiian Electric (2020). Cumulative Installed PV – As of Mar 31, 2020.

[46] Weaver, J. (2019). "Residential solar plus storage is taking over Hawaii's grid." PV Magazine. Sept. 4, 2019.

[47] Bloomberg New Energy Finance (2020). "Scale-up of Solar and Wind puts Existing Coal, Gas at Risk." Bloomberg NEF. Apr. 28, 2020

[48] Misbrener, K. (2019). "Cyberattacks threaten smart inverters, but scientists have solutions." Solar Power World. Apr. 30, 2019.

[49] Pagliery, J. (2015). "Sniper attack on California power grid may have been 'an insider,' DHS says." CNNBusiness. Oct. 17, 2015.

[50] National Research Council (NRC) (2012). Terrorism and the Electric Power Delivery System. National Academies Press.

[51] Congressional Research Service (CRS) (2014). Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations. P.W. Parfomak. CRS 7-5700, R43604.

[52] POWER (2018). "Disaster Preparedness: The Quest for Transformer Resilience." POWER Magazine. Mar. 31, 2018.

[53] Sobczak, B. and P. Behr (2019). "China and America's 400-ton electric albatross." E&E News. Apr. 25, 2019.

[54] Eaton, S. (2020). "Trump administration to prove whether imported transformer parts threaten Cleveland Cliffs subsidiary AK steel." Cleveland.com. May 4, 2020.

[55] Grid Assurance (2020). Industry Solution for a Resilient Grid.

[56] Edison Electric Institute (EEI) (2020). Spare Transformers.

[57] U.S. Department of Energy (2017). Strategic Transformer Reserve: Report to Congress; RESTORE (2017). "Utilities partner to boost power grid resilience." PRNewswire. Oct. 3, 2017.

[58] BBC News (2014). "EDF France: Inquiry after drones buzz nuclear sites." BBC News. Oct. 30, 2014.

[59] Bryant, L. (2014). "France Intensifies Probe into Drone Flights." VOA News. Nov. 4, 2014.

[60] Lichfield, J. (2014). "French government on high alert after unexplained drone flights over nuclear power stations." Independent. Nov. 9, 2014.

[61] Associated Press (2014). "Over a Dozen Mysterious Drones Have Flown Over French Nuclear Sites In The Past Month." Business Insider. Nov. 3, 2014.

[62] Daly, S. (2019). "France: Greenpeace flies two c-drones over nuclear site in Normandy, drops ignited flare on roof." The C-drone Review. Jan. 26, 2019.

[63] American Foreign Policy Council (AFPC) (2018). Strategic Primer: Electromagnetic Threats: Current Capabilities and Emerging Threats.

[64] Foster, Jr., J.S., et al. (2008). Critical National Infrastructures: Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack.

[65] North American Electric Reliability Corporation (NERC) (2019). EMP Task Force Strategic Recommendations.

[66] AFPC, 2018, supra n63.

[67] NERC, 2019, supra n65.

[68] North American Electric Reliability Corporation (NERC) (1989). March 13, 1989 Geomagnetic Disturbance.

[69] Kappenman, J. (2010). Geomagnetic Storms and Their Impacts on the U.S. Power Grid. Metatech Corporation. Prepared for Oak Ridge National Laboratory, Subcontract 6400009137. Washington, D.C.: FERC.

[70] Klein, C. (2018). "A Perfect Solar Superstorm: The 1859 Carrington Event." History. Aug. 22, 2018.

[71] NASA Science (NASA) (2014). "Near Miss: The Solar Superstorm of July 2012." NASA Science. July 23, 2014.

[72] Stockton, P. (2014). Resilience for Black Sky Days. The National Association of Regulatory Utility Commissioners.

[73] National Commission on Terrorist Attacks upon the United States (9/11 Commission) (2004). The 9/11 Commission Report.

[74] Anbaric (2020). OSW Goals + Transmission Goals by the States Fact Sheet; Ørsted (2020). U.S. Wind Projects.

[75] U.S. Bureau of Ocean Energy Management (BOEM) (2020). Lease and Grant Information.

[76] U.S. Department of Energy and U.S. Department of the Interior (DOE and DOI) (2016). National Offshore Wind Strategy: Facilitating the Development of the Offshore Wind Industry in the United States.

[77] National Cybersecurity and Communications Integration Center (NCCIC) (2018). Incident Report: Intrusions Affecting Multiple Victims Across Multiple Sectors. Department of Homeland Security. Reference Number: IR-ALERT-MED-17-093-01C.

[78] Doffman, Z. (2019). "Chinese State Hackers Suspected of Malicious Cyberattack on U.S. Utilities." Forbes. Aug. 3, 2019.

[79] Proofpoint (2019). "LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards." Proofpoint Threat Insight. Aug. 1, 2019.

[80] Freeman, E.C. (ed.) (1995). MIT Lincoln Laboratory: Technology in the National Interest. Lexington, Massachusetts: MIT Lincoln Laboratory.

[81] Hughes, T.P. (1998). Rescuing Prometheus: Four Monumental Projects that Changed the Modern World. New York: Pantheon Books.

[82] Page, H. (2018). "What Big Tech Has Acquired From In-Q-Tel, The CIA's VC Arm." Crunchbase News. Jun. 8, 2018.

[83] Newman, L.H. (2018). "The Hail Mary Plan to Restart a Hacked US Electric Grid." Wired. Nov. 14, 2018.

[84] Ton, D.T. and M.A. Smith (2012). "The U.S. Department of Energy's Microgrid Initiative." The Electricity Journal 25: 84-94.

[85] Reed, A., et al. (2019). "Interrogating Uncertainty in Energy Forecasts: The Case of the Shale Gas Boom." Energy Transitions 3: 1-11.

[86] Rickerson, W., M. Wu, and M. Pringle (2018). Beyond the Fence Line: Strengthening Military Capabilities Through Energy Resilience Partnerships. Association of Defense Communities. November, 2018; Merchant, E.F. (2018). "US Military Microgrids are Using More Renewables and Batteries." Greentech Media. Nov. 9, 2018.

[87] Defense Science Board (2016). Task Force on Energy Systems for Forward/Remote Operating Bases Final Report. U.S. Department of Defense Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

[88] Herring, D. (2019). Tactical Microgrid Standard. Massachusetts Institute of Technology. Mar. 3, 2019.

[89] MacDonald, A.E., et al. (2016). "Future cost-competitive electricity systems and their impact on US CO_2 emissions." Nature Climate Change 6: 526-531.

[90] Temple, J. (2018). "The $2.5 trillion reason we can't rely on batteries to clean up the grid." MIT Technology Review. July 27, 2018.

[91] Apt, J., G. Freeman, and M. Dworkin (2018). "The Natural Gas Grid Needs Better Monitoring." Issues in Science and Technology 34, no. 4 (Summer 2018).

[92] *Nutall et al.*, 2020, *supra* n29; *Hopkins*, J.L. (2020). Building a 100 Percent Clean Energy Economy: Advanced Nuclear Technology's Role in a Decarbonized Future. *Testimony of NuScale Power before the House Committee on Energy and Commerce, Subcommittee on Energy*; DSB, 2016, *supra* n86.

[93] DSB, 2016, *supra* n87.

[94] *Gilbert*, 2020, *supra* n30.

[95] *Hopkins*, 2020, *supra* n92.

[96] *Mehta*, A. (2020). "*Pentagon awards contracts to design mobile nuclear reactor.*" DefenseNews. *Mar.* 9, 2020.

[97] *Lyman*, E. (2019). "*The Pentagon wants to boldly go where no nuclear reactor has gone before. It won't work.*" Bulletin of the Atomic Scientists. *February* 22, 2019.

[98] *Vitali*, J.A., *et al.* (2018). Mobile Nuclear Power Plants for Ground Operations. *Deputy Chief of Staff, United States Army. Oct.* 26, 2018.

[99] *Sterbentz*, J.W., *et al.* (2017). Special Purpose Nuclear Reactor (5 MW) for Reliable Power at Remote Sites assessment Report: Using Phenomena Identification and Ranking Tables (PIRTs). *Idaho National Laboratory* INL/EXT-16-40741. *April* 2017; *Sterbentz*, J.W., *et al.* (2018). Preliminary Assessment of Two Alternative Core Design Concepts for the Special Purpose Reactor. *Idaho National Laboratory* INL/EXT-17-43212. *May* 2018.

[100] DOE *and* DOI, 2016, *supra* n76.

[101] *Anbaric*, 2020, *supra* n74.

[102] *Morehouse*, C. (2020). "*FERC schedules technical conferences on carbon pricing, offshore wind integration challenges.*" Utility Dive. *Jun.* 19, 2020.

[103] *See e.g., Tennet* (2017). Connecting Wind Energy: The Offshore Grid in the Netherlands.

[104] *Rutigliano*, T. (2020) "*Transforming PJM is the Key to a Clean Energy Grid.*" Sustainable FERC Project. *July* 14, 2020.

[105] *Trabish*, H.K. (2018). "*Has FERC's landmark transmission planning effort made transmission building harder?*" Utility Dive. *July* 17, 2018; *Clark*, 2018, *supra* n12.

[106] *See e.g., Murphy et al.*, 2020, *supra* n7; DOE, 2019, *supra* n16; *Electricity Advisory Committee* (EAC) (2019). Policy and Research Opportunities for Grid Resilience: Recommendations for the U.S. Department of Energy; *Schwartz*, L., *et al.* (2019). Utility Investments in Resilience of Electricity Systems: Organization of MISO States, National Rural Electric Cooperative Association, Edison Electric Institute, National Association of State Utility Consumer Advocates. *Lawrence Berkeley National Laboratory. Future Electric Utility Regulation / Report No.* 11; *Mann*, W.N., *et al.* (2018). A Study of Grid Reliability and Resilience. *Idaho National Laboratory*. INL/EXT-18-45010; *Taft*, 2018, *supra* n16; *Vugrin*, E., A. *Castillo, and C. Silva-Monroy* (2017). Resilience Metrics for the Electric Power System: A Performance-Based Approach. *Sandia National Laboratory. Sandia Report* SAND2017-1493; *Arghandeh*, 2016, *supra* n24; *Electric Power Research Institute* (EPRI) (2016). Electric Power System Resiliency: Challenges and Opportunities; *Preston*, B.L., *et al.* (2016). Resilience of the U.S. Electricity System: A Multi-Hazard Perspective. *U.S. Department of Energy Office of Energy Policy and Systems Analysis*; *Panteli, M. and P. Mancarella* (2015). "*The Grid: Stronger, Bigger, Smarter?*" *IEEE Power & Energy Magazine May/June* 2015; *Watson*, J.P., *et al.* (2014). Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States. *Sandia National Laboratory. Sandia Report* SAND2014-18019.

