



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURING RENEWABLE ENERGY THROUGH PUBLIC-PRIVATE PARTNERSHIPS

by

Christian H. Holleman

September 2021

Thesis Advisor:
Second Reader:

Emily L. Meierding
Daniel Eisenberg

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2021		3. REPORT TYPE AND DATES COVERED Master's thesis
4. TITLE AND SUBTITLE SECURING RENEWABLE ENERGY THROUGH PUBLIC-PRIVATE PARTNERSHIPS				5. FUNDING NUMBERS
6. AUTHOR(S) Christian H. Holleman				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000				8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				10. SPONSORING / MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.				12b. DISTRIBUTION CODE A
13. ABSTRACT (maximum 200 words) While the utilization of electricity to support human needs is a staple of modern society, the organizations and legal frameworks underlying the generation, transmission, and distribution of electricity differ across world regions. In the United States, diverse public and private entities are enmeshed throughout the power grid and work to maintain electrical security, i.e., a stable and continuous supply of electricity to customers in the presence of threats. This cooperative relationship appears to be effective given legacy systems and economic structures. However, the incorporation of renewable energy technologies presents a challenge given new system complexity, economic structures, and organizational relationships they create. This thesis assesses the existing organizational structures and relationships that form between public and private electric power entities in the United States and their efficacy for ensuring electrical security given high penetration of renewable energy. Despite gaps in the partnership structure and a lack of renewable energy inclusion in federal electrical security policy, this thesis suggests that renewable energy security can be achieved with existing partnership structures. Future partnerships must continue to leverage information sharing, funding, and reform from lessons learned to successfully navigate future security challenges.				
14. SUBJECT TERMS clean energy, public private partnerships, energy security, electrical security, renewable energy, critical infrastructure				15. NUMBER OF PAGES 99
				16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified		18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified		19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified
				20. LIMITATION OF ABSTRACT UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**SECURING RENEWABLE ENERGY THROUGH PUBLIC-PRIVATE
PARTNERSHIPS**

Christian H. Holleman
Lieutenant, United States Navy
BS, U.S. Naval Academy, 2015

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2021**

Approved by: Emily L. Meierding
Advisor

Daniel Eisenberg
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

While the utilization of electricity to support human needs is a staple of modern society, the organizations and legal frameworks underlying the generation, transmission, and distribution of electricity differ across world regions. In the United States, diverse public and private entities are enmeshed throughout the power grid and work to maintain electrical security, i.e., a stable and continuous supply of electricity to customers in the presence of threats. This cooperative relationship appears to be effective given legacy systems and economic structures. However, the incorporation of renewable energy technologies presents a challenge given new system complexity, economic structures, and organizational relationships they create. This thesis assesses the existing organizational structures and relationships that form between public and private electric power entities in the United States and their efficacy for ensuring electrical security given high penetration of renewable energy. Despite gaps in the partnership structure and a lack of renewable energy inclusion in federal electrical security policy, this thesis suggests that renewable energy security can be achieved with existing partnership structures. Future partnerships must continue to leverage information sharing, funding, and reform from lessons learned to successfully navigate future security challenges.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	RESEARCH QUESTION	1
B.	LITERATURE REVIEW	3
	1. Critical Infrastructure in U.S. Government Policy Documents	3
	2. Identifying and Managing Threats to America’s Electrical System	5
	3. Securing Infrastructure through Public-Private Cooperation	7
C.	POTENTIAL EXPLANATIONS AND HYPOTHESES	9
D.	RESEARCH DESIGN	12
E.	THESIS OVERVIEW	13
II.	ELECTRICITY THREATS	15
A.	ELECTRICAL SYSTEM BASICS	15
B.	ELECTRICITY AND ENERGY SECURITY	17
C.	ELECTRICAL SECURITY FAILURES	17
D.	ELECTRICAL SECURITY THREATS	19
	1. Physical Attack.....	19
	2. Cyber Attack	22
	3. Natural Disasters and Weather	25
	4. Aging Infrastructure.....	25
	5. Workforce Capability	27
E.	EFFORTS TO DEFEND AND REMAIN RESILIENT.....	27
F.	CONCLUSION	30
III.	ELECTRICAL PUBLIC-PRIVATE PARTNERSHIPS.....	31
A.	BUSINESS MODELS AND REGULATORY STRUCTURES.....	31
B.	SECURING THE ELECTRICAL SECTOR: ACTORS	36
C.	SECURING THE ELECTRICAL SECTOR: FEDERAL GOVERNMENT POLICY INITIATIVES	38
	1. Presidential Decision Directive 63: Critical Infrastructure Protection (PDD-63).....	39
	2. Executive Order 13636: Improving Critical Infrastructure Cybersecurity (E.O. 13636)	40
	3. Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21)	41
	4. National Infrastructure Protection Plan 2013 (NIPP).....	41

5.	Executive Order 13920: Securing the United States Bulk-Power System (E.O. 13920)	42
D.	PUBLIC-PRIVATE PARTNERSHIPS FOR SECURING THE U.S. ELECTRICAL SYSTEM.....	43
1.	Information Sharing	44
2.	Funding	47
3.	Lessons Learned.....	48
E.	ASSESSMENT	50
F.	CONCLUSION	53
IV.	RENEWABLE ENERGY SECURITY	55
A.	THREAT COMPARISON.....	57
B.	SECURING RENEWABLE ENERGY	61
1.	Public and Private Unilateral Renewable Energy Security Efforts.....	62
2.	Public-Private Renewable Energy Partnerships.....	64
C.	CONCLUSION	70
V.	CONCLUSION	71
A.	THE FUTURE OF PUBLIC-PRIVATE RENEWABLE ENERGY PARTNERSHIPS.....	71
1.	Information Sharing	71
2.	Funding	72
3.	Reform from Lessons Learned	73
B.	CONCLUSION	73
	LIST OF REFERENCES.....	75
	INITIAL DISTRIBUTION LIST	81

LIST OF FIGURES

Figure 1.	Electrical System Basics	16
Figure 2.	U.S. Electrical Power Interconnections	35
Figure 3.	U.S. Electric Power Market ISOs and RTOs	36
Figure 4.	Electrical Security Public-Private Partnerships	43
Figure 5.	Electrical Security Information Cycle	46
Figure 6.	Electrical Security Cooperation	50
Figure 7.	Annual U.S. Electricity Generation by Sector.	57

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Business Models in the U.S. Electrical Sector.....	33
Table 2.	Regulatory Organizations in the U.S. Electrical Sector.....	34
Table 3.	Electrical Security Entities.....	38

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARPA-E	Advanced Research Project Agency-Energy
ASCE	American Society of Civil Engineers
BRIC	Building Resilient Infrastructure & Communities
CEDS	Cybersecurity of Energy Delivery Systems
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CISA	Cybersecurity and Infrastructure Security Agency
CO-OP	Cooperative
DHS	Department of Homeland Security
DOE	Department of Energy
EERE	Office of Energy Efficiency & Renewable Energy
E-ISAC	Electricity Information Sharing and Analysis Center
E.O.	Executive Order
ERCOT	Electric Reliability Council of Texas
ESCC	Electricity Subsector Coordinating Council
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
GCC	Government Coordinating Council
IOU	Investor-Owned Utility
ISO	Independent System Operator
kV	Kilovolt
LPT	Large Power Transformer
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
OE	Office of Electricity
PCII	Protected Critical Infrastructure Information
PDD	Presidential Decision Directive
PPP	Public-Private Partnership
R&D	Research & Development
RTO	Regional Transmission Operator

SCC

Sector Coordinating Council

ACKNOWLEDGMENTS

I would like to sincerely thank Dr. Emily Meierding and Dr. Daniel Eisenberg for their advisement throughout the thesis process. Dr. Meierding, thank you for your guidance and recommendations. Each draft of every chapter improved thanks to your expertise and, more importantly, patience. I have also thoroughly enjoyed the plethora of coursework that I have been able to take under your instruction at NPS. Dr. Eisenberg, you opened my eyes to an interest in critical infrastructure that ultimately led to my selection of electrical security for a thesis topic. Your insights and perspectives led to stronger frameworks and arguments throughout the process.

To Kamile, Beau, Charlotte, and Otis, thank you for your patience and understanding as I locked myself in the upstairs office for countless weekend hours to complete this research. I love you all very much!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

The utilization of electric power is a staple of American society. It is utilized to light our homes and businesses, cook our meals, and fosters our access to avenues of entertainment and socialization. Maintaining the security of the electric system is not a new need. Due to their pervasive nature, power systems have always been vulnerable to disasters and a common target for malicious attacks, both of which can disrupt the flow of electricity and adversely impact communities. Given these threats, public and private entities have been working to maintain the stable and continuous supply of electricity to customers across the nation for years. This cooperative relationship appears to be effective as the United States has not experienced widespread catastrophic failures in the electric system from security failures. However, the incorporation of renewable energy technologies presents an additional layer of complexity within an already challenging problem set. New challenges and intricate complexities will lead this research to explore, what are the roles of public and private entities in securing renewable energy infrastructure?

The research question has several layers that are worth unpacking. First, it is widely acknowledged by the U.S. government and electric power industry that energy security and resilience efforts are a shared responsibility between private industry and government.¹ This prompts questions such as is that partnership effectively managed; does each party adequately contribute; and what is the role of each entity? These are important questions as government and industry have opposing interests that intersect at the crossroads of energy security. Answering these questions requires research into the intersection of electrical security and renewable energy.

Electrical security is a broad concept dealing with managing threats to ensure stable and continuous delivery of electricity to U.S. customers. Analysis conducted by the

¹ Department of Homeland Security and Department of Energy, “Energy Sector-Specific Plan 2015,” 2015, vii.

Department of Homeland Security (DHS) and the Department of Energy (DOE), include cyber and physical security threats; extreme weather conditions and natural disasters; capability reduction within the workforce; aging infrastructure; and changes in the technical and operational environment as the most substantial risks to the energy sector.² Each of these threats is distinctly diverse in its origination as well as the response required to prevent its negative effects upon the United States electrical system. However, the greater concern is the fallout from a major disruption of the nation's power supply. Such an event would affect every critical infrastructure sector and the nation's economy.

Renewable energy encompasses many technologies meant to reduce the use of fossil fuels for electricity production. Historically, the U.S. has relied on fossil fuels like coal, oil, and natural gas for the majority of its power generation. Two key renewable energy technologies disrupting existing systems are wind turbines and solar photovoltaics (i.e., solar panels). However, other new technologies like solar thermal, wave energy, and geothermal power, alongside legacy technologies considered renewable like nuclear and hydroelectric power are also disrupting existing systems. Moreover, there are many power system technologies that enable renewables and lead to new transmission and distribution systems, such as smart grid and control systems that enable household energy production. Overall, renewable energy introduces many novel built and organizational structures to the existing grid that bring new security challenges.

The rapid growth and implementation of renewable energy initiatives further emphasizes a need to understand if existing electric security practices work with renewable energy. The effects of climate change and rising carbon emissions are facilitating persuasive calls for the United States to become increasingly dependent on renewable energy sources. However, there is no standard approach to implementing renewable energy, and there are diverse methods and different business structures utilized in different U.S. regions for energy supply. The implementation of renewable energy within the United States remains in its infancy. Therefore, the research and examination of these issues are timely as the nation prepares for dramatic shifts within our electrical infrastructure.

² Department of Homeland Security and Department of Energy, 5.

B. LITERATURE REVIEW

In the research surrounding this topic there are varying levels of analytical depth and perspective. This literature review will explore three areas of the topic: critical infrastructure in U.S. government policy, threats to critical electrical infrastructure, and securing infrastructure through public-private partnership.

1. Critical Infrastructure in U.S. Government Policy Documents

The USA PATRIOT Act provided the current definition of critical infrastructure used by the United States. It describes critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”³

The first high-level policy guidance on critical infrastructure in the modern era was Presidential Decision Directive 63 (PDD-63) in 1998.⁴ PDD-63 recognized that various infrastructure systems were becoming increasingly critical to the operation of the economy and the U.S. government, it acknowledged the growing interdependence of these systems due to technological advances, and it underlined the importance of a public-private partnership to facilitate cooperation on these issue.⁵

Although there is acknowledgement of critical infrastructure in the USA PATRIOT Act, the next major policy push did not occur until 2013, with Presidential Policy Directive 21 (PDD-21), Executive Order 13636, and the National Infrastructure Protection Plan (NIPP).⁶ These documents outlined sixteen critical infrastructure sectors that continue to be utilized for understanding and organizing security of our nation’s infrastructure. One of these sectors is the energy sector. They also provide a definition of critical infrastructure

³ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. L. No. 107–56 (2001).

⁴ Brian E. Humphreys, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress* (Washington, DC: Congressional Research Service, July 8, 2019), 1.

⁵ William Clinton, *Presidential Decision Directive 63: Critical Infrastructure Protection*, PDD-63 (Washington, DC: The White House, 1998).

⁶ Humphreys, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, 2–3.

resilience that underpins all federal policy on electrical security. Here, resilience is defined as “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.”⁷

Government and private entities of the energy sector worked collectively to produce the sector specific plan in 2015. On the government side, these included the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Government Coordinating Council (GCC), and, the private side, the Electricity Subsector Coordinating Council (ESCC). The GCC and the ESCC are commonly referred to as partnership councils. Each critical infrastructure sector was mandated to produce a sector specific security plan such in the 2013 NIPP. The Energy Sector-Specific Plan attempts to outline energy sector partnerships, goals, and priorities.⁸ Although the cooperation to produce such a plan is positive, the document itself is merely a strategy. It is not representative of the action necessary by the respective actors to increase security of electrical assets.

This review emphasizes that critical infrastructure has become increasingly important to the federal government since the 1990s, yet legislation and policy efforts are far from complete. Research suggests that there are several areas that future critical infrastructure legislation should focus on. These focus areas include information sharing and regulation.⁹ Information sharing is primarily complicated by the number and variety of entities involved. Within the public sphere there are federal, state, and local governments and agencies. This includes the intelligence agencies that are collecting and reproducing information for security purposes. There is also information sharing within the private sector and between the public and private entities. Analysis of the methods and processes of information sharing may provide further insight into the effectiveness of the current public-private partnerships.

⁷ Barack Obama, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*, PPD-21 (Washington, DC: The White House, 2013), <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

⁸ Department of Homeland Security and Department of Energy, “Energy Sector-Specific Plan 2015.”

⁹ John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, CRS Report No. RL30153 (Washington, DC: Congressional Research Service, 2015), 27.

2. Identifying and Managing Threats to America's Electrical System

Threats to the country's electric system are a prominent topic of U.S. government documents and scholarly literature. The PATRIOT ACT recognized that terrorist organizations may target our infrastructure because of the potential damage an attack would likely cause.¹⁰ PDD-63 recognized the vulnerability of a cyber attack.¹¹ The Energy Sector Specific Plan asserts that the key threats are physical attacks, cyber attacks, natural disasters, aging infrastructure, and workforce capability.¹² Each of these examples present a viable threat to American electrical security.

Physical attacks are arguably the easiest threat to conceptualize. A malicious actor desires to destroy physical infrastructure equipment or assets that will harm American interests. The introduction of smart grid and microgrid technologies, while much more efficient, present an increase of vulnerable cyber access points to the electric grid.¹³ Natural disasters and weather events have always been a vulnerability to energy assets. Their unpredictable forces hold the potential to disrupt power systems by damaging or destroying equipment. Moreover, the impacts of climate change are increasing the damage and frequency of disruption within energy systems. The age of our electrical infrastructure is another vulnerability of our electrical system. The majority of transmission and distribution lines in the U.S. have surpassed their recommended fifty-year life expectancy. Additionally, many power lines were not designed to sustain the current levels of electric demand.¹⁴ Similar to electric infrastructure equipment, the base of electric utility workers has become aged. Some estimates state that more than half of these workers will be eligible

¹⁰ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act.

¹¹ Clinton, *Presidential Decision Directive 63: Critical Infrastructure Protection*.

¹² Department of Homeland Security and Department of Energy, "Energy Sector-Specific Plan 2015," 5.

¹³ Thomas F. McLarty et al., *Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid* (Washington, DC: Center for the Study of the Presidency & Congress, 2014), 5.

¹⁴ American Society of Civil Engineers, *Infrastructure Report Card: Energy* (Reston, VA: American Society of Civil Engineers, 2017).

for retirement within the next several years.¹⁵ This could produce massive gaps in the work forces capability and knowledge.

Although they have not had devastating effects, physical attacks against the electric grid have occurred within the past decade.¹⁶ These incidents provide an opportunity for further analysis due to their respective differences in location, means, actor, and motive. The reality of physical attacks upon infrastructure is addressed in various literature. Scholarly work analyzing physical attacks stress the importance of optimization and system redundancies.¹⁷ Other research displays which physical attack mitigation methods are most effective.¹⁸ By understanding where attacks can cause optimal damage and what methods best defend assets, electrical entities can more accurately implement defensive security measures.

The current understanding of primary threats to the electric grid remain applicable in the context of renewable energy. However, the implementation of renewable energy technology will create increased diversity in energy production. This will apply to the technological methods employed for generation and number of private companies managing those assets. Scholars suggest that more diversity of technologies brought by renewable energy will make it more difficult to balance the supply and demand needs of the electric grid.¹⁹ Although renewable energy is largely considered a domestic energy effort without import reliance, some European nations have explored the importation of solar energy from North Africa.²⁰ No literature suggests that the United States would have to explore similar transnational import efforts. However, based on the United States various uses of renewable energy and expansive geographic footprint, it is possible that energy

¹⁵ Department of Homeland Security and Department of Energy, “Energy Sector-Specific Plan 2015,” 18.

¹⁶ McLarty et al., *Securing the U.S. Electrical Grid*, 2014.

¹⁷ Gerald Brown et al., “Defending Critical Infrastructure,” *Interfaces* 36, no. 6 (December 2006): 530–44.

¹⁸ Jenna K. McGrath, “Will Updated Electricity Infrastructure Security Protect the Grid? A Case Study Modeling Electrical Substation Attacks,” *Infrastructures* 3, no. 53 (November 20, 2018): 1–17.

¹⁹ Bengt Johansson, “Security Aspects of Future Renewable Energy Systems-A Short Overview,” *Energy* 61 (2013): 598–605.

