2023-03

WE ARE ALL GONNA DIE: HOW THE WEAK POINTS OF THE POWER GRID LEAVE THE UNITED STATES WITH AN UNACCEPTABLE RISK

Matthews, Michael D.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WE ARE ALL GONNA DIE: HOW THE WEAK POINTS OF THE POWER GRID LEAVE THE UNITED STATES WITH AN UNACCEPTABLE RISK

by

Michael D. Matthews

March 2023

Co-Advisors: Carolyn C. Halladay
Shannon A. Brown

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE WE ARE ALL GONNA DIE: HOW THE WEAK POINTS OF THE POWER GRID LEAVE THE UNITED STATES WITH AN UNACCEPTABLE RISK	**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael D. Matthews	
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)

Federal regulations aim to ensure grid reliability and harden it against outages; however, widespread outages continue. This thesis examines the spectrum of regulations to evaluate them. It outlines their structure, the regulations' intent, and weighs them against evolving cyber and physical threats and natural disaster risks. Currently, the regulatory structure is incapable of providing uniform security. Federal standards protect only the transmission portion of the grid, leaving the distribution section vulnerable to attack due to varying regulations from state to state, or county to county. The regulations cannot adapt quickly enough to meet dynamic threats, rendering them less effective. Cyber threats can be so agile that protectors are unaware of vulnerabilities, and patching requirements are too lengthy, which increases the risk exposure. No current weather mitigation or standard is capable of protecting the grid despite regular natural disasters that cause power shutdowns. The thesis concludes that bridging these gaps requires not increasing protection standards, but redundancy. Redundancy, mirrored after the UK's infrastructure policy, is more likely to reduce failure risk through layered components and systems. Microgrids are proven effective in disasters to successfully deliver such redundancy and should be implemented across all critical infrastructure sectors.

14. SUBJECT TERMS power grid, redundancy, electrical resiliency, security standards	**15. NUMBER OF PAGES** 87
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

WE ARE ALL GONNA DIE: HOW THE WEAK POINTS OF THE POWER GRID LEAVE THE UNITED STATES WITH AN UNACCEPTABLE RISK

Michael D. Matthews
Protective Security Advisor, Cybersecurity & Infrastructure Security Agency,
Department of Homeland Security
BA, Chapman University, 2009

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
March 2023**

Approved by: Carolyn C. Halladay
Co-Advisor

Shannon A. Brown
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Federal regulations aim to ensure grid reliability and harden it against outages; however, widespread outages continue. This thesis examines the spectrum of regulations to evaluate them. It outlines their structure, the regulations' intent, and weighs them against evolving cyber and physical threats and natural disaster risks. Currently, the regulatory structure is incapable of providing uniform security. Federal standards protect only the transmission portion of the grid, leaving the distribution section vulnerable to attack due to varying regulations from state to state, or county to county. The regulations cannot adapt quickly enough to meet dynamic threats, rendering them less effective. Cyber threats can be so agile that protectors are unaware of vulnerabilities, and patching requirements are too lengthy, which increases the risk exposure. No current weather mitigation or standard is capable of protecting the grid despite regular natural disasters that cause power shutdowns. The thesis concludes that bridging these gaps requires not increasing protection standards, but redundancy. Redundancy, mirrored after the UK's infrastructure policy, is more likely to reduce failure risk through layered components and systems. Microgrids are proven effective in disasters to successfully deliver such redundancy and should be implemented across all critical infrastructure sectors.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BES	bulk electrical system
CIP	Critical Infrastructure Protection
CISA	Cybersecurity & Infrastructure Security Agency
CRS	Congressional Research Service
DC	direct current
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EIA	Energy Information Administration
E-ISAC	Electricity Information Sharing and Analysis Center
EOP	emergency operating procedures
ERO	Electric Reliability Organization
FAA	Federal Aviation Administration
FERC	Federal Energy Regulatory Commission
GAO	Government Accountability Office
ICS	industrial control systems
IDS	intrusion detection system
kV	kilovolts
NERC	North American Electric Reliability Corporation
NYU	New York University
PG&E	Pacific Gas and Electric
SAFETY	Support Anti-terrorism by Fostering Effective Technologies
TSA	Transportation Security Administration
V	volts

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis explores the potential causes behind widespread power outages despite federal reliability standards designed to prevent these disruptions. It compares federal protection mandates against increasingly common physical threats, agile cyber threats, and natural disasters. This thesis finds that the grid is not secure or resilient because widespread outages continue despite the existing federal protection standards.

The federal government's regulatory power grid protection structure is convoluted. Federal regulations task the Federal Energy Regulatory Commission (FERC) with grid resilience. In turn, FERC designated North American Electric Reliability Corporation (NERC), a non-profit organization, with grid reliability. In this role, NERC employs regional entities, separate organizations not affiliated with NERC nor FERC, to enforce standards.[1] In summary, regional entities enforce grid reliability standards that NERC creates and FERC approves. No single responsible agency or body ensures the nation's most critical infrastructure system is secure.

NERC's reliability standards have historically addressed the threat of yesterday and not the threats of tomorrow. NERC's CIP standards have not stopped kinetic attacks, nor cyber threats. Unknown vulnerabilities or risks, called Zero Day, persist throughout the critical infrastructure community. Zero Day threats can be severe vulnerabilities, but NERC standards (CIP-007) allow 35 days to apply a patch, a significant lag in cybersecurity.[2]

Unlike physical and cyber threats, natural disasters consistently wreak more havoc on the grid, but NERC lacks appropriate reliability standards to mitigate disaster risk. Hurricanes, wildfires, and severe winter storms have devastated grid operations and caused

[1] North American Electric Reliability Corporation, "ERO Enterprise | Regional Entities," About NERC – Key Players, accessed December 30, 2022, https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx.

[2] North American Electric Reliability Corporation, *Reliability Standards for the Bulk Electric Systems of North America* (Atlanta, GA: North American Electric Reliability Corporation, 2022), 356, https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf.

outages. Currently, only one enforced standard addresses adverse weather, but it focuses on emergency grid operations in response to impacts, not mitigating them. NERC's absence of disaster mitigation standards creates greater grid vulnerability.

Regardless of these gaps, increasing reliability standard strictness or expanding existing resilience requirements is unlikely. NERC's standard creation and approval process are consensus-based. It allows energy providers a vote in compliance language.[3] Power providers have also dodged federal regulations by not upgrading or removing equipment that would require compliance.[4] Even if all organizations complied with NERC's standards, most of the grid (the distribution portion) is not subject to regulatory compliance. Yet the distribution portion of the grid accounts for 94 percent of the outages.[5] Furthermore, the regional entities vary in their approach and view of risk.[6] Since standards are enforced differently across the nation, uniform security cannot be achieved. Therefore, achieving electrical resilience merits considering a different approach using redundancy rather than raising physical and cyber security standards.

What if the United States employed redundant electrical capabilities to achieve power grid security instead of raising physical and cyber security standards? For comparison, the United Kingdom (UK) approaches infrastructure security through redundancy. Redundancy focuses on having backup capabilities to take over infrastructure delivery if the primary methods fail. The UK has found that redundancy is more cost-efficient than hardening single sites for specific threats.[7] As such, the UK's Civil

---

[3] Richard Humphreys, *Critical Infrastructure Security and Resilience: Countering Russian and Other Nation-State Cyber Threats*, CRS Report No. IF12061 (Washington, DC: Congressional Research Service, 2022), 2, https://sgp.fas.org/crs/homesec/IF12061.pdf.

[4] Marlene Z. Ladendorff, "The Effect of North American Electric Reliability Corporation Critical Infrastructure Protection Standards on Bulk Electric System Reliability" (PhD diss., Capella University, 2014), 109, ProQuest.

[5] Joseph H. Eto et al., "Distribution System Versus Bulk Power System: Identifying the Source of Electric Service Interruptions in the Us," *IET Generation, Transmission & Distribution* 13, no. 5 (2019): 717, https://doi.org/10.1049/iet-gtd.2018.6452.

[6] Ladendorff, "Effectiveness of NERC CIP Standards," 109.

[7] Civil Contingencies Secretariat, *Keeping the Country Running: Natural Hazards and Infrastructure* (London: Civil Contingencies Secretariat, Cabinet Office, 2011), 52, https://www.gov.uk/government/publications/strategic-framework-and-policy-statement-on-improving-the-resilience-of-critical-infrastructure-to-disruption-from-natural-hazards.

Contingencies Secretariat states, "Critical circuits will have two levels of redundancy so that in the event of any minor faults, the service will remain operational."[8] An outage's risk diminishes when multiple backups are in place to support damaged components. Thus, redundancy is a successful route to electrical continuity.

Microgrids are another option to instill reliability in grid operations. Microgrids have established themselves as reliable, stable, and resilient electrical solutions. Microgrids remained functional during disasters or otherwise affected areas where legacy grid components did not.[9] Moreover, the Department of Defense (DOD) has employed microgrids to ensure it can defend the nation regardless of the larger grid's current operation.[10] Due to the reliability of microgrids, scholars suggest the federal government fund microgrids for critical facilities such as hospitals.[11] Microgrids must be a part of the nation's electrical resilience discussion.

Research points toward mandated redundancy. Microgrids can achieve this redundancy. Microgrid grant options or federal incentives should be examined further to promote electrical resilience. Similarly, the distribution grid should be brought into federal regulatory oversight to ensure a more uniform grid security standard. Lastly, cyber patching requirements should be reduced from 35 days to 48 hours, reducing the time the risk is exposed. Electrical resilience is achievable, but only if significant changes are made.

---

[8] Civil Contingencies Secretariat, 30.

[9] David O. Jones, "Reliability and Resilience Evaluation of a Stand-Alone Mobile Microgrid-Analysis and Experimental Measurements" (master's thesis, Naval Postgraduate School, 2022), 76, https://hdl.handle.net/10945/71070.

[10] H.R., *Lessons Learned from the Texas Blackouts: Research Needs for a Secure and Resilient Grid*, House of Representatives, 117th Cong., 1st sess. (2021), March 2021, 124, https://www.govinfo.gov/app/details/CHRG-117hhrg43633/CHRG-117hhrg43633/context.

[11] Tara Kirk Sell, Onora Lien, and Eric Toner, "A Framework for Healthcare Resilience during Widespread Electrical Power Loss," *Journal of Critical Infrastructure Policy* 1, no. 1 (Spring 2020): 22, https://doi.org/10.18278/jcip.1.1.3.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I am grateful for my wife Sarah's steadfast and steady support. Sarah has stood by me without question, constantly pushing me forward. Seeing her smile as I walk out of a class or a long thesis revision session was the perfect medicine to continue the day. I missed a lot of my best friend since starting this program, and I'm looking forward to resuming our blessed life together. I am thankful to my four amazing children, Kie, Noah, Emma and Jacob, who all weathered my academic storm. Thanks for the understanding and patience when I had none.

I want to thank the leadership of the Cybersecurity & Infrastructure Security Agency (CISA) Region 9 for their endorsement and support over the past 18 months. Allowing an employee to dedicate half (or more) of their work time to this program is a significant commitment and speaks to our regional leadership's quality. Along those lines, I'm thankful for my partners who backfilled my absences while on travel. From wildfires to critical assessments, my peers covered me without question—thank you.

Last and certainly not least, the Center for Homeland Defense & Security (CHDS) thesis team. A particular thank you goes to Marianne Taflinger and Greta Marlatt, and to Michael Thomas of the NPS Graduate Writing Center, who delivered me from "close but not quite there" to "done." Their guidance and seemingly endless reviews were instrumental to finishing. Finally, I'd like to thank my advisors, Dr. Carolyn Halladay and Dr. Shannon Brown. Their consistent leadership, thoughts, and handling kept this thesis on track and prevented it from becoming "an attack template" for our adversaries. I am appreciative of their detailed reviews and encouraging Zoom sessions.