[107] *Bertolotti*, A., *et al* (2019). "Climate Risk in the US Electric Utility Sector: A Case Study." *Working Paper, March* 2019.

[108] *Standard and Poors* (2019). "*Will California Still Have An Investment-Grade Investor-Owned Electric Utility?*" *February* 19, 2019.

[109] *Solar Energy Industries Association* (SEIA) (2020). Solar Investment Tax Credit (ITC).

[110] *World Bank* (2019). Public-Private Partnerships.

[111] *See e.g., Peters*, A. (2020). "*How have Puerto Rico's new microgrids performed during its massive power outage?*" Fast Company. *Jan.* 14, 2020.

[112] *Brady*, J. (2018). "*Public-Private Partnerships, A Tool in the Toolbox.*" 2017 Infrastructure Report Card. *American Society of Civil Engineers.*

[113] *Peters*, 2020, *supra* n111.

Annex I

Prior Recommendations of Expert Commissions on Grid Resilience and Security

We reproduce here, in abridged excerpts of their respective reports, recent recommendations of prior expert commissions on grid resilience and security that have informed our effort. We include them in this annex both to reiterate their importance, and to recognize the contributions of prior commissions to our own fact-finding and deliberative processes. The NCGR's recommendations should not be construed to supersede any of these prior recommendations, which remain both critical and, in many cases, unfulfilled by both government and private action.[1]

We reproduce excerpts of recommendations from three general reports on resilience from the National Infrastructure Advisory Council; the National Academies of Sciences, Engineering, and Medicine; and the Electricity Advisory Council:

- The President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation* (December 2018);
- National Academies of Sciences, Engineering, and Medicine (NAS), *Enhancing the Resilience of the Nation's Electricity System* (2017);
- Electricity Advisory Council (EAC), *Policy and Research Opportunities for Grid Resilience: Recommendations for the U.S. Department of Energy* (March 2019).

We have also included excerpts of recommendations from the following reports that are specific to cyber, physical, or EMP threats, respectively:

- Cyberspace Solarium Commission (CSC), *Final Report of the Cyberspace Solarium Commission* (2020);
- National Research Council (NRC), *Terrorism and the Electric Power Delivery System* (2012);
- Electric Power Research Institute (EPRI), *High-Altitude Electromagnetic Pulse and the Bulk Power System* (2019);
- North American Electric Reliability Corporation (NERC), *EMP Task Force: Strategic Recommendations* (2019).

Finally, we reproduce observations and recommendations from two recent grid exercises:

- NERC Energy Information Sharing and Analysis Center, *GridEx V Exercise* (2020); and
- Department of Energy (DOE) Infrastructure Security & Energy Restoration Office (ISER), *Liberty Eclipse Energy Assurance Exercise and Event* (2017).

The President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation* (December 2018).

[1] The National Infrastructure Advisory Council (NIAC), for example, requested a response from the National Security Council within 9 months of its December 2018 report, and after 20 months has yet to receive a reply.

Design a National Approach for Catastrophic Power Outages. Design a national approach for catastrophic power outage planning, response, and recovery to create a cross-sector, cross-government strategy.

1. **Examine and clarify the federal authorities that may be exercised** during a catastrophic power outage and grid security emergency and clearly identify the cabinet-level leadership and decision-making processes.
2. **Develop a federal design basis and the design standards/criteria** that identify what infrastructure sectors, cities, communities, and rural areas need to reduce the impacts and recover from a catastrophic power outage.
3. **Develop guidance and provide resources for states, territories, cities, and localities to design community enclaves—**areas that co-locate critical services and resources to sustain surrounding populaces, maintain health and safety, and allow residents to shelter in place.
4. **Design and support a portfolio of incentives** that provide financial support or remove financial and regulatory barriers to help companies, nongovernmental organizations, and state, local, tribal, and territorial governments implement the recommendations included in this report.

Mitigate Cross-Sector Interdependencies and Cascading Failures. Identify cascading failures impacting key sectors, especially natural gas supply and communications, to ensure their availability to aid power restoration, and identify actions to improve resilience to a catastrophic power outage.

5. **Conduct a series of regional catastrophic power outage exercises** that identify the second- and third-order cascading failures of an outage over time, as backup resources and mutual aid agreements are exhausted, and examine cross-sector supply chain and cyber risks that could delay re-energizing the grid.
6. **Ensure that all critical natural gas transmission pipeline infrastructure has the appropriate standards, design, and practices to continue service** during a catastrophic power outage and maintain rapid availability to support blackstart generation.
7. **Develop or support a flexible, adaptable emergency communications system** that all sectors can interoperably use, that is self-powered, and is reasonably protected against all hazards to support critical service restoration and connect infrastructure owners and operators, emergency responders, and government leaders.

National Academies of Science, *Enhancing the Resilience of the Nation's Electricity System* (2017).

Overarching Recommendations:

Overarching Recommendation 1: Operators of the electricity system, including regional transmission organizations, investor-owned utilities, cooperatives, and municipally owned utilities, should work individually and collectively, in cooperation with the Electricity Subsector Coordinating Council, regional and state authorities, the Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation, to conduct more regional emergency preparedness exercises that simulate accidental failures, physical and cyber attacks, and other impairments that result in large-scale loss of power and/or other critical infrastructure sectors—especially communication, water, and natural gas.

Counterparts from other critical infrastructure sections should be involved, as well as state, local, and regional emergency management offices.

The challenges that remain to achieving grid resilience are so great that they cannot be achieved by research- or operations-related activities alone. While new technologies and strategies can improve the resilience of the power system, many existing technologies that show promise have yet to be fully adopted or implemented. In addition, more coordination between research and implementation activities is needed, building on the specific recommendations made throughout this report. Immediate action is needed both to implement available technological and operational changes and to continue to support the development of new technologies and strategies.

Overarching Recommendation 2: Operators of the electricity system, including regional transmission organizations, investor-owned utilities, cooperatives, and municipals, should work individually and collectively to more rapidly implement resilience-enhancing technical capabilities and operational strategies that are available today and to speed the adoption of new capabilities and strategies as they become available.

The Department of Energy (DOE) is the federal entity with a mission to focus on the longer-term issues of developing and promulgating technologies and strategies to increase the resilience and modernization of the electric grid. No other entity in the United States has the mission to support such work, which is critical as the electricity system goes through the transformational changes described in this report. The committee views research, development, and demonstration activities that support reliable and resilient electricity systems to constitute a public good. If funding is not provided by the federal government, the committee is concerned that this gap would not be filled either by states or by the private sector. In part this is because the challenges and solutions to ensuring grid resilience are complex, span state and even national boundaries, and occur on time scales that do not align with business models. At present, two offices within DOE have responsibility for issues directly and indirectly related to grid modernization and resilience.

Overarching Recommendation 3: However the Department of Energy chooses to organize its programs going forward, Congress and the Department of Energy leadership should sustain and expand the substantive areas of research, development, and demonstration that are now being undertaken by the Department of Energy's Office of Electricity Delivery and Energy Reliability and Office of Energy Efficiency and Renewable Energy, with respect to grid modernization and systems integration, with the explicit intention of improving the resilience of the U.S. power grid. Field demonstrations of physical and cyber improvements that could subsequently lead to widespread deployment are critically important. The Department of Energy should collaborate with parties in the private sector and in states and localities to jointly plan for and support such demonstrations. Department of Energy efforts should include engagement with key stakeholders in emergency response to build and disseminate best practices across the industry.

The U.S. grid remains vulnerable to natural disasters, physical and cyber attacks, and other accidental failures.

Overarching Recommendation 4: Through public and private means, the United States should substantially increase the resources committed to the physical components needed to ensure that critical electric infrastructure is robust and that society is able to cope when the grid fails. Some of this

investment should focus on making the existing infrastructure more resilient and easier to repair, including the following:

- The Department of Energy should launch a program to manufacture and deploy flexible and transportable three-phase recovery transformer sets that can be prepositioned around the country. These recovery transformers should be easy to install and use temporarily until conventional transformer replacements are available. This effort should produce sufficient numbers (on the order of tens compared to the three produced by the Department of Homeland Security's RecX program) to provide some practical protection in the case of an event that results in the loss of a number of high-voltage transformers. This effort should complement, instead of replace, ongoing initiatives related to spare transformers.
- State and federal regulatory commissions and regional transmission organizations should then evaluate whether grids under their supervision need additional pre-positioned replacements for critical assets that can help accelerate orderly restoration of grid service after failure.
- Public and private parties should expand efforts to improve their ability to maintain and restore critical services—such as power for hospitals, first responders, water supply and sewage systems, and communication systems.
- The Department of Energy, the Department of Homeland Security, the Electricity Subsector Coordinating Council, and other federal organizations, such as the U.S. Army Corps of Engineers, should oversee the development of more reliable inventories of backup power needs and capabilities (e.g., the U.S. Army Corps of Engineers' mobile generator fleet), including fuel supplies. They should also "stress test" existing supply contracts for equipment and fuel supply that are widely used in place of actual physical assets in order to be certain these arrangements will function in times of major extended outages. Although the federal government cannot provide backup power equipment to everyone affected by a large-scale outage, these resources could make significant contributions at select critical loads.

In addition to providing redundancy of critical assets, transmission and distribution system resilience demands the ability to provide rapid response to events that impair the ability of the power system to perform its function. These events include deliberate attacks on and accidental failures of the infrastructure itself, as well as other causes of grid failure.

Overarching Recommendation 5: The Department of Energy, together with the Department of Homeland Security, academic research teams, the national laboratories, and companies in the private sector, should carry out a program of research, development, and demonstration activities to improve the security and resilience of cyber monitoring and controls systems, including the following:

- Continuous collection of diverse (cyber and physical) sensor data;
- Fusion of sensor data with other intelligence information to diagnose the cause of the impairment (cyber or physical);
- Visualization techniques needed to allow operators and engineers to maintain situational awareness;
- Analytics (including machine learning, data mining, game theory, and other artificial intelligence-based techniques) to generate real-time recommendations for actions that should be taken in response to the diagnosed attacks, failures, or other impairments;

- Restoration of control system and power delivery functionality and cyber and physical operational data in response to the impairment; and
- Creation of post-event tools for detection, analysis, and restoration to complement event prevention tools.