²⁰ Johansson, 600.

transportation or transmission of renewable energy may occur between our current energy regions.²¹ The facilitation of such efforts creates another credible risk to the security of renewable energy initiatives within the United States. Additionally, consideration must be given to electric assets being imported. This raises the possibility of device-level attacks, such as built-in backdoors to access control equipment.

3. Securing Infrastructure through Public-Private Cooperation

Policy documents, reports, and scholarly works state that infrastructure security is a cooperative effort between government and the private sector. However, the responsibilities within the relationship are vague. Although the federal government has established means to foster cooperation such as partnership councils and bureaucratic agencies that oversee security efforts, it is often difficult to judge their respective effectiveness. In order to understand the literature of public-private cooperation, I will address what has been written in the context of energy partnerships.

There are countless public-private partnerships that exist between private electric companies and various levels of government. The point of these partnerships is to facilitate cooperation that will bolster electrical security. The manner in which these partnerships do so varies tremendously. This thesis will focus largely on the federal government as the public participant and the effectiveness of information sharing, funding, and reform-based partnerships.

Scholarly work addressing public-private partnerships and renewable energy appears to target community level government as the primary public entity of interest. Some scholars recognize that national government has a role to play, but that it is “often unable or unwilling to address some challenges on their own.”²² This inaction by the federal government increases that importance of local government in the problem set. Additionally, it aligns with the theory that the introduction of renewable energy assets will

²¹ U.S. Department of Energy: Office of Energy Policy and Systems Analysis, *Climate Change and the U.S. Energy Sector: Regional Vulnerabilities and Resilience Solutions* (U.S. Department of Energy: Office of Energy Policy and Systems Analysis, 2015).

²² Avri Eitan et al., “Community-Private Sector Partnerships in Renewable Energy,” *Renewable and Sustainable Energy Reviews* 105 (2019): 95–104.

allow much greater decentralization of our electrical infrastructure.²³ However, other scholars argue that this approach is too dismissive of the federal government. Renewable energy projects experience an entanglement of unavoidable relationships across local, regional, and national divides. Furthermore, it is necessary to have an appropriate combination of top-down policy and bottom-up initiatives to facilitate any large-scale reconfiguration such as renewable energy.²⁴ Although these works are not written explicitly in the context of security, analysis of the relationships discussed remains applicable to the research question.

The U.S. federal government is expending tremendous effort on countering the threat of cyber attacks. The cyber threat is unique in its expanse across numerous infrastructure sectors. Yet, the implementation of smart grid technology and other advancements have increased the relevance of cyber security and its necessary partnerships within the energy sector. Enacted simultaneously with PDD-21 Executive Order 13636 was implemented to reduce cyber vulnerabilities within all U.S. critical infrastructure systems.²⁵ This was followed in 2018 by legislation that created the Cybersecurity and Infrastructure Security Agency (CISA).²⁶ CISA seeks to lead the national effort to defend against cyber attacks. The establishment of CISA demonstrates the commitment that the federal government is directing towards cyber security. Although there does not appear to be a comparable document specifically addressing cyber threats within the electrical sector, Executive Order 13920 seeks to address vulnerabilities of acquiring electrical power assets from foreign entities. The order prevents acquisition of any bulk-power system electric

²³ Eitan et al., 95.

²⁴ Emily Creamer et al., “Community Energy: Entanglements of Community, State, and Private Sector,” *Geography Compass* 12, no. 7 (May 2018): 8–9.

²⁵ Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013), <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

²⁶ Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278 (2018), <https://www.congress.gov/bill/115th-congress/house-bill/3359>.

equipment from any foreign country.²⁷ Written and issued with broad scope, it includes the acquisition of cyber components and software.

However, the establishment of a new bureaucratic agency is unlikely to relieve infrastructure managers of their cyber related woes. Scholars have argued that the flaw in our cyber approach lies within the operation and reliance on public-private partnerships. They argue that the parameters of partnerships are ambiguous. Public and private entities have both been hesitant to exercise authority or responsibility over cyber security.²⁸ Although this argument is presented in the context of cyber security, it is indicative of the other relationships across the public-private divide of the energy sector. Furthermore, it is troublesome as it presents a major national security concern.

Overall, there appears to be a lack of scholarly material that directly analyzes the work of energy partnership councils. As a primary avenue for cooperation between federal government representatives and the private sector, this structure requires more scholarly analysis. Additionally, membership of the electricity subsector coordinating council does not appear to include members who represent renewable energy companies or renewable energy technology producers.²⁹ Although renewable energy assets are in the early stages of implementation, this may be indicative of a lack of inclusion for renewable energy managers and operators in partnership efforts.

C. POTENTIAL EXPLANATIONS AND HYPOTHESES

After initial review of the literature surrounding this research question, it is clear that public and private entities both have a role to play in securing renewable energy infrastructure. However, it is less clear what that role explicitly is for each entity. In this

²⁷ Executive Order 13920: Securing the United States Bulk-Power System (2020), <https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/>.

²⁸ Madeline Carr, “Public-Private Partnerships in National Cyber-Security Strategies,” *International Affairs* 92, no. 1 (2016): 43–62.

²⁹ Electricity Subsector Coordinating Council, “Electricity Subsector Coordinating Council Brochure,” September 2020, https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure.ashx?la=en&hash=00901B6AD252F5AF940C1012619A43C39967F9C9.

thesis, I make two interrelated arguments about public-private relationships in the electricity sector. First, the current structure of public-private governance has created gaps in the United States' energy security. Second, the public private partnership model has failed to account for the inclusion of renewable energy in electrical security policy and priorities.

The current public-private governance structure should not be viewed as a failure. Rather it should be viewed as a structural foundation that has cracks. Although the structure currently remains intact, time and stress could potentially cause this foundation to crumble. There are three cracks in the public-private partnership that create gaps in security. First, the current partnership focuses too much on coordination and collaboration, and not enough on defining responsibility. Although coordination is a vital part of this partnership, there must be an explicit understanding of responsibilities within the relationship. Second, the current partnership structure is voluntary for private entities. This voluntary mindset is applicable to private sector participation and implementation of many security practices. For example, the NIPP repeatedly uses the term “encourage” to describe how the federal government seeks to persuade private entities.³⁰ This language is commonly used within and among many government and private security plans. The federal government must acknowledge that encouragement does not produce the same results as mandates. Third, the current partnership is operated across a plethora of agencies, councils, regions, and organizations. It would be ignorant to believe that an issue as complicated and important as electrical security does not require a vast amount of participation. However, it is possible that efforts conducted across such a wide range of entities enable confusion and inefficiency. Further consolidation of organizations, information sharing avenues, and collaborative efforts may be beneficial to security.

In order to assign responsibility for security threats, there must be an accepted understanding of electrical security. This research views electrical security as the effort to maintain stable electrical delivery to U.S. customers without disruption. However, critical

³⁰ *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Department of Homeland Security, 2013), 1–50.

infrastructure policy acknowledges that a zero-defect mentality is unrealistic. PPD-21 states that resilience efforts allow the U.S. to “recover rapidly from disruptions.”³¹ Security and resilience efforts operate in tandem. Striving to prevent any disruption, while unlikely, is arguably the necessary mindset for electrical security professionals.

Assignment of responsibility does not negate the necessity for collaboration and coordination. Rather it seeks to define who maintains authority over the situation and drives the problem towards solution. This thesis argues that appropriate assignment of responsibility depends on the type of threat that the electricity sector is facing. Specifically, the federal government should exercise authority over any threat that can be labeled an “attack.” The primary examples are physical and cyber attacks. In contrast, threats created by natural disasters and aging infrastructure should be managed by utility owners: usually private entities or local government. Finally, workforce vulnerabilities should remain under the explicit authority of the respective private entity.

Although this thesis assigns primary governmental responsibility for managing many traditional electrical security threats to the federal government, It argues that state and local governments will acquire increased levels of responsibility within the security strategy as a result of the implementation of renewable energy initiatives. Renewable energy and technology advancements, such as microgrids and smart grids, will drive a more localized approach to electricity generation.

Critics of these perspectives may argue that the current public-private governance structure is adequate to manage existing and renewable energy related emerging threats to the electricity sector. These critics may also argue that changes to the governance structure may place undue demand on energy businesses seeking to gain a profit. This thesis will provide evidence that challenges their perspective.

In addition to structural gaps, public and private actors have fallen short of adequately accounting for the inclusion of renewable energy assets in electrical security policy and partnership efforts. Both sides of the partnership are overly reliant on legacy

³¹ Obama, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*.

policies and efforts to address renewable energy security. It appears that this is likely because public and private entities are more concerned with the implementation and operation of renewable energy assets rather than their explicit security.

D. RESEARCH DESIGN

Due to the early stage of renewable energy within the United States, there is minimal research that directly addresses the security of renewable energy initiatives. Therefore, this research must address several related topics that influence the understanding of the research question. This includes critical infrastructure policy, the current public-private governance strategy employed for the electric sector, threats to the electric system, and the implementation and impact of renewable energy to the U.S. electric system. Analysis of these topics will allow a diagnosis of any issues regarding their facilitation. To conduct this diagnosis, the research will incorporate analysis of policy documents, think tank reports, case studies, and scholarly journal articles.

The first portion of this research will explore the prominent threats on the current U.S. electric system. This section will rely heavily on the Energy Sector Specific Plan and think tank reports that address these diverse threats. Additionally, I will provide historical examples of disruptions to the American power grid. These examples are not meant to facilitate lengthy case study analysis, but rather to display their relevance and influence on our understanding of electrical security.

The second portion of the research will explore public-private governance in the electric sector. Critical infrastructure security, to include electricity, has developed over the past three decades due to several major policy initiatives. These initiatives laid the foundation for how public and private entities interact within the electric sector. It is easy to assume that our current management strategy is effective because the United States has not experienced a complete failure of the electric system. The most devastating events have largely been limited to certain regions over several days. Analysis of these policies and the governance structure they created will seek to diagnose any gaps or weaknesses in security coverage.

The third portion of this research will compare conventional electrical security threats with those anticipated with renewable energy. Additionally, this portion will review the applicability of previously reviewed federal policies to the implementation of renewable energy. By analyzing aspects of the current system and what the future system will entail, I will be able to ascertain improvements that public-private partnerships should embrace to secure renewable energy infrastructure. This result will serve as the culmination of this research.

There is a lack of scholarly literature for some aspects of this research. For example, there does not appear to be significant scholarly analysis of the electrical sector partnership councils. However, this literature gap can be overcome through analysis of sources that discuss other aspects of partnership or operation of the electric energy sector. Additionally, even though there does not appear to be much literature explicitly pertaining to the security of renewable energy, there appears to be significant analysis of the implementation of renewable energy.

E. THESIS OVERVIEW

This thesis will include five chapters. Chapter I will serve as an introduction to the research question, literature review, and argument. Chapter II will explore the primary threats to the electrical sector. Chapter III will discuss the public-private partnership that facilitates security, operation, and regulation of the current electric sector. Chapter IV will introduce renewable energy considerations to the research and assess how findings in Chapters II and III will impact renewable energy security. Chapter V will serve as a conclusion to synthesize the findings within this research and provide recommendations to improve public-private partnerships for the inclusion of renewable energy assets.

THIS PAGE INTENTIONALLY LEFT BLANK

II. ELECTRICITY THREATS

This chapter will explore the prominent vulnerabilities of the United States electric system. First, this chapter will provide some basic background knowledge of the electric system and the definition of electrical security utilized during this research. Second, it will provide a brief account of two events that can be considered electrical security failures: the 2003 Northeast Blackout and Hurricane Maria in Puerto Rico. The brief descriptions of these events are intended to demonstrate the scope of damage that can occur during large scale electric outages. Third, this chapter will discuss the five most prominent vulnerabilities to the electric system as recognized by the 2015 Energy Sector-Specific Plan.

A. ELECTRICAL SYSTEM BASICS

The U.S. electric system is operated through a vast network of equipment and organizations. The organizational structure will be further explored in chapter three of this thesis. To understand the vulnerabilities faced by the system, one must have a basic understanding of the equipment and functions within the electrical system. The electric power system is formed by three major functions: generation, transmission, and distribution. Each of these concepts are simple, but they are vital to the production and supply of electrical power.

Electrical generation is performed at a variety of power plant facilities. These facilities differ and are characterized by the energy source that they utilize to generate electricity. Generation plants may use turbines to convert the combustion of fossil fuels such as natural gas or coal into electric power. Additionally, renewable energy technology such as hydroelectric dams, nuclear power, solar panels, and wind turbines serve as generation sources across the country.³²

Following generation, the movement of electricity within the system is controlled by transmission assets. Electric power transmission in the U.S. is largely completed using

³² Union of Concerned Scientists, “How the Electricity Grid Works,” February 17, 2015, <https://www.ucsusa.org/resources/how-electricity-grid-works#.WQeYXFPyuYU>.

alternating current. First, the voltage of generated electricity is increased by a transformer placed between the generation plant and the transmission lines. The utilization of high voltage is necessary because as the electricity is transmitted through the system, resistance will cause portions of the electricity to dissipate as heat. Many generation facilities are not in close proximity to customers. Transmission lines are typically implemented as overhead power lines or underground cables. The transmission portion of the system is the strongest point of redundancy within the electrical system. Transmission lines are interconnected so that reliability is increased across the country.³³

The final function is distribution. Distribution networks facilitate the final stage of electrical delivery to homes or businesses via localized distribution networks. As electricity transitions from transmission to distribution, another transformer will reduce the voltage to an appropriate amount. Distribution networks are constructed of wiring that transports electricity to consumers. Once electricity reaches the consumer it can be utilized for a variety of activities and functions.³⁴ Figure 1 illustrates these processes of the electric power system.

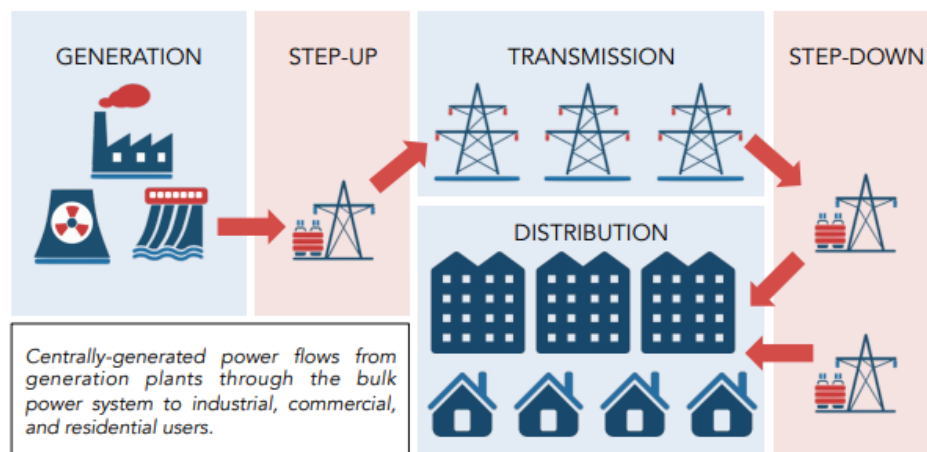


Figure 1. Electrical System Basics³⁵

³³ Union of Concerned Scientists.

³⁴ Union of Concerned Scientists.

³⁵ Source: Thomas F. McLarty et al., "Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid" (Washington, DC.: Center for the Study of the Presidency & Congress, July 2014), 7.

B. ELECTRICITY AND ENERGY SECURITY

As one of the most prominent forms of energy, electricity and its security initiatives can be viewed as a direct subset of energy security. Therefore, the definition of electrical security and associated concepts should reflect this link. The definition of energy security has been debated by scholars without receiving a consensus to its terminology. The definition formulated by Jewell et al. defines energy security as ‘low vulnerability of vital energy systems.’³⁶ Use of the term electrical security in this research reflects the use of this definition with the specific referral to electrical systems. This analysis favors this definition because it allows a level of flexibility and realism.

In addition to flexibility, this definition provides a practical goal for power systems as ‘low vulnerability’. While utilities should strive to provide completely uninterrupted electrical services, the reality is some level of power disruptions on electric grids will continue. That being said, the critical nodes and system components of vital energy systems must remain protected, resilient, and incorporate redundancies.

Understanding electrical security is important because of the criticality of the electric grid on American society. The electric sector serves as the backbone to all other critical infrastructure sectors. This is not to say that the electric sector does not maintain a level of dependence on other sectors to support operations, but that the inherent dependence of other services on electricity increases the importance of uninterrupted operations. A failure of the electric system can quickly result in reduced operation or failure of other systems and sectors.

C. ELECTRICAL SECURITY FAILURES

Prolonged and large-scale losses of electricity are rare in the United States. Two specific instances underline the importance of electrical security efforts: the 2003 Northeast blackout and the loss of Puerto Rico’s power system due to Hurricane Maria. These examples reflect the vulnerabilities that impact the electrical system. However, they are

³⁶ Jessica Jewell, Aleh Cherp, and Keywan Riahi, “Energy Security under De-Carbonization Scenarios: An Assessment Framework and Evaluation under Different Technology and Policy Choices,” *Energy Policy* 65 (2014): 744.

important because they provide a snapshot of the impacts from a loss of the electric system to other threats

In August 2003, a series of cascading system failures resulted in an electrical blackout that affected customers across the Northeast, Midwest, and parts of Canada. Approximately 50 million Americans were affected by the blackout.³⁷ The initial failure was caused by a 345-kV transmission line contacting an overgrown tree. This shifted the electrical load to other transmission lines, but they became overstressed and began to cause power surges at power plants and major interconnections. Electrical failures were experienced in more than 256 power plants and several major cities including New York City, Detroit, Cleveland, Hartford, and Albany. Some areas did not have power restored for four days after the failure occurred.³⁸ This example demonstrates the limitations of the nations outdated electrical infrastructure. Furthermore, it demonstrates the downside of over reliance on interoperability. The inability to isolate the outage resulted in its cascading effect resulting in millions without power.