In keeping with the theme of power grid reliability, I'm also thankful for my household generator for keeping my household items and laptop powered during a 78-hour winter power outage while trying to finish this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In the early morning hours of April 2013, an unknown person or persons attacked Pacific Gas and Electric's (PG&E) Metcalf Substation.[1] This substation, located on the outskirts of San Jose, California, is a 500-kilovolt (kV) (a kilovolt is 1,000 volts) substation critical for transmitting high voltage across the grid. Attackers cut fiber optics lines that PG&E used to monitor the substation, and then, from a nearby hill, shot more than 100 rounds into the oil tanks and transformers. The perpetrator(s) destroyed 17 of the 19 transformers, dropping power to portions of the San Jose area for four hours and costing PG&E more than $15 million in repairs and another $100 million in upgrading the substation's security.[2] It took four weeks to restore the substation's capabilities and resume entire operations. PG&E and the South Bay Area of California escaped severe punishment in many ways. At least one scholar has warned that "more coordination and firepower" would have led to "disaster" and drastically increased outages.[3]

Congressional reports have cited other attacks similar to the Metcalf attack, including significant incidents in Arkansas and Florida. In both attacks, someone disabled an electrical substation with a rifle. Although these incidents demonstrate the vulnerability of high-voltage transformer stations to the threat posed by kinetic attacks, the power grid's reliability is threatened by a variety of other risks as well, including natural disaster, cyberattacks and supply chain issues. For example, hurricanes Katrina (Louisiana), Sandy

[1] Rich Heidorn Jr., "Substation Saboteurs 'No Amateurs,'" RTO Insider, November 15, 2013, https://www.rtoinsider.com/articles/23246-substation-saboteurs-no-amateurs-; National Academies of Sciences, Engineering, and Medicine, *Enhancing the Resilience of the Nation's Electricity System* (Washington, DC: National Academies Press, 2017), https://doi.org/10.17226/24836.

[2] Paul Parfomak, *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, CRS report No. R43604 (Washington, DC: Congressional Research Service, 2014), 19.

[3] Brendan Teague, TJ Goss, and Mark Weiss, "Applying Risk and Resilience Metrics to Energy Investments" (MBA professional report, Naval Postgraduate School, 2015), 5, https://hdl.handle.net/10945/47883.

(New York area), Rita (Texas), and the 2021 Texas Winter Storm significantly damaged grid components and impeded electricity transmission.[4]

As a result of the Metcalf attack, the Department of Energy tasked the North American Electric Reliability Corporation (NERC) to create security standards, commonly called the "Critical Infrastructure Protection (CIP) Standards."[5] But the CIP standards that were created still do not address all threats to the grid. Even if the physical standards (addressed by CIP-014) managed to halt all physical attacks, the other threats remain.

An examination of the risks related to supply-chain and manufacturing issues may prove useful in illustrating how even mundane repair issues introduce undue risk to the nation's critical power grid. The security standards in place, for example, do not address the lag time associated with supply-chain and manufacturing issues. Some grid components are custom manufactured, and the wait time can be nearly two years.[6] NERC's report summarizing the 2009 workshop advised that outages could be expected to range from months to years while components were purchased, manufactured, and installed.[7] NERC further advised that the grid could potentially be unable to deliver electricity to end users for months to years.[8] In "An Assessment of Threats to the American Power Grid," Matthew Weiss and Martin Weiss discuss a potential three-year wait for high-voltage transformers at the cost of $10 million apiece.[9] Citing a Federal Energy Regulatory Commission (FERC)

---

[4] Department of Homeland Security, *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long Term Power Outage* (Washington, DC: Department of Homeland Security, 2017), https://www.fema.gov/sites/default/files/2020-07/fema_incident-annex_power-outage.pdf; Marcy de Luna and Amanda Drane, "What Went Wrong with the Texas Power Grid?," *Houston Chronicle*, February 16, 2021, https://www.houstonchronicle.com/business/energy/article/Wholesale-power-prices-spiking-across-Texas-15951684.php.

[5] "Project 2014–04 Physical Security," NERC Standards, May 7, 2015, https://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx.

[6] Parfomak, *Physical Security of the U.S. Power Grid*, 4.

[7] North American Electric Reliability Corporation and Department of Energy, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* (Washington, DC: Department of Energy, 2010), 12.

[8] North American Electric Reliability Corporation and Department of Energy, 88.

[9] Matthew Weiss and Martin Weiss, "An Assessment of Threats to the American Power Grid," *Energy, Sustainability and Society* 9, no. 1 (2019): 2, https://doi.org/10.1186/s13705-019-0199-y.

memorandum, the Weisses further suggest that coordinated attacks could potentially knock out the nationwide grid for eighteen months or longer.[10]

Natural disasters are likewise illustrative of the risks to the national infrastructure. In the 2021 Texas winter outage, more than 4 million people were left without power, and complete restoration took anywhere from one to several days.[11] The system demonstrated limited redundancies, or points of overlap which may be relied on when one or more other sources fail. Redundancy has emerged as one of the critical lessons of the Texas outage. Yet outside of a few niche industries, little literature covers the 200 "redundant capabilities that saved Texas."[12] Along the same lines, media coverage of the recovery from Hurricane Sandy did not discuss redundant capabilities or, most notably, New York University's (NYU's) microgrid, which remained operational during the Sandy-caused grid failure.[13] Unfortunately, news of the widespread failure overshadowed the success of the small but capable NYU microgrid.

Most microgrids are redundant to the grid—that is, the facilities that make up a microgrid are generally already connected to the larger grid.[14] A microgrid provides a redundant source of power.[15] Furthermore, most microgrids are powered by several sources of electrical production.[16] Within a microgrid are redundancies, which improves their ability to provide power during outages. Microgrids may be usefully compared to the generators that families and businesses across the nation purchase for backup power. Tesla created a "Power Wall" that provides redundant backup power via a bank of lithium

---

[10] Weiss and Weiss, 6.

[11] de Luna and Drane, "What Went Wrong with the Texas Power Grid?"

[12] Elisa Wood, "Microgrids Help Texas as It's Forced to Undertake Rolling Blackouts," Microgrid Knowledge, February 16, 2021, https://microgridknowledge.com/microgrids-texas-blackouts/.

[13] Jeremy Deaton, "Here's Why the Lights Stayed on at NYU While the Rest of Lower Manhattan Went Dark During Hurricane Sandy," *Business Insider*, June 11, 2016, https://www.businessinsider.com/new-york-microgrids-2016-6.

[14] Kelsey Adkisson, "Are Microgrids a Key to Grid Resiliency?," Pacific Northwest National Laboratory, December 2, 2021, https://www.pnnl.gov/news-media/are-microgrids-key-grid-resiliency.

[15] Adkisson.

[16] Adkisson.

batteries.[17] National Laboratories, the official U.S. government-funded research labs, acknowledge the benefits of redundant systems through extensive studies.[18] Redundancy arguably lowers the risk to the grid more substantially than hardening locations through layers of security.[19] After all, hurricanes easily bypass both physical security and cybersecurity protection standards. Perhaps electrical resilience is not achieved through higher security standards but through redundant capabilities.

A. RESEARCH QUESTION

Given the vulnerability of the power grid to a variety of physical, natural, cyber, and supply chain threats, what protective measures--ranging from regulatory initiatives to infrastructure measures--are most likely to address multiple simultaneous threats to the power grid?

B. LITERATURE REVIEW

This literature review examines the well-documented concerns about grid vulnerabilities and the hesitancy to address grid security. The risk to the grid is well-known and substantial. Improving the grid's dependability has been attempted since at least the 1960s.[20] This literature review also discusses power grid reliability and the risk to that reliability[21] and highlights grid protection regulations and the outages that continue despite the protections in place.

---

[17] "Powerwall," Tesla, accessed March 15, 2022, https://www.tesla.com/powerwall.

[18] Sean J. Ericson and Daniel R. Olis, *A Comparison of Fuel Choice for Backup Generators*, NREL/TP-6A50-72509 (Golden, CO: National Renewable Energy Laboratory, 2019), https://doi.org/10.2172/1505554.

[19] Civil Contingencies Secretariat, *Keeping the Country Running*, 52.

[20] S, *Electric Power Reliability: Hearing before the Committee on Commerce*, Senate, 90th Cong., 1st sess., August 22, 1967, ProQuest.

[21] David B. Hinchman, *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance*, GAO-22-105103 (Washington, DC: Government Accountability Office, 2022), https://www.gao.gov/products/gao-22-105103; Richard J. Campbell, *Electric Grid Cybersecurity*, CRS Report No. R45312 (Washington, DC: Congressional Research Service, 2018), https://crsreports.congress.gov/product/pdf/R/R45312/2; Trevor Maynard and Nick Beecroft, *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*, Lloyd's Emerging Risk Report – 2015 (London: Lloyds of London and University of Cambridge, 2015), https://www.lloyds.com/news-and-insights/risk-reports/library/business-blackout; and North American Electric Reliability Corporation and Department of Energy, *High-Impact, Low-Frequency Event Risk*.

1. Risks to the Grid

As loosely implied by Zhen Zhang in "Environmental Review & Case Study: NERC's Cybersecurity Standards for the Electric Grid: Fulfilling Its Reliability Day Job and Moonlighting as a Cybersecurity Model," the grid evolves as technology evolves, and as the grid evolves, so do its risks.[22] Electrical security and resiliency, however, significantly lag the risk curve. Weiss and Weiss state that the threat to the grid grows more quickly than the ability to address the new vulnerabilities.[23] Along these lines, the Department of Energy (DOE) has stated it must prioritize some risks while omitting others.[24] As reported by the Government Accountability Office (GAO), industrial control systems (ICS) used to control grid operations are susceptible to a higher risk. As the GAO reported, as remote monitoring or remote access to the ICS increases, so does the opportunity for attack.[25]

According to government reports, previous attempts to reduce risk to the power grid have failed, including regulation and resource allocation. The GAO released reports depicting the shortfalls of the federal government's ability to protect the grid as early as 1981.[26] Moreover, the GAO published additional reports (March 2021 and April 2022) declaring the federal government is "inadequate" to address the risk.[27]

While federal agencies highlight grid vulnerabilities, academics, such as Robert W. Rose, and experts, such as Sean S. Baggott and Joost R. Santos, introduce systematic ways to address risk. In his Naval Postgraduate School (NPS) master's thesis, Rose developed a

---

[22] Zhen Zhang, "Environmental Review & Case Study: NERC's Cybersecurity Standards for the Electric Grid: Fulfilling Its Reliability Day Job and Moonlighting as a Cybersecurity Model," *Environmental Practice* 13, no. 3 (September 2011): 250, https://doi.org/10.1017/S1466046611000275.

[23] Weiss and Weiss, "Grid Threat Assessment," 6.

[24] Frank Rusco and Nick Marinos, *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, GAO-21-81 (Washington, DC: Government Accountability Office, 2021), 31, https://www.gao.gov/assets/gao-21-81.pdf.

[25] Rusco and Marinos, 11.

[26] Chuck Young, *Federal Electrical Emergency Preparedness Is Inadequate*, EMD-81-50 (Washington, DC: Government Accounting Office, 1981), https://www.gao.gov/assets/emd-81-50.pdf.

[27] Tina Won Sherman, *Critical Infrastructure Protection: DHS Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure*, GAO-22-105973 (Washington, DC: Government Accountability Office, 2022), https://www.gao.gov/products/gao-22-105973.

model to protect the grid with "limited defensive resources."[28] Rose's limited-response model could suggest even the protector's lack of urgency to protect the grid or the threat is too pervasive to adequately shield the nation, hence the limited defensive resources. Baggott and Santos, in addition to their research published in the *Risk Analysis Journal*, have developed models that can address the overall risk to the grid.[29] While some models aim to improve the operational employment of automated systems, others focus on targeted security upgrades based on the risk of loss. Creating novel methods to address grid reliability would not be necessary if standards adequately addressed the risks.