Because no single entity is in charge of planning the evolution of the grid, there is a risk that society may not adequately anticipate and address many elements of grid reliability and resilience and that the risks of this systemwide failure in preparedness will grow as the structure of the power industry becomes more atomized and complex. There are many opportunities for federal leadership in anticipating potential system vulnerabilities at a national level, but national solutions are then refined in light of local and regional circumstances. Doing this requires a multistep process, the first of which is to anticipate the myriad ways in which the system might be disrupted and the many social, economic, and other consequences of such disruptions. The second is to envision the range of technological and organizational innovations that are affecting the industry (e.g., distributed generation and storage) and how such developments may affect the system's reliability and resilience. The third is to figure out what upgrades should be made and how to cover their costs. For simplicity, the committee will refer to this as a "visioning process." While the Department of Homeland Security (DHS) has overarching responsibility for infrastructure protection, DOE, as the sector-specific agency for energy infrastructure, has a legal mandate and the deep technical expertise to work on such issues.

Overarching Recommendation 6: The Department of Energy and the Department of Homeland Security should jointly establish and support a "visioning" process with the objective of systematically imagining and assessing plausible large-area, long-duration grid disruptions that could have major economic, social, and other adverse consequences, focusing on those that could have impacts related to U.S. dependence on vital public infrastructures and services provided by the grid.

Because it is inherently difficult to imagine systematically things that have not happened (Fischhoff et al., 1978; Kahneman, 2011), exercises in envisioning benefit from having multiple groups perform such work independently. For example, such a visioning process might be accomplished through the creation of two small national power system resilience assessment groups (possibly at DOE national laboratories and/or other federally funded research and development centers or research universities). However such visioning is accomplished, engagement from staff representing relevant state and federal agencies is essential in helping to frame and inform the work. These efforts can build on the detailed recommendations in this report to identify technical and organizational strategies that increase electricity system resilience in numerous threat scenarios and to assess the costs and financing mechanisms to implement the proposed strategies. Attention is needed not just to the average economy-wide costs and benefits, but also to the distribution of these across different levels of income and vulnerability. It is important that these teams work to identify common elements in terms of hazards and solutions so as to move past a hazard-by-hazard approach to a more systems-oriented strategy. Producing useful insights from this process will require mechanisms to help these groups identify areas of overlap while also characterizing the areas of disagreement. A consensus view could be much less helpful than a mapping of uncertainties that can help other actors—for example, state regulatory commissions and first responders—understand the areas of deeper unknowns.

Of course national laboratories, other federally funded research and development centers, and research universities do not operate or regulate the power system. At the national level, the Federal Energy

Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) both have relevant responsibilities and authorities.

Overarching Recommendation 7A: The Federal Energy Regulatory Commission and the North American Electric Reliability Corporation should establish small system resilience groups, informed by the work of the Department of Energy/Department of Homeland Security "visioning" process, to assess and, as needed, to mandate strategies designed to increase the resilience of the U.S. bulk electricity system. By focusing on the crosscutting impacts of hazards on interdependent critical infrastructures, one objective of these groups would be to complement and enhance existing efforts across relevant organizations.

As the discussions throughout this report make clear, many different organizations are involved in planning, operating, and regulating the grid at the local and regional levels. By design and of necessity in our constitutional democracy, making decisions about resilience is an inherently political process. Ultimately the choice of how much resilience our society should and will buy must be a collective social judgment. It is unrealistic to expect firms to make investments voluntarily whose benefits may not accrue to shareholders within the relevant commercial lifetime for evaluating projects. Moreover, much of the benefit from avoiding such events, should they occur, will not accrue to the individual firms that invest in these capabilities. Rather, the benefits are diffused more broadly across multiple industries and society as a whole, and many of the decisions must occur on a state-by-state basis.

Overarching Recommendation 7B: The National Association of Regulatory Utility Commissioners should work with the National Association of State Energy Officials to create a committee to provide guidance to state regulators on how best to respond to identified local and regional power system-related vulnerabilities. The work of this committee should be informed by the national "visioning" process, as well as by the work of other research organizations. The mission of this committee should be to develop guidance for, and provide technical and institutional support to, state commissions to help them to more systematically address broad issues of power system resilience, including decisions as to what upgrades are desirable and how to pay for them. Guidance developed through this process should be shared with appropriate representatives from the American Public Power Association and the National Rural Electric Cooperative Association.

Overarching Recommendation 7C: Each state public utility commission and state energy office, working with the National Association of Regulatory Utility Commissioners, the National Association of State Energy Officials, and state and regional grid operators and emergency preparedness organizations, should establish a standing capability to identify vulnerabilities, identify strategies to reduce local vulnerabilities, develop strategies to cover costs of needed upgrades, and help the public to become better prepared for extended outages. In addition, they should encourage local and regional governments to conduct assessments of their potential vulnerabilities in the event of large-area, long duration blackouts and to develop strategies to improve their preparedness.

Throughout this report, the committee has laid out a wide range of actions that different parties might undertake to improve the resilience of the United States power system. If the approaches the committee has outlined can be implemented, they will represent a most valuable contribution. At the same time, the committee is aware that the benefits of such actions—avoiding large-scale harms that are rarely observed—are easily eclipsed by the more tangible daily challenges, pressures on budgets, public attention, and other scarce resources. Too often in the past, the United States has made progress on the issue of resilience by "muddling through" (Lindblom, 1959). Even if the broad systematic

approach outlined in this report cannot be fully implemented immediately, it is important that relevant organizations develop analogous strategies so that when a policy window opens in the aftermath of a major disruption, well-conceived solutions are readily available for implementation (Kingdon, 1984).

Specific Recommendations

Recommendation 1 to DOE: Improve understanding of customer and societal value associated with increased resilience and review and operationalize metrics for resilience.

Recommendation 2 to DOE: Support research, development, and demonstration activities to improve the resilience of power system operations and recovery by reducing barriers to adoption of innovative technologies and operational strategies.

Recommendation 3 to DOE: Advance the safe and effective development of distributed energy resources and microgrids.

Recommendation 4 to DOE: Work to improve the ability to use computers, software, and simulation to research, plan, and operate the power system to increase resilience.

Recommendation 5 to DOE: Work to improve the cybersecurity and cyber resilience of the grid.

Recommendation 6 to the electric power sector and DOE: The owners and operators of electricity infrastructure should work closely with DOE in systematically reviewing previous outages and demonstrating technologies, operational arrangements, and exercises that increase the resilience of the grid.

Recommendation 7 to DHS and DOE: Work collaboratively to improve preparation for, emergency response to, and recovery from large-area, long-duration blackouts.

Recommendation 8 to DHS and DOE: With growing awareness of the electricity system as a potential target for malicious attacks using both physical and cyber means, DHS and DOE should work closely with operating utilities and other relevant stakeholders to improve physical and cyber security and resilience.

Recommendation 9 to state offices and regulators: Work with local utilities and relevant stakeholders to assess readiness of backup power systems and develop strategies to increase investments in resilience enhancing technologies.

Recommendation 10 to the National Association of Regulatory Utility Commissioners and federal organizations: Work with DHS and DOE to develop guidance regarding potential social equity implications of resilience investments as well as selective restoration.

Recommendation 11 to FERC and the North American Energy Standards Board: FERC, which has regulatory authority over both natural gas and electricity systems, should address the growing risk of interdependent infrastructure.

Recommendation 12 to NERC: Review and improve incident investigation processes to better learn from outages that happen and broadly disseminate findings and best practices.

Electricity Advisory Council, *Policy and Research Opportunities for Grid Resilience: Recommendations for the U.S. Department of Energy* (March 2019)

1. **DOE should develop a comparison of bulk power and distribution resiliency standards and methodologies utilized across the country and, if appropriate, a list of best practices.**

DOE should use the expertise and analytical capability of its National Laboratories to develop a methodology to compile a regional or state list of the most cost-effective resiliency and reliability improvement projects, ranked from highest to the least effective for risk reduction, including potential costs.

The comparison should compare values of various methodologies and potential efficacies. This comparison should distinguish different resiliency and reliability risks for the bulk power and distribution system; the improvement projects that address the risks to each system, including the impact of customer choice and a high penetration DER environment; and incorporate a holistic view of sector interdependencies.

DOE, if possible and appropriate, should develop a "promising practices" document for distribution to interested stakeholders with methodology, standards, recovery techniques, mitigation options, and other pertinent information for recovery from or preparing for a resiliency event.

2. **DOE should direct Lawrence Berkeley National Laboratory to modify its Interruption Cost Estimate (ICE) Calculator tool to evaluate costs of power outages beyond 24 hours and make evaluation of alternative resiliency investments more appropriate.**

DOE should prepare a version of the ICE Calculator or similar planning tool specifically designed to calculate the long-term expected value and prudency of alternative resiliency improvements. Ensure the tool(s) accounts for the potential social value of technologies, costs contributing to customer rate fatigue, affordability issues, and other relevant concerns, such as regional differences contributing to the value of lost load at the industrial, commercial and residential levels.

DOE should investigate resilience solutions through the Grid Modernization Lab Consortium, targeted Funding Opportunity Announcements, its research portfolio, and other ongoing initiatives.

3. **DOE should make certain that tools (including the ICE Calculator) appropriate for grid decision-making are known to state utility commissions, consumer advocate offices, and legislatures nationwide.**

DOE, working in conjunction with the National Association of Regulatory Utility Commissioners, should prepare a directory of all state utility commissions' technical staff members and commissioners responsible for resilience matters. DOE and the National Laboratories should use this list as a resource for consulting commission technical experts. DOE should identify the entity responsible for updating the document as well as the frequency with which it is updated considering the high turnover at the commission level.

DOE should also consider creating and publicizing broad training webinars on resilience-related tools and inviting state utility commission staff to these webinars. Attendees should be tracked and trained, with lists updated annually to keep regions with insufficient training identified and apprised of the latest methodologies and tools.

DOE should also consider workshops to discuss the output of the ICE Calculator, including how to appropriately balance the impacts of the output, rate fatigue, and value of lost load for different rate classes.

4. **DOE should develop a resiliency framework handbook.**

DOE should develop a handbook that details the process by which a state or region can rigorously develop resiliency standards and metrics which includes regional values and weightings. DOE should benchmark costs of alternative technologies so regulators have an objective data set to measure against rate impacts.

In the development of this handbook, DOE should consider the risks of cyber-attacks on power electronics (inverters) and the difficulties in restoring a blacked-out grid with a large quantity of voltage-following inverters. Absent grid forming capabilities in some inverters, it may be impossible to provide the voltage reference required to restore the grid.