Some may criticize the inclusion of Puerto Rico in this analysis due to its lack of statehood. I believe that despite the complicated relationship between the U.S. government and the territory of Puerto Rico the analysis conducted remains indicative of many issues plaguing the electrical system of the U.S. mainland. In September 2017, Hurricane Maria made landfall on Puerto Rico as a category 4 hurricane (The storm was only 1 mph less than the windspeed required to be classified as a category 5). The hurricane caused flooding at several power plants, damage to wind turbines, and severe damage to transmission and distribution lines across the island. The damage to the system resulted in many customers remaining without power for more than ten months.³⁹

The prolonged outages on Puerto Rico can be attributed to more than the strength of Hurricane Maria. The hurricane was merely a catalyst for exposing many underlying

³⁷ McLarty et al., *Securing the U.S. Electrical Grid*, 2014, 25.

³⁸ McLarty et al., 25–26.

³⁹ Alexis Kwasinski et al., “Hurricane Maria Effects on Puerto Rico Electric Power Infrastructure,” *IEEE Power and Energy Technology Systems Journal* 6, no. 1 (February 19, 2019): 85–94.

issues within the island's electric infrastructure. For example, only 15% of transmission lines were constructed or implemented to the necessary specifications allowing them to endure the forces of a category 4 hurricane.⁴⁰ As a frequent victim of major hurricanes, it is startling that the Puerto Rican electric sector and governmental leadership would allow themselves to remain susceptible to a threat that is overwhelmingly probable. These types of operational and management decisions over decades resulted in a lowered level of resilience for Puerto Rico's electrical system leading up to Hurricane Maria.

The brief description of these two events barely scratches the surface of explaining what happened during these outages. Their inclusion is intended to demonstrate the fallout of major electrical outages that have occurred within U.S. jurisdictions. The concept of 50 million Americans losing power is startling. Furthermore, the idea that American citizens could remain without power for more than ten months is arguably unbelievable. These types of large scale and prolonged outages can quickly inhibit public health, safety, security, telecommunication and economic interests. These two specific incidents can be primarily attributed to insufficient or outdated infrastructure baring the effects of natural weather occurrences. Although these issues remain major vulnerabilities to the electric grid, it is plausible that the vulnerability of a targeted attack could be even more damaging to the system and the nation.

The next portion of this chapter will explore the most prominent risks to U.S. electrical security as outlined by government and industry officials alike in the 2015 Energy Sector-Specific Plan. Many of these risks have already damaged the grid to some degree in various cases. After outlining each risk, I will describe historical examples of how these risks have caused negative effects on the electrical system or been exploited by adversaries.

D. ELECTRICAL SECURITY THREATS

1. Physical Attack

More than any other vulnerability, physical attacks are the easiest to conceptualize within our understanding of electrical security. The American psyche has been forced to

⁴⁰ Kwasinski et al.

believe since September 11 that terrorists using force against American interests are one of the biggest risks to our security and well-being. It is undeterminable whether this statement is true. However, physical attacks against the electrical system by nefarious actors remain a plausible threat.

Electricity networks are complex systems that cover vast geographic areas via various physical equipment. Furthermore, portions of the systems frequently operate within and serve multiple governmental jurisdictions. For example, transmission lines often cross multiple state boundaries or utilities may support multiple counties within a region, without the county in its entirety being covered by the same utility.

Physical attacks may include targeting generation facilities, transformers, transmission lines or other system components. Destruction of any physical components within the system will result in some level of disruption of redundancy within the system. The large geographic footprint of the system makes security efforts across the entirety of the system difficult. The manpower required to provide surveillance across the miles of system equipment is unrealistic. Therefore, security efforts and personnel are primarily concentrated at nodes within the system.

These vital nodes include equipment such as Large Power Transformers (LPTs) that frequently facilitate the increase and decrease of voltage across the grid. LPTs allow for the necessary change in voltage as electricity travels through the system. The loss of an LPT could potentially result in large electrical disruptions downstream in the system. To further complicate the issue, the U.S. has strongly relied on overseas manufacturers to supply LPTs. The complexity of the LPT procurement process frequently causes these overseas manufacturers to take more than a year to provide replacements.⁴¹ There are some cases which the time to replace an LPT has been more than twenty months.⁴² This has

⁴¹ Department of Homeland Security and Department of Energy, “Energy Sector-Specific Plan 2015,” 16.

⁴² U.S. Department of Energy: Office of Electricity Delivery and Energy Reliability, *Large Power Transformers and the U.S. Electric Grid* (U.S. Department of Energy: Office of Electricity Delivery and Energy Reliability, 2012), v, https://www.energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.

resulted in efforts to stockpile replacement transformers. However, experts have in turn raised concern about the security of storage facilities that maintain this stockpiled equipment.⁴³

There are two prominent examples of physical attacks occurring against U.S. electrical system assets: the Metcalf substation attack and a series of attacks on Entergy facilities in Arkansas. Physical attacks can occur through a variety of means and actors. These two examples provide a diverse sampling of both those factors.

In the first example, in 2013 a group of individuals attacked the Metcalf Substation in San Jose, California. Prior to the attack, the attackers severed the fiber-optic phone lines at the facility. This disrupted communication services with customers and made it more difficult for on-site personnel to notify emergency services. The attackers proceeded to use assault rifles to fire at transformers from outside a chain-link fence.⁴⁴ The bullet holes caused thousands of gallons of oil to leak from the transformers. As the transformers lost oil, they began to overheat resulting in a total of 17 transformers being disabled. Due to the attack occurring during a period of low demand, utility workers were able to reroute power and prevent a blackout.⁴⁵ Unfortunately, the substation was unable to return to normal operation for 27 days as the transformers were repaired and replaced as necessary. The Federal Bureau of Investigation (FBI) has been unable to determine who was responsible for the attack.⁴⁶

The second notable example is a series of three physical attacks that occurred in Lonoke County, Arkansas against Entergy Arkansas assets. Interestingly, these attacks occurred within several months of the Metcalf Substation attack. During the first attack, the perpetrator forcefully entered an area securing a 500 kV electrical line, then removed nearly all of the bolts from the line's support tower. The tower proceeded to fall on a nearby

⁴³ McLarty et al., *Securing the U.S. Electrical Grid*, 2014, 9.

⁴⁴ McLarty et al., 27.

⁴⁵ Evan Halper and Marc Lifsher, "Attack on Electric Grid Raises Alarm," *Los Angeles Times*, February 6, 2014, <https://www.latimes.com/business/la-fi-grid-terror-20140207-story.html#axzz2t2mkWwrd>.

⁴⁶ McLarty et al., *Securing the U.S. Electrical Grid*, 2014, 27–28.

railroad track where multiple power lines later became severed by a transiting train. The severed lines caused the town of Cabot, Arkansas to lose power. A second attack occurred about a month later at an Entergy station when a fire was intentionally set resulting in approximately \$2 million in damages. In the final attack, the perpetrator damaged a power pole and proceeded to pull it down with a tractor. The attack caused damage to a 115 kV transmission line and resulted in electrical outages for more than 9,000 customers. The FBI arrested a lone actor, Jason Woodring, for the attacks. The authorities determined that Woodring did not have ties with a larger terrorist organization.⁴⁷

There are several differences between the attacks, which display the varying methods that could be used for physical attacks. The Metcalf incident was carried out by a group utilizing small arms against a manned facility. The specificity of targeting the transformer oil tanks and the foresight to remove emergency communication methods suggests a high level of planning and sophistication for the attack. In contrast, the series of attacks in Arkansas were carried out by a lone actor utilizing multiple methods against various unmanned electrical system components. While the perpetrator certainly planned to some degree, it is clear that his goals were focused much more on ease of access.

2. Cyber Attack

The threat of cyber attacks has grown within the energy sector and more broadly with U.S. interests. One can even argue that the modern political push for protection of critical infrastructure is as much based in the protection of cyber systems as it is physical structures. Presidential Decision Directive 63, released in 1998, clearly discusses how American interests are increasingly reliant upon cyber-based information systems.⁴⁸ Time and further technological advances have made this assertion even more of a reality.

There are several reasons why cyber attacks are of such great concern. The field of cyber security is constantly evolving. As officials rapidly work to implement protections, new vulnerabilities are created and discovered just as quickly. Additionally, the nature of

⁴⁷ McLarty et al., 29–30.

⁴⁸ Clinton, *Presidential Decision Directive 63: Critical Infrastructure Protection*.

the cyber threat allows nefarious actors to be located anywhere around the globe. The risk of being physically present to commit an attack is removed from the equation.

Although there is evidence of malware intrusions by sophisticated adversaries, the United States has yet to experience a significant cyber attack against the electric grid.⁴⁹ However, cyber attacks against the Ukrainian electric grid and cyber intrusions into American water facilities offer comparable case studies for what future attacks will likely target.

In December 2015, hackers began to target the control systems of the Ukrainian power grid in the Ivano-Frankivsk region. The attack was coordinated against the systems at three different distribution centers. By remotely opening dozens of circuit breakers, numerous substations were taken offline and more than 230,000 residents were left without power to endure the winter temperatures. Workers at the distribution centers were helpless to stop the attack even as they noticed the perpetrators controlling the computer cursor. Furthermore, operators at two of the distribution centers were without power because the hackers disabled the backup power supplies.⁵⁰

Officials involved in the investigation of the attack suggest that the operation took place over several months as the hackers studied the network setup based on reconnaissance efforts and gradually gained access to operator credentials. Due to political tensions, Ukraine attributes the attack to Russia. However, investigators suggest that multiple actors collaborated to conduct the attack. It is possible that a team of cybercriminals gained access to the network prior to transitioning the rest of operation to nation-state actors.⁵¹

The method of the attack against the Florida water facility is extremely similar to the attack in Ukraine. They both began when an operator noticed the systems computer cursor began to take distinct actions to alter the normal operation of the system. In the

⁴⁹ McLarty et al., *Securing the U.S. Electrical Grid*, 2014, 25.

⁵⁰ Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016.

⁵¹ Zetter.

Florida incident, the hacker increased the level of sodium hydroxide in the water by a factor of 100. Fortunately, the local operator was able to correct the sodium hydroxide levels before it left the facility for distribution.⁵²

The Ukraine attack is the first confirmed attack to incapacitate an electrical grid.⁵³ This case presents itself as an example of the damage that an effective cyber attack can do. However, the damage could have been much worse. The circuit breakers that were altered by the hackers are designed to function manually as a backup. This functionality is the primary reason the Ukrainian grid was restored within several hours after the attack. Experts have directly commented that this type of backup operation is absent from many American grid control systems.⁵⁴ This means that attempts to restore power following an attack would be prolonged and experience increased difficulty.

The attack on the Florida water facility is notable two reasons. First, it occurred against an American facility. Second, the attack further demonstrates the possibility and probability of cyber vulnerabilities to exercise nefarious intentions. The fact that the American attack was against a water facility rather than an electrical facility does not make a significant difference. By briefly analyzing the Ukrainian and the Florida attack in parallel, the use of control systems in both instances should be a blinking red light for security specialists, operators, owners, and government officials alike.

Of the electrical vulnerabilities this chapter will discuss, physical and cyber attacks are the only ones that are carried out by actors who intend to inflict harm upon United States interests. Whether they are committed by state, non-state, international, or domestic groups, or by lone actors, these types of attacks will have a direct human element involved. This means that there should be a reasonable expectation of sophistication and planning involved to exploit known and unknown weaknesses in our systems and operations.

⁵² Bill Chappell, “FBI Called In after Hacker Tries to Poison Tampa-Area City’s Water with Lye,” *NPR*, February 9, 2021, <https://www.npr.org/2021/02/09/965791252/fbi-called-in-after-hacker-tries-to-poison-tampa-area-citys-water-with-lye>.

⁵³ Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.”

⁵⁴ Zetter.

It is possible that this sophistication could be applied to a coordinated attack that combines physical and cyber elements. Consider the Ukrainian example. If the manual backup circuit breaker switches or other vital equipment and structures were targeted while a cyber attack was occurring the damaging effects would certainly increase. It is almost assured that this type of attack would prolong electrical outages and disrupt response efforts.

3. Natural Disasters and Weather

Historically, weather events are the greatest threat to electric infrastructure.⁵⁵ Their effects can range from minor disruptions in a single neighborhood due to a fallen tree on a distribution line to multi-state regions experiencing disruptions and outages due to severe snow and ice, wind and rain storms, or hurricanes. The inherent variety and variability of weather threats make them an incredibly difficult problem set. Additionally, climate change is exacerbating this issue by causing more frequent and severe episodes of extreme weather. These events commonly cause damage to equipment and facilities, large shifts in electricity supply and demand, and disruption of operations and supply chains.⁵⁶ Earlier in this chapter, I briefly discussed that impact of Hurricane Maria. There is no shortage of weather and natural disaster examples that display the impact these events can have. The fact is that weather will continue to be a major vulnerability for maintaining electrical security.

4. Aging Infrastructure

The majority of the United States electric system was constructed in the 1950s and 1960s, particularly transmission and distribution lines. This equipment has surpassed its designed 50-year life expectancy. Additionally, most transmission lines are operating at full capacity.⁵⁷ The demands on aging infrastructure working at its operational limits are

⁵⁵ Department of Homeland Security and Department of Energy, “Energy Sector-Specific Plan 2015,” 16.

⁵⁶ U.S. Department of Energy: Office of Energy Policy and Systems Analysis, *Climate Change and the U.S. Energy Sector: Regional Vulnerabilities and Resilience Solutions*, 1–1.

⁵⁷ American Society of Civil Engineers, *Infrastructure Report Card*, 1–2.

colliding with the implementation of technological advances that are changing how the grid is operating. This includes the increased incorporation of renewable energy and the implementation of smart grid and microgrid technology.

Regardless of how the grid is changing, ageing of electricity infrastructure increases the risk of disruption to customers. Most experts agree that the solution is continued monetary investment to maintain, update, and adapt the nations electric infrastructure as appropriate. However, the electric power industry already invests tens of billions of dollars each year for such initiatives.⁵⁸ Organizations such as the American Society of Civil Engineers (ASCE) state that it is still not enough. The ASCE estimates there will be a \$208 billion investment shortfall by 2029 to ensure a reliable electrical system.⁵⁹

Still, the implication of ageing infrastructure is difficult to quantify. When power outages occur, officials are unlikely to state that they were caused by a component that is outdated or beyond its intended operational life, they commonly communicate what component failed, but not why. This allows officials to acknowledge that they know what component broke without admitting an explanation that would foster bad publicity. Considering the general age of our systems, in combination with the known strain on the grid, it is reasonable to assume that aging infrastructure is at least a contributing factor in many outages. For example, in July 2019, approximately 39,000 customers lost power in the District of Columbia due to an issue at a single substation.⁶⁰ During the outage, traffic lights and the Metro were impacted, restricting transportation. Numerous people became trapped in elevators, requiring the response of firefighters, and the capability to conduct business screeched to halt as shops had no means of completing electronic transactions.⁶¹ Aging electrical infrastructure, specifically outdated substations, is one aspect being

⁵⁸ Department of Homeland Security and Department of Energy, “Energy Sector-Specific Plan 2015,” 17–18.

⁵⁹ American Society of Civil Engineers, *Failure to Act: Electrical Infrastructure Investment Gaps in a Rapidly Changing Environment* (American Society of Civil Engineers, 2020), 3.

⁶⁰ Cortlynn Stark, “Power Restored after Outage Affected 39,000 in Northwest DC on Saturday,” *The Washington Post*, July 28, 2019, https://www.washingtonpost.com/local/dc-politics/2019/07/27/7b6c43cc-b0a3-11e9-a0c9-6d2d7818f3da_story.html.

⁶¹ Neil Vigdor, “Washington, DC Power Failure Affects More Than 30,000 Customers,” *The New York Times*, July 27, 2019, <https://www.nytimes.com/2019/07/27/us/dc-power-outage.html>.

addressed by the Capital Grid project. The project is ushering equipment upgrades at several substations across the District.⁶² Although the issue of aged infrastructure is known, until it is corrected it poses a risk of causes outages for customers.

Occurrences such as this demonstrate two imperatives for our aging electric infrastructure. First, reliability issues must be acknowledged. Second, the concentration of electricity dependency within the system must be minimized. It is very problematic that 39,000 people should be affected by a single equipment failure.

5. Workforce Capability

The Energy Sector Specific Plan recognizes that workforce development is a major vulnerability for the electrical sector. Specifically, the industry has experienced an increased gap in available skilled labor as older workers are retiring from the workforce.⁶³ As these older workers commence their retirements, years of knowledge and expertise is removed from the industry and these are not being adequately replenished.

Electrical managers and the Department of Energy are working to address this issue via various training programs and recruitment methods.⁶⁴ Additionally, President Biden has expressed that the U.S. transition to clean energy will seek to create more than 10 million well-paying jobs.⁶⁵ Time will tell whether industry and government initiatives will be able to close the labor gap within the electrical sector. If this issue is not addressed, customers are more likely to experienced prolonged outages.

E. EFFORTS TO DEFEND AND REMAIN RESILIENT

Each of these vulnerabilities presents a unique challenge. Furthermore, these vulnerabilities are not all-inclusive. These five areas discussed simply represent the areas

⁶² Potomac Electric Power Company, “The Capital Grid Project: Overview,” October 2019, https://www.pepco.com/MyAccount/MyBillUsage/Documents/CAPITAL%20GRID%20PROJECT%20OVERVIEW%20FACT%20SHEET%20ENG%20-%20OCT%202019_NP%20final.pdf.

⁶³ Department of Homeland Security and Department of Energy, “Energy Sector-Specific Plan 2015,” 18.

⁶⁴ Department of Homeland Security and Department of Energy, 18.

⁶⁵ joebiden.com, “Climate: 10 Million Clean Energy Jobs,” joebiden.com, February 20, 2021, <https://joebiden.com/climate-labor-fact-sheet/>.

that industry and government officials agree are the most likely to create a negative impact on electrical security.

In recent years, those involved in the critical infrastructure field have embraced the idea of resilience, to minimize some of these vulnerabilities. For example, Presidential Policy Directive-Critical Infrastructure Security and Resilience (PPD-21) appears to be the first policy directive to address the concept of resilience. The document states, “critical infrastructure must be secure and able to withstand and rapidly recover from all hazards.”⁶⁶ This singular quote from PPD-21 addresses several aspects of resilience as addressed by scholars. Prominent scholars such as Woods have contended that there are four aspects of resilience that must be addressed concerning critical infrastructure such as the electrical system: resilience as rebound, resilience as robustness, resilience as extensibility, and resilience as adaptability.⁶⁷

First, resilience as rebound is the ability of a system to return to normal operation.⁶⁸ So, for the electrical system, this means how quickly outages and disruptions can be ended. Every outage is different, but there are several areas where officials can concentrate their efforts to increase resilience as rebound. Despite the cause, every outage is likely to require personnel and replacement equipment. With more trained workers available, they can quickly be dispatched to correct system damages. During severe weather, many utilities will do this by partnering with other companies in nearby locations and sharing repair crews as necessary. Regarding equipment, maintaining and managing stockpiles is vital. If necessary equipment is not on hand, repairs can be delayed by days or even weeks as items work their way through difficult supply chains. An inability to quickly make repairs directly hampers the system’s ability to rebound.