Based on a congressional research report by Paul W. Parfomak, *Physical Security of the U.S. Power Grid*, the deficiencies of the electrical grid and its capacity for resilience are compounded through the grid's supply chain.[30] Physically damaged equipment highlights this phenomenon. Parfomak states that in the case of high-voltage transformers, the wait time for a replacement part can range from five months to nearly two years, depending on the particular piece of equipment.[31] The bigger the transformer, the more custom engineering and design are required. The report mentions that high-voltage systems are custom designed, and are not interchangeable.[32] Parfomak expands on this predicament by stating that, as of 2014, only five manufacturers within the United States could produce the biggest, and, arguably, the most critical transformers.[33] A 2009 DOE report indicates that "little manufacturing capability" remains in the United States.[34] The report states that

[28] Robert W. Rose, "Defending Electrical Power Grids" (master's thesis, Naval Postgraduate School, 2007), 1, https://hdl.handle.net/10945/3677.

[29] Sean S. Baggott and Joost R. Santos, "A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid," *Risk Analysis* 40, no. 9 (September 2020): 1744–61, https://doi.org/10.1111/risa.13511; Teague, Goss, and Weiss, "Applying Risk to Energy Investments"; and Clark Petri, "Assessing the Operational Resilience of Electrical Distribution Systems" (master's thesis, Naval Postgraduate School, 2017), https://hdl.handle.net/10945/56166.

[30] Parfomak, *Physical Security of the U.S. Power Grid*.

[31] Parfomak, 4.

[32] Parfomak, 4.

[33] Parfomak, 5.

[34] North American Electric Reliability Corporation and Department of Energy, *High-Impact, Low-Frequency Event Risk*, 12.

essential equipment has "lower overall inventory levels."[35] The GAO also observes and reports supply chain risk from a cybersecurity standpoint.[36] These increasing risks to the grid are well known and raise the threat of an extended outage while awaiting replacement parts, echoing Parfomak's contention that poor manufacturing resources increase the risk to the grid.

2. Hindrances in Improving Federal Protection Regulations

The answer to these multiple threats and varieties of risk has, since the 1960s, been sought in part through federal regulations and an increase in federal funding. Yet Parfomak points out that one risk to grid security is the difficulty of procuring funds meant to address grid security.[37] Matthew E. McQuinn, in his master's thesis "Energy Regulation Effects on Critical Infrastructure Protection," also cites lack of funding as a contributing factor, observing that companies are reluctant to pay for cyber or physical security upgrades, especially in their transmission infrastructure. According to McQuinn, a single company upgrade can benefit others without a similar competitor investment because most companies use transmission architecture regardless of ownership. In other words, a trucking company would not likely pay to upgrade road surfaces because it helps competitors as much as themselves. It would be financially safer to develop better tires for their own company than improve the road.[38]

Government attempts to mandate security upgrades tend to fail, at least in recent efforts. Congressional legislation, for example, allows power companies to regulate themselves by enacting their own security mandates.[39] Further, the Department of Homeland Security, arguably the agency with the most advanced expertise in hazards and

---

[35] North American Electric Reliability Corporation and Department of Energy, 30.

[36] Rusco and Marinos, *Electricity Grid Cybersecurity*.

[37] Paul Parfomak, *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?*, CRS Report No. R45135 (Washington, DC: Congressional Research Service, 2018), 18, https://sgp.fas.org/crs/homesec/R45135.pdf.

[38] Matthew E. McQuinn, "Energy Regulation Effects on Critical Infrastructure Protection" (master's thesis, Naval Postgraduate School, 2008), 38, https://hdl.handle.net/10945/3753.

[39] Parfomak, *NERC Standards for Bulk Power Physical Security*, 17.

threats, has no regulatory power over electrical infrastructure.[40] Yet, according to McQuinn, "most authors agree that companies have not invested sufficiently in infrastructure capability and security."[41] Congressional reports conclude that regulations have improved security but have not "reached the level of physical security needed based on the sector's assessment of risk."[42] GAO reports echo the same warning: "plans do not fully address risks to the grid's distribution systems."[43]

Counterintuitively, government oversight may decrease rather than increase infrastructure security; McQuinn argues that increasing regulations decrease overall security.[44] Charles P. Young's master's thesis, "Method or Madness: Federal Oversight Structures for Critical Infrastructure Protection," indicates other infrastructure sectors report the same plight.[45] Young even contends that the regulator role of the government hurts infrastructure restoration times.[46] Nicholas Catrantzos, in his master's thesis "No Dark Corners: Defending against Insider Threats to Critical Infrastructure," explains that grid ownership further complicates holistic security upgrades and repairs because 85 percent of critical infrastructure is privately owned and operated.[47] The Energy Information Administration (EIA) cites a slightly different ownership figure: approximately 77 percent is not publicly owned.[48] Michael S. Schaefer's NPS thesis, "Operating in Uncertainty; Growing Resilient Critical Infrastructure Organizations," implies that moving private infrastructure companies into the "publicly owned" arena may

---

[40] McQuinn, "Energy Regulation Effects," 6.

[41] McQuinn, 7.

[42] Parfomak, *NERC Standards for Bulk Power Physical Security*.

[43] Rusco and Marinos, *Electricity Grid Cybersecurity*.

[44] McQuinn, "Energy Regulation Effects."

[45] Charles P. Young, "Method or Madness: Federal Oversight Structures for Critical Infrastructure Protection" (master's thesis, Naval Postgraduate School, 2007), v, https://hdl.handle.net/10945/3022.

[46] Young, i.

[47] Nicholas Catrantzos, "No Dark Corners: Defending against Insider Threats to Critical Infrastructure" (master's thesis, Naval Postgraduate School, 2009), 6, https://www.hsdl.org/c/abstract/?docid=33503.

[48] "Electric Sales, Revenue, and Average Price," Electricity, October 6, 2022, https://www.eia.gov/electricity/sales_revenue_price/.

not work either. Schaefer suggests that publicly owned and operated utilities are not agile enough to meet the threat environment, let alone the incredibly dynamic cyber threats.[49] Optional standards are not much better. Young concludes that "Voluntary compliance" fails to achieve the expected outcome.[50] Ronald L. Lendvay, writing on cyber defense and infrastructure, and Gregory M. Jaksec, writing on the need for public and private defense in infrastructure, suggest incentives may motivate voluntary adherence to federal standards, slightly supporting Young's position, in their own NPS master theses.[51] But the nation's most critical infrastructure remains vulnerable to a variety of threats while a hodgepodge of companies, headed by owners with different motivations and financial goals, delay maintenance for monetary and competitive reasons while the government relies on voluntary compliance.

C. RESEARCH DESIGN

This thesis examines the power grid and the variety of physical, natural, cyber, and supply chain threats it faces, and thus reviews the security regulations currently in place, exploring the extent to which the standards adequately protect against the risk of power disruption from any of these causes. It will identify the most critical gaps that threaten national security and provide policy recommendations needed to bridge those gaps.

Scholarly journals, theses, published books, news sources, and federal grid security regulations form the basis of research covering risks and security solutions. The sources of incident data and post-regulation implementation will be news reporting and the Department of Energy's incident database.[52] The incident database assesses these incidents

[49] Michael L. Schaefer, "Operating in Uncertainty; Growing Resilient Critical Infrastructure Organizations" (master's thesis, Naval Postgraduate School, 2011), v, https://www.hsdl.org/?abstract&did=5540.

[50] Young, "Method or Madness," 58.

[51] Ronald L. Lendvay, "Shadows of Stuxnet: Recommendations for U.S. Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack" (master's thesis, Naval Postgraduate School, 2016), https://www.hsdl.org/?abstract&did=792239; Gregory M. Jaksec, "Public-Private-Defense Partnering in Critical Infrastructure Protection" (master's thesis, Naval Postgraduate School, 2006), https://www.hsdl.org/?abstract&did=461639.

[52] "Electric Disturbance Events (OE-417) Annual Summaries," Office of Cybersecurity, Energy Security, & Emergency Response, accessed April 14, 2022, https://www.oe.netl.doe.gov//OE417_annual_summary.aspx.

against the regulations to determine whether the mandates are sufficient to ensure grid resilience. With respect to recommendations to strengthen grid resilience, this thesis relies on journals, theses, and books focused on evolving risk and ongoing incidents. Congressional testimony, National Laboratory reports and studies, and emerging technologies are also included in the research. Additionally, grid protection strategies from other countries, as applicable, are drawn upon for reference.

Open-source information from government channels has been reviewed, omitting all restricted information, including detailed information about vulnerability exploitation. Since this thesis does not examine how the grid *could* be compromised, only how it *has* been compromised, this open-source information is useful for its insights into the nature of regulation changes in the aftermath of incidents. The only hypothetical scenarios are based on actual events.

D. THESIS OVERVIEW

The thesis is divided into five chapters. Chapter I reviews the literature and the variety of incidents, threats, and regulatory initiatives that have been attempted and the gaps that persist. Chapter II offers a primer on grid transmission and architecture, as well as a review of regulatory structure and grid-focused standards. Chapter III provides an assessment of current regulations and their efficacy in the context of the multiple threats to the grid. Chapter IV offers three policy options and critiques of their abilities to realistically bridge existing regulatory gaps. Chapter V summarizes findings, provides recommendations, and points the way to future research.

II. A PRIMER ON THE GRID AND FEDERAL REGULATIONS

On December 3, 2022, an attack on two power substations in rural North Carolina blacked out approximately 40,000 customers for several days and required a mandatory curfew–an act facilitated by a regulatory loophole, carried out by unknown assailants with firearms.[53] As North Carolina demonstrated, physical attacks on the grid are likely to continue and vulnerabilities to remain open to exploitation. Cyber vulnerabilities continue to be highlighted through zero-day attacks as well. In response to these and other threats, the industry has taken action to improve grid security and ensure reliable operations, primarily through regulatory initiatives referred to hereafter as regulations and standards.

Industry and government regulations, however, face the challenge not only of adequately protecting the grid, but of instilling increased resilience. To achieve these critical goals, electricity organizations are given "considerable discretion" regarding risk assessment and adherence to security plans, and the question of self-governance as a viable path to electrical resilience has begun to loom large.[54] The degree of discretionary latitude inherent in self-governance does not inspire confidence at a time when electrical substations can be put out of commission with a rifle. Many more factors, including insufficient protective measures, minimal criteria to meet baseline levels of satisfactoriness, the normal susceptibility to accident and incompetence, and incidental regulatory loopholes, emerge as concerns on par with physical attacks.

This chapter provides an overview of the grid and federal regulations as of this writing, along with some analysis of the degree to which current regulations may—or may not—be considered commensurate with today's fast-paced threats.

---

[53] Nicole Grether et al., "North Carolina County Announces Curfew as Nearly 40,000 Customers Remain without Power after 2 Substations Damaged by Gunfire," CNN, December 2022, https://www.cnn.com/2022/12/04/us/power-outage-moore-county-criminal-investigation?cid=external-feeds_iluminar_msn; Miranda Willson, "North Carolina Substation Attack Exposes Grid Risks," *Energywire*, December 7, 2022, https://www.eenews.net/articles/n-c-substation-attack-exposes-grid-risks/.

[54] Parfomak, *NERC Standards for Bulk Power Physical Security*, 17.

A. TRANSMISSION AND DISTRIBUTION OF ELECTRICITY TO THE GRID

To begin, not all aspects of the grid are subject to federal regulation. For example, federal regulations generally cover the grid components called the bulk electrical or transmission system, defined as 200kV and above.[55] In contrast, the distribution system, which is below the 200kV threshold, does not fall under federal governance, but, rather, private ownership. Figure 1 depicts the electrical system and its different components.