If possible, the handbook should include sets of regional resilience metrics for different geographic regions.

The handbook should include recommendations on coordinating with other entities to leverage work, avoid duplication, and efficiently use resources.

Cyberspace Solarium Commission, *Final Report of the Cyberspace Solarium Commission* (2020)

Note: The Cyberspace Solarium Commission (CSC) report provides over 75 detailed recommendations for action on cyber strategy, many of them beyond the immediate scope of power grid resilience. Due to space considerations, we reproduce here only the top-line recommendations specifically directed toward protecting critical infrastructure from cyber attacks. This of course does not imply that we consider the report's other recommendations unimportant, and highly recommend a full and thorough review the CSC's report as a comprehensive plan for establishing a national cyber strategy.

Key Recommendation 3.1: Codify Sector-specific Agencies into Law as "Sector Risk Management Agencies" and Strengthen Their Ability to Manage Critical Infrastructure Risk

Enabling Recommendation 3.1.1: Establish a Five-Year National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy

Enabling Recommendation 3.1.2: Establish a National Cybersecurity Assistance Fund to Ensure Consistent and Timely Funding for Initiatives That Underpin National Resilience

Key Recommendation 3.2: Develop and Maintain Continuity of the Economy Planning

Key Recommendation 3.3: Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund"

Enabling Recommendation 3.3.1: Designate Responsibilities for Cybersecurity Services under the Defense Production Act

Enabling Recommendation 3.3.2: Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts

Enabling Recommendation 3.3.3: Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts

Enabling Recommendation 3.3.4: Expand Coordinated Cyber Exercises, Gaming, and Simulation

Enabling Recommendation 3.3.5: Establish a Biennial National Cyber Tabletop Exercise

Enabling Recommendation 3.3.6: Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard

Key Recommendation 3.4: Improve the Structure and Enhance Funding of the Election Assistance Commission

Enabling Recommendation 3.4.1: Modernize Campaign Regulations to Promote Cybersecurity

Key Recommendation 3.5: Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations

Enabling Recommendation 3.5.1: Reform Online Political Advertising to Defend against Foreign Influence in Elections

Key Recommendation 5.1: Codify the Concept of "Systemically Important Critical Infrastructure"

Enabling Recommendation 5.1.1: Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector

Enabling Recommendation 5.1.2: Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities

Enabling Recommendation 5.1.3: Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities

Key Recommendation 5.2: Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information

Enabling Recommendation 5.2.1: Expand and Standardize Voluntary Threat Detection Programs

Enabling Recommendation 5.2.2: Pass a National Cyber Incident Reporting Law

Enabling Recommendation 5.2.3: Amend the Pen Register Trap and Trace Statute to Enable Better Identification of Malicious Actors

Key Recommendation 5.3: Strengthen an Integrated Cyber Center within CISA and Promote the Integration of Federal Cyber Centers

Key Recommendation 5.4: Establish a Joint Cyber Planning Cell under the Cybersecurity and Infrastructure Security Agency

Enabling Recommendation 5.4.1: Institutionalize Department of Defense Participation in Public-Private Cybersecurity Initiatives

Enabling Recommendation 5.4.2: Expand Cyber Defense Collaboration with Information and Communications Technology Enablers

---

National Research Council, *Terrorism and the Electric Power Delivery System* (2012)

What Should the Department of Homeland Security Do?

The level of protection for and resiliency of the electric power grid against terrorist attacks needs to increase. However, the level of security that is economically rational for most infrastructure operators will be less than the level that is optimal from the perspective of the collective national interest. Therefore, the DHS should develop a coherent plan to address the incremental cost of upgrading and protecting critical infrastructure to that higher level.

In the specific context of electric power delivery, the Department of Homeland Security should:

Recommendation 1: Take the lead and work with the DOE and with relevant private parties to develop and stockpile a family of easily transported high-voltage recovery transformers and other key equipment. Although the expected benefits to the nation of such a program are difficult to quantify, they would certainly be many times its cost if the transformers are needed.

Recommendation 2: Work to promote the adoption of many other technologies and organizational changes, identified in this report, that could reduce the vulnerability of the power delivery system and facilitate its more rapid restoration should an attack occur.

Recommendation 3: Work with the power industry to better clarify the role of power system operators after terrorist events through the development of memoranda of understanding and planned and rehearsed response programs that include designating appropriate power-system personnel as first responders.

Recommendation 4: Offer assistance to the Federal Energy Regulatory Commission, to state public service commissions, and to other public and private parties in finding ways to ensure that utilities and transmission operators have appropriate incentives to accelerate the process of upgrading power delivery and eliminating its most obvious vulnerabilities.

Recommendation 5: Work with the Department of Energy and the Office of Management and Budget to substantially increase the level of federal basic technology research investment in power delivery. The committee notes that (1) much of what is needed has the nature of a “public good” that the private sector will not develop on its own; (2) current levels of research investment are woefully inadequate; and (3) most of the system’s vulnerabilities to terrorism are integrally linked to other more general problems and vulnerabilities of the system and cannot be resolved in isolation.

Recommendation 6: Take the lead in initiating planning at the state and local level to reduce the vulnerability of critical services in the event of disruption of conventional power supplies, and offer pilot and incremental funding to implement these activities where appropriate.

Recommendation 7: Develop a national inventory of portable generation equipment that can be used to power critical loads during an extended outage. Explore public and private strategies for building and maintaining an adequate inventory of such equipment.

Electric Power Research Institute, *High-Altitude Electromagnetic Pulse and the Bulk Power System* (2019)

Recommendations for Future Research

There were a number of research gaps that were identified during this three-year effort. Many of them were evaluated during the course of the research, but some could not be acted upon due to lack of resources or scope limitations. Several areas where additional EMP research is warranted are described below.

8.1 Integrated Energy Network Assets

The use of microgrids and an integrated energy network (IEN) is often described as a potential approach for increasing the resiliency of electric power networks. Additionally, because of socio-economic reasons, the existing bulk power system will likely morph into a hybrid system that consists of traditional assets and newer technologies. Because these newer systems consist of assets with considerable electronics-based protection, controls and communication systems (e.g., microgrids, utility-scale inverter-based generation, demand response, smart meters) it is important to understand the potential impact that E1 EMP may have on these devices and system operation. Although E2 EMP is not considered a threat for transmission assets, it may be a threat for assets that operate at lower voltages (e.g., low-voltage inverters connected to rooftop PV). Additionally, some types of technologies (e.g., inverters and uninterruptible power supply systems) could be susceptible to the high levels of harmonic voltage distortion that could propagate from the high-voltage system as a result of E3 EMP impacts.

Additional research in this area could identify classes of technologies within the IEN framework that may be at risk of potential damage from E1 EMP and/or E3 EMP, and that if damaged could significantly degrade the resiliency of the electric grid. Research following a similar framework as the project described in this report could be performed to assess potential impacts and establish hardening and mitigation options for these systems.

8.2 Generation Facilities and End-Use Equipment

This research project focused on the potential impacts of HEMP on the electric transmission system, which included substations at generation facilities (i.e., switchyards). Additional research is needed to evaluate the potential impacts of HEMP on generation facilities themselves and on the end-use equipment that makes up the electric demand of the system. Research following a similar framework to that described in this report could be performed to assess potential impacts and establish hardening and mitigation options for these systems.

8.3 Software Tools and Methods for Performing HEMP Assessments

The assessments that were performed as a part of this research required the development of “in house” software tools. Many of the calculations, for example E1 EMP coupling, are very complex and require expertise that is not common among electric utility engineers. Performing complex studies such as the interconnection-scale E1 EMP + E3 EMP assessment requires significant investment resources to first gain the knowledge and experience necessary to develop the simulation capability that is required and then to develop the capability to perform these kinds of studies. Traditionally, these types of studies have been performed by the government and other research entities; however, electric utilities have the

most knowledge of their systems and would be in the best position to perform the studies, if resources such as commercially available software tools and training were available. Additional research and development could be used to enhance the capability and methods for performing HEMP assessments so that they can be more easily translated into commercial software tools that are used by utility engineers. Additional training is also warranted to provide additional technical background to those performing the studies.

8.4 Equipment Testing

Significant direct voltage surge injection testing of equipment was performed as a part of this research. When evaluating the waveform of the simulated overvoltages obtained from the E1 EMP coupling calculations, it was discovered that the pulse shape of the overvoltage was much wider than the MIL-STD-188-125-1 pulse. In many cases the resulting overvoltage had a rise time that was orders of magnitude slower than the rise time defined in the standard. Future research could investigate how these differences manifest themselves in terms of damage thresholds in equipment.

When the direct injection testing and free field illumination tests were performed, they were performed in isolation. Additional research and development is needed to test equipment such as DPRs when they are simultaneously exposed to threat-level radiated and conducted transients, to determine if developing damage thresholds based on testing that decouples these threats is providing an acceptable level of immunity.

8.5 HEMP Environments

Additional unclassified E1 EMP and E3 EMP environments that included high-fidelity spatio-temporal characteristics necessary for interconnection-scale assessments were made available to this research project. However, these environments are not publicly available. Work should continue by U.S. government agencies to develop and distribute E1 EMP and E3 EMP environments with proper spatio-temporal characteristics that are suitable for civilian use. Knowledge gained as a part of this research could inform utility requirements in this space.

8.6 Field Trials of E1 EMP Hardening of Substations

Because of the risk of unintended consequences with implementing E1 EMP mitigations in a substation environment, a deliberate approach to hardening substations is recommended. Evaluating field deployments of these mitigation technologies and approaches could provide a unique opportunity for identifying potential unintended consequences and associated engineering solutions, identifying/developing maintenance processes and procedures, and providing realistic cost data to inform future decision making. EPRI launched a follow-on research effort in 2019 to further evaluate the E1 EMP mitigation options that were identified through this initial research project.

North American Electric Reliability Corporation, *EMP Task Force: Strategic Recommendations* (2019)

Policy Recommendation #1: Establish BPS Performance Expectations for an EMP Event

The ERO Enterprise, through its authority under the Federal Power Act, should work closely with other agencies to establish performance expectations for all sectors of the BPS regarding a predefined EMP event.

Policy Recommendation #2: Industry and Public Education

Provide consistent/endorsed educational materials about EMPs and their impact to electronic devices and BPS stability to industry and general public.

Policy Recommendation #3: Coordination with Other Sectors

Provide guidance to the electricity industry on how to coordinate with interdependent utility sectors (telecommunications, fuel supply, water) as it relates to an EMP event.