Second, resilience as robustness is a system’s ability to absorb attempted perturbations and continue to operate without disruption.⁶⁹ This concept is primarily

⁶⁶ Obama, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*.

⁶⁷ David D. Woods, “Four Concepts for Resilience and the Implications for the Future of Resilience Engineering,” *Reliability Engineering and System Safety*, April 3, 2015, 5–9.

⁶⁸ Woods, 6.

⁶⁹ Woods, 6–7.

enacted through the design phase of a system. For example, consider a network of above ground poles for power lines that are located in an area that frequently experiences severe winds during the annual hurricane season. Recognizing this, planners would benefit from installing poles that are specifically engineered to withstand high wind forces from severe hurricanes. On the surface this appears simple. However, it is likely that this type of power pole is more expensive to implement. Therefore, budget constraints or other competing interests may deter decision makers from installing the power poles that are more likely to endure weather conditions that the area will likely experience at some point in time.

Third, resilience as extensibility refers to a system's ability to maintain capacity in the event of a surprise event.⁷⁰ Similar to resilience as robustness, extensibility is enacted within a system prior to a possible vulnerability being exploited. A system can enact extensibility by ensuring there are redundancies within the system. Redundancies ensure the system does not collapse due to a singular point of failure. The electrical system attempts to do this with transmission networks. Ideally, if a transmission line goes down, another portion of the system picks up the slack. Unfortunately, not every network has this redundancy or lines can become overloaded as they did during the 2003 Northeast Blackout.

Fourth, resilience as adaptability is the ability to manage new system capacities following system disruptions.⁷¹ This concept is commonly experienced with the willingness to implement emerging technology to combat system disruptions. For example, the implementation of microgrid technology can enable portions of the grid to isolate and continue to operate even if a larger system is experiencing a disruption. Therefore, if a disruption happens to the system, the scope of its effects are limited. However, microgrids are a relatively new, expensive, and complicated system that need to be proven in more contexts before wider adoption is possible. Adaptability in the current power grid would be its capacity to incorporate microgrids despite these challenges.

⁷⁰ Woods, 7.

⁷¹ Woods, 8.

F. CONCLUSION

This chapter has discussed the leading vulnerabilities to the U.S. electric system. It is clear that the vulnerabilities presented are extremely diverse. Attacks committed by physical or cyber actors present themselves as more traditional security concerns. In recent decades, Americans have accepted the fact that there are individuals, internationally and domestically, who want to negatively impact our interests. Severe weather will continue to be a major vulnerability for our electrical system. The inherent variability of the type, scale, and severity of storms and other weather conditions is a complicated challenge. Unfortunately, the effects of climate change appear to be increasing the damage inflicted during weather events. Although there is significant investment to address the nation's aged electrical infrastructure, there is concern that it will fall short of what is required to maintain a reliable system. Finally, there are major concerns about the health of the workforce that operates, maintains, and manages our electrical infrastructure. If not corrected, this shortfall of expertise and experience may result in equipment damages, prolonged outages, and other negative impacts against electrical security.

It is interesting that all these vulnerabilities have been recognized as the prominent vulnerabilities for several decades. As PDD-63 began the push to secure the nation's critical infrastructure, each of these vulnerabilities was specifically mentioned.⁷² The discussion throughout this chapter provides evidence that several of these vulnerabilities have disrupted operation of the U.S. electric grid since their recognition. Overall, it appears that the U.S. has been able to minimize the frequency of large-scale electrical outages to few, salient events. However, that does not mean the current system cannot be improved to reduce its vulnerability given future operational and technological needs.

⁷² Clinton, *Presidential Decision Directive 63: Critical Infrastructure Protection*, 2.

III. ELECTRICAL PUBLIC-PRIVATE PARTNERSHIPS

Electrical security partnership that exists between government and business are a collaborative effort. However, these entities have opposing interests and goals. Government is foundationally responsible for providing security and stability to its citizens. The purpose of business is to earn a profit. However, to be profitable, businesses must protect their assets. Within this dynamic there is plenty of gray area to describe where the responsibilities of each entity should begin and end with respect to electrical security. This analysis will explore whether the current electrical security public-private partnership structure has gaps that negatively impact security.

This chapter will initially provide a foundational overview of common business models and regulatory structures in the U.S. electrical sector. Next, I will identify prominent government and private actors that contribute to securing the United States' electric supply, as well as federal policy initiatives that have sought to enhance electrical security since the late 1990s. I will then discuss the current state of public-private partnerships by evaluating information sharing efforts, funding, and the ability to implement lessons learned. Finally, I offer that further consideration should be given to the complexity of electrical organizational structures and the dependence on private entities to voluntarily participate in security structures and implement security relevant guidance.

A. BUSINESS MODELS AND REGULATORY STRUCTURES

The core operations of the electric grid are creating and managing the supply of electricity to consumers. These systems include entities that are responsible for power generation, transmission, and distribution. There are numerous business models utilized within the American electrical grid, with varying authority structures. For example, one entity may control the entire electrical supply process, from generation to distribution. Alternatively, an entity may contribute to merely a single portion, such as the generation of electricity at a power plant. This section briefly explores some of the most prominent operational models, regulatory organizations, and transmission structures. Table 1 summarizes these business models with a brief description.

Electric power that is supplied by private entities will typically be managed by a for-profit utility, owned by shareholders; these are frequently referred to as investor-owned utilities (IOUs). IOUs have service territories that are granted by licenses from their respective state commissions. It is also possible for these utilities to provide services in multiple states.⁷³ IOUs tend to have some degree of vertical organization to supply power within an authorized geographic region. However, in an alternative operational model, private entities known as independent power producers contribute to electricity generation. These independent power producers generate electricity from their assets, then sell it to other utilities or directly to consumers.⁷⁴

Although the majority of electrical infrastructure is owned and operated by private entities, there are instances where federal, state or local government oversees grid operations.⁷⁵ Federal power programs, such as the Tennessee Valley Authority or the Bonneville Power Administration, are wholesale power entities that provide electrical service functions to smaller-scale local utilities. These programs operate as government-owned corporations that own generation and transmission facilities and carry out operations.⁷⁶ In another government-controlled models, cities and counties can own not-for-profit public power utilities. These are commonly referred to as municipals or munis. In addition to owning these utilities, the local governments regulate rather than federal or state authorities.⁷⁷ An additional not-for-profit model utilized in the U.S. is cooperatives (Co-ops). Co-ops are owned by their members who elect representatives to oversee operations. Excess revenue is returned and distributed among Co-op members. This model is typically utilized in rural areas that are not served by other utilities.⁷⁸

⁷³ Matthew Gilstrap, Shravan Amin, and Kevin DeCorla-Souza, *United States Electricity Industry Primer*, DOE/OE-0017 (U.S. Department of Energy: Office of Electricity Delivery and Energy Reliability, 2015), 27, <https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf>.

⁷⁴ Gilstrap, Amin, and DeCorla-Souza, 28.

⁷⁵ Department of Homeland Security and Department of Energy, “Energy Sector-Specific Plan 2015,” vii.

⁷⁶ Gilstrap, Amin, and DeCorla-Souza, *United States Electricity Industry Primer*, 28.

⁷⁷ Gilstrap, Amin, and DeCorla-Souza, 27.

⁷⁸ Gilstrap, Amin, and DeCorla-Souza, 27.

Table 1. Business Models in the U.S. Electrical Sector

Business Model	Description
IOU (Investor-Owned Utility)	Private entity that is shareholder controlled. Profit oriented.
IPP (Independent Power Producer)	Private entity focused explicitly on electrical generation.
Government Controlled	Federal: Typically, government owned corporations with range of services (Ex: Tennessee Valley Authority). Supports smaller utilities in geographic region.
	Local: Typically, not-for-profit operation.
Cooperative (Co-op)	Owned by members. Managed by elected representatives. Common in rural areas.

Utilities are the primary player involved in electrical operations. However, their operational environment is shaped by regulatory organizations. Just as there are federal, state, and local levels of ownership and operations, electrical regulation is conducted at various levels of scope and authority (see Table 2). The two federal-level organizations involved in regulation of the electrical grid are the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC). FERC operates as an independent agency within the DOE to oversee the interstate transmission of electricity and other regulatory matters. FERC does not regulate retail electricity sales, activities of nuclear power plants, or approve construction of electrical generation assets.⁷⁹ In 2006, FERC designated NERC with the authority to regulate and oversee the electrical market to meet designated reliability standards. Some of NERC's responsibilities include the development and enforcement of reliability standards; assessing long-term reliability; monitoring the bulk power system; and the education, training, and certification of electrical industry personnel.⁸⁰ Due to the U.S. and Canada sharing large portions of the North American bulk power system, FERC and NERC have very close ties.

⁷⁹ Gilstrap, Amin, and DeCorla-Souza, 24.

⁸⁰ Gilstrap, Amin, and DeCorla-Souza, 25.

State and local regulatory agencies and commissions also have a vital role to play in regulation and oversight of electrical assets. Although their scope of authority varies, lower-level regulation typically addresses issues such as facility inspections, electrical asset maintenance, and concerns such as vegetation management within service areas.⁸¹ Additionally, commissions may regulate profits which in turn impacts utility budgets and planning capabilities.

Table 2. Regulatory Organizations in the U.S. Electrical Sector

Entity	Focus
FERC	Independent agency within DOE. Large focus on regulation of electrical transmission.
NERC	Designated by FERC to regulate electrical reliability standards.
State/Local	Address concerns such as inspections, maintenance, and vegetation management of local assets.

In addition to being shaped by business models and regulatory structures, U.S. electrical sector operations are dictated by the physical structure of the grid in different areas. In some areas, localized grid networks are connected to create larger networks that increase reliability and redundancy. The largest of these networks are referred to as interconnections. Interconnections have limited power transfers between them as they are meant to operate autonomously from one another. The electric grid of the continental United States has three interconnections: the Eastern Interconnection, the Western Interconnection, and the Electric Reliability Council of Texas (ERCOT) that covers most of Texas.⁸² Figure 2 illustrates the boundaries of these three interconnections.

⁸¹ Gilstrap, Amin, and DeCorla-Souza, 27.

⁸² Sara Hoff, "U.S. Electric System Is Made up of Interconnections and Balancing Authorities," Energy Information Agency, July 20, 2016, <https://www.eia.gov/todayinenergy/detail.php?id=27152>.

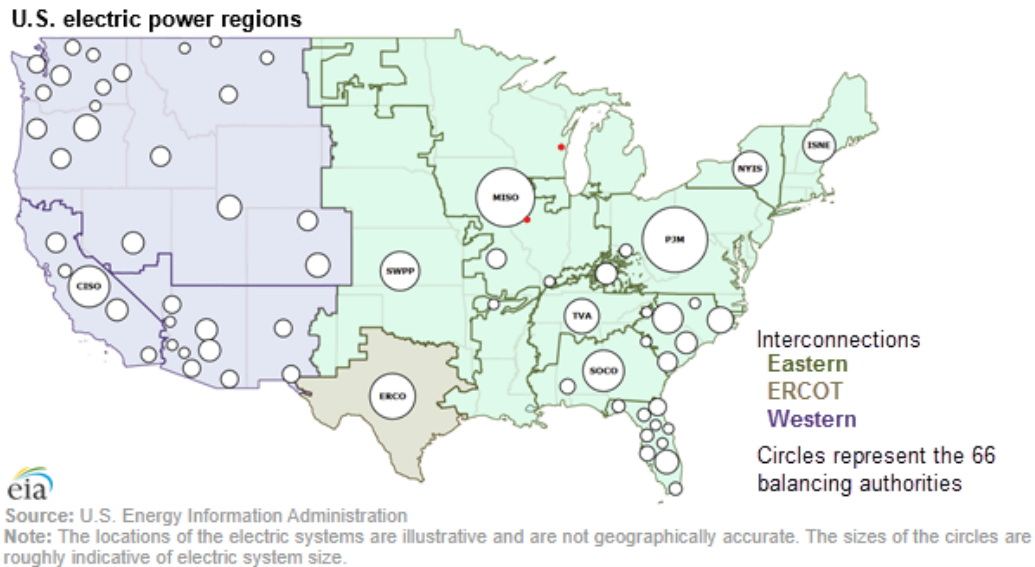


Figure 2. U.S. Electrical Power Interconnections⁸³

Within the Eastern and Western Interconnections there are several regionally associated markets that are managed by Independent System Operators (ISOs) or Regional Transmission Organizations (RTOs). Figure 3 illustrates the locations of ISOs and RTOs across the U.S. The terms ISO and RTO are largely synonymous. These groups operate the transmission system and manage equitable competition amongst electricity providers in horizontally integrated markets where generation, transmission, distribution, and customers can be managed by separate entities. In contrast, other regions have vertically integrated markets where a single organization owns and operates assets across all across all network scales from generation to customer. These regions do not necessarily have RSO or RTO entities.⁸⁴ Moreover, some vertically integrated power utilities also act as an ISO due to their large market region, such as PJM in the Eastern Interconnection.

Both regions with and without ISOs and RTOs are comprised of a group of balancing authorities who ensure safe system operation. Typically, a large-scale electric

⁸³ Source: Hoff.

⁸⁴ Federal Energy Regulatory Commission, "Electric Power Markets," Federal Energy Regulatory Commission, October 23, 2020, <https://www.ferc.gov/industries-data/market-assessments/electric-power-markets>.

utility acts as a balancing authority to manage the balance between supply and demand of its assets and connected regions. This is done by ensuring that electrical demand does not exceed the supply of electricity to the grid and that generation dispatch is capable to reach customers through transmission and distribution networks without exceeding operational thresholds. When this balance is not correctly managed, blackouts can occur at various scales across the grid. When necessary, balancing authorities will conduct electricity transfers between each other to guarantee adequate supply.⁸⁵ Some entities hold multiple roles with this operational structure. For example, ERCOT acts as its own interconnection, ISO, and balancing authority.⁸⁶



Figure 3. U.S. Electric Power Market ISOs and RTOs⁸⁷

B. SECURING THE ELECTRICAL SECTOR: ACTORS

A wide variety of actors share responsibility for security of the U.S. electrical grid (Table 3). As the sector-specific agency for energy infrastructure, the Department of Energy (DOE) is the primary federal department responsible for electrical security matters.

⁸⁵ Hoff, “U.S. Electric System Is Made up of Interconnections and Balancing Authorities.”

⁸⁶ Federal Energy Regulatory Commission, “Electric Power Markets.”

⁸⁷ Source: Federal Energy Regulatory Commission.

Although the DOE's mission acknowledges that it will address energy challenges such as security, the department priorities are much more expansive than security matters. Reflecting this plethora of government priorities, security responsibilities are distributed across program offices within the DOE. The Office of Electricity (OE) and the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) are the primary players.⁸⁸ The DOE also contributes to innovation efforts and broader energy policy initiatives.⁸⁹ Program offices such as the Office of Energy Efficiency & Renewable Energy (EERE) and Advanced Research Projects Agency-Energy (ARPA-E) are heavily involved in such efforts.⁹⁰ The Department of Homeland Security (DHS) is also engaged in electrical security, as DHS is involved in any issue that can be painted as a security matter. The recently established Cybersecurity & Infrastructure Security Agency (CISA) would be a logical entity to address many of the issues that affect infrastructure security and, more specifically, electrical grid security.⁹¹ However, it appears that CISA will not be the lead for matters of electrical security. Instead, CISA will take the reins as the sector-specific agency for critical infrastructure sectors that were previously assigned to DHS.⁹²

In addition to these two major players at the federal level, there are other federal organizations that contribute, such as the Federal Bureau of Investigation. Additionally, state and local governments make important, although different contributions to providing electrical security. State governments do not typically support equivalent entities to the federal governments sprawling security apparatus, but instead they impact electrical security through a combination of legislation and regulatory initiatives.⁹³

⁸⁸ "Offices," Department of Energy, accessed July 18, 2021, <https://www.energy.gov/offices>.

⁸⁹ Department of Energy, "Mission: Department of Energy," Department of Energy, accessed May 5, 2021, <https://www.energy.gov/mission>.

⁹⁰ Department of Energy, "Offices."

⁹¹ Cybersecurity and Infrastructure Security Agency Act of 2018.

⁹² Cybersecurity & Infrastructure Security Agency, "Cybersecurity & Infrastructure Security Agency Services Catalog" (Cybersecurity & Infrastructure Security Agency, Autumn 2020), 15, https://www.cisa.gov/sites/default/files/publications/FINAL_CISA%20Services%20Catalog%20v1.1_20201029_508_0.pdf.

⁹³ J. Phillips et al., "State Energy Resilience Framework" (Argonne National Laboratory, December 2016), 7.

Although government entities are commonly portrayed as the sole actors engaged in electrical security efforts, private entities also have parts to play. In particular, electric utilities have a tremendous interest in protecting their assets. To accomplish this, utilities finance measures that will prevent the interruption of power. For example, following the 2013 California substation attacks, the utility impacted invested several hundred million dollars to enhance security measures at numerous vital substations.⁹⁴

Table 3. Electrical Security Entities

Entity	Purpose & Scope
DOE	Primary federal department responsible for electrical security. Various program offices within the department are focused on security matters.
DHS	Primary federal department responsible for all internal national security matters. Not specifically focused on critical infrastructure or electrical security. Supports and collaborates on these security areas but is not the lead entity.
CISA	Primary federal agency responsible for security over several critical infrastructure sectors. Not directly responsible for electrical security but supports and collaborates.
State & Local Entities	Utilization varies by geographic area. Implements legislation and regulation to support electrical security.
Electric Utilities	Invests in security of assets to ensure provision of service and protect ability to earn profitable returns.