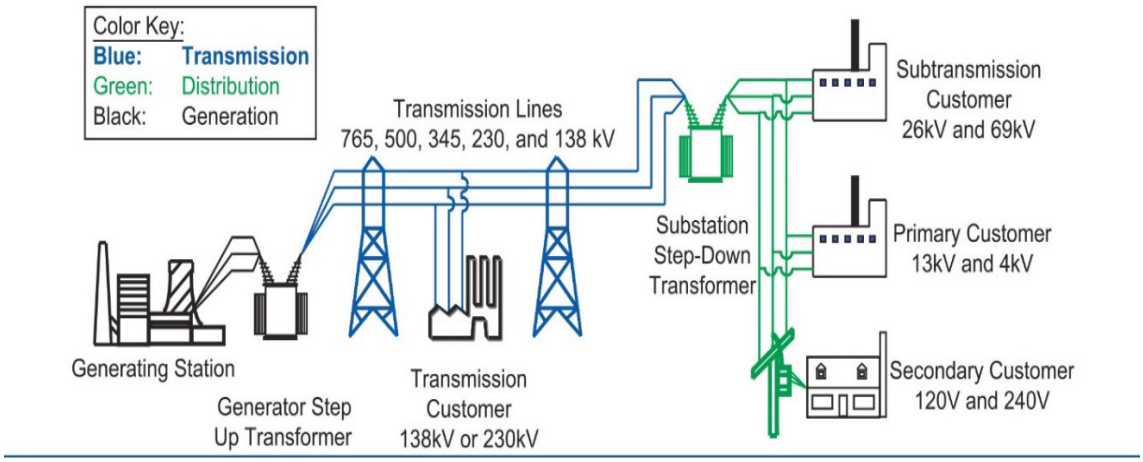

Figure 1. An Overview of the Electrical System[56]

Starting with the black lines on the left side of the picture, power-generating stations create electricity from solar, wind, coal, natural gas, or nuclear, to name a few. The Department of Energy (DOE) explains that power travels through a "step up" transformer which amplifies it significantly to travel more efficiently and effectively.[57] The DOE describes that once the energy leaves the step-up substation, it enters the "transmission" system, the blue lines in Figure 1. The transmission system conveys electricity at a very

[55] North American Electric Reliability Corporation, *NERC Reliability Standards*.

[56] Source: "Electrical Power Transmission and Distribution," Renewable Energy, September 21, 2016, https://www.nps.gov/subjects/renewableenergy/transmission.htm.

[57] Office of Electricity Delivery and Energy Reliability, *United States Electricity Industry Primer*, DOE/OE-0017 (Washington, DC: Department of Energy, 2015), 13, https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf.

high voltage; along the way, some customers receive it in this form. The DOE further explains that electricity then travels to a "step down" transformer which reduces the voltage, similar to diverting water from the city main beneath the street to smaller pipes that deliver water into and within a home. This step, depicted with green lines, begins the "distribution" system of the overall power grid. As depicted by DOE and Figure 1, the distribution grid delivers electricity to commercial and residential customers.

Transmission and distribution systems fulfill entirely different objectives. The transmission system aims to move vast quantities of electricity across distances using extremely high voltages ranging from 138 to 765 kilovolts (kV). The distribution system, after the stepdown, delivers low-voltage electricity (69kV to 120V) to end users within a small geographic area. Federal security standards and regulations mainly apply to the transmission system because its voltages are above 200kV (see Figure 2). The distribution system is only minimally subject to federal regulations.

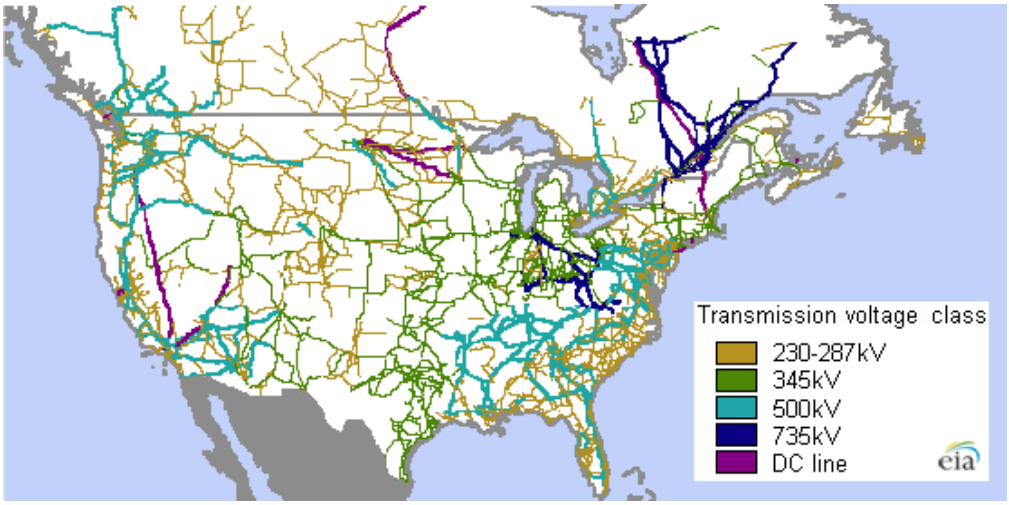

Figure 2. Transmission System[58]

The grid's complicated and convoluted nature and fragmented ownership make regulation and oversight difficult. Maps of the distribution system are generally unavailable

[58] Source: "Canada Week: Integrated Electric Grid Improves Reliability for United States, Canada," Today in Energy, November 27, 2012, https://www.eia.gov/todayinenergy/detail.php?id=8930.

because nearly every city street may have power lines. Company ownership is equally convoluted and comprises of private and for-profit companies, government utilities, co-operatives, and non-profit corporations. According to the U.S. Energy Information Administration, of the approximately 1,648 different electrical utilities, 484 are privately held, five are federally owned, nine are owned by states, and municipalities oversee 369.[59] The remaining vary between "Behind the Meter" (e.g., residential solar panels), co-operatives, Retail Power Marketers (seller of electricity to other utilities), and "other," or all of which create a complicated system of ownership and oversight. Co-operatives, non-profits, and government-owned utilities pursue competing interests and, based on the jurisdiction, may observe greater or lesser oversight than a neighboring utility. The lack of regulation uniformity over the entire grid adds complexity and invites risk to the grid through those facilities operating with weaker protection measures.

B. THE REGULATORY STRUCTURE

This section briefly outlines the federal electrical regulation organizations, their regulatory authorities, and the specific security regulations as they apply to the power grid. In summary, the electrical grid regulatory landscape is inefficient and convoluted, with varied enforcement standards, increasing risk and inviting catastrophe.

Power grid oversight is convoluted because Congress ultimately delegates authority to a nonprofit organization that creates but does not actually enforce their own standards. Congress delegates energy regulation authority to the Federal Energy Regulatory Commission (FERC).[60] FERC, in turn, delegates electricity regulation to the North American Electrical Reliability Corporation (NERC), a non-profit organization.[61] But FERC does not enforce NERC standards; instead, six organizations called regional entities

[59] Energy Information Administration, "Electric Sales, Revenue, and Average Price."

[60] "Frequently Asked Questions (FAQs) About FERC," What is FERC?, January 25, 2022, https://www.ferc.gov/about/what-ferc/frequently-asked-questions-faqs/frequently-asked-questions-faqs-about-ferc.

[61] North American Electric Reliability Corporation, *NERC Frequently Asked Questions* (Atlanta, GA: North American Electric Reliability Corporation, 2013), 3, https://www.nerc.com/AboutNERC/Documents/NERC%20FAQs%20AUG13.pdf.

enforce regulations.[62] This structure creates regulatory difficulties in that a single point of responsibility is lacking.

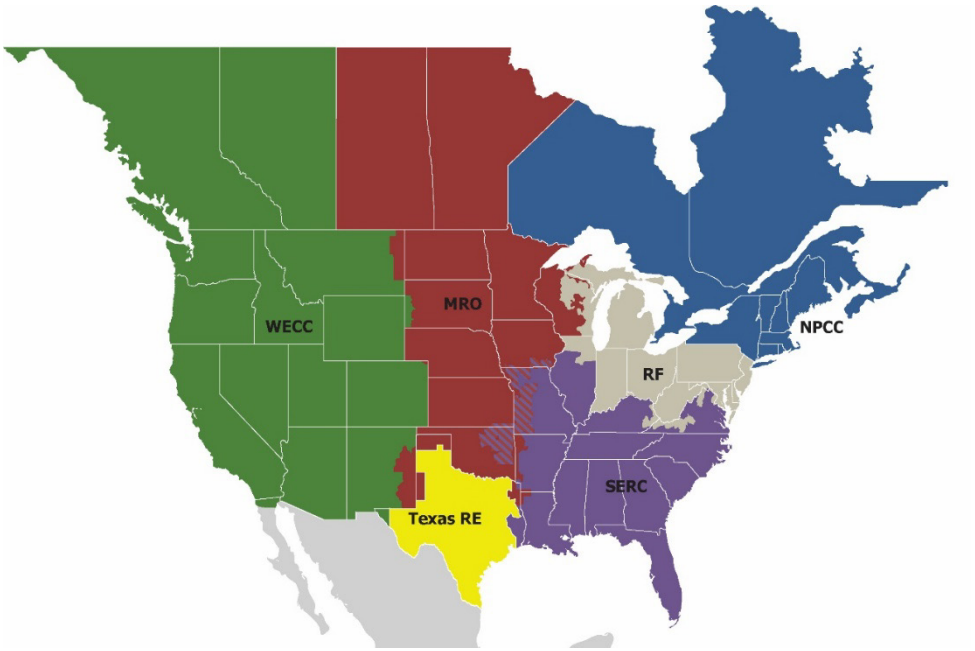

Figure 3. NERC's Regional Entities[63]

NERC, the federal government's regulation organization, reflects successive revising in response to ongoing needs. NERC was formed in 1968 as a council by twelve large utility organizations following the 1965 Northeast Blackout.[64] NERC desired to address grid reliability from within the industry itself.[65] At the time, NERC authored best practice standards designed to increase the reliability and coordination of the transmission system and help develop adequate future transmission system planning.[66] Up until 2005, compliance was voluntary. The 2003 Northeast Blackout demonstrated that voluntary

[62] North American Electric Reliability Corporation, "ERO Enterprise | Regional Entities."

[63] Source: North American Electric Reliability Corporation.

[64] David Nevius, *The History of the North American Electric Reliability Corporation* (Washington, DC: North American Electric Reliability Corporation, 2020), 5, https://www.nerc.com/AboutNERC/Resource%20Documents/NERCHistoryBook.pdf.

[65] Nevius, 5.

[66] Nevius, 14.

adherence did not produce reliable grid operations.[67] NERC claimed that violations of the voluntary reliability standards caused the power outage.[68] In 2006, FERC approved NERC as the Electric Reliability Organization (ERO), responsible for creating and enforcing reliability standards under FERC's federal authority. NERC also conducted reliability and risk assessments to include emerging risks.[69]

1. NERC's Grid Reliability Standards Overview

NERC's grid reliability standards, which took effect in 2007 as "Version 0," apply only to the transmission system, the blue portion in Figure 1. NERC, by all accounts, is currently enforcing the fifth revision of 93 reliability standards. The standards cover a myriad of topics, including Contingency Energy Supply, Coordination, Emergency Operations, Black Start Events, Frequency, Error Correction, Security, and Required Training, to name a few. These standards are grouped by theme or the intent of the protection. These standards are outside the scope of this study.

Standards, in general, are risk-based and can take years to receive approval and implementation.[70] For NERC, it can take 18 months from the time the NERC board approves the standard to the first effective date.[71] An implementation plan for a new NERC standard, EOP-012, for example, which addresses adverse weather plans, states that full implementation and enforcement will not happen for 78 months.[72] NERC's standards, even when risk-based, are not immediately implemented.

---

67 Nevius, 69.

68 Nevius, 70.

69 Nevius, 83.

70 Nevius, *History of NERC*; North American Electric Reliability Corporation, "Project 2016–02 Modifications to CIP Standards," NERC Standards, accessed December 29, 2022, https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx.