Policy Matters #1: Cost Recovery Mechanisms

Provide industry with clear, consistent cost recovery mechanisms (federal financial support) for planning, mitigation, and recovery plans to ensure the performance expectations as it relates to Policy Recommendation #1 are met.

Policy Matters #2: Industry Access to Classified Information

Provide industry with access to relevant currently classified research by the National Labs, DTRA, and any additional third-party research conducted on electric utility equipment by the Department of Energy.

Policy Matters #3: Declassification of Information

Work to declassify industry-relevant information on E1, E2, and E3 EMP environments and any other research.

Research Recommendation #1: Monitor Current Research and Report on National Initiatives

Monitor and communicate to [sic] the industry research pertaining to EMP and EMP-related national security initiatives that impacts [sic] the BPS.

Research Recommendation #2: Identify Gaps in Research

Additional research is needed to close existing knowledge gaps into the complete impact of an EMP event. This is needed to understand vulnerabilities, develop mitigation strategies, and how to plan response and recovery efforts.

Research Recommendation #3: Develop Industry Specifications for Equipment

Undertake efforts to design equipment specifications for the electric sector utility industry around EMP hardening and mitigation strategies.

Vulnerability Assessment Recommendation #1: Collaboration and Coordination with Federal Government

Consider maintaining an EMP Task Force within the ERO Enterprise Technical Committees to regularly coordinate and collaborate with governmental authorities to procure and effectively disseminate information needed by industry.

Vulnerability Assessment Recommendation #2: EMP Vulnerability Assessment Methods

The ERO Enterprise should develop tools and methods for system planners and equipment owners to use in assessing EMP impacts on the BPS.

Vulnerability Assessment Recommendation #3: Critical Assets Identification

Provide guidance to the industry on how to identify and prioritize hardening of assets that are needed to maintain and restore critical BPS operations.

Mitigation Recommendation #1: Develop Guidance on EMP Mitigation

The ERO Enterprise should develop guidelines for industry to use in developing strategies for mitigating the effects of an EMP on the BPS (control centers/plant controls, substations, and power plants).

Response and Recovery Recommendation #1: Establish National EMP Notification System

The ERO Enterprise should consider partnering with the appropriate agencies to develop a real-time national notification system for the electric sector to System Operators and Plant Operators pertaining to an EMP event and its parameters.

Response and Recovery Recommendation #2: Coordinated Response Planning

Develop response planning guidelines for electric utility industry members for pre and post-contingency of an EMP event that aligns with the DHS and FEMA.

Response and Recovery Recommendation #3: Enhance Operating Procedures

Work with industry to develop criteria to incorporate into operating plans and procedures and system restoration plans pertaining to EMP event [sic].

Response and Recovery Recommendation #4: Incorporate EMP Events into Industry Exercises and Training

Develop training for system and plant operators about EMP events and what to anticipate and incorporate EMP events in industry exercises to test response planning and system restoration recovery efforts.

Response and Recovery Recommendation #5: Strategies for Supporting Recovery

The ERO Enterprise should provide guidance to industry for supporting systems and equipment (including spare equipment strategy) needed for BPS recovery post-EMP event.

NERC Energy Information Sharing and Analysis Center, *GridEx V Exercise* (2020)

Executive Tabletop Recommendations

1. **Ensure grid emergency response and restoration plans account for the complexity of national security emergencies and describe coordination with federal and state or provincial authorities.** Utilities and Reliability Coordinators (RCs) should review their grid restoration and crisis management plans and evaluate how they would identify and manage events in support of governmental national security priorities.

2. **Incorporate natural gas providers and pipeline operators into restoration planning and drills.** Natural gas providers should coordinate with natural-gas-fired generator operators to identify alternate supply arrangements in the event of a significant or sustained natural gas supply disruption. Governments at the federal and state or provincial levels in Canada and the United States should evaluate how their authorities could assist in the event of a severe natural gas supply disruption.

3. **Enhance coordination with communications providers to support restoration and recovery and advocate for continued availability of 6 GHz spectrum.** Utilities should document critical communications facilities as part of their grid restoration plans. To assist with the utilities' own prioritization, they should work with providers to understand broader communication industry restoration priorities. Utilities and RCs should continue to pursue the use of resilient communications systems to enhance their ability to operate through extended disruptions of traditional communications. Electricity tabletop participants agreed that proposed changes to utility-used 6 GHz spectrum could impede resilient communications that support grid reliability during emergencies—the 6 GHz spectrum must be available to utilities during an emergency to ensure the reliable function of the grid.

4. **Build consensus with the U.S. Department of Energy (DOE) on the design, issuance, and liability protections for grid security emergency (GSE) orders issued under Section 215A of the Federal Power Act.** The U.S. government should continue to refine consultative and communications mechanisms with industry to support the development of GSE orders. Utilities agreed that a GSE should specify restoration priorities but leave the detailed engineering approach of how to achieve the priority up to the utilities and RCs. The entities responsible for implementing the order would then have the flexibility to take necessary actions while respecting safe grid operating practices and knowing the current status and overall strategy for grid restoration. DOE should collaborate with industry to consider whether to provide additional liability protections for electricity entities and supporting sectors, such as telecommunications and mid-stream natural gas companies that implement the GSE orders. This would especially apply to lawsuits from customers or others who are disadvantaged or suffer loss because of the GSE order.

5. **Identify key supply chain elements and consider the formation of shared inventory programs for the most critical components.** Tabletop participants agreed on the need to understand how critical electricity sector manufacturers would respond to a security incident and share capabilities to include in utility planning efforts. Participants also discussed the benefits of identifying key components in their systems and the supporting supply chains as well as

developing a shared inventory capability for essential equipment similar to the transformer reserve.

6. **Continue to grow participation in the Electricity Subsector Coordinating Council (ESCC) cyber mutual assistance (CMA) program.** Utilities should consider activating the CMA program as a resource for supporting response and recovery efforts in a cyber incident in advance of, or in the event of, disruption of electric or natural gas service. The CMA program provides resources (e.g., information sharing, services, personnel, equipment) that can assist an entity during an incident.

7. **Continue to strengthen the operational industry and government coordination between the United States and Canada.** NERC, in partnership with CEA, should invite Canadian government representatives to be part of the next GridEx executive tabletop and continue to use a scenario with an incident scope that includes Canada and the United States.

Department of Energy (DOE) Infrastructure Security & Energy Restoration Office (ISER), *Liberty Eclipse Energy Assurance Exercise and Event* (2017)

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

Proposed Actions:

- Energy assurance plans should provide more detailed plans and approaches for dealing with cyber incidents, and they should include roles and responsibilities of all the state agencies that could be involved in the responses and public messaging. States should be prepared to identify what planning, policy, and regulatory actions have already taken place, and align them with Presidential Policy Directive (PPD)-41.
- States should work with the energy sector on their energy assurance plans and response efforts to provide better coordination between the public and private sectors. Meetings at a state level on this subject, if not already underway, should be considered.
- DOE should identify opportunities to best align and communicate coordination procedures with states and industry for cyber incidents in the energy sector.
- DOE, the U.S. Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI) should coordinate to identify legal restrictions on sharing cybersecurity information gathered during an FBI law enforcement action.
- FBI, DHS, the Office of the Director of National Intelligence, and DOE should more clearly define their roles and responsibilities in cyber incident coordination in the energy sector than what is currently outlined in PPD-41. They should also communicate thresholds and expectations more clearly to states and industry.
- Federal cybersecurity advisories to infrastructure owners and operators relating to cyber threats should be coordinated between the FBI, DHS, and the relevant sector-specific agencies.
- States and electric utilities should be prepared to understand the implications of the rules enacted in the event that the President should declare a Grid Security Emergency, as well as the

Secretary of Energy's authority under this declaration. State and electric utilities emergency response plans should include consideration for the Grid Security Emergency authority.

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

Proposed Actions:

- Public information programs should be part of energy emergency response plans. Public and private Public Information Officers (PIOs) should review existing plans and identify improvements to address a long-term power outage or incident that may create considerable public concern.
- Social media is an important communications mechanism that can reduce misinformation and provide the public with information on response and recovery efforts. It can also provide the public with actions that they can take to ensure their safety and the safety of their family and neighbors.
- PIOs should be invited to participate in future exercises so that this can be more fully addressed.

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

Proposed Actions:

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

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

Proposed Actions:

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

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

Proposed Actions:

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

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

Proposed Actions:

- DOE and NASEO should consult with petroleum suppliers to develop model petroleum shortage response plans, also called "Fuel Plans." States could then adopt them when they update their energy assurance plans. These "Fuels Plans" should address the roles and responsibilities for implementation and operations, and they should include draft executive orders accompanied by press releases to notify the public of their implementation.
- As a precursor to the development of model plans, a webinar should be held to present and discuss select state petroleum or fuels plans that have been developed in greater detail.
- States should review their energy assurance plans and work with the oil and natural gas subsector within their states to update those plans, as well as develop more operation fuel plans.
- Additional guidance should be developed for states on the use of the waivers for gasoline fuel specification from the Environmental Protection Agency, and regarding Jones Act waivers for allowing foreign-flagged tankers to make marine fuel shipments.

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

Proposed Actions:

- Exercise participants and those responsible for energy assurance and preparedness need to understand the energy infrastructure and its capacity, flows, and operations. If there is a gap in their knowledge base, they should take advantage of the many resources available to achieve such an understanding.
- PUCs can work with utilities to understand what their networks and infrastructure look like and to develop or identify visualizations such as maps, which are very helpful to workers providing aid in emergency situations. PUCs should also work with utilities to have a common understanding of what assets and systems should be the priority during restoration.
- State energy offices and PUCs should develop robust workforce training and development programs to ensure appropriate levels of preparedness, so workers can address events such as those contemplated in the exercise and other related energy emergency exercises.

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

Proposed Actions:

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

Annex II

Pending Legislation, Congressional Bodies, Executive Agencies, and Industry Associations Related to Grid Resilience and Security

Grid Security Legislation Sampling (prior two sessions):

1. H.R.359 — 116th Congress (2019-2020) Enhancing Grid Security through Public-Private Partnerships Act **Sponsor:** Rep. McNerney, Jerry [D-CA-9] (Introduced 01/09/2019) **Cosponsors:** (3) **Committees:** House - Energy and Commerce **Committee Reports:** H. Rept. 116-254 **Latest Action:** House - 10/28/2019 Placed on the Union Calendar, Calendar No. 202. (All Actions)

This bill directs the Department of Energy to facilitate and encourage public-private partnerships in order to address and mitigate the physical security and cybersecurity risks of electric utilities.