C. SECURING THE ELECTRICAL SECTOR: FEDERAL GOVERNMENT POLICY INITIATIVES

For more than two decades, the federal government has attempted to be the driving force behind enacting electrical security initiatives. There are several common characteristics within this line of effort. First, policy efforts for improving electrical security are often enacted within a more encompassing effort to improve overall critical infrastructure protection. Second, action has been taken almost explicitly by the executive

⁹⁴ Phillips et al., 12.

branch. Third, security policy has consistently pursued voluntary cooperation from private business. To demonstrate these common themes, I will provide a brief recap of recent noteworthy government policy initiatives.

1. Presidential Decision Directive 63: Critical Infrastructure Protection (PDD-63)

The Clinton administration released PDD-63 in 1998, following the establishment and review of the President’s Commission on Critical Infrastructure Protection.⁹⁵ The presidential directive clearly recognized a growing concern about the interdependency of United States infrastructure systems, particularly with respect to the growth of utilizing cyber information systems across all sectors.⁹⁶ This interdependency led efforts after PDD-63 to encompass critical infrastructure as the overarching issue, even if vulnerabilities in specific sectors were truly the focus.

Several aspects of PDD-63 would set the precedent for future action. The most significant is voluntary participation by the private sector. “In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.”⁹⁷ The document also states that “private sector owners and operators should be *encouraged* to provide maximum feasible security for the infrastructure they control (emphasis added).”⁹⁸ PDD-63 sought to persuade the private sector to participate by stating an intention to favor market solutions for infrastructure protection over regulation.⁹⁹ This was likely included to assure the private sector that the federal government did not want to appear overly forceful in this endeavor. However, in contrast to voluntary participation, this preference was not explicitly stated in follow-on policies.

⁹⁵ Humphreys, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, 3–4.

⁹⁶ Clinton, *Presidential Decision Directive 63: Critical Infrastructure Protection*, 1–2.

⁹⁷ Clinton, 5.

⁹⁸ Clinton, 5.

⁹⁹ Clinton, 4.

The government clearly recognized that vulnerabilities to critical infrastructure were a clear and present threat to national security interests. However, the use of terminology such as “voluntary” and “encouraged” in conjunction with a promise not to increase regulation seems to express a light-handed approach towards the government relationship with the private sector on this matter. Regardless, PDD-63 commenced an increased prioritization of securing critical infrastructure.

2. Executive Order 13636: Improving Critical Infrastructure Cybersecurity (E.O. 13636)

E.O. 13636 was the first of several policy initiatives under the Obama administration that sought to address the continued concerns about critical infrastructure. As its title indicates, this executive order primarily sought to address cyber vulnerabilities that affect all critical infrastructure sectors. The primary proposal to address these concerns was through information sharing efforts between federal government intelligence and security focused agencies with businesses and their commercial security partners when applicable.¹⁰⁰ However, the trend for voluntary cooperation is repeated throughout the order. The proposal for voluntary cooperation and participation is included in discussion of information sharing efforts as well as the development of a baseline set of cybersecurity standards. Additionally, the administration sought to discuss and develop incentives that would lure business entities to participate.¹⁰¹

Aside from maintaining the theme of previous policy, there is an interesting portion of E.O. 13636 that addresses security responsibility. The document states that information will be shared with the private sector “so that these entities may better protect and defend themselves against cyber threats.”¹⁰² This raises an interesting line of thought. Obviously, businesses are entitled to protect their assets, but this makes it appear as though the federal government is pushing at least a portion of the responsibility for cyber security to the private sector. At best this can be perceived as a matter of necessary burden sharing across

¹⁰⁰ Executive Order 13636: Improving Critical Infrastructure Cybersecurity.

¹⁰¹ Executive Order 13636: Improving Critical Infrastructure Cybersecurity.

¹⁰² Executive Order 13636: Improving Critical Infrastructure Cybersecurity.

the public-private divide. In contrast, it is easy to interpret this declaration as a matter of the federal government passing the buck to the private sector on a highly recognized security matter.

3. Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21)

PPD-21 was released in February 2013, concurrently with E.O. 13636. While E.O. 13636 sought to specifically address aspects of cyber security that impact critical infrastructure, PPD-21 was released to initiate a review of how the federal government approaches the security of critical infrastructure. As part of this review DHS was directed to evaluate the existing public-private partnership model. The directive does not specifically address the voluntary nature of the existing partnership. Rather it seeks to evaluate and consider possible improvements. Additionally, the directive ordered a review of the relationships within the federal government pertaining to critical infrastructure security and resilience.¹⁰³ This would essentially clarify who was expected to be the point of contact within the federal government for coordination with owners and operators.

It is also worth noting that PPD-21 directly acknowledges the energy sector. The directive describes how energy systems are distinctively important due to their interconnected operation with other sectors.¹⁰⁴ This clearly underscores the importance of electrical security within the broader critical infrastructure protection strategy.

4. National Infrastructure Protection Plan 2013 (NIPP)

The NIPP, released by DHS in 2013, is the national strategy intended to guide the security and resilience efforts across critical infrastructure sectors. The document acknowledges that it is “the government’s mandate to preserve public safety and ensure national security,” but that “coordination with infrastructure stakeholders is essential” to

¹⁰³ Obama, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*.

¹⁰⁴ Obama.

do so.¹⁰⁵ Despite this acknowledgement of government responsibility, the strategy perpetuates the dependence on cooperation through voluntary mechanisms.

From the federal perspective, a large portion of this cooperation is expected to occur within the network of sector and cross sector councils. The two most notable groups within this structure are the Sector Coordinating Councils (SCCs) and the Government Coordinating Councils (GCCs). SCCs are run and organized by representatives of private industry. Members interact on strategies and policies aimed to benefit their respective critical infrastructure sector. Additionally, the SCCs are meant to serve as the primary link of collaboration between the federal government and the private sector. The complement to the SCC is the GCC. The GCC includes representatives from across government that have a stake in the operation and security of an infrastructure sector. Therefore, the GCC enables the necessary effort to coordinate across departments, jurisdictions, or even levels of government.¹⁰⁶ Although the coordinating councils were established prior to the 2013 NIPP, it underscores the importance that the federal government has placed upon them to facilitate cooperation with the private sector.

5. Executive Order 13920: Securing the United States Bulk-Power System (E.O. 13920)

E.O. 13920, issued in 2020, can be considered an outlier within this set of policy initiatives to an extent. It is the only policy that solely addresses electrical sector concerns. However, it does so with the clear intent of specifically protecting the bulk-power system as a major asset within critical infrastructure. It is also unique that it is not based on voluntary cooperation. On the contrary, this executive action is a mandate to those in the business of supplying electrical power to American citizens. Essentially this executive order prevents the acquisition of major electrical grid components from businesses based in adversarial nations.¹⁰⁷ The LPTs discussed in Chapter II would be an example of the type of electrical equipment this executive order would prevent from being purchased

¹⁰⁵ Department of Homeland Security, *National Infrastructure Protection Plan 2013*, 1.

¹⁰⁶ Department of Homeland Security, 10–12.

¹⁰⁷ Executive Order 13920: Securing the United States Bulk-Power System.

outside the U.S. This is the first broad critical infrastructure policy decision that explicitly restricts acquisition by the private sector, rather than rely on incentives or coordination. The structure of this policy implemented under the Trump administration is in contrast with past policy decisions under the Clinton, Bush, and Obama administrations. It is unclear whether the current Biden administration will resume seeking voluntary cooperation with the private sector.

D. PUBLIC-PRIVATE PARTNERSHIPS FOR SECURING THE U.S. ELECTRICAL SYSTEM

The purpose of electrical public-private partnerships is to enhance grid security (Figure 4). The provision of electricity is considered a necessary and vital public service. Yet, the sector is largely maintained and operated by private businesses. Both types of actors recognize that they have a self-interest in ensuring the provision of electricity is reliable and secure. To achieve this, they must work together. This section will discuss three types of activities that contribute to the effectiveness of the public-private electrical security partnerships: information sharing, funding, and the ability to reform based on lessons learned.

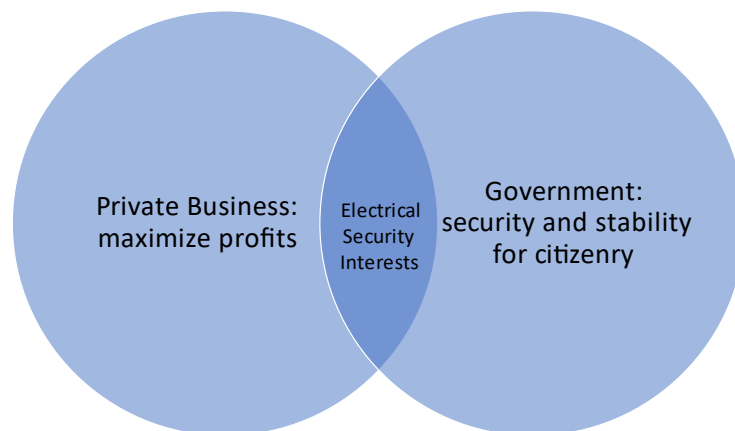


Figure 4. Electrical Security Public-Private Partnerships

1. Information Sharing

A plethora of federal policy documents emphasize the importance of information sharing across the public-private divide for ensuring electrical security. At a basic level, both sets of actors need to be on the same page and understand electrical security threats and vulnerabilities. There are multiple means by which public-private information sharing can take place.

A general cycle for how information sharing occurs in diverse public-private partnerships is presented in Figure 5. I detail how this occurs in two key organizations identified in federal policy: the ESCC and the Electricity Information Sharing and Analysis Center (E-ISAC). Overall, the most prominent pathways for information sharing is through the coordinating council structure defined in federal policies like the NIPP described above. However, there appear to be several weak points with such a strong dependence on this relationship. The first is that the ESCC is voluntary and self-governed. Businesses' participation is neither regulated nor mandated by any federal agency.¹⁰⁸

The ESCC is led and managed by private business executives with support from their respective staffs. Their official roster indicates 32 members participate in the coordinating council.¹⁰⁹ Some of the executives represent larger organizations with smaller sub-entities. However, there is no explicit lower-level set of organizations or associations that must receive information. This means there is no guarantee that the information sharing, coordination, and progress facilitated by ESCC efforts will be passed on to the entirety of the electrical power industry. Furthermore, there are significant differences between the organizations that each executive represents. It is only natural for an executive to prioritize sharing information that has a higher probability to impact their own organization.

¹⁰⁸ Electricity Subsector Coordinating Council, "Electricity Subsector Coordinating Council Charter" (Electricity Subsector Coordinating Council, August 5, 2013), 1, <https://www.cisa.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf>.

¹⁰⁹ Electricity Subsector Coordinating Council, "Electricity Subsector Coordinating Council Brochure," 4.

Beyond the voluntary nature of membership and limited scope of participation, the characteristics of the ESCC and its activities are difficult to assess. Other than a handful of generic public relations press releases, the ESCC does not appear to release any substantial amount of information to the public on its activities.¹¹⁰ Perhaps because of the limited amount of source material available, academics have largely not addressed the organization and its contributions. Without these analyses, it is difficult to assess the value of the ESCC as an information sharing asset within electrical security efforts.

The E-ISAC is another important organization that facilitates information sharing across the public-private divide, but there are distinct differences between the two entities. E-ISAC contributes within the larger ISAC structure that supports critical infrastructure, comparable to the SCC structure. However, E-ISAC is a federal government construct and falls under the NERC. Additionally, membership and participation in the organization are geared towards high level security and intelligence specialists who work for electrical operators, rather than towards electrical company executives. These experts may be better qualified to understand technical information and analyses that are shared within the organization.

¹¹⁰ Electricity Subsector Coordinating Council, “ESCC: Electricity Subsector Coordinating Council,” Electricity Subsector Coordinating Council, 2021, <https://www.electricitysubsector.org/>.

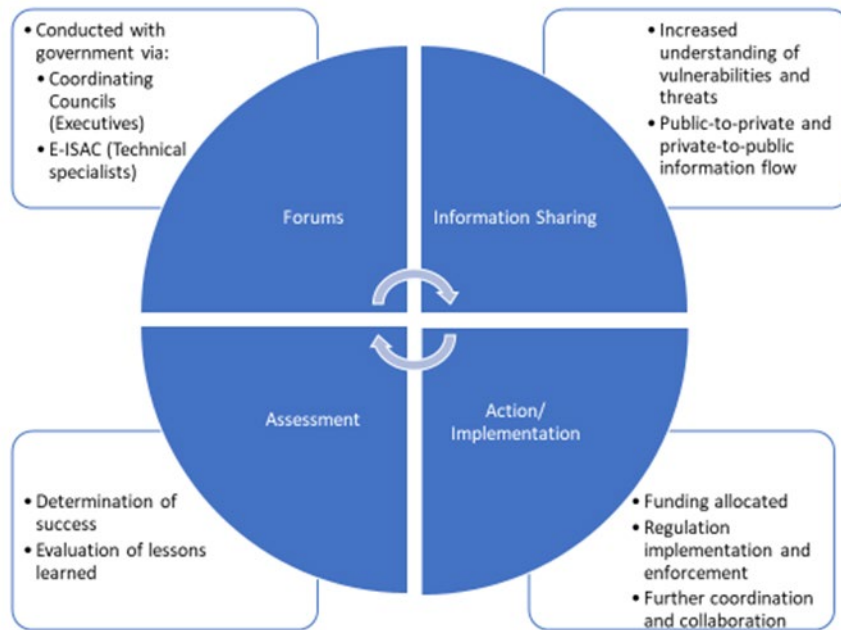


Figure 5. Electrical Security Information Cycle

A substantial concern with both organizations is the quality of shared information. Private business stakeholders are naturally hesitant to share information about their systems or processes for fear of competitive exploitation and wish to maintain trade secrets as much as possible. To counter this disincentive for private entities to voluntarily cooperate and share information, the federal government created a new classification that provided restrictive limits for sharing. Protected Critical Infrastructure Information (PCII) limits information sharing between those trained, certified, or have a ‘need to know’. It even has exemptions from Freedom of Information Act requests.¹¹¹ Consequently, the classification severely inhibits the ability to share information between organizational entities.

The constraints created by PCII classification are acknowledged within the E-ISAC Strategic Plan. The document states that a long-term focus is to “enhance the E-ISAC’s capability to better leverage classified and other critical threat and intelligence information (both nonpublic governmental and private sector) to provide timely and actionable

¹¹¹ David L. Alderson, “Overcoming Barriers to Greater Scientific Understanding of Critical Infrastructure Resilience,” in *Handbook on Resilience of Socio-Technical Systems* (Northampton, MA: Edward Elgar Publishing, 2019), 71–72.

information to the sector regarding security risks.”¹¹² The organization therefore acknowledges that security information could be shared more effectively.

2. Funding

Funding is a vital aspect of successful electrical security. It finances improved security measures and modernized infrastructure assets and assert the level of priority based on the scope of funding allotted. The plethora of funding mechanisms contribute to diverse electrical security goals such as research and risk reduction.

One path for funding is the utilization to conduct research and development (R&D). Due to the nature of the threat, a large portion of electrical security R&D has focused on cyber security concerns through the DOE’s Cybersecurity of Energy Delivery Systems (CEDS) program. Research projects in the program are led by private industry, university, and national lab representatives who receive funding and collaborate with DOE personnel through the program.¹¹³ Since the CEDS program began in 2010, approximately \$240 million dollars has been invested into the research conducted with positive results. 35 various tools and technologies developed through CEDS research are actively being utilized to strengthen the resilience of U.S. energy delivery systems.¹¹⁴

Another funding avenue that will impact electrical security efforts is FEMA’s Building Resilient Infrastructure and Communities (BRIC) program. Since the passage of the Disaster Recovery Reform Act of 2018, FEMA has been working to get the BRIC program up and running. The grant funding provided by the program aims to aid state and local governments in the pursuit of hazard mitigation projects that will reduce the risks that

¹¹² Electricity Information Sharing and Analysis Center, “E-ISAC Long-Term Strategic Plan Update” (Electricity Information Sharing and Analysis Center, October 2020), i, https://www.eisac.com/cartella/Asset/00009261/2020_E-ISAC_Strategic_Plan_Update_FINAL.docx?parent=127465.

¹¹³ Patricia A. Hoffman, “OE Announces Funding to Improve the Cybersecurity of the Nation’s Power Grid,” Department of Energy, accessed July 10, 2021, <https://www.energy.gov/oe/articles/oe-announces-funding-improve-cybersecurity-nation-s-power-grid>.

¹¹⁴ Department of Energy, “Cybersecurity Research, Development, and Demonstration (RD&D) for Energy Delivery Systems,” Department of Energy, accessed July 10, 2021, <https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and>.

applicant communities face from natural disasters and hazards.¹¹⁵ Although any attempt to mitigate risk should be viewed positively, the program remains in its infancy and its effectiveness is yet to be determined. From an electrical security perspective, the question should be what portion of this funding is going to impact electrical assets? The program is intended to address infrastructure in its entirety. Therefore, funding will be diluted across a wide swath of needed projects in applicant communities. If application data is any indication as to how funding will be allotted, the overwhelming majority will be granted to implement flood control measures over infrastructure protection.¹¹⁶

Although the BRIC program is not demonstrative of a direct partnership between public and private entities, the trickle-down effects of the program justify its discussion. The BRIC program is reducing risk and hazards at the community level which should reduce required federal support in the future. Although funding is granted to local governments, the application process also produces further public-private cooperation as well as insight into local level priorities which can be representative of the utilities they host.

3. Lessons Learned

Effective public-private electrical partnership must be able to implement reforms based on lessons learned from past failures. The 2021 winter storm that disabled power throughout Texas provides an example of the obstacles to reform. The Texas power grid is not under federal jurisdiction which exempts it from federally mandated rules and safeguards.¹¹⁷ Therefore, the interactions within this public-private partnership are inherently different from those involving the federal government. Additionally, this event is relatively recent, meaning that analyses and various legislative inquiries into the event

¹¹⁵ Federal Emergency Management Agency, “Building Resilient Infrastructure and Communities (BRIC),” Federal Emergency Management Agency, July 1, 2021, <https://www.fema.gov/grants/mitigation/building-resilient-infrastructure-communities>.