71 North American Electric Reliability Corporation, *NERC Reliability Standards*.

72 North American Electric Reliability Corporation, *Implementation Plan: Project 2021–07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination Reliability Standards EOP-011-3 and EOP-012-1* (Atlanta, GA: North American Electric Reliability Corporation, 2022), 3, https://www.nerc.com/pa/Stand/Project202107ExtremeColdWeatherDL/2021-07%20Implementation%20Plan_second%20posting_082022.pdf.

NERC also provides guidelines to be followed on a voluntary basis.[73] These guidelines are perhaps best considered best practices, because of their voluntary rather than mandatory nature. Of course, guidelines, while certainly helpful and offering good ideas, are ultimately unenforceable and not monitored by NERC.[74]

2. Grid Security-Focused Standards

NERC standards aim to lower the risk of an adverse event to the electrical transmission system, thereby ensuring the continuity of power. Thirteen standards make up the Critical Infrastructure Protection (CIP) standards. All the CIP standards are focused on security. While there are a total of 93 NERC standards, this thesis is only discussing the security related ones, denoted primarily by "CIP" in the standard number. The thirteen CIP standards aim to protect the grid from cyber or physical events that lead to disruption. These standards evolve and change over time. For example, standard CIP-001 is no longer active, but standard CIP-014 (outlined below) still applies under its third revision. Furthermore, the dates when the standards are enforceable vary. Twelve security standards focus on cyber-security, with the remaining standard is dedicated to physical security and resiliency. Table 1 lists the U.S.-based security-focused (CIP) standards enforced by NERC.

[73] "Reliability Guidelines, Security Guidelines, Technical Reference Documents, and White Papers," North American Electric Reliability Corporation, accessed November 30, 2022, https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx.

[74] North American Electric Reliability Corporation.

Table 1. NERC's U.S. Enforceable CIP Security Standards[75]

Standard	Title	Purpose
CIP-002-5.1a	Bulk Electrical System (BES) Cyber System Categorization	To identify cyber components of the transmission control system that should be protected under CIP guidance. These components would significantly impact the grid if they were compromised.
CIP-003-8	Security Management Controls	Establish a cybersecurity program that outlines policies for transmission cyber systems to include: Personnel and Training; Electronic Security Perimeters; Physical Security of Cyber systems; System Security Management; cyber Incident Reporting and Response Planning; Recovery Plans for transmission cyber systems; System Configurations and Assessments; Information Protection; and Declaring and Responding to abnormal circumstances. This list spans most other CIP standards, including minimum aspects of the required security program and enforceable protection for low-impact sites.
CIP-004-6	Personnel & Training	Regular cybersecurity training and different levels of cyber access are required based on the need and risk for personnel accessing the cyber transmission controls. This standard also requires background checks or similar approved risk assessments.
CIP-005-7	Electronic Security Perimeter(s)	Establish risk-based cyber perimeter controls for system access. These include router protocols, access point procedures, connectivity controls, remote access, encryption, and multi-factor authentication.
CIP-006-6	Physical Security of BES Cyber Systems	Requires adequate (and risk-based) physical access controls for cyber system spaces. This policy would include intrusion detection systems (IDS), motion sensors, proximity card access, electronic lock controls, essential control, escorted or unescorted access to spaces, access logs, and testing of systems.
CIP-007-6	System Security Management	Specifies "technical, operational, and procedural" system requirements, including patching, removable media storage devices, malicious code, event logs, user controls, password requirements and management, and unsuccessful access attempts.
CIP-008-6	Incident Reporting and Response Planning	Outlines procedures to report an adverse cyber incident and outlines cyber response plans administrative management, i.e., review and refresh

[75] Adapted from North American Electric Reliability Corporation, *NERC Reliability Standards*.

Standard	Title	Purpose
		timelines, lessons learned documentation, and plan testing.
CIP-009-6	Recovery Plans for BES Cyber Systems	Specifies the required cyber response plan elements and processes, including activation of cyber recovery plans, roles and responsibilities, cyber backups, data preservation, plan testing, and lessons learned processes following a cyber event.
CIP-010-4	Configuration Change Management and Vulnerability Assessments	Document how the cyber system is configured to include operating systems, firmware editions, custom software, security patches, accessible ports, and software change management/authorization.
CIP-011-2	Information Protection	How to identify information that is required to be protected. This policy includes sanitizing or destroying hardware that is no longer used.
CIP-012-1	Communications between Control Centers	Documents self-identified risks and protection measures for compromises to real-time monitoring or assessments between transmission control centers.
CIP-013-2	Supply Chain Risk Management	Develop risk-based plans and procedures that address risks encountered through procuring cyber assets (commonly referred to as the cyber supply chain). This includes vendor access to facilities, remote access to the cyber system, and policy review/updates.
CIP-014-3	Physical Security	Identifies transmission substations and control centers that would harm the electrical system if compromised. This standard (CIP-014) requires self-identified risk assessments (every 30 – 60 months, depending on the previous assessment results). This threat assessment includes prior attack history, physical substation vulnerabilities, and last intelligence regarding attacks or threats. CIP-014 requires physical security plans for identified substations and their control centers that include: law enforcement coordination, security upgrades and timeline to implement, assessment of dynamic threats coupled with mitigation security measures, and existing protective security methods that identify active threats, delay or deter their attacks, and methods to communicate attacks to law enforcement. This policy also requires organization response plans to physical attacks on transmission substations.

C. SUMMARY

Although the goal of these federal regulations is to instill reliability in grid operations and harden critical facilities against physical and cyberattacks, they focus only on the transmission system above 200kV, and thus do not cover the full grid. There are many agencies involved, all with specific responsibilities to grid reliability. As such, there is no single entity responsible for full grid security. Consequently, the federal grid regulatory environment is complex and incomplete.

III. REVIEWING THE EFFICACY OF REGULATIONS AGAINST TODAY'S THREATS

The Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response maintains a database of grid emergencies.[76] From January to August 2022, the database lists 104 separate intentional attacks on the grid, impacting approximately 22,905 customers. The database excludes the recent December attacks in North Carolina and the Pacific Northwest. The same database lists severe weather as the cause for 56 separate outages spanning approximately 4,798,452 customers. Similar to the physical attacks, the weather list excludes the recent extreme December weather experienced nationwide. Four cyber events occurred, but no outages were reported. Lastly, DOE lists 92 other significant incidents which impacted approximately 457,520 customers. Widespread outages persist despite regulations, also referred to as standards, designed for reliability.

Standards aim to instill reliability in grid performance, but the extent to which reliability has been achieved remains in question. Bad actors continue to exploit previously unknown vulnerabilities or use novel attack methods (both cyber and kinetic) that bypass fixed security standards.[77] NERC's standards must adequately protect against these methods, as well as weather disruptions and disasters such as wildfires, hurricanes, or abnormally severe winter weather.[78] NERC's authority and standards do not yet apply to the distribution components of the power grid.

This chapter examines the efficacy of regulations designed to protect the grid, by considering the four biggest threats—physical impacts, cyber issues, natural hazards, and governance failure—and the regulations that apply to each.

[76] Department of Energy, "Electric Disturbance Events (OE-417) Annual Summaries."

[77] Campbell, *Electric Grid Cybersecurity*; Parfomak, *Physical Security of the U.S. Power Grid*.

[78] North American Electric Reliability Corporation, *NERC FAQ*, 1.

A. PHYSICAL IMPACTS

Congress, law enforcement, and the energy sector have been aware of physical threats to the grid for decades. Congressional reports from 1990 outlined the potential for "long-term blackouts" across the country following physical attacks at transformer substations.[79] These reports illustrate a longstanding concern at the highest levels of the vulnerability of high-voltage transformer stations and the threat posed by kinetic attacks.

To date, only three NERC standards (CIP-003, CIP-006, and CIP-014) address physical security. Furthermore, they apply only to systems above 200kV, i.e., the transmission system.[80] The distribution system—power systems below 200kV—is not regulated by NERC but by each state or United States territory in which the system resides.

NERC's CIP-014 standard (physical security plans for identified substations and their control centers) may serve as a useful example of issues related to ensuring security against physical attacks. CIP-014 includes five specific requirements: reoccurring risk assessments, proper notification of inclusion or removal of transmission assets from the standard requirements, a physical attack threat and vulnerability assessment, physical security plans, and an independent review of standard compliance by a third party, which may or may not include recommended changes.[81] The CIP-014 standard was enacted in 2014 after the 2013 Metcalf incident.[82] While CIP-014 is a welcome addition to the standards, it also illustrates the reactive, rather than proactive, process by which grid vulnerabilities are addressed: physical security standards are enacted based on previous events and protect only a small portion of the nation's grid, leaving enormous protection gaps.

Furthermore, physical threats to the electrical grid extend beyond the scope of NERC's regulations. According to the FBI, a suspect conducted multiple physical attacks

---

[79] Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage* (Washington, DC: U.S. Government Printing Office, 1990), 37, https://ota.fas.org/reports/9034.pdf.

[80] North American Electric Reliability Corporation, *NERC Reliability Standards*.

[81] North American Electric Reliability Corporation, 553.

[82] Parfomak, *NERC Standards for Bulk Power Physical Security*.

in 2013 on Arkansas electrical components, dropping power to thousands of customers. The first attack in the series used a train to sever downed 500kV transmission electricity lines. This site showed evidence of previous failed sabotage attempts. Approximately a month later, the same perpetrator set fire to a substation control facility within the substation fences. Six days after that, two power poles supporting electric lines were toppled by a tractor.[83] According to the FBI, this series of attacks cost the power companies approximately $4.6 million.[84] The Arkansas powerline attack occurred before CIP-014; however, this regulation would not have prevented this attack. The standard covers substations, not power lines between substations. CIP-014 might have prevented the substation arson, but the details needed to determine whether that substation is subject to NERC regulations are unavailable. The Arkansas attack implies that CIP-014 may be too narrow to prevent attacks on key transmission infrastructure.

The North Carolina December 2021 attacks on two substations dropped power to approximately 40,000 customers.[85] The CIP-014 protection requirements, however, did not factor in substations exempt from NERC regulations.[86] Attacks such as those in Arkansas and North Carolina demonstrate that threats persist and therefore, raise the question of whether the current NERC standards are sufficient to address the existing threat.

NERC's CIP-014 standard addresses the security only of transmission substations and transmission control centers, but the physical threat does not stop at such high-voltage transmission stations. As seen in the Arkansas attack, electrical lines are subject to similar risks as the distribution portions, even if the outage risk is significantly smaller. Distribution substations far outnumber transmission substations, in the same way city streets outnumber highways. Even if NERC CIP-014 were a more substantial standard, it

83 "Attacks on Arkansas Power Grid: Perpetrator Sentenced to 15 Years," FBI News, August 10, 2015, https://www.fbi.gov/news/stories/attacks-on-arkansas-power-grid.

84 Chelsea J. Carter, "Arkansas Man Charged in Connection with Power Grid Sabotage," CNN, October 12, 2013, https://www.cnn.com/2013/10/08/us/arkansas-grid-attacks/index.html; Federal Bureau of Investigation, "Attacks on Arkansas Power Grid."

85 Grether et al., "North Carolina County Announces Curfew."

86 Willson, "NC Attack."

does not apply to distribution grid pieces. This vulnerability was emphasized in the North Carolina attack. Since distribution lines carry an estimated 78 percent of all electrical services, the majority of electricity services lack federal regulation.[87]

CIP-014 illustrates three key challenges of NERC protections: 1) they are reactive rather than proactive; 2) they lack coverage of all parts of the transmission system (e.g., powerlines); and 3) distribution substations are exempt from NERC regulations.