2. S.2095 — 116th Congress (2019-2020) Enhancing Grid Security through Public-Private Partnerships Act **Sponsor:** Sen. Gardner, Cory [R-CO] (Introduced 07/11/2019) **Cosponsors:** (1) **Committees:** Senate - Energy and Natural Resources **Committee Reports:** S. Rept. 116-147 **Latest Action:** Senate - 10/24/2019 Placed on Senate Legislative Calendar under General Orders. Calendar No. 267. (All Actions)

To provide for certain programs and developments in the Department of Energy concerning the cybersecurity and vulnerabilities of, and physical threats to, the electric grid, and for other purposes.

3. H.R.5760 — 116th Congress (2019-2020) Grid Security Research and Development Act **Sponsor:** Rep. Bera, Ami [D-CA-7] (Introduced 02/05/2020) **Cosponsors:** (1) **Committees:** House - Science, Space, and Technology; Homeland Security **Latest Action:** House - 02/19/2020 Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation. (All Actions)

To provide for a comprehensive interdisciplinary research, development, and demonstration initiative to strengthen the capacity of the energy sector to prepare for and withstand cyber and physical attacks, and for other purposes.

4. S.2333 — 116th Congress (2019-2020) Energy Cybersecurity Act of 2019 **Sponsor:** Sen. Cantwell, Maria [D-WA] (Introduced 07/30/2019) **Cosponsors:** (1) **Committees:** Senate - Energy and Natural Resources **Committee Reports:** S. Rept. 116-144 **Latest Action:** Senate - 10/23/2019 Placed on Senate Legislative Calendar under General Orders. Calendar No. 264. (All Actions)

This bill directs the Department of Energy (DOE) to develop advanced cybersecurity applications and technologies for the energy sector.

5. H.R.3597 — 116th Congress (2019-2020) Solar Energy Research and Development Act of 2019 **Sponsor:** Rep. McAdams, Ben [D-UT-4] (Introduced 06/28/2019) **Cosponsors:** (4) **Committees:** House - Science, Space, and Technology **Latest Action:** House - 07/24/2019 Ordered to be Reported (Amended) by the Yeas and Nays: 21 - 13. (All Actions)

This bill requires the Department of Energy to carry out a grant program to research, develop, and evaluate solar energy technologies and systems.

6. S.2668 — 116th Congress (2019-2020) Solar Energy Research and Development Act of 2019 **Sponsor:** Sen. Sinema, Kyrsten [D-AZ] (Introduced 10/22/2019) **Cosponsors:** (1) **Committees:** Senate - Energy and Natural Resources **Committee Reports:** S. Rept. 116-202 **Latest Action:** Senate - 01/09/2020 By Senator Murkowski from Committee on Energy and Natural Resources filed written report. Report No. 116-202. (All Actions)

This bill requires the Department of Energy to establish a grant program to research, develop, evaluate, and commercialize solar energy technologies and systems.

7. S.1498 — 116th Congress (2019-2020) Department of Defense Climate Resiliency and Readiness Act **Sponsor:** Sen. Warren, Elizabeth [D-MA] (Introduced 05/15/2019) **Cosponsors:** (2) **Committees:** Senate - Armed Services **Latest Action:** Senate - 05/15/2019 Read twice and referred to the Committee on Armed Services. (All Actions)

This bill requires the Department of Defense (DOD) to provide a strategy to achieve aggregate net zero energy by non-operational sources by no later than December 31, 2029. The term "net zero energy" means a reduction in overall energy use, maximized energy efficiency, implementation of energy recovery and cogeneration capabilities, and an offset of the remaining demand for energy with production of energy from onsite renewable energy sources.

8. H.R.2759 — 116th Congress (2019-2020) Department of Defense Climate Resiliency and Readiness Act **Sponsor:** Rep. Escobar, Veronica [D-TX-16] (Introduced 05/15/2019) **Cosponsors:** (5) **Committees:** House - Armed Services **Latest Action:** House - 05/16/2019 Referred to the Subcommittee on Readiness. (All Actions)

This bill requires the Department of Defense (DOD) to provide a strategy to achieve aggregate net zero energy by non-operational sources by no later than December 31, 2029. The term "net zero energy" means a reduction in overall energy use, maximized energy efficiency, implementation of energy recovery and cogeneration capabilities, and an offset of the remaining demand for energy with production of energy from onsite renewable energy sources.

9. H.R.2741 — 116th Congress (2019-2020) Leading Infrastructure for Tomorrow's America Act **Sponsor:** Rep. Pallone, Frank, Jr. [D-NJ-6] (Introduced 05/15/2019) **Cosponsors:** (43) **Committees:** House - Education and Labor; Transportation and Infrastructure; Ways and Means; Science, Space, and Technology; Natural Resources; Energy and Commerce **Latest Action:** House - 06/04/2019 Referred to the Subcommittee for Indigenous Peoples of the United States. (All Actions)

To rebuild and modernize the Nation’s infrastructure to expand access to broadband and Next Generation 9–1–1, rehabilitate drinking water infrastructure, modernize the electric grid and energy supply infrastructure, redevelop brownfields, strengthen health care infrastructure, create jobs, and protect public health and the environment, and for other purposes.

10. H.R.2 — 116th Congress (2019-2020) Moving Forward Act **Sponsor:** Rep. DeFazio, Peter A. [D-OR-4] (Introduced 06/11/2020) **Cosponsors:** (129) **Committees:** House - Transportation and Infrastructure **Committee Reports:** H. Rept. 116-437 **Latest Action:** Senate - 07/20/2020 Received in the Senate. (All Actions)

This bill addresses provisions related to federal-aid highway, transit, highway safety, motor carrier, research, hazardous materials, and rail programs of the Department of Transportation (DOT).

11. H.R.5240 — 115th Congress (2017-2018) Enhancing Grid Security through Public-Private Partnerships Act **Sponsor:** Rep. McNerney, Jerry [D-CA-9] (Introduced 03/09/2018) **Cosponsors:** (2) **Committees:** House - Energy and Commerce **Committee Reports:** H. Rept. 115-795 **Latest Action:** House - 06/28/2018 Placed on the Union Calendar, Calendar No. 615. (All Actions)

This bill directs the Department of Energy to facilitate and encourage public-private partnerships in order to address and mitigate the physical security and cybersecurity risks of electric utilities.

12. S.3677 — 115th Congress (2017-2018) Enhancing Grid Security through Public-Private Partnerships Act **Sponsor:** Sen. Gardner, Cory [R-CO] (Introduced 11/29/2018) **Cosponsors:** (1) **Committees:** Senate - Energy and Natural Resources **Latest Action:** Senate - 11/29/2018 Read twice and referred to the Committee on Energy and Natural Resources. (All Actions)

This bill directs the Department of Energy to facilitate and encourage public-private partnerships in order to address and mitigate the physical security and cybersecurity risks of electric utilities.

13. S.2444 — 115th Congress (2017-2018) Energy Cybersecurity Act of 2018 **Sponsor:** Sen. Cantwell, Maria [D-WA] (Introduced 02/15/2018) **Cosponsors:** (2) **Committees:** Senate - Energy and Natural Resources **Latest Action:** Senate - 02/15/2018 Read twice and referred to the Committee on Energy and Natural Resources. (All Actions)

This bill directs the Department of Energy (DOE) to develop advanced cybersecurity applications and technologies for the energy sector.

14. S.2991 — 115th Congress (2017-2018) Promoting Cybersecurity for Rural Electric Utilities Act **Sponsor:** Sen. Bennet, Michael F. [D-CO] (Introduced 06/05/2018) **Cosponsors:** (1) **Committees:** Senate - Agriculture, Nutrition, and Forestry **Latest Action:** Senate - 06/05/2018 Read twice and referred to the Committee on Agriculture, Nutrition, and Forestry. (All Actions)

This bill amends the Rural Electrification Act of 1936 to authorize the Department of Agriculture to make or guarantee loans for cybersecurity and grid security improvements.

15. S.613 — 115th Congress (2017-2018) Ratepayer Fairness Act **Sponsor:** Sen. Flake, Jeff [R-AZ] (Introduced 03/13/2017) **Cosponsors:** (0) **Committees:** Senate - Energy and Natural Resources **Latest Action:** Senate - 03/13/2017 Read twice and referred to the Committee on Energy and Natural Resources. (All Actions)

To amend the Public Utility Regulatory Policies Act of 1978 to provide for the consideration by State regulatory authorities and nonregulated electric utilities of whether subsidies should be provided for the deployment, construction, maintenance, or operation of a customer-side technology.

16. H.R.1572 — 115th Congress (2017-2018) Ratepayer Fairness Act of 2017 **Sponsor:** Rep. Hudson, Richard [R-NC-8] (Introduced 03/16/2017) **Cosponsors:** (1) **Committees:** House - Energy and Commerce **Latest Action:** House - 03/17/2017 Referred to the Subcommittee on Energy. (All Actions)

To amend the Public Utility Regulatory Policies Act of 1978 to provide for the consideration by State regulatory authorities and nonregulated electric utilities of whether subsidies should be provided for the deployment, construction, maintenance, or operation of a customer-side technology.

17. H.R.2479 — 115th Congress (2017-2018) Leading Infrastructure for Tomorrow's America Act **Sponsor:** Rep. Pallone, Frank, Jr. [D-NJ-6] (Introduced 05/17/2017) **Cosponsors:** (26) **Committees:** House - Energy and Commerce; Science, Space, and Technology; Transportation and Infrastructure; Ways and Means; Natural Resources **Latest Action:** House - 05/22/2018 Referred to the Subcommittee on Energy. (All Actions)

To rebuild and modernize the Nation's infrastructure to expand access to broadband internet, rehabilitate drinking water infrastructure, modernize the electric grid and energy supply infrastructure, redevelop brownfields, strengthen health care infrastructure, create jobs, protect public health and the environment, and for other purposes.

18. S.1460 — 115th Congress (2017-2018) Energy and Natural Resources Act of 2017 **Sponsor:** Sen. Murkowski, Lisa [R-AK] (Introduced 06/28/2017) **Cosponsors:** (1) **Latest Action:** Senate - 09/19/2017 Committee on Energy and Natural Resources. Hearings held. Hearings printed: S.Hrg. 115-485. (All Actions)

This bill amends the Energy Conservation and Production Act, the Energy Policy and Conservation Act, and the Energy Independence and Security Act of 2007 with respect to energy efficiency for sectors such as buildings, transportation, schools, and manufacturing.