¹¹⁶ Federal Emergency Management Agency, “Building Resilient Infrastructure and Communities FY 2020 Subapplication Status,” Federal Emergency Management Agency, accessed July 10, 2021, <https://www.fema.gov/grants/mitigation/building-resilient-infrastructure-communities/fy2020-subapplication-status>.

¹¹⁷ Hasna Nazir, “Lessons Learned from the February 2021 Texas Power Outage,” *CERI Electricity Report*, April 2021, 2, https://ceri.ca/assets/files/Electricity%20Commodity%20Update_April%202021.pdf.

remain ongoing. However, its severe impacts on the grid and population of Texas justifies its consideration for analysis.

The 2021 winter storm was not the first to impact Texas on a massive scale. Comparable cold snaps previously struck Texas in 1899, 1951, 1983, 1989, and 2011.¹¹⁸ Examining the period between 2011 and 2021 paints a bleak picture for public-private collaboration in implementing reforms based on lessons learned. Following the 2011 storm, despite its limited jurisdiction, the FERC issued guidance to ERCOT, which manages most of the grid in Texas. The guidance focused primarily on the need to conduct weatherization efforts to strengthen the grid during future winter storms. However, this guidance was strictly voluntary.¹¹⁹ ERCOT and utility operators subsequently decided that the cost to conduct weatherization was unwarranted due to the perceived frequency with which severe winter weather events occur. As it turned out, the anticipated costs were dwarfed by the cost of the 2021 storm. The economic losses in Texas are estimated at approximately \$130 billion. Additionally, 4.5 million households lost power and at least 111 lives were lost.¹²⁰ It is also worth noting that Texas cities not part of the ERCOT interconnection, such as El Paso and Beaumont, experienced little to no loss of power during the 2021 cold snap. These areas, which were subject to greater federal oversight, invested in winter preparations and drew upon power from other portions of the grid that were unstrained by the adverse weather.¹²¹

The Texas case demonstrates that electrical security reforms are possible with appropriate cooperation between public and private partners. However, adaptations are limited by a reliance on voluntary cooperation. Private entities are less inclined to enact voluntary guidance when it is perceived to prevent a minimally frequent risk against their assets.

¹¹⁸ James Doss-Gollin et al., “How Unprecedented Was the February 2021 Texas Cold Snap?,” *Environmental Research: Letters* 16 (June 8, 2021): 2, <https://iopscience.iop.org/article/10.1088/1748-9326/ac0278/pdf>.

¹¹⁹ Joshua W. Busby et al., “Cascading Risks: Understanding the 2021 Winter Blackout in Texas,” *Energy Research & Social Science*, no. 77 (July 2021): 6–7, <https://www.sciencedirect.com/science/article/pii/S2214629621001997>.

¹²⁰ Busby et al., 1.

¹²¹ Busby et al., 7.

However, reform is not always cooperative. There are times when it may be necessary for public officials and regulatory agencies to forcefully enact regulation. For example, this may occur as information concerning electric power failures becomes highlighted following a system disruption or disaster.

E. ASSESSMENT

Figure 6 illustrates how the three types of public-private engagement discussed above can interact to successfully maintain U.S. electrical security by exercising an effective electrical security strategy. Information sharing and lessons learned often result in the implementation of regulation or ‘regulation-like’ standards that guide operations for utilities. Funding is frequently used to improve electric power systems. In combination with lessons learned, the result is a substantial increase in hazard prevention and reduction of risk to system operations. Research requires a substantial amount of information sharing and funding. These factors work together to produce advances in security oriented technology and innovation. However, the information presented in the previous sections indicates that there are at least two significant gaps in the current electrical security partnership structure. First, organizational structures and the responsibilities of entities involved are extremely diverse and convoluted. Second, the government’s dependence on voluntary cooperation by the private sector is highly problematic.



Figure 6. Electrical Security Cooperation

Although operators seem to clearly understand where their operational boundaries lie, the complex structure makes it more difficult for government entities to provide security assistance. The variations across the operational structure weaken security efforts. While it is unrealistic to expect a cookie cutter approach to organizing the grid, more standardization could prove advantageous for security efforts. However, to create any degree of standardization, stakeholders must decide whether any operational structure is more advantageous than another. Is it better to have electricity supplied in a monopolized manner or have a dispersal of organizational responsibility?

A wider distribution of operational participants can make coordination more difficult as it creates an increased number of entities that must be included within the planning, decision making, and enactment of policy. However, when issues arise it can be easier to delineate which entity holds responsibility based on which portion of the grid or location is affected. In contrast, it is always easy to assign responsibility in a monopolized structure because the singular entity controls all aspects of the operational structure. Unfortunately, when this organization makes mistakes, they tend to compound across the entirety of the structure which they control. This applies to the February 2021 power outages in Texas. When severe winter weather struck, generation sources went offline across the state and demand could not be met. This left millions of Texans to endure the relatively uncommon freezing temperatures without power to generate heat for their homes.¹²²

To be sure, while large scale losses such as the 2021 Texas outages or other events discussed in Chapter II have certainly happened, they do not occur frequently enough to suggest that public-private security partnerships persistently fail. There has not been a catastrophic loss of the U.S. power grid. However, the lack of standardization can make it difficult for federal security agencies to provide guidance or mandates for a complex set of entities overseeing operation of the grid.

¹²² Russell Gold and Katherine Blunt, “Texas Power Outages to Drag Into Third Day as Deep Freeze Persists,” *Wall Street Journal*, February 16, 2021.

Additionally, while diverse, the operational structures present some challenges, the voluntary nature of the relationship between public and private entities is a greater concern. Recent security breaches in other critical infrastructure sectors should serve as a blinking red light to federal officials and operators alike. More must be done by the public and private sector to ensure that the U.S. power grid is protected from the wide range of malicious and natural threats that can prevent their operation.

To begin with, the federal government needs to change course on its reliance on voluntary compliance by the private sector. At a certain point, the criticality of the service should outweigh voluntary participation. The impact upon the citizenry is too great to solely rely on the private sector to respond to voluntary guidance or requests. There are aspects of security that should be mandated and regulated to force businesses to meet an expected standard. This does not mean that any kind of security regulations should be issued unilaterally without the cooperation of private sector representatives. Private sector stakeholders, such as the E-ISAC and ESCC, should partake in the formulation of such mandates to provide expertise and acknowledge where shortcomings or vulnerabilities are likely to occur. Additionally, there may be instances where the private sector or not-for-profit local utilities will need increased funding assistance to implement necessary security standards. Federal officials cannot forget that the highest priority for businesses is their bottom line. Security may be a factor in their calculations, but in the end, businesses are focused on profits. There will surely be advocates who oppose an increase in the regulation of businesses. However, with respect to electrical security and critical infrastructure protection in general, this should be accepted as the price of doing business in areas that directly affect the well-being and stability of the American people and its economy.

Due to the wide array of threats against the electric grid, it may be helpful for public and private entities to consider specifying certain themes of threats that each should be primarily responsible for. As the number of threats and complex integration of systems has increased, one can see how security responsibilities have expanded to a point that the government cannot step in to take complete control. However, as the federal government maintains primary responsibility for security of its citizens, it should take the lead on any threat that is considered an attack. This would predominantly mean physical and cyber

attacks against the electrical grid. This plays into its traditional role of protecting the citizenry against malicious state and non-state actors that wish to harm national interests. Additionally, the federal government has the necessary intelligence apparatus to address these types of threats. As part of this delineation of responsibility, the federal government could take the lead on providing mandated security requirements and the majority of the necessary funding to implement required standards.

Other threat areas such as natural disasters and aging infrastructure concerns should fall primarily within the scope of the private sector and not-for-profit utilities managing the grid. While these areas certainly fall within the parameters of electrical security, these threats are not malicious in nature and are to a degree more predictable. For the foreseeable future, severe weather will continue to disrupt the provision of power to some extent. Infrastructure will continue to age and need to be replaced to provide reliable service. However, these issues are within the means of the private sector and utility operators to address within their own risk analysis while receiving guidance and continued cooperation from federal agencies. When necessary, state and local governments can be the primary means of funding assistance for these issues as the impacts of these threats will most heavily impact their respective citizenry and local economy. An organization such as FEMA will still have a role in response efforts, but prevention efforts for these threat areas can be led by the private sector. These examples do not justify the dismantling or removal of public-private partnerships to address these vulnerabilities. The increasing complexity and frequency of electrical security vulnerabilities suggests that a delineated leader within the partnership might strengthen efforts pursued.

F. CONCLUSION

The response of electricity operational and security structures has not been tested by a complete failure of the electrical grid. Even the large-scale outages that have occurred within the U.S. have been contained to respective regions and occurred over a limited span of time. Electrical organizational structures are particularly diverse and complex. These organizations on each side of the public-private divide have room for improvement with respect to information sharing, funding, and implementing lessons learned. Aside from the

organizational complexity of the electric grid and its supporting entities, there are other aspects of the public private partnership that should be updated. The voluntary cooperation of private entities is an outdated concept. A lack of security cooperation can create severe consequences for the American public if private entities fail to implement adequate protections. The federal government should consider implementing increased regulation to boost the security of the electrical grid rather than depending on voluntary cooperation. Businesses will have to accept this as the price of profiting from the provision of what is considered an essential service. Additionally, although cooperation should continue between public and private electrical entities to address electrical security concerns, consideration should be given to distinguish threat areas that public and private entities respectively should have primary responsibility over. Federal agencies can take the lead on attacks against electrical infrastructure, while private entities can take the lead on non-malicious threats such as natural disasters and aging infrastructure concerns.

IV. RENEWABLE ENERGY SECURITY

The federal government defines renewable energy as “electric energy generated from solar, wind, biomass, landfill gas, ocean (including tidal, wave, current, and thermal), geothermal, municipal solid waste, or new hydroelectric generation capacity achieved from increased efficiency or additions of new capacity at an existing hydroelectric project.”¹²³

Although they do not always mean the same thing, other terms such as clean or green energy are frequently used synonymously. Regardless of the terminology used, renewable energy is sourced from naturally replenishing resources. However, these resources are flow limited meaning they are restricted by the amount of energy that is available within a defined period.¹²⁴

The establishment of renewable energy is intrinsically linked to the growing concern and addressal of climate change and carbon emissions. The federal government began to address these concerns under the Obama administration with the Climate Action Plan. The first goal within this plan was to cut carbon emissions by 26 to 28 percent below 2005 levels by 2025. Strategies to meet this goal relied heavily on the power sector to pursue renewable energy projects and energy efficiency.¹²⁵ Despite progress beginning under the Obama administration, the Trump White House sought to weaken attempts to transition to renewable energy. In addition to removing the U.S. from the Paris Climate Agreement and directly supporting fossil fuel initiatives, the Trump administration hindered solar development by imposing tariffs on solar panels under the veil of broader trade hostilities with Asian countries.¹²⁶ Since the Biden administration has taken office,

¹²³ Executive Order 14008: Tackling the Climate Crisis at Home and Abroad (2021), 7853, <https://www.federalregister.gov/documents/2021/02/01/2021-02177/tackling-the-climate-crisis-at-home-and-abroad>.

¹²⁴ “Renewable Energy Explained,” U.S. Energy Information Administration, May 20, 2021, <https://www.eia.gov/energyexplained/renewable-sources/>.

¹²⁵ Environmental and Energy Study Institute, “Fact Sheet: Timeline of Progress in Made in President Obama’s Climate Action Plan,” Environmental and Energy Study Institute, August 5, 2015, <https://www.eesi.org/papers/view/fact-sheet-timeline-progress-of-president-obama-climate-action-plan>.

¹²⁶ Tim Dickinson, “Trump’s War on Solar,” *Rolling Stone*, April 3, 2020, <https://www.rollingstone.com/politics/politics-features/trumps-war-on-solar-power-968511/>.

they have clearly outlined that the federal government will strongly support the pursuit of renewable energy across America's electric grid. In comparison, many state governments began to take action to enact renewable energy legislation in the late 1990s continuing into the following decade. This legislation trend is referred to as renewable portfolio standards. Although standards vary within each state, they require that a percentage of electricity comes from renewable sources.¹²⁷

It is all but certain that the U.S. electric grid is going to transition towards being predominantly sourced from renewable energy. Largely due to the increasing impact of climate change, governments, businesses, and individuals have been driven to begin adopting renewable energy as a means to enact change. In January 2021, this transition was officially endorsed by the federal government via Executive Order 14008. This document called for the development of plans to achieve “a carbon pollution-free electricity sector no later than 2035.”¹²⁸ Even if the federal government loses focus or shifts priorities, it appears that many states will continue to push the electrical sector towards renewable energy. This is demonstrated by the wide adoption of renewable portfolio standards by state legislatures across the country.

Renewable energy generation is already being introduced into the U.S. electrical power mix at a variety of scales. In fact, as shown in Figure 7, renewable energy is now the second largest source of electricity in the U.S., producing 834 billion kilowatt hours (kWh) of electricity in 2020. The leading power generation source, natural gas, produces 1,617 billion kWh annually. Many states, regions, businesses, and individual residences are reaping the security benefits of renewable energies like solar power. For example, the introduction of solar power for individual homes and businesses makes customers less susceptible to a loss of electricity, since each building essentially becomes its own grid network.

¹²⁷ National Conference of State Legislatures, “State Renewable Portfolio Standards and Goals,” National Conference of State Legislatures, August 13, 2021, <https://www.ncsl.org/research/energy/renewable-portfolio-standards.aspx>.

¹²⁸ Executive Order 14008: Tackling the Climate Crisis at Home and Abroad.

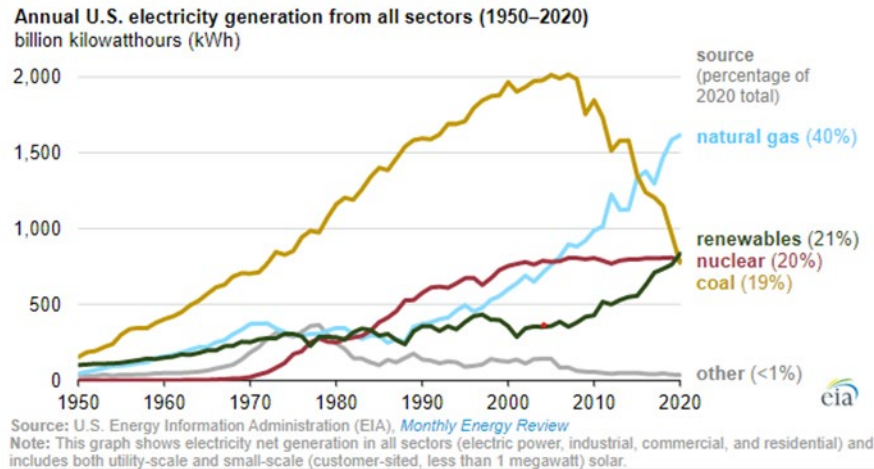


Figure 7. Annual U.S. Electricity Generation by Sector.¹²⁹

Further transition to renewable electricity assets will transform the physical and organizational makeup of the electric grid. This transformation will usher in additional security challenges to the ones already being managed and mitigated through the public-private partnerships. This chapter will begin by comparing the threats to a conventional and a renewables-based energy grid. Next, it will assess the applicability of federal electrical security policy initiatives to renewable energy security. Lastly, it will examine how new renewable energy public-private partnerships are impacting the approach to renewable energy security.

A. THREAT COMPARISON

By and large, the threats to renewable energy appear to align with our understanding of the major threats to traditional electrical energy. The threat of physical attacks on renewable generation assets will largely mirror the threats associated with conventional energy assets, particularly the fact that many facilities will cover large areas of land where it is difficult to maintain adequate security oversight. While many renewable energy technologies can be deployed at a household or micro level, the majority of current and planned generation is deployed at grid-scale in large mono-purpose facilities. For

¹²⁹ Source: U.S. Energy Information Administration, “Renewables Became the Second-Most Prevalent U.S. Electricity Source in 2020,” U.S. Energy Information Administration, July 28, 2021, <https://www.eia.gov/todayinenergy/detail.php?id=48896>.

example, many of the largest solar farms in the U.S. cover areas greater than ten square kilometers.¹³⁰ Like the conventional installations described in Chapter II, these facilities are in isolated areas. This combination of geographic isolation and concentration of valuable energy assets within a relatively large area increases vulnerability. This logic for large scale solar farms can be applied to other renewable energy assets such as wind farms and various off shore systems.

Cyber threats will also continue to be a major concern for electrical security as the grid transitions to increased incorporation of renewable power generation. In fact, renewable energy facilities in the U.S. have already become victims of cyber attack. In March 2019, unidentified actors launched a denial of service attack that compromised the monitoring of approximately 500 MW of wind and solar assets in California, Wyoming, and Utah. Luckily, there was no loss of generation from the attack.¹³¹ Regardless, this demonstrates the persistent threat and severe impacts that interconnected cyber systems and assets may have on electrical security.

Renewable energy generation assets are not currently threatened by the age of their infrastructure, as they are just beginning to be introduced. However, these new generation sources continue to rely on old transmission networks, where most of the concern for aging electrical infrastructure exists. Reports claim that most of the transmission lines in the U.S. have surpassed their intended lifespan. Furthermore, these dated transmission lines were not designed to carry the amount of demand currently placed upon them.¹³² The incorporation of renewable energy sources and the potential introduction of more complex energy flow networks into the grid will intensify challenges to transmission infrastructure. In particular, distribution systems located in communities or at the household level can lead to voltage imbalances that impact the operation of legacy transmission and distribution

¹³⁰ Lubwa Leonard, "Top 5 Biggest Solar Farms in the US," Construction Review Online, June 25, 2021, <https://constructionreviewonline.com/biggest-projects/top-5-biggest-solar-farms-in-the-us/>.

¹³¹ Robert Walton, "First Cyberattack on Solar, Wind Assets Revealed Widespread Grid Weaknesses, Analysts Say," *Utility Dive*, November 4, 2019, <https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weakness/566505/>.

¹³² American Society of Civil Engineers, *Infrastructure Report Card*, 2.

assets.¹³³ One means of enhancing U.S. electrical security during the introduction of generation assets would be to conduct it in tandem with updating the nations electrical transmission infrastructure, thereby removing the risks associated with the continued operation of outdated systems.