B. CYBER RISKS

Current NERC cyber mandates started in 2009 and have slowly evolved to meet the cyber threat. Yet relying on fixed cybersecurity standards is an inadequate strategy to protect the grid from rapidly evolving cyber threats. A 2014 dissertation that surveyed the effectiveness of NERC standards noted improvements in grid cyber security and reliability for the regulated systems.[88] Congressional research since then, however, somewhat contradicts that dissertation by directly stating that existing regulations are insufficient for today's threats.[89] As a 2017 Department of Defense report bluntly offered, "the cyber threat to critical U.S. infrastructure is outpacing efforts to reduce pervasive vulnerabilities."[90] Even NERC's 2010 report stated that advanced persistent cyber threats could remain undetected inside critical systems for years.[91] One standard, CIP-007, requires grid operators to prevent, deter, or detect malicious code to secure against cyber threats.[92] Yet, cyber threats can evolve daily, and if the standards do not adapt to meet the changing threat, adversaries will exploit those vulnerabilities.

---

87 North American Electric Reliability Corporation and Department of Energy, *High-Impact, Low-Frequency Event Risk*, 86.

88 Ladendorff, "Effectiveness of NERC CIP Standards," 110.

89 Parfomak, *NERC Standards for Bulk Power Physical Security*, i.

90 Defense Science Board (DSB) Task Force on Cyber Deterrence, *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence* (Washington, DC: Defense Science Board, 2017), https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

91 North American Electric Reliability Corporation and Department of Energy, *High-Impact, Low-Frequency Event Risk*, 33.

92 "US Reliability Standards," NERC Standards, November 28, 2022, https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx.

Cybersecurity standards also do not adequately address zero-day attacks. Zero-day attacks exploit a target system's vulnerability or weakness which is previously unknown by the target.[93] CIP-007 discusses patching requirements, but patching occurs only after the software vendor has discovered the vulnerability and disseminated a patch; before discovery, the vulnerability remains unaddressed. Nearly every day, new vulnerabilities are found by both software vendors and bad actors.[94] Yet NERC's CIP-007 standard allows patching to occur every 35 days, potentially allowing cyber vulnerabilities to persist for weeks.[95] Unfortunately, zero-day attacks reinforce that cyber security standards and best practices are inadequate to fully protect the grid against evolving cyber threats; further, the process to amend regulations moves slowly. Cybersecurity standards are routinely playing catch-up against evolving and emerging threats. NERC acknowledges this situation in a 2017 report: "the security threat landscape is constantly changing and requires adaptation."[96] Zhang bluntly opined that NERC's lengthy regulation process "prevents the changes necessary to keep up with technological advancements."[97] NERC's standards only partially meet evolving cyber threats, do not anticipate scenarios where vulnerabilities are previously unknown, and are subject to getting bogged down in the revision process.

Achieving CIP cyber compliance is but one part of achieving a secure grid. Cybersecurity standards require only that organizations meet the minimum requirements, a "static regulatory requirement," instead of adapting or evolving with dynamic threats and vulnerabilities.[98] With little accountability in place, electric providers tend to meet the barest minimum of the standard, then say "Done."[99] This approach, such as it is, invites

---

93 Kelley Dempsey et al., *Automation Support for Security Control Assessments: Software Asset Management*, vol. 3, NISTIR 8011 (Gaithersburg, MD: National Institute of Standards and Technology, 2018), 4, https://doi.org/10.6028/NIST.IR.8011-3.

94 Cybersecurity & Infrastructure Security Agency, "CISA National Cyber Awareness System – Current Activity," Cybersecurity Alerts & Advisories, accessed January 9, 2023, https://www.cisa.gov/uscert/ncas/current-activity.

95 North American Electric Reliability Corporation, *NERC Reliability Standards*, 356.

96 Parfomak, *NERC Standards for Bulk Power Physical Security*, 20.

97 Zhang, "Environmental Review & Case Study," 261.

98 Ladendorff, "Effectiveness of NERC CIP Standards," 113.

99 Ladendorff, 113.

exploitation.[100] Some of the best practices, like "air gaps," have already been "jumped" by Russian hackers, compromising the industry standard for control systems.[101] "Air gaps" are computers physically disconnected from internet-capable systems. In theory, an "air-gapped" system should be inaccessible to anything located outside of the physical server location. Russia has managed to bypass the gap, a threat commonly referred to as "jumping the gap."[102] Simply meeting CIP compliance has proven insufficient to address existing threat.

Neglecting cybersecurity protections on the distribution side results in vulnerabilities that remain unprotected because they are not subject to NERC requirements. State regulations vary greatly with differing degrees of success.[103] The lack of cybersecurity resources makes distribution system attacks more attractive to attackers.[104] The electrical and energy sectors receive the highest number of cyber threats of any industry, followed by the healthcare and financial sectors.[105] Congress cited a DHS report showing that the energy sector receives 40 percent of all critical infrastructure threats.[106] Yet, federal regulations continue to omit the distribution grid despite the excessive number of cyber threats, making it a ready target for cyberhackers domestically and internationally. A 2017 National Laboratory report suggests that distribution systems have no "baseline" of cybersecurity preparedness.[107] Some electrical distributors lack a simple cybersecurity

---

[100] Ladendorff, 116.

[101] Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin Press, 2019), 159.

[102] Jason F. Clemente, "Cyber Security for Critical Energy Infrastructure" (master's thesis, Naval Postgraduate School, 2018), 15, https://hdl.handle.net/10945/60378.

[103] Ivonne Pena, Michael Ingram, and Maurice Martin, *States of Cybersecurity: Electricity Distribution System Discussions*, NREL/TP-5C00-67198 (Golden, CO: National Renewable Energy Laboratory, 2017), vi, https://doi.org/10.2172/1347682.

[104] Rusco and Marinos, *Electricity Grid Cybersecurity*, 15.

[105] Seppo Borenius et al., "Expert-Guided Security Risk Assessment of Evolving Power Grids," *Energies* 15, no. 9 (2022): 20, https://doi.org/10.3390/en15093237.

[106] H.R., *Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure of the Electrical Grid?: Hearing before the Committee on Transportation and Infrastructure*, House of Representatives, 114th Cong., 2nd sess. (2016), 2, https://www.govinfo.gov/app/details/CHRG-114hhrg99931/context.

[107] Pena, Ingram, and Martin, *States of Cybersecurity*, v.

policy, let alone a history of adherence to best cybersecurity practices or stringent NERC standards.[108] Likewise, government overseers cite the absence of cybersecurity standards for distribution. A GAO report (21-81) plainly states, "the Department of Energy (DOE) has developed plans to implement the national cybersecurity strategy for the grid, but these plans do not fully address risks to the grid's distribution systems."[109] The report further explains that the distribution components of the electrical grid are increasing due to "technological advances" and are becoming increasingly vulnerable.[110] As federal standards do not apply to the distribution grid, only the transmission side, grid protection is unlikely since standards do not span the entire grid.

Beyond regulations, cybersecurity inconsistency and vulnerable spots may affect the cybersecurity of the whole grid. On the one hand, the nation shows a massive lack of cybersecurity consistency.[111] Smaller states or organizations governing distribution systems may lack the resources to hire cyber experts who guide cyber protection standards.[112] An adversary can use a weaker, more accessible link to penetrate a more fortified location or to set off cascading impacts in the grid. Therefore, cyber attackers may focus on organizations that lack adequate cybersecurity for distribution systems to undermine more secure sites. Despite verified and dynamic cyber threats, the portion of the grid not subject to NERC cyber standards may pose a risk to the entire grid.

Cyber threats to the distribution system constitute a substantial risk. Cyberattacks on the distribution center can still have national significance, even if outages are localized and attackers have identified the key outage locations.[113] Imagine the national attention if a children's hospital lost power for several days. Yet there has been, to date, little indication of a distinction being made, in terms of cyber risk, between the electrical distribution system vice the transmission system, much less an awareness of the physical impacts of a

[108] Pena, Ingram, and Martin, vi.

[109] Rusco and Marinos, *Electricity Grid Cybersecurity*, 2.

[110] Rusco and Marinos, 11.

[111] Ladendorff, "Effectiveness of NERC CIP Standards," 121.

[112] Rusco and Marinos, *Electricity Grid Cybersecurity*, 24.

[113] Rusco and Marinos, 31.

cyberattack on either.[114] Granted, an attacker would need to target a high number of disparate distribution systems to achieve the same widespread results as a single attack on a transmission system. A determined state adversary, however, with the resources and personnel, could easily expend the time and effort needed to target multiple distribution components to achieve widespread power outages. Although distributed in numerous and smaller geographical areas, the components that make up the electrical distribution system remain vulnerable, and the regulations enacted to date reflect an underappreciation of the significant risk they represent.

C. NATURAL HAZARDS

Natural disasters bypass existing protocols and governance, a point reinforced by continued outages following a natural disaster. In 1968, NERC came about to protect the nation from future blackouts, in response to widespread outages.[115] Yet in August 2003, 35 years after NERC's inception, fifty million customers suffered a two-week outage known as the "Northeast Blackout." This massive outage was attributed to trees connecting with power lines.[116] NERC assumed full governance responsibilities for the bulk transmission grid in 2005.[117] The blackouts have persisted, however; in 2014, Climate Central's Alyson Kenward and Urooj Raja found that "since 2003 after stricter reporting requirements were widely implemented, the average annual number of weather-related power outages doubled."[118] It is inferred that the increase in numbers reflects increased news coverage and higher-quality reporting. Yet, the number of severe weather events has have also increased, according to FEMA. From 1983 to 2002, there were 760 major disaster declarations compared to the 1,224 declarations from 2003 to 2022.[119] Kenward and Raja

[114] Rusco and Marinos, 22.

[115] Nevius, *History of NERC*, 5.

[116] Sell, Lien, and Toner, "A Framework for Healthcare Resilience," 16.

[117] Nevius, *History of NERC*, 83.

[118] Alyson Kenward and Urooj Raja, *Blackout: Extreme Weather, Climate Change and Power Outages* (Princeton, NJ: Climate Central, 2014), 3, https://assets.climatecentral.org/pdfs/PowerOutages.pdf.

[119] "Declared Disasters," FEMA Declared Disasters, accessed February 21, 2023, https://www.fema.gov/disaster/declarations.

establish that eighty percent of the outages are caused by weather.[120] As recently as December 2022, grid operators declared a grid emergency in response to a severe winter storm in the eastern US.[121] The mitigating measures were insufficient; an estimated 1.7 million people were left without power.[122] NERC standard EOP-011-11 includes weather impacts, but only references an emergency plan that describes extreme weather response. The standard mentions mitigating the emergency, which typically means load shed (stopping delivery of electricity) or preventing cascading grid failure (increased failures based on preceding failures similar to falling dominos).[123] Of course, no standard can lower the chances of severe weather occurring, only the risk level of a weather-caused outage; yet the current standard addresses only the impacts of severe weather after they have already started.[124] Simply put, NERC's weather standard, focused only on response, is incomplete in the face of natural hazards, as evidenced by consistent weather outages.

In June 2022, FERC released a press statement indicating that NERC would be required to produce enforceable weather-related reliability standards.[125] FERC publicly stated that NERC must create weather planning scenarios based on previous events or future expectations, conduct studies of abnormal weather events, provide required resources for those abnormal events, and create a response plan for expected gaps during rare events.[126] Although the actual content is currently included in the draft (EOP-012), and while the new standard focuses on abnormal weather events, the focus is solely on cold

120 Kenward and Raja, *Blackout*, 3.

121 Victoria Fetcher, "Eastern U.S. Power Grid Orders Cuts, Triggering System-Wide Emergency," *Canada Today*, December 23, 2022, sec. Economy, https://canadatoday.news/ca/eastern-us-power-grid-orders-cuts-triggering-system-wide-emergency-200346/.

122 Rebecca Leber, "Winter Storms Put the U.S. Power Grid to the Test. It Failed.," Vox, December 27, 2022, https://www.vox.com/energy-and-environment/2022/12/27/23527327/winter-storm-power-outages.