19. S.3042 — 115th Congress (2017-2018) Agriculture Improvement Act of 2018 **Sponsor:** Sen. Roberts, Pat [R-KS] (Introduced 06/11/2018) **Cosponsors:** (1) **Committees:** Senate - Agriculture, Nutrition, and Forestry **Latest Action:** Senate - 06/18/2018 Placed on Senate Legislative Calendar under General Orders. Calendar No. 470. (All Actions)

To provide for the reform and continuation of agricultural and other programs of the Department of Agriculture through fiscal year 2023, and for other purposes.

Congressional Caucuses:

Advanced Energy Storage Caucus

Mark Takano (D), Chris Collins (R)

Congressional Energy Savings Performance Caucus
Adam Kinzinger (R), Peter Welch (D), Marsha Blackburn (R), Seth Moulton (D)

Northwest Energy Caucus
Pete DeFazio (D), Cathy McMorris Rodgers (R)

Congressional Grid Innovation Caucus
Jerry McNerney (D), Bob Latta (R)

Congressional Cyber Security Caucus
Jim Langevin (D), Mike McCaul (R)

Congressional Nuclear Security Working Group
Jeff Fortenberry (R), Pete Visclosky (D)

Congressional Ports Opportunity, Renewal, Trade and Security (PORTS) Caucus
Ted Poe (R), Alan Lowenthal (D)

House National Security Caucus
Liz Cheney (R), Mike Gallagher (R)

Congressional Committees:

House of Representatives Committees:

Appropriations:

- Commerce, Justice, Science, and Related Agencies Subcommittee
- Defense Subcommittee
- Energy and Water Development, and Related Agencies Subcommittee
- Homeland Security Subcommittee
- Interior, Environment, and Related Agencies Subcommittee
- Military Construction, Veterans Affairs, and Related Agencies Subcommittee

Armed Services

Budget

Energy and Commerce

Foreign Affairs

Homeland Security

Natural Resources

Science, Space, and Technology

Transportation and Infrastructure

Ways and Means

Permanent Select Committee on Intelligence

Select Committee on the Climate Crisis

Senate Committees:

Appropriations:

- Subcommittee on Commerce, Justice, Science, and Related Agencies
- Subcommittee on Department of Defense
- Subcommittee on Department of Homeland Security
- Subcommittee on Department of the Interior, Environment, and Related Agencies
- Subcommittee on Energy and Water Development
- Subcommittee on Military Construction and Veterans Affairs, and Related Agencies

Armed Services

Budget

Commerce, Science, and Transportation

Energy and Natural Resources

Environment and Public Works

Finance

Foreign Relations

Homeland Security and Governmental Affairs

Select Committee on Intelligence

Joint Committees:

Joint Committee on Taxation

Executive Agencies:

A massive array of executive agencies have missions that intersect with grid resilience. We list the most important ones here, though the list should not be considered comprehensive. In the interest of accuracy, in most cases we have excerpted agencies' own language describing their responsibilities from

their websites. While not detailed, we encourage readers to review the following high-level responsibilities of each agency—in their own words—in order to glimpse the current state of institutional complexity that would be involved in coordinating resilience activities and responding to catastrophic power outages. In the words of the President's National Infrastructure Advisory Council (NIAC): "our existing plans, response resources, and coordination strategies would be outmatched by an event of this severity. Significant action is needed to prepare for a catastrophic power outage that could last for weeks or months."[1]

Department of Energy (DOE)

Presidential Policy Directive 21 designates the Department of Energy (DOE) as the sector-specific agency for the energy sector, and DOE is responsible for the development of the sector specific plan (SSP) for energy.[2] In doing so, it coordinates with the Department of Homeland Security (DHS), which is responsible for the National Infrastructure Protection Plan (NIPP). The most critical program offices within DOE for electric power grid resilience are listed below, along with brief descriptions of the offices excerpted from their websites:

Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

> The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) addresses the emerging threats of tomorrow while protecting the reliable flow of energy to Americans today by improving energy infrastructure security and supporting the Department of Energy's (DOE) national security mission. CESER's focus is preparedness and response activities to natural and man-made threats, ensuring a stronger, more prosperous, and secure future for the Nation.[3]

Office of Electricity (OE)

> The Office of Electricity (OE) provides national leadership to ensure that the Nation's energy delivery system is secure, resilient and reliable. OE works to develop new technologies to improve the infrastructure that brings electricity into our homes, offices, and factories, and the federal and state electricity policies and programs that shape electricity system planning and market operations.[4]

Office of Energy Efficiency and Renewable Energy (EERE)

> The mission of EERE is to create and sustain American leadership in the transition to a global clean energy economy. Its vision is a strong and prosperous America powered by clean, affordable, and secure energy.[5]

Office of Science

> The Office of Science supports the Nation's best minds, using the world's best facilities, to keep America at the forefront of discovery. From astronomy to zeolites, our researchers are unveiling secrets of the basic building blocks of matter, such as quarks, neutrinos, and the Higgs boson. They peer deep into outer space to understand the dark

matter and dark energy that seem to dominate the universe and yet have eluded our attempts to observe them directly. They peer deep into inner space, too, examining and manipulating matter at nanoscale and atomic resolutions.

. . . Cutting-edge technology and scientific tools drive world-shaping discoveries at DOE. The Office of Science accelerates discovery with the world's largest array of major scientific user facilities that includes particle colliders, powerful X-ray light sources, and delicate sensors and optics. Some of the most powerful supercomputers in the world reside in DOE user facilities – the Summit supercomputer at Oak Ridge National Laboratory is currently the world leader – and enable technological innovation while speeding insights into everything from the properties of plasma in fusion reactors, to complex weather and climate patterns, to the geophysics of earthquakes.[6]

National Labs

An outgrowth of immense investment in scientific research initiated by the U.S. Government during World War II, the National Laboratories have served as the leading institutions for scientific innovation in the United States for more than seventy years.

The Energy Department's 17 National Labs tackle the critical scientific challenges of our time -- from combating climate change to discovering the origins of our universe -- and possess unique instruments and facilities, many of which are found nowhere else in the world. They address large scale, complex research and development challenges with a multidisciplinary approach that places an emphasis on translating basic science to innovation.[7]

Federal Energy Regulatory Commission (FERC)

FERC is an independent regulatory agency that regulates the interstate transmission of oil, natural gas, and electricity. Under the Energy Policy Act of 2005, FERC received additional powers and responsibilities, which the agency lists as follows:

- Regulates the transmission and wholesale sales of electricity in interstate commerce;
- Reviews certain mergers and acquisitions and corporate transactions by electricity companies;
- Regulates the transmission and sale of natural gas for resale in interstate commerce;
- Regulates the transportation of oil by pipeline in interstate commerce;
- Approves the siting and abandonment of interstate natural gas pipelines and storage facilities;
- Reviews the siting application for electric transmission projects under limited circumstances;
- Ensures the safe operation and reliability of proposed and operating LNG terminals;
- Licenses and inspects private, municipal, and state hydroelectric projects;
- Protects the reliability of the high voltage interstate transmission system through mandatory reliability standards;

- Monitors and investigates energy markets;
- Enforces FERC regulatory requirements through imposition of civil penalties and other means;
- Oversees environmental matters related to natural gas and hydroelectricity projects and other matters; and
- Administers accounting and financial reporting regulations and conduct of regulated companies.[8]

North American Electric Reliability Corporation (NERC)

> The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 400 million people.[9]

Department of Homeland Security (DHS)

Cybersecurity and Infrastructure Agency (CISA)

> The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.
>
> . . . CISA builds the national capacity to defend against cyber attacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies.
>
> We coordinate security and resilience efforts using trusted partnerships across the private and public sectors, and deliver technical assistance and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.[10]

CISA contains multiple grid resilience relevant bodies. We list them below:

National Cybersecurity and Communications Integration Center (NCCIC)

> The NCCIC serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC's partners include other government agencies, the private sector, and international entities. Working closely with its partners, NCCIC analyzes cybersecurity

and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts.

. . . The NCCIC's missions include:

- Leading the protection of federal civilian agencies in cyberspace;
- Working closely together with critical infrastructure owners and operators to reduce risk;
- Collaborating with state and local governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC);
- Cooperating with international partners to share information and respond to incidents;
- Coordinating national response to significant cyber incidents in accordance with the National Cyber Incident Response Plan (NCIRP);
- Analyzing data to develop and share actionable mitigation recommendations
- Creating and maintaining shared situational awareness among its partners and constituents;
- Orchestrating national protection, prevention, mitigation, and recovery activities associated with significant cyber and communication incidents;
- Disseminating cyber threat and vulnerability analysis information;
- Assisting in the initiation, coordination, restoration, and reconstitution of National Security or Emergency Preparedness (NS/EP) telecommunications services and facilities under all conditions, crises, or emergencies; and
- Executing Emergency Support Function 2- Communications (ESF-2) responsibilities under the National Response Framework (NRF).

The NCCIC is comprised of four branches:

- NCCIC Operations & Integration (NO&I);
- United States Computer Emergency Readiness Team (US-CERT);
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); and
- National Coordinating Center for Communications (NCC).[11]

National Infrastructure Coordinating Center

The National Infrastructure Coordinating Center (NICC) is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation’s critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our nation’s infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets. The NICC is part of the Cybersecurity and Infrastructure Security Agency's Infrastructure Security division and the DHS National Operations Center.[12]

National Risk Management Center (NRMC)

The National Risk Management Center (NRMC) is leading the Nation's effort for secure and resilient critical infrastructure both now and into the future. There are 16 critical infrastructure sectors that are important to the functioning of our country and everyday lives, including communications, energy, transportation, and water. With most of the critical infrastructure owned by the private sector, managing risk is a priority shared by industry and government.

Through collaborative efforts with the private sector, government agencies, and other key stakeholders, the NRMC uses a dynamic, cross-sector risk management process to identify, analyze, prioritize, and manage the most significant risks—cyber and physical—to these important national functions.

Central to the NRMC's work is understanding criticality—what functions are so vital that if disrupted or sabotaged may cause cross-sector impacts or nationwide degradation? Understanding criticality enables the NRMC to strategically focus on those functions at the highest risk.

Critical Infrastructure Partnership Advisory Council (CIPAC)

The U.S. Department of Homeland Security established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate interaction between governmental entities and representatives from the community of critical infrastructure owners and operators.