Although it will take time for large numbers of renewable energy assets to be concerned with their age, the concept of aging infrastructure will have a different dynamic with renewable energy. The average solar photovoltaic panel has an anticipated lifespan between twenty and thirty years.¹³⁴ This is interesting because it is roughly half the lifespan of conventional electric assets. As solar panels have a shorter lifespan, consideration will need to be given to their replacement and the demand that places on the supply chain. Many renewable energy goals fall between the years 2035 and 2050. It is possible that just as many of these national level goals are achieved, assets will be due for renewal.

Another new consideration for renewable energy security is the integration with cyber based devices connected to individual residences. With technology such as solar panels, a home essentially becomes its own power generation facility. However, as aspects of home energy control systems are connected via cyber networks, the susceptibility to cyber attack increases. When power is centralized, there is a more compelling incentive to ensure cyber security is maintained. In contrast, cyber assets at individual households are likely to not be nearly as secure. However, coordinated attacks against distributed electric resources and technologies that have a low barrier to entry are a probable scenario that could threaten security and create large scale impacts across the electric grid.

The transition to renewable energy will usher a change in how power delivery is conceptualized. Although renewable energy assets will eventually dominate the electric grid, some degree of conventional electricity generation assets are likely to remain as backup

¹³³ Pepco, “Challenges for Distribution Feeder Voltage Regulation with Increasing Amounts of PV,” https://www1.eere.energy.gov/solar/pdfs/hpsp_grid_workshop_2012_steffel_pepco.pdf.

¹³⁴ Solar Energy Industries Association, “Recycling and End of Life Considerations for Photovoltaics,” Solar Energy Industries Association, 2021, <https://www.seia.org/initiatives/recycling-end-life-considerations-photovoltaics>.

power sources. Many conventional fossil fuel assets provide stable baseload power. However, the fossil fuel that most likely to survive the renewable energy transition is natural gas as it has lower emissions. The problem is that many natural gas power plants are designed to deliver power for peak load periods and quickly ramping up supply. This demands new consideration for how this energy source is effectively utilized. Additionally, with continued reliance on natural gas, consideration must be given to pipeline vulnerabilities. The Texas cold snap is a perfect example of how a natural disaster can interrupt the delivery of natural gas resulting in cascading failures operating the electric grid.

One aspect of renewable energy that will present new security challenges is the variability of renewable resources. For example, the sun isn't always shining, and the wind isn't always blowing. This weather variability threatens the uninterrupted provision of electrical power to Americans by straining the already precarious balance between generation and consumption. However, this variability is expected to be addressed by developments in energy storage technology that will drastically change the manner by which balancing the grid is conducted.¹³⁵

Although the introduction of storage technologies is a challenge, the use of improved storage technologies could simultaneously improve electrical security. In addition to managing the fluctuations within renewable energy power generation, storage technologies can provide backup power when outages occur. They can also potentially facilitate “black start recoveries,” which restore power during shutdowns of the national transmission system.¹³⁶

Although power will still be lost during weather events and natural disasters to some degree, cascading failures are preventable when individual building units have their own power generation and storage assets. Additionally, the cost-benefit calculation of attacking an individual building unit, provided it is not a major government building or

¹³⁵ National Academies of Sciences, Engineering, and Medicine 2021, *The Future of Electric Power in the United States* (Washington, DC: The National Academies Press, 2021), 171, <http://nap.edu/25968>.

¹³⁶ Sadie Cox, Laura Beshilas, and Eliza Hotchkiss, “Renewable Energy to Support Energy Security” (National Renewable Energy Laboratory, October 2019), 3, <https://www.nrel.gov/docs/fy20osti/74617.pdf>.

other high visibility target, will not align with the “shock and awe” desired by actors who target the electrical grid

B. SECURING RENEWABLE ENERGY

The federal government demonstrated its commitment to transitioning the generation structure of America’s electric grid in E.O. 14008. It appears that the most influential private entities and utility organizations are on board with this transition, particularly those who are involved in the current public-private partnership structure. Analysis of the ESCC roster demonstrates that nearly the entirety of its membership has recognized the importance of transitioning to the use of renewable generation sources within their portfolio.¹³⁷ While some of this may be an exercise of public relations, the nearly unanimous recognition of renewables as well as the explicit decarbonization goals of some organizations makes it difficult to dismiss the predicted inclusion and expansion of renewables. This buy-in from the private sector has pros and cons. It is certainly positive that the public and private entities are of a shared mindset that the grid needs to transition to renewable energy sources. This should easily enable cooperative efforts within the partnership. However, the continued presence of the same organizations within the partnership structure will make it more difficult to implement structural change. An inability to exercise structural change means that the complex organization of the electrical sector is likely to persist.

Just as the introduction of renewable generation remains in its infancy, the same can be said of renewable energy security. It is advantageous for electrical security experts that the deliberate threats on the grid conceptually align with those they are already attempting to address with protection of the conventional grid. Thus far, this has allowed

¹³⁷ My analysis consisted of a basic review of the public websites for each member organization on the ESCC roster. 30 of 32 members included recognition of renewable energy uses, transition to carbon neutrality goals, environmental sustainability, or comparable terminology. The 2 members who did not appear to highlight these topics were the National Infrastructure Advisory Council (NIAC) and North American Electric Reliability Corporation (NERC). ESCC roster can be found at https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure.ashx?la=en&hash=00901B6AD252F5AF940C1012619A43C39967F9C9.

renewable security efforts to have a slightly different perspective that focuses more on the introduction and operation of a renewables-dominant grid, rather than explicitly shielding it from attack.

1. Public and Private Unilateral Renewable Energy Security Efforts

Chapter III discussed several of the federal government policy initiatives that aimed to drive security efforts within the electrical sector. Analysis of these policy measures demonstrated three consistent themes amongst these policy initiatives. First, electrical security efforts are often enacted within broader efforts to improve the security of all critical infrastructure. Second, the executive branch is typically the one who has taken or led actions to bolster electrical security. Third, policy initiatives have consistently pursued voluntary cooperation from private businesses to participate in the necessary security partnership.

Further analysis of these policy initiatives shows that there is no explicit discussion of renewable energy in any of them. Over a span of more than twenty years, the federal government failed to factor in the security of renewable energy assets in any of its prominent electrical security policy initiatives. At best, these policies address issues that are common to renewable and conventional energy security such as cyber security and critical infrastructure interdependency.

This suggests that many of the federal government policy initiatives aimed at conventional grid security may be insufficient to address new challenges associated with introduction of renewable energy generation. While some address issues that are simultaneously related to renewable energy security, the overwhelming focus for energy security remains on its application to the conventional grid. Thus far, it appears that the federal government is predominantly focused on the implementation of renewable energy rather than the security of these energy assets. This is demonstrated within the most important federal policy document to recognize renewable energy, E.O. 14008. This order never explicitly addresses energy security or renewable energy security. However, it repeatedly mentions the ‘transition to’, ‘shift to’, and ‘deployment of’ clean and renewable

energy. All discussion of security within E.O. 14008 is applied to the broader application of national security within the context of climate change and its implications.¹³⁸

There are three probable reasons that the government is focusing on implementation rather than security of renewable energy: the federal government's commitment to the public-private security partnership model, the alignment of conventional and renewable electrical threats, and the inherent increase in electrical security that is expected to occur as a result of adding more diverse and decentralized power generation to the electrical system.

First, the renewable energy security efforts that have been carried out by the federal government are public-private partnerships, but they pursue slightly different approaches. Several of these efforts will be discussed later in this chapter. The government is not seeking to seize control over electrical security efforts. Doing so would likely be ineffective and convey the wrong message to private electrical business entities. Even with the introduction of renewable energy, the U.S. government remains committed to ensuring electrical security is enacted by the public-private partnership model.

Second, renewable energy threats appear to align with current conventional electricity threats. There is not an urge to create problems that do not exist. That does not mean new renewable energy threats will not emerge. Rather, the most significant threat to renewable energy assets appears to be the successful and consistent operation of such systems. As such, conventional electrical security responses will continue to be applicable in the federal government approach to renewable energy security and for the near future, additional efforts will be aimed at ensuring the operation and design of renewable energy systems continue to provide consistent uninterrupted power.

Third, most experts believe that renewable energy will be inherently more secure compared to conventional electrical systems. Increased diversity of generation sources, increased geographic dispersion of generation assets, and the inclusion of energy storage are just a few reasons that electrical security is likely to improve with the implementation

¹³⁸ Executive Order 14008: Tackling the Climate Crisis at Home and Abroad.

of renewable energy systems.¹³⁹ Although electrical disruption is likely to naturally decrease due to renewable energy, it would be troubling to believe that disruptions will no longer occur.

Similar to the federal government, it appears that private utilities are focusing more on the implementation and operation of renewable energy, rather than the security of these new generation assets. As previously mentioned, utilities have broadly accepted the idea that the electrical grid is transitioning to being predominantly sourced by renewable generation assets. However, private utilities are not unilaterally pursuing efforts explicitly targeted at renewable energy security.

2. Public-Private Renewable Energy Partnerships

Although previous federal policies fail to incorporate security for renewable energy, there are some renewable energy security efforts taking shape. These efforts continue to utilize and leverage the strengths of the public-private partnership model. As previously discussed within the context of conventional grid security, these efforts primarily entail information sharing, funding, and reform initiatives. As in conventional energy PPPs, the federal government appears to be the lead actor in renewable energy security PPPs.

a. Information Sharing

Chapter III demonstrated how information sharing efforts for conventional electrical grid security relied heavily on the utilization of organizations such as ESCC and E-ISAC. While these organizations remain important, the growth of renewables is introducing a new perspective on information sharing. Previous efforts to share information across the public-private divide have sought to expose design vulnerabilities and strengthen the grid against possible deliberate attacks. New efforts are focusing more on analytics R&D to ensure that a renewables dominant grid can function and maintain operation.

¹³⁹ Cox, Beshilas, and Hotchkiss, “Renewable Energy to Support Energy Security,” 2–3.

As an example, the Hawaiian island of Maui is set to become one of the first interconnected electric transmission systems in the world that is completely supplied by renewable energy generation. Some estimates claim the island will achieve this goal as early as 2024.¹⁴⁰ However, there is still substantial uncertainty about the variability and reliability of a renewables-reliant grid. To better understand and predict potential problems, the private electric utility on Maui, Hawaiian Electric, has partnered with the National Renewable Energy Laboratory (NREL), a national laboratory that focuses on renewable energy research for the DOE.

The NREL is utilizing multi-timescale modeling tools to provide advanced systems analysis for Maui's highly renewable-dependent electric system.¹⁴¹ Although Maui's grid will operate with complete renewables generation for many hours each year, these models will help grid managers at Hawaiian Electric understand the parameters that will trigger the use of conventional electricity-generation sources to continue the uninterrupted provision of power. Furthermore, the modeling conducted by NREL is driving further exploration of grid stability options under renewable generation. Conventional electrical systems manage grid stability via the spinning generators that minimize electromagnetic disturbances. However, many prominent renewable generation assets, such as wind and solar, remove the ability to stabilize the grid in this manner. The NREL's simulation-based modeling is exploring the use of synchronous condensers to stabilize renewable powered systems as an alternative.¹⁴² Increased information sharing via modeling initiatives appears to be a promising public-private pathways towards enhancing renewable energy security.

The Maui example provides a single example of information sharing efforts. In particular, research and work conducted by the national lab system with an array of private partners produces data and results that are vital to the advancement of renewable energy

¹⁴⁰ Ryan Kennedy, "As Maui Approaches 100% Renewables, NREL Models Grid Options," *PV Magazine*, August 2, 2021, <https://pv-magazine-usa.com/2021/08/02/as-maui-approaches-100-renewables-nrel-models-grid-options/>.

¹⁴¹ Kennedy.

¹⁴² Kennedy.

security. It is important to note that these efforts are advancing security in a less traditional manner. Typically, security oriented organizations, such as DHS, would have the greatest influence upon security issues. For renewable energy, it appears that federal entities that are more research minded, such as the national labs and DOE, are taking the lead to advance security efforts.

b. Funding

Of the three levers of the public-private partnership discussed in Chapter III, funding appears to be the most stable and effective means of facilitating cooperation between the federal government and private actors, to achieve electrical security. Numerous federal programs and offices, including CEDS, CESER, EERE, and national labs are poised to provide further, significant renewable security solutions via the funding they are distributing for collaborative research. For example, DOE recently announced two funding initiatives that will advance electrical security initiatives. The first initiative will provide \$42.3 million of funding to support research that will usher clean energy innovation targeted at manufacturing processes. Specifically, the research aims to “improve the systems and processes for how energy is stored, converted, and used.”¹⁴³ The second initiative will provide technical assistance funding to five private manufacturing partners that will test clean energy technologies in industrial settings. Each private partner will receive \$300,000 worth of funding.¹⁴⁴ These examples are a minimal portion of the funding allocated to renewable energy programs. In 2020, renewable energy programs received in excess of \$1 billion.¹⁴⁵ However, it is difficult to ascertain how much of that funding went to partnership programs such as the two examples provided.

The federal government is also undertaking funding initiatives to support private entities efforts to strengthen electrical infrastructure. Although these initiatives are not

¹⁴³ Department of Energy, “DOE Announces \$42.3 Million and New Industry Partners to Decarbonize American Manufacturing,” Department of Energy, July 29, 2021, <https://www.energy.gov/articles/doe-announces-423-million-and-new-industry-partnerships-decarbonize-american-manufacturing>.

¹⁴⁴ Department of Energy.

¹⁴⁵ Lynn J. Cunningham and Rachel J. Eck, *Renewable Energy and Energy Efficiency Incentives: A Summary of Federal Programs*, CRS Report No. R40913 (Washington, DC: Congressional Research Service, 2021), 2–8, <https://sgp.fas.org/crs/misc/R40913.pdf>.

specifically focused on renewable energy, strengthening the electrical grid will enhance renewable electrical security, as well as conventional electrical security. A significant portion of the proposed funding in the Infrastructure Investment and Jobs Act that is currently before Congress is targeted for the electrical sector. Although the details of the legislation continue to be debated, approximately \$73 billion has been allocated to upgrade electric transmission lines and another \$73 billion is allocated to assist the expansion of renewable energy sources.¹⁴⁶ The approval of funding for these electrical line items in tandem is quite important. Without replacement and revitalization of transmission infrastructure, the widespread implementation of renewable electricity generation is putting the cart before the horse. Updating transmission infrastructure will support the implementation of more sophisticated renewable generation sources and complex energy sharing strategies. The bill does not offer much granularity on who these funds will be specifically distributed to. However, it is reasonable to assert that a significant amount of this funding will trickle down to utilities to enact the improvements and expansion that Congress has designated. As the bill navigates the American bureaucracy, it would be overly critical to highlight the current degree of specificity that the legislation has in its draft format.

Further analysis of the funding proposals within the draft bill reinforces two concepts. First, with respect to explicit grid security concerns, the federal government has placed tremendous focus on cybersecurity. There is even a section that clearly delineates the importance of public-private partnerships to enhance grid security.¹⁴⁷ Second, the aspects of the bill that discuss renewable energy are focused on implementation, not security.¹⁴⁸ If this legislation ultimately passes, it will assuredly provide a tremendous shove from the federal government towards a transition of the electrical sector, needed infrastructure improvements, and further electrical innovation and research. However, it is

¹⁴⁶ Josh Lederman, “Clean Energy, Aging Grid to Get Big Boosts under Infrastructure Deal,” *NBC News*, July 28, 2021, <https://www.nbcnews.com/politics/congress/clean-energy-aging-grid-get-big-boosts-under-infrastructure-deal-n1275350>.

¹⁴⁷ Rep. Peter Defazio (D-OR-4), “Infrastructure Investment and Jobs Act,” Pub. L. No. H.R. 3684 (2021), 1374–78, <https://www.congress.gov/117/bills/hr3684/BILLS-117hr3684eas.pdf>.

¹⁴⁸ Rep. Peter Defazio (D-OR-4), 1304–1871.

interesting that funding for security efforts is not as forward looking as it could be. With the existing assumption that the grid is transitioning to become dominated by renewable sources, increased funding should be allocated to focus explicitly on renewable energy security.

c. Reform from Lessons Learned

Because renewable energy is in its infancy, it is difficult to implement reform measures for PPPs based on lessons learned; there are simply few cases of renewable energy failure to draw upon. Generation from wind turbines were disrupted during the Texas cold snap.¹⁴⁹ Some renewable energy pursuits, such as concentrated solar power facility Crescent Dunes, have been ineffective despite utilizing hundreds of millions of dollars in DOE loan guarantees.¹⁵⁰ However, the cyber attack against renewable assets mentioned previously in this chapter provides the strongest opportunity to analyze a renewable energy security failure and identify lessons learned.

Although the attack did not result in an inability to produce power, there are several other aspects that are just as important. First, the attack is believed to be the first cybersecurity incident to disrupt operation in the U.S. electrical sector.¹⁵¹ This reaffirms the belief that cybersecurity of the electrical grid is a legitimate threat to electrical security. Second, the attack targeted renewable energy assets. As the country continues to integrate renewable energy, this suggests that renewable energy sources will persistently be subject to cyber threats as the electrical grid transforms. Third, cyber security experts have expressed dismay over the simplicity with which the attack was conducted. The equipment targeted was accessible through the public internet.¹⁵² This allowed the intruder to

¹⁴⁹ Busby et al., “Cascading Risks: Understanding the 2021 Winter Blackout in Texas,” 2.

¹⁵⁰ Jason Deign, “America’s Concentrated Solar Power Companies Have All but Disappeared,” January 20, 2020, <https://www.greentechmedia.com/articles/read/americas-concentrated-solar-power-companies-have-all-but-disappeared>.

¹⁵¹ Sean Lyngaas, “Utah Renewables Company Was Hit by Rare Cyberattack in March,” *Cyber Scoop*, October 31, 2019, <https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/>.

¹⁵² Lyngaas.

infiltrate the system via an unpatched firewall, even though the patch was available for implementation.¹⁵³

This raises several concerns regarding the design of the system, the preparedness of operators to prevent intrusion, and awareness of system managers. It is baffling that a network utilized for providing power would be accessible through the public internet. This appears to be a design flaw that is ripe for public-private cooperation to facilitate correction. Neither the federal government nor private business can afford the negative impact such a weakness presents.