123 North American Electric Reliability Corporation, *Glossary of Terms Used in NERC Reliability Standards* (Atlanta, GA: North American Electric Reliability Corporation, 2022), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

124 North American Electric Reliability Corporation, *NERC Reliability Standards*, 682.

125 "FERC Acts to Boost Grid Reliability against Extreme Weather Conditions," FERC News Releases, June 16, 2022, https://www.ferc.gov/news-events/news/ferc-acts-boost-grid-reliability-against-extreme-weather-conditions.

126 Federal Energy Regulatory Commission.

weather and power generation in freezing temperatures, not transmission, distribution, or other weather events.[127] Furthermore, EOP-012 could take 78 months—over six years—to be enforced fully.[128] Outside of response and power generation protection in freezing weather, NERC regulations have not included comprehensive weather reliability standards despite the massive outages caused by all types of weather. The entire grid remains vulnerable to natural hazards without a uniform protection mandate spanning all forms of abnormal weather.

Another form of abnormal weather that occurs yet is not sufficiently covered by current standards is the superstorm. One of the most notable weather caused grid failures was caused by Superstorm Sandy in 2012. Following Sandy's east coast landfall, twenty-one states and Washington, D.C., were subject to significant power outages that affected 8.5 million customers.[129] The shorthand of "customers" does not cover the true total number of people involved, just the location of the service—an account may cover several members of a family living under one roof, for example. Sandy is yet another example of severe weather for which standards related to freezing temperatures do not apply.

Adapting from lessons learned during disasters or incidents such as Superstorm Sandy is reflected in the reactive development of NERC's standards. However, adaptation in the energy oversight community, particularly outside of NERC, is struggling. The GAO observes that the DOE lacks a comprehensive approach for its disaster assignment across the entire agency.[130] DOE's attempts to address this gap are ad hoc and likely insufficient.[131] They are significantly deficient considering repeated outages that have occurred in the same geographical location, e.g., Puerto Rico. Equally, local jurisdictions

---

[127] North American Electric Reliability Corporation, *Extreme Cold Weather Preparedness and Operations*, Draft 1 of EOP-012-1 (Atlanta, GA: North American Electric Reliability Corporation, 2022), https://www.nerc.com/pa/Stand/Project202107ExtremeColdWeatherDL/2021-07%20Initial%20Ballot_EOP-012-1_clean_051922.pdf.

[128] North American Electric Reliability Corporation, *Implementation Plan*, 3.

[129] Department of Homeland Security, *Power Outage Incident Annex*, 2.

[130] Frank Rusco, *Electricity Grid: DOE Should Address Lessons Learned from Previous Disasters to Enhance Resilience, Report to Congressional Committees*, GAO-22-105093 (Washington, DC: Government Accountability Office, 2022), 21, https://www.hsdl.org/?abstract&did=868221.

[131] Rusco and Marinos, *Electricity Grid Cybersecurity*, 24.

(as part of the distribution system) are not taking advantage of the resources designed to further protect the grid under their governance.[132] Not learning from previous mistakes and not enforcing reliability standards on the distribution grid increases the risk to the nation and national security.

D. GOVERNANCE SHORTFALLS

Current regulations do not match the risks to the grid, and overall compliance does not match the participation levels needed for security. For example, ninety percent of the grid is not subject to the NERC CIP regulations.[133] But, according to Joseph H. Eto, the distribution portion of the grid accounts for about 94 percent of all outages.[134] Despite this large outage percentage, the distribution portion lies outside federal reliability regulations, allowing risk and outages to continue unabated.

Existing regulation efforts negatively affect the grid's resilience in unexpected ways.[135] Organizations resist meeting standards because of the expense and effort required. A 2014 dissertation claimed forty-six percent of the surveyed electrical organizations required their equipment experts to spend less time maintaining equipment so they could complete regulatory paperwork.[136] Furthermore, some electrical organizations are replacing modern components under CIP regulation with aged components outside of governance because doing so was less expensive than complying with the standard.[137] Similarly, others will not upgrade equipment requiring compliance where compliance did not previously exist.[138] Instead, organizations leave outdated and vulnerable equipment in place. The older equipment does not have the features that were regulated. The electrical utilities avoid compliance in much the same way that classic car

132 H.R., *Blackout!,* 35.

133 Clarke and Knake, *The Fifth Domain*, 158.

134 Eto et al., "Distribution System Versus Bulk Power System," 717.

135 McQuinn, "Energy Regulation Effects," v.

136 Ladendorff, "Effectiveness of NERC CIP Standards," 111.

137 Ladendorff, 109.

138 Ladendorff, 114.

owners avoid smog checks for older cars. These regulation avoidance techniques increase the risk to the grid by creating security weaknesses or allowing them to persist.[139] Regulatory loopholes and weakened maintenance practices increase the risk to the entire grid.

Ongoing outages have called into question the effectiveness of NERC's self-governance (with FERC oversight) and the federal government's allowing the electrical industry to make its own security and resilience regulations and standards.[140] The Congressional Research Service has referred to NERC governance standards as "consensus-based."[141] NERC requires electrical organizations to conduct risk analysis and create a security plan addressing the risk as they see it (CIP-014).[142] This assessment and subsequent plan are audited and measured against best practices verified by the regional entity to ensure compliance.[143] The flexibility of the audit and interpretation of risk goes both ways. The regional entities observe varied audits and compliance enforcement rules, leaving a lack of uniformity across the regulated system.[144] The lack of a standardized audit invites contradiction and increases the risk to a fragile power grid.[145] The apparent looseness of the audit requirement seems designed to allow organizations to tailor security to the risk and add flexibility for unique situations. This creates a situation for grid providers to view risk differently than the security or intelligence industry does.[146] As such, the lack of uniform assessments, differing views of risk, and audit practices ensures vulnerabilities and increases the risk to the grid.

---

139 Ladendorff, 114.

140 Young, "Method or Madness," 25.

141 Humphreys, *Critical Infrastructure Security and Resilience*, 2; Campbell, *Electric Grid Cybersecurity*, 3.

142 North American Electric Reliability Corporation, *NERC Reliability Standards*, 555.

143 Parfomak, *NERC Standards for Bulk Power Physical Security*, 3; North American Electric Reliability Corporation, *Physical Security*, CIP Reliability Standards, CIP-014-1 (Atlanta, GA: North American Electric Reliability Corporation, 2014), https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

144 Ladendorff, "Effectiveness of NERC CIP Standards," 115.

145 Ladendorff, 109.

146 Parfomak, *NERC Standards for Bulk Power Physical Security*, 5.

Another challenge with respect to regulations is updating them quickly enough to meet evolving threats.[147] Rapid policy or regulation changes require constant threat monitoring and assessments and the capability to increase security rapidly. These changes would require federal regulations which are rapidly modifiable. Yet, Congressional research states that although grid security has increased, the security standards fail to meet the risk previously assessed by the sector.[148] NERC has stated that raising standards to cover more threats would be "inefficient" and "unnecessary."[149] Government oversight policies struggle to keep up with the rapid evolution of technologies and dynamic threats.[150] Self-regulation requires comprehensive knowledge of a variety of dynamic threats including physical, cyber, and natural threats. NERC has acknowledged resistance to deviating from their flexible approach to a "rule-based approach for physical security."[151] Herster Dudley's master's thesis, "Building Resilience within DOD Microgrids by Considering Human Factors in Recovery Procedures," straightforwardly called the current state of electrical security insufficient to achieve DOD mission assurance.[152] Standards do not change based on threats, only the adherence or perception of threat risk within the existing standard. Based on NERC's above statements, evolving or threat based protection standards are unlikely to be enacted.

Along these lines, some arguments indicate that increasing regulations, to include additional oversight agencies, might actually "reduce the efficiency of grid operations."[153] NERC called increased standards a "burden."[154] McQuinn argued that regulations have

147 Debra K. Decker and Kathryn Rauhut, "Incentivizing Good Governance beyond Regulatory Minimums: The Civil Nuclear Sector," *Journal of Critical Infrastructure Policy* 2, no. 2 (Fall 2021): 19–43, https://doi.org/10.18278/jcip.2.2.3.

148 Parfomak, *NERC Standards for Bulk Power Physical Security*, i.

149 Parfomak, *Physical Security of the U.S. Power Grid*, 25.

150 Young, "Method or Madness," 6.

151 Parfomak, *Physical Security of the U.S. Power Grid*, 25.

152 Marcella R. HersterDudley, "Building Resilience within DOD Microgrids by Considering Human Factors in Recovery Procedures" (master's thesis, Naval Postgraduate School, 2021), 87, https://hdl.handle.net/10945/67135.

153 Robert Knake, *A Cyberattack on the U.S. Power Grid* (Washington, DC: Council on Foreign Relations, 2017), 4, https://www.cfr.org/report/cyberattack-us-power-grid.

154 Parfomak, *Physical Security of the U.S. Power Grid*, 25.

diminished grid security and reliability.[155] McQuinn cites the above example where electrical providers elect not to upgrade their infrastructure as it could also require costly compliance measures. Increasing federal oversight may not be the most logical protective option because it has the potential to be counterproductive, ultimately hindering grid operations.

E. SUMMARY

Existing regulations, standards, and governance efforts offer only partial coverage against the four biggest threats to the grid—physical impacts, cyber issues, natural hazards, and governance failure. The nation's regulatory efforts have improved reliability, yet the grid remains vulnerable to a variety of dynamic threats, raising questions about the efficacy of existing measures and the process required for updating them as expediently as possible.

[155] McQuinn, "Energy Regulation Effects," 7.

IV. BRIDGING REGULATORY FAILURES

Existing efforts have fallen short of establishing grid reliability. Bad actors have found methods to exploit protection gaps to launch kinetic and cyber attacks, and natural disasters remain a threat capable of dropping power to critical facilities and citizens. Requiring multiple layers of components would address the gaps outlined in Chapter II, so if a threat were successful, a redundant capacity would continue to power the grid. Alternatively, gaps could be drastically reduced if more of the grid were subject to mandated protection. This chapter examines different policy options that might directly reduce existing shortfalls.

A. POLICY OPTION A: REQUIRED REDUNDANCY

Redundancies are mitigating risk in a large footprint grid overseas and within other infrastructure systems. A report by DOE states that technological innovations improve dependability but may introduce new weaknesses if there is lower or no redundancy.[156] This situation implies that fewer redundancies increase vulnerabilities, from which it can be further extrapolated that increasing redundancies decreases vulnerabilities or mitigates their existence. For example, having a single flashlight when the power goes out is essential, but a person could still be left in the dark. The batteries could be dead; the bulb could be broken. If a person has two flashlights, however, as well as a camping lantern, a small generator, and a box of spare parts, the likelihood of being left in the dark is significantly less. Redundant layers—in this example, the extra flashlights and the camping lantern—ensure the person still has light regardless of the circumstances. Multiple backup solutions mitigate the vulnerability of being left in the dark.

Outside the United States, governing agencies have included redundancy as a path to resilience. For example, the United Kingdom's (UK) Cabinet Office for Civil Contingencies includes redundancy as a critical element of infrastructure security. The

156 ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats* (Reston, VA: ICF International, 2016), 1, https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf.

government articulates four strategic areas (see Figure 4) which help achieve infrastructure resilience: Resistance, Reliability, Redundancy, and Response and Recovery.[157]

Figure 4. United Kingdom's Four Strategies for Infrastructure Resilience[158]

Redundancy focuses on having backup capabilities to take over infrastructure delivery if the primary methods fail. Returning to the flashlight example, if the power grid fails, the multiple flashlights and small generator may take over, providing energy and light to the person without power. This excess capacity ensures resilience even if there is an unforeseen failure. Response and Recovery speak directly to the capabilities of the infrastructure owner and operator in addressing the impact and restoring normal operations. The United Kingdom's approach increases its resiliency by including redundancy nationwide.