CIPAC is aligned with and supports the implementation of the National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience to provide a forum in which the government and private sector entities, organized as coordinating councils, can jointly engage in a broad spectrum of activities to support and collaborate critical infrastructure security and resilience efforts.

Federal Emergency Management Agency (FEMA)

Our mission is to help people before, during and after disasters. At FEMA, we employ more than 20,000 people nationwide. Headquartered in Washington, D.C., we have 10 regional offices located across the country. We leverage a tremendous capacity to coordinate within the federal government to make sure America is equipped to prepare for and respond to disasters.[13]

FEMA takes responsibility of most federal disaster response activities under the Stafford Act. The agency's 2018-2022 Strategic Plan creates a framework for supporting the nation before, during, and after disasters, and aims to mobilize "a whole community approach to disaster response."[14]

National Institute of Standards and Technology (NIST): Community Resilience Program

> Community resilience has emerged as a way to reduce the direct and indirect costs due to natural, technological, and human-caused hazard events. There continues to be a need for additional guidance on how to plan for and implement measures to improve community resilience as well as science-based tools to measure resilience and support evaluation of alternative strategies to achieve resilience. The National Institute of Standards and Technology (NIST) program is (1) developing science based tools and metrics to support and measure resilience at the community-scale and support economic evaluation of alternative solutions to improve resilience and (2) engaging community resilience stakeholders for input and feedback to products, such as guidance, tools, and metrics, for planning and implementing resilience measures.

Department of Defense (DOD)

The National Defense Strategy charges the DOD with maintaining capacity to support civil authorities in the wake of a national emergency.[15] DOD launched a Complex Catastrophe Initiative in 2012 to improve those capacities.[16]

U.S. Northern Command (NORTHCOM)

> USNORTHCOM plans, organizes and executes homeland defense and civil support missions, but has few permanently assigned forces. The command is assigned forces whenever necessary to execute missions, as ordered by the president or secretary of defense.
>
> . . . USNORTHCOM's civil support mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes. Support also includes counter-drug operations and managing the consequences of a terrorist event employing a weapon of mass destruction. The command provides assistance to a Primary Agency when tasked by DOD. Per the Posse Comitatus Act, military forces can provide civil support, but cannot become directly involved in law enforcement.
>
> In providing civil support, USNORTHCOM generally operates through established Joint Task Forces subordinate to the command. An emergency must exceed the capabilities of local, state and federal agencies before USNORTHCOM becomes involved. In most cases, support will be limited, localized and specific. When the scope of the disaster is reduced to the point that the Primary Agency can again assume full control and

management without military assistance, USNORTHCOM will exit, leaving the on-scene experts to finish the job.[17]

U.S. Indo-Pacific Command (INDOPACOM)

INDOPACOM has four U.S. jurisdictions within its area: Hawaii, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands. It serves the same disaster relief functions for these jurisdictions as NORTHCOM does for North American U.S. Jurisdictions.[18]

Defense Threat Reduction Agency (DTRA)

DTRA is a Combat Support Agency and a Defense Agency with a three-pronged mission:

1. to counter the threats posed by the full spectrum of weapons of mass destruction (WMD), including chemical, biological, radiological, nuclear, and high-yield explosives;

2. counter the threats posed by the growing, evolving categories of improvised threats, including improvised explosive devices, car bombs and weaponized consumer drones, as well as the tactics, technologies and networks that put them on the battlefield;

3. ensure the U.S. military maintains a safe, secure, effective and credible nuclear weapons deterrent.

As a Combat Support Agency, we support the Combatant Commands and the military services with both defensive and offensive capabilities. With a focus on our combat support mission, and through leveraging and expanding our collaboration with interagency and international partners, DTRA is uniquely prepared to address some of the most immediate, consequential and non-conventional weapon threats to our national security. In our role as a Defense Agency, we work with rest of the U.S. government, allies and partner countries, and international organizations to counter WMD and improvised threats. As the DoD's research and development leader focused on WMD and improvised threats, DTRA facilitates innovation as we combine traditional research with unconventional means to develop and quickly field solutions to the most complex, deadly and urgent threats facing the U.S. and the rest of the world.[19]

Industry and State Regulatory Associations

Electricity Subsector Coordinating Council (ESCC)

The CEO-led Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power industry on efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure.

> The ESCC works across the sector, and with the Electricity Information Sharing and Analysis Center (E-ISAC), to develop actions and strategies that help protect the North American energy grid and prevent a spectrum of threats from disrupting electricity service.
>
> The ESCC includes CEOs and executives from electric companies, public power utilities, and rural electric cooperatives, as well as their trade association leaders, who represent all segments of the industry. Through the ESCC, the industry works closely with its government counterparts, including senior administration officials from the White House, cabinet agencies, federal law enforcement, and national security organizations. Canadian electric company executives also are represented on the ESCC due to the international make-up of the North American energy grid.[20]

ESCC manages the Cyber Mutual Assistance Program, a voluntary program for providing cyber assistance within the electric power and natural gas sub-sectors.

ISO/RTO Council (IRC)

A collaborative organization for Independent System Operators and Regional Transmission Operators—who manage organized wholesale energy markets in some parts of the country, the IRC aims to "share innovative ideas and real-world best practices . . . to build a smarter and more efficient electric grid."[21]

National Association of Regulatory Utility Commissioners (NARUC)

> Founded in 1889, the National Association of Regulatory Utility Commissioners (NARUC) is a non-profit organization dedicated to representing the state public service commissions who regulate the utilities that provide essential services such as energy, telecommunications, power, water, and transportation.
>
> NARUC's members include all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands. Most state commissioners are appointed to their positions by their governor or legislature, while commissioners in 14 states are elected. For a complete breakdown, click here.
>
> Our mission is to serve in the public interest by improving the quality and effectiveness of public utility regulation. Under state law, NARUC's members have an obligation to ensure the establishment and maintenance of utility services as may be required by law and to ensure that such services are provided at rates and conditions that are fair, reasonable, and nondiscriminatory for all consumers.[22]

National Conference of State Legislatures (NSCL)

NCSL, founded in 1975, represents the legislatures in the states, territories and commonwealths of the U.S. Its mission is to advance the effectiveness, independence and integrity of legislatures and to foster interstate cooperation and facilitate the exchange of information among legislatures.

NCSL also represents legislatures in dealing with the federal government, especially in support of state sovereignty and state flexibility and protection from unfunded federal mandates and unwarranted federal preemption. The conference promotes cooperation between state legislatures in the U.S. and those in other countries.

In addition, NCSL is committed to improving the operations and management of state legislatures, and the effectiveness of legislators and legislative staff. NCSL also encourages the practice of high standards of conduct by legislators and legislative staff.[23]

Electric Power Research Institute (EPRI)

EPRI provides thought leadership, industry expertise, and collaborative value to help the electricity sector identify issues, technology gaps, and broader needs that can be addressed through effective research and development programs for the benefit of society.

The Electric Power Research Institute (EPRI) conducts research, development, and demonstration projects for the benefit of the public in the United States and internationally. As an independent, nonprofit organization for public interest energy and environmental research, we focus on electricity generation, delivery, and use in collaboration with the electricity sector, its stakeholders and others to enhance the quality of life by making electric power safe, reliable, affordable, and environmentally responsible.

EPRI has collaborated with the electricity sector and its stakeholders since 1972 and our membership has grown to represent approximately 90% of the electric utility revenue generated in the United States and extends to participation in more than 38 countries. The worldwide membership that supports our work comprises more than 1,000 organizations. While most members are electric utilities, others are businesses, government agencies, regulators and public or private entities engaged in some aspect of the generation, delivery, or use of electricity. Through their advisory roles in EPRI, its research sectors and programs, EPRI members help inform the development of EPRI's annual research portfolio, identify critical and emerging electricity industry issues, and support the application and technology transfer of EPRI's research and development.[24]

Edison Electric Institute (EEI)

The Edison Electric Institute (EEI) is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for about 220 million Americans, and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. In addition to our U.S. members, EEI has more than 65 international electric companies, with operations in more than 90 countries, as International Members, and hundreds of industry suppliers and related organizations as Associate Members.

Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums.[25]

National Emergency Management Association (NEMA)

The National Emergency Management Association (NEMA) is a nonpartisan, nonprofit 501(c)(3) association dedicated to enhancing public safety by improving the nation's ability to prepare for, respond to, and recover from all emergencies, disasters, and threats to our nation's security. NEMA is the professional association of and for emergency management directors from all 50 states, eight U.S. territories, and the District of Columbia. NEMA provides national leadership and expertise in comprehensive emergency management; serves as a vital emergency management information and assistance resource; and advances continuous improvement in emergency management through strategic partnerships, innovative programs, and collaborative policy positions.

Electric Infrastructure Security Council (EIS Council)

EIS Council facilitates national and international collaboration and planning to protect our societies' critical utilities against uniquely severe Black Sky Hazards. Our programming and special projects help utilities and their partners develop and implement cost effective, consensus-based protection measures by hosting frameworks for sustained coordination, planning and best practice development.[26]

---

[1] National Infrastructure Advisory Council (2018). SURVIVING A CATASTROPHIC POWER OUTAGE: HOW TO STRENGTHEN THE CAPABILITIES OF THE NATION.
[2] Department of Energy (DOE) and Department of Homeland Security (DHS) (2015). ENERGY SECTOR SPECIFIC PLAN.
[3] DOE CESER. *About Us*.
[4] DOE OE. *About the Office of Electricity*.
[5] DOE EERE. *About the Office of Energy Efficiency and Renewable Energy*.
[6] DOE Office of Science. *About the Office of Science*.
[7] DOE. *National Laboratories*.
[8] FERC. *What FERC Does*.
[9] NERC. *About NERC*.
[10] CISA. *About CISA*.
[11] CISA. *National Cybersecurity and Communications Integration Center*.

[12] CISA. *National Infrastructure Coordinating Center*.
[13] FEMA. *About Us*.
[14] FEMA (2018). 2018-2022 STRATEGIC PLAN.
[15] Mattis, J. (2018). SUMMARY OF THE NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA.
[16] EIS Council. *Protection Initiatives: Restoration and Response*.
[17] U.S. Northern Command. *About USNORTHCOM*.
[18] U.S. Indo-Pacific Command. *About USINDOPACOM*.
[19] DTRA. *About DTRA*.
[20] ESCC. *Home*.
[21] ISO/RTO Council. *About the IRC*.
[22] NARUC. *About NARUC*.
[23] NCSL. *About Us*.
[24] EPRI. *About Us*.
[25] EEI. *About EEI*.
[26] EIS Council. *About Us*.