PPPs can improve the flaws experienced within information sharing and security standards. In this case, the shortfalls of information sharing were between private actors: the utility and the cyber security provider. However, common sense improvements can be implemented through regulation to serve as an enforcement mechanism and prevent future system intrusion. Such reform would require a variety of actors to collaborate. The federal government would need to lean heavily on CISA as the hub for cyber security developments across infrastructure sectors. The private sector should utilize the security expertise within the E-ISAC to seek adequate protection that makes sense for private actors. Of course, other entities such as DOE and the ESCC are assured to be involved, but most of the regulation development should be done by the security experts with eventual buy in from the business focused advisors. Regulation for cyber security will be complicated because the field is constantly evolving. Therefore, cyber and security experts should be placed at the center of the apparatus seeking to find a solution.

In addition to the referenced cyber security incident, public and private actors can also extrapolate lessons learned from past mistakes with the conventional electric grid to provide a secure foundation for the use of larger amounts of renewable energy in the United States. Reform is a constant process that seeks to improve based upon the lessons learned in previous experiences and incidents.

¹⁵³ Walton, "First Cyberattack on Solar, Wind Assets Revealed Widespread Grid Weaknesses, Analysts Say."

C. CONCLUSION

The electrical grid and its corresponding security environment are already tremendously complex. The increased use of renewable energy sources will create new and more complicated challenges for operators, policy makers, and security specialists. The federal government and private business actors appear to be more concerned with the implementation of renewable energy rather than the security of these new energy assets.

Overall, it appears the threats against the electric grid will not be very different than today. Many of the same threats will continue to exist, but they will present new impacts to electrical security through the utilization of renewable energy assets. Events such as cyber attacks are likely to be distributed across many customers utilizing coordinated low barriers to entry, rather than centralized facilities.

Although the comparison of threats against conventional and renewable energy is similar, the federal government has failed to account for the inclusion of renewable energy generation in electrical security policies. Despite any explicit mention of renewable energy security within public policy, public-private partnerships are forming. Although there are few examples of these efforts, cases such as the research and collaboration on Maui's renewable electrical grid suggest that renewable public-private partnerships are enabling renewable energy security cooperation. Refinement of the mechanisms within public-private partnerships, such as information sharing, funding, and reform, will continue to strengthen their effectiveness as the electrical security environment becomes increasingly complex.

V. CONCLUSION

A. THE FUTURE OF PUBLIC-PRIVATE RENEWABLE ENERGY PARTNERSHIPS

The cases discussed in Chapter IV demonstrate that the foundation of public-private renewable energy partnerships has already been laid. Information sharing and funding efforts are already being reimagined and revitalized to ensure the establishment of renewable energy assets and continued security of the grid. However, more can be done using the public-private partnership to enhance renewable energy security. Based on conclusions about the strengths and weaknesses of various public-private partnerships, this chapter identifies recommendations for improvements in information sharing, funding, and reforms, which can be implemented as the grid transitions to strengthen renewable electrical security.

1. Information Sharing

As discussed in Chapter IV, the type of data analysis and information sharing conducted by NREL and Hawaiian Electric is a necessary advancement for information sharing efforts, particularly with regard to understanding renewable energy vulnerabilities. Although this is a positive example of information sharing, there are weak points of current information sharing organizations such as the ESCC and E-ISAC. The analysis in Chapter III revealed how voluntary membership hinders the capability of these organizations. A federal requirement for all electric utilities to participate in information sharing efforts should be the price of profiting from an essential service. Further participation and representation can be achieved through a more defined hierarchal structure to facilitate information flow.

One example of how to do this might be to shift towards a model of state representatives within the ESCC and E-ISAC organizational structure. These representatives and their staffs would be responsible for facilitating information flow down to their respective state electric utility association as well as laterally to other state delegations. Although issues such as many utilities providing energy to multiple states still

remain to be resolved, a deliberately defined hierarchy with mandated membership could increase productive information sharing efforts, resulting in a more secure electrical grid.

Another weak point of information sharing is PCII classification practices. E-ISAC should reassess the utility and administration of this classification. Trade secrets and security measures are not at odds with one another. E-ISAC, with participation from private company stakeholders, need to reform PCII classification to ensure that security relevant information can be shared. Any reform measures should be formulated without disregard for the concerns of private companies.

Anticipated decentralized grid structures are going to share a tremendous amount of data. Private entities will have to come to terms with what is shared by the data and what organizations know about the technology that supports that data transfer. While making everything an ‘open book’ makes organizations vulnerable to hacking or corporate espionage, the environment with which information and data is shared and transmitted within the electrical sector has security and operational implications that will have to be considered moving forward. Adjustment of the PCII classification and information sharing in its entirety will be a balancing act. Too much unrestricted flow of information could invite cyber attacks and system intrusions as discussed in Chapter IV. If information sharing is inhibited, the ability to collaborate and share knowledge is severely impeded.

2. Funding

Eitan et al. identify six types of renewable energy partnerships between public and private actors, at the community level.¹⁵⁴ One of these highlights how a private entity can assist the funding efforts of establishing community-level renewable energy projects. This is important considering the decentralized nature of renewable energy. Although this example accounts for funding flowing from private entities to local government, there is no reason to ignore the possibility of funding being provided by local governments, rather than the federal government, to assist private entities in the establishment of renewable energy projects in their community. Furthermore, although this literature focuses on the

¹⁵⁴ Eitan et al., “Community-Private Sector Partnerships in Renewable Energy.”

establishment of renewable assets, the same funding schemes can be applied to the maintenance and upgrades of electrical security measures.

3. Reform from Lessons Learned

The primary focus area for reform should be the dependence on voluntary compliance. Whether it is applied to participation in information sharing or equipment security standards, asking companies to voluntarily comply is not enough. Voluntary recommendations have proven to be a hollow and inefficient mechanism to address security concerns. This is not to suggest that mandatory regulation should be excessively used as a blunt application for demanding government compliance. Rather with respect to electrical security, the relied upon preference towards voluntary implementation can have disastrous effects that are entirely preventable. When appropriately applied, regulation can be a tremendous means to strengthen the security of the grid. However, public and private stakeholders need to be equally involved in the formulation process.

B. CONCLUSION

The U.S. electrical grid is beginning to undertake a monumental shift in how it operates. This shift demands a reassessment of how electrical security will be ensured once the electrical grid operates primarily with renewable energy generation assets. This research focused on three areas: vulnerabilities and threats to electrical security, the public-private electrical security partnership model, and how it can be used to enhance the security of renewable energy assets.

The most prominent vulnerabilities of the U.S. electrical grid can be organized into two categories: first, the classic malicious security challenge carried out via a physical or cyber attack, and second, disruptions of electrical system operations by infrastructure and equipment malfunctions or natural weather events. Each category is a significant concern for present and future electrical security. Although these concerns are rational, based on their correlation to historical electrical outages, the scope by which electrical outages have occurred in the U.S. is relatively minimal. It is unrealistic to have a zero-defect mentality with respect to the electrical grid. However, the more that design and protocols are driven

to be resilient the more it will increase electrical security and minimize the disruption of electrical power.

Public-private partnerships are recognized by the government and private businesses alike as a lynchpin of successful electrical security initiatives. Despite the diversity and complexity of organizations within this partnership structure, public and private entities leverage partnerships to cooperate. This is primarily observed through information sharing, funding, and reform from lessons learned. Each of these three tools have pros and cons that are open to critique, but they are all vital to the successful formulation and execution of an effective electrical security strategy.

The transition to renewable energy assets is likely to continue leveraging public-private partnerships for electrical security. Existing conventional vulnerabilities and threats will remain applicable and relevant to a renewable dominant energy grid. U.S. renewable generation facilities have already demonstrated that they are susceptible to intrusion from cyber attacks. However, thus far, it appears that there is an elevated focus on supporting the implementation and operation of renewable electricity over what are viewed as traditional electrical threats. The federal government is working to increase funding and expand collaborative information sharing to facilitate a secure transition to renewable energy generation assets. Although action is being taken to implement and strengthen renewable energy provision, there remains room for progress within the public-private partnership model.

There are varied levels of academic analysis and government policy pertaining to the topics discussed within this thesis. Admittedly, this analysis often emphasized the perspective or shortfalls of the federal government within security efforts. Further research would benefit from diving deeper into the impacts of actions and programs carried out by the electric utilities. Additionally, a multidisciplinary approach to these issues could be advantageous. Many academic writings focus on the security, business, environmental, or public policy aspects of this issue, but electrical security is a multifaceted problem that requires the expertise of differing disciplines to ensure the continued provision of electrical power to the populace.

LIST OF REFERENCES

- Alderson, David L. “Overcoming Barriers to Greater Scientific Understanding of Critical Infrastructure Resilience.” In *Handbook on Resilience of Socio-Technical Systems*. Northampton, MA: Edward Elgar Publishing, 2019.
- American Society of Civil Engineers. *Failure to Act: Electrical Infrastructure Investment Gaps in a Rapidly Changing Environment*. American Society of Civil Engineers, 2020.
- . *Infrastructure Report Card: Energy*. Reston, VA: American Society of Civil Engineers, 2017.
- Brown, Gerald, Matthew Carlyle, Javier Salmeron, and Kevin Wood. “Defending Critical Infrastructure.” *Interfaces* 36, no. 6 (December 2006): 530–44.
- Busby, Joshua W., Kyri Baker, Morgan D. Bazilian, Alex Q. Gilbert, Emily Grubert, Varun Rai, Joshua D. Rhodes, Sarang Shidore, Caitlin A. Smith, and Michael E. Webber. “Cascading Risks: Understanding the 2021 Winter Blackout in Texas.” *Energy Research & Social Science*, no. 77 (July 2021).
<https://www.sciencedirect.com/science/article/pii/S2214629621001997>.
- Carr, Madeline. “Public-Private Partnerships in National Cyber-Security Strategies.” *International Affairs* 92, no. 1 (2016): 43–62.
- Chappell, Bill. “FBI Called in after Hacker Tries to Poison Tampa-Area City’s Water with Lye.” *NPR*, February 9, 2021.
<https://www.npr.org/2021/02/09/965791252/fbi-called-in-after-hacker-tries-to-poison-tampa-area-citys-water-with-lye>.
- Clinton, William. *Presidential Decision Directive 63: Critical Infrastructure Protection*. PDD-63. Washington, DC: The White House, 1998.
- Creamer, Emily, Will Eadson, Bregje van Veelen, Annabel Pinker, Margaret Tingey, Tim Brauholtz-Speight, Marianna Markantoni, Mike Foden, and Max Lacey-Barnacle. “Community Energy: Entanglements of Community, State, and Private Sector.” *Geography Compass* 12, no. 7 (May 2018): 1–16.
- Cybersecurity & Infrastructure Security Agency. “Cybersecurity & Infrastructure Security Agency Services Catalog.” Autumn 2020.
https://www.cisa.gov/sites/default/files/publications/FINAL_CISA%20Services%20Catalog%20v1.1_20201029_508_0.pdf.
- Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115–278 (2018). <https://www.congress.gov/bill/115th-congress/house-bill/3359>.

- Department of Energy. “Cybersecurity Research, Development, and Demonstration (RD&D) for Energy Delivery Systems.” Accessed July 10, 2021. <https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and>.
- . “Mission: Department of Energy.” Accessed May 5, 2021. <https://www.energy.gov/mission>.
- . “Offices.” Accessed July 18, 2021. <https://www.energy.gov/offices>.
- Department of Homeland Security. *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013.
- Department of Homeland Security and Department of Energy. “Energy Sector-Specific Plan 2015,” 2015.
- Doss-Gollin, James, David J. Farnham, Upmanu Lall, and Vijay Modi. “How Unprecedented Was the February 2021 Texas Cold Snap?” *Environmental Research: Letters* 16 (June 8, 2021). <https://iopscience.iop.org/article/10.1088/1748-9326/ac0278/pdf>.
- Eitan, Avri, Lior Herman, Itay Fischhendler, and Gillad Rosen. “Community-Private Sector Partnerships in Renewable Energy.” *Renewable and Sustainable Energy Reviews* 105 (2019): 95–104.
- Electricity Information Sharing and Analysis Center. “E-ISAC Long-Term Strategic Plan Update.” Electricity Information Sharing and Analysis Center, October 2020. https://www.eisac.com/cartella/Asset/00009261/2020_E-ISAC_Strategic_Plan_Update_FINAL.docx?parent=127465.
- Electricity Subsector Coordinating Council. “Electricity Subsector Coordinating Council Brochure,” September 2020. https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure.ashx?la=en&hash=00901B6AD252F5AF940C1012619A43C39967F9C9.
- . “Electricity Subsector Coordinating Council Charter.” August 5, 2013. <https://www.cisa.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf>.
- . “ESCC: Electricity Subsector Coordinating Council.” 2021. <https://www.electricitysubsector.org/>.
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013). <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

- Executive Order 13920: Securing the United States Bulk-Power System (2020).
<https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/>.
- Federal Emergency Management Agency. “Building Resilient Infrastructure and Communities (BRIC).” July 1, 2021.
<https://www.fema.gov/grants/mitigation/building-resilient-infrastructure-communities>.
- . “Building Resilient Infrastructure and Communities FY 2020 Subapplication Status.” Accessed July 10, 2021.
<https://www.fema.gov/grants/mitigation/building-resilient-infrastructure-communities/fy2020-subapplication-status>.
- Federal Energy Regulatory Commission. “Electric Power Markets.” October 23, 2020.
<https://www.ferc.gov/industries-data/market-assessments/electric-power-markets>.
- Gilstrap, Matthew, Shravan Amin, and Kevin DeCorla-Souza. *United States Electricity Industry Primer*. DOE/OE-0017. U.S. Department of Energy: Office of Electricity Delivery and Energy Reliability, 2015.
<https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf>.
- Gold, Russell, and Katherine Blunt. “Texas Power Outages to Drag Into Third Day as Deep Freeze Persists.” *Wall Street Journal*. February 16, 2021.
- Halper, Evan, and Marc Lifsher. “Attack on Electric Grid Raises Alarm.” *Los Angeles Times*. February 6, 2014. <https://www.latimes.com/business/la-fi-grid-terror-20140207-story.html#axzz2t2mkWwrd>.
- Hoff, Sara. “U.S. Electric System Is Made up of Interconnections and Balancing Authorities.” Energy Information Agency, July 20, 2016.
<https://www.eia.gov/todayinenergy/detail.php?id=27152>.
- Hoffman, Patricia A. “OE Announces Funding to Improve the Cybersecurity of the Nation’s Power Grid.” Department of Energy. Accessed July 10, 2021.
<https://www.energy.gov/oe/articles/oe-announces-funding-improve-cybersecurity-nation-s-power-grid>.
- Humphreys, Brian E. *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*. CRS Report No. R45809. Washington, DC: Congressional Research Service, 2019.
- Jewell, Jessica, Aleh Cherp, and Keywan Riahi. “Energy Security under De-Carbonization Scenarios: An Assessment Framework and Evaluation under Different Technology and Policy Choices.” *Energy Policy* 65 (2014): 743–60.

- joebiden.com. “Climate: 10 Million Clean Energy Jobs.” February 20, 2021.
<https://joebiden.com/climate-labor-fact-sheet/>.
- Johansson, Bengt. “Security Aspects of Future Renewable Energy Systems—A Short Overview.” *Energy* 61 (2013): 598–605.
- Kwasinski, Alexis, Fabio Andrade, Marcel J. Castro-Sitiriche, and Efrain O’Neill-Carrillo. “Hurricane Maria Effects on Puerto Rico Electric Power Infrastructure.” *IEEE Power and Energy Technology Systems Journal* 6, no. 1 (February 19, 2019): 85–94.
- McGrath, Jenna K. “Will Updated Electricity Infrastructure Security Protect the Grid? A Case Study Modeling Electrical Substation Attacks.” *Infrastructures* 3, no. 53 (November 20, 2018): 1–17.
- McLarty, Thomas F., Thomas J. Ridge, Maxmillian Angerholzer, Frank J. Cilluffo, Dan Mahaffee, and Madeline Vale. *Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid*. Washington, DC: Center for the Study of the Presidency & Congress, 2014.
- . *Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid*. Washington, DC: Center for the Study of the Presidency & Congress, 2014.
- Moteff, John D. *Critical Infrastructures: Background, Policy, and Implementation*. CRS Report No. RL30153. Washington, DC: Congressional Research Service, 2015.
- Nazir, Hasna. “Lessons Learned from the February 2021 Texas Power Outage.” *CERI Electricity Report*, April 2021.
https://ceri.ca/assets/files/Electricity%20Commodity%20Update_April%202021.pdf.
- Obama, Barack. *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*. PPD-21. Washington, DC: The White House, 2013.
<https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
- Phillips, J., M. Finster, J. Pillon, F. Petit, and J. Trail. “State Energy Resilience Framework.” Argonne National Laboratory, December 2016.
- Potomac Electric Power Company. “The Capital Grid Project: Overview,” October 2019.
https://www.pepco.com/MyAccount/MyBillUsage/Documents/CAPITAL%20GRID%20PROJECT%20OVERVIEW%20FACT%20SHEET%20ENG%20-%20OCT%202019_NP%20final.pdf.

- Stark, Cortlynn. "Power Restored after Outage Affected 39,000 in Northwest DC on Saturday." *The Washington Post*, July 28, 2019. https://www.washingtonpost.com/local/dc-politics/2019/07/27/7b6c43cc-b0a3-11e9-a0c9-6d2d7818f3da_story.html.
- Union of Concerned Scientists. "How the Electricity Grid Works," February 17, 2015. <https://www.ucsusa.org/resources/how-electricity-grid-works#.WQeYXFPyuYU>.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. L. No. 107–56 (2001).
- U.S. Department of Energy: Office of Energy Policy and Systems Analysis. *Climate Change and the U.S. Energy Sector: Regional Vulnerabilities and Resilience Solutions*. 2015.
- Vigdor, Neil. "Washington, , Power Failure Affects More Than 30,000 Customers." *The New York Times*, July 27, 2019. <https://www.nytimes.com/2019/07/27/us/dc-power-outage.html>.
- Woods, David D. "Four Concepts for Resilience and the Implications for the Future of Resilience Engineering." *Reliability Engineering and System Safety*, April 3, 2015, 5–9.
- Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired*, March 3, 2016.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California