The United Kingdom emphasizes redundancy as a more significant risk reducer than standards. The Cabinet Office explicitly states, "spare capacity will enable operations to be switched or diverted to alternative parts of the network in the event of disruptions to ensure continuity of services."[159] The Office further indicates that good design includes

[157] Civil Contingencies Secretariat, *Keeping the Country Running*, 14.

[158] Source: Civil Contingencies Secretariat, 15.

[159] Civil Contingencies Secretariat, 16.

redundancy.[160] The strategy uses telecommunications as an example. The telecommunications system design has additional capacity and switches beyond the peak demand, allowing the system to absorb any component failures. This design allows the system to absorb failures without delay.[161] More pointedly, the Office asks infrastructure owners and operators to evaluate the cost-benefit of redundancy over protection from a single threat, in contrast to the United States NERC efforts.[162] The Office labels redundancy as a more intelligent investment than single hazard protection.[163] Redundancy is a viable and proven method of ensuring grid security for the United Kingdom.

The UK further requires systems to be able to operate in extreme conditions, not just within operating norms. The UK's Civil Contingency Secretariat emphasizes "increasing the robustness and resilience of existing services or assets by building additional network connections or providing backup facilities to ensure continuity of services."[164] These additional network connections or "backup facilities" create reliable infrastructures through multiple redundant systems.

Federal plans and regulations currently lack a redundancy requirement, making the grid vulnerable through single points of failure. Even so, some sub-federal jurisdictions are beginning to explore and implement redundancy to achieve electrical resiliency. Texas, for example, is considering connecting its power grid to neighboring grids.[165] Ideally, such a measure would provide alternative feeds into Texas in the event of another major catastrophe. Still, even those linkages will not prevent blackouts entirely.[166] In 2021,

---

160 Civil Contingencies Secretariat, 16.

161 Civil Contingencies Secretariat, 16.

162 Civil Contingencies Secretariat, 52.

163 Civil Contingencies Secretariat, 52.

164 Christina Scott, *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards* (London: Cabinet Office, Civil Contingencies Secretariat, 2010), 7, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf.

165 Thomas Popik and Richard Humphreys, "The 2021 Texas Blackouts: Causes, Consequences, and Cures," *Journal of Critical Infrastructure Policy* 2, no. 1 (Spring 2021): 63, https://doi.org/10.18278/jcip.2.1.6.

166 Popik and Humphreys, 63.

nearby grids (outside of Texas) were suffering their own winter emergencies and thus, unable to adequately support Texas' failed grid.[167]

As such, Berkshire Hathaway is exploring the option of building ten new power generation plants for Texas that would "operate only during emergency events," according to Thomas Popik and Richard Humphreys.[168] Ten generation plants are a significant investment for emergencies, but it acknowledges the efficacy of redundancies. Popik and Humphreys indicate that electrical competitors call the initiative "unfair" as it threatens their profits and existing contracts.[169] Berkshire competitors complain that they are resistant to the proposal because it would challenge their ability to recover their cold-weather reliability investments if Berkshire undercut some of their highest profit periods.[170] Regardless of the implementation hurdles of redundant solutions, they are a viable solution to existing grid vulnerabilities.

Additional discussions within the United States have centered on increasing grid redundancies. *Energies Journal* identified redundant power lines and components as a risk mitigation measure for physical threats.[171] In other words, additional power lines results in fewer choke points and therefore requires extra attacks to achieve the same outage results. These extra layers thereby increase grid security and reliability. Congressional testimony from nearly twenty years ago cites redundancies as a solution to grid unreliability. Specific infrastructure sectors are pursuing redundancies. Hospitals in New York use redundant solutions across their industry to experience "virtually no loss in service."[172] The same 2003 Congressional testimony cites redundancy examples in

[167] Popik and Humphreys, 63.

[168] Popik and Humphreys, 62.

[169] Popik and Humphreys, 63.

[170] Popik and Humphreys, 63.

[171] Borenius et al., "Expert-Guided Security Risk Assessment," 6.

[172] H.R., *Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: Joint Hearing*, House of Representatives, 108th Cong., 1st sess. (2003), 73, https://www.govinfo.gov/app/details/CHRG-108hhrg99793/CHRG-108hhrg99793/context.

telecommunications that lessen extended outages.[173] However, federal electrical regulations ignore the obvious: grid redundancies are a must and should be mandated.

B. POLICY OPTION 2: EXPANDING SCOPE OF GOVERNANCE

Congress and/or FERC could expand NERC's authorities to maintain awareness of all threats and make protection standard adjustments as a threat emerges or evolves. For example, the Cybersecurity & Infrastructure Security Agency (CISA) releases information on cyber threats on a near-daily basis.[174] Congress could mandate that all electrical service providers comply with applicable CISA cyber advisories within 24 hours. A regional entity or NERC at large or even CISA could inspect compliance. This solution aligns with CIP-007 patching requirements, which require patching within 35 days.[175] However, CIP-007 applies only to cyber assets and not physical threats. This solution addresses physical and cyber threats within a much shorter timeline than 35 days. Requiring timely compliance with emerging threat advisories protects grid providers against known threats as they happen.

Along these lines, constant threat awareness is already available (without compliance requirements) through the CISA's advisories and the Electricity Information Sharing and Analysis Center (E-ISAC). The E-ISAC continually assesses incidents and changing threat information and then provides recommendations based on the evolving threat.[176] As updating laws or NERC regulations to keep up with E-ISAC's analysis (which can change daily), and keeping up with currently unknown threats is difficult, complying with advisories' suggested actions will make regulations stronger rather than constantly updating the regulations themselves. This point is further emphasized in a 2017 report indicating that electrical sector threats are growing.[177] Furthermore, employing existing resources such as CISA and E-ISAC eliminates the lag time it would take for

[173] H.R., 128.

[174] Cybersecurity & Infrastructure Security Agency, "CISA CERT Advisories."

[175] North American Electric Reliability Corporation, "US Reliability Standards."

[176] Parfomak, *NERC Standards for Bulk Power Physical Security*, 7.

[177] Parfomak, 2.

NERC to obtain security clearances and intelligence expertise needed for rapid threat assessment. Moreover, sharing dynamic threat information with congressional oversight committees or NERC to make regulation updates often prove cumbersome with information-sharing restrictions.[178] Lastly, this potential solution addresses only known threats and misses unknown or zero-day threats. Young's thesis loosely implies the government remains reactive, adjusting regulations and guidance based on the incident already experienced, and not meeting tomorrow's threat.[179] Compressing the existing compliance timeline is needed, but the threat information should come from outside of the electrical community. Relying on threat and risk information from outside the intelligence community is not a viable solution as organizations typically cannot keep up with everyday intelligence analysis, nor do they usually extrapolate yesterday's threat into tomorrow's threat adjusting accordingly.

Along similar lines that adjust existing regulations, the United States could widen protection mandates to include previously ignored distribution systems as outlined in NERC's 2010 report.[180] Miles Keogh and Christina Cody argue that "distribution system redundancy" may be a pricey resilience option, but the bill to the ratepayers might be lower over time with reduced outages.[181] Keogh and Cody explain that conducting a cost-benefit analysis to eliminate distribution outages will paint a clearer picture than looking strictly at the bottom line cost. Because distribution systems account for a vast majority of the outages, increased reliability is a likely outcome if the goal of eliminating outages remains a budgetary decision metric. If electrical companies focus on resilience rather than cost, strategic investments could significantly reduce outages.

Rewarding voluntary resilience achievements above existing mandates may increase security and reliability without additional mandates. For example, most federal

178 Parfomak, 17.

179 Young, "Method or Madness," 16.

180 North American Electric Reliability Corporation and Department of Energy, *High-Impact, Low-Frequency Event Risk*, 14.

181 Miles Keogh and Christina Cody, *Resilience in Regulated Utilities* (Washington, DC: National Association of Regulatory Utility Commissioners, 2013), 11, https://pubs.naruc.org/pub/536f07e4-2354-d714-5153-7a80198a436d.

employees have a performance plan they must achieve by the end of an evaluation period. Avoiding adverse actions requires a minimum of points. Bonuses, financial and time-off incentives, however, motivate performances that are higher than the minimum performance plan.[182] Achieving higher standing earns the employee a reward not available to employees who complete only the plan minimum and nothing further. In another example, private sector entities including organizations such as Everbridge, the American Water Works Association, and Northrup Grumman have freely pursued DHS certification to reduce terrorism-related liability. The "Support Anti-terrorism by Fostering Effective Technologies" (SAFETY) Act limited liability from acts of terrorism for certified organizations.[183] The act encourages organizations to pursue DHS SAFETY certification, which limits their liability in the event of a terror incident. In July 2018, DHS certified their 1,000th organization. These examples incentivized behavior to achieve certification but did not mandate it. Incentivizing higher standards, mainly when an organization goes above and beyond the recommended protection measures, might be a viable path to achieving increased reliability.[184] Thus, the federal government should implement voluntary incentives to achieve higher than minimum regulation compliance, and review performance to determine whether higher security protocols have been achieved.

Transitioning away from NERC's governing model to different models is a suggestion as well. Other governing models do not adequately meet grid needs either, however. Duke Environmental Law and Policy Forum argue that governance is the answer to electrical reliability but opines that a "nodal governance" solution versus a federal blanket solution is required.[185] Nodal governance is a model that describes and maps the state, county, city, non-state organizations and associated regulations spanning the full

182 "Approaches to Calculating Performance-Based Cash Awards," Policy, Data, Oversight: Performance Management, accessed January 11, 2023, https://www.opm.gov/policy-data-oversight/performance-management/performance-management-cycle/rewarding/approaches-to-calculating-performance-based-cash-awards/.

183 Homeland Security Act of 2002" Support Anti-Terrorism by Fostering Effective Technologies, 6 U.S.C. § 441–444 (2006).

184 Decker and Rauhut, "Incentivizing Good Governance beyond Regulatory Minimums," 31.

185 Alison Gocke, "Nodal Governance of the U.S. Electricity Grid," *Duke Environmental Law & Policy Forum* 29, no. 2 (Spring 2019): 205, https://scholarship.law.duke.edu/delpf/vol29/iss2/1.

jurisdictional spectrum which all share the responsibility of grid security. Mapping these jumbled responsibilities will reveal where the grid is governed weakly. This model then points to the appropriate actions needed to effectively govern the grid.

An article in *Duke Environmental Law & Policy Forum* argues that solutions outside this varied governance model are not viable because their model is more accurate and encompassing than simply looking to NERC. Alison Gocke, the article's author, reasons this is due to the varying levels of grid control as these systems span states and counties and vary between public and private sector control. Gocke indicates that engineering is not an ideal answer and argues for an appropriate governance model.[186] In this option, the NERC would delegate most, if not all, reliability mandates to states to include both transmission and distribution. A nodal option places the responsibility on the states to manage their reliability unique to their geography and risk climate, in the way gun laws or tax rates differ by state. The grid spans well past state boundaries, however, with potential impacts that can cascade throughout the rest of the nation. The varying levels of security among states create risk and invite catastrophe into the entire U.S. grid through one less regulated state similar to the varied way existing standards are enforced.

C. POLICY OPTION 3: MICROGRID AS A REDUNDANCY

Microgrids are a widely accepted and proven capability that delivers resilience to the nation's power grid. They are most often used in conjunction with the nation's grid either as a redundant source of power, a source of cost savings, or a way to meet a more reliable power need.

A microgrid is a small power grid that may or may not be connected to the nation's power grid. Figure 5 depicts a generic microgrid with multiple power generation sources, primarily solar and wind. Multiple power generation sources are a hallmark of microgrids and are a major source of their resilience. Microgrids generally have generator backups, energy storage (batteries), and a controller that determines how electricity is moved and consumed through the microgrid, which can be as large as several city blocks or as small

[186] Gocke, 207.

as a single facility. Microgrids may have a power generation source that is controllable, enabling the microgrid to surge electricity when needed, or limit production when warranted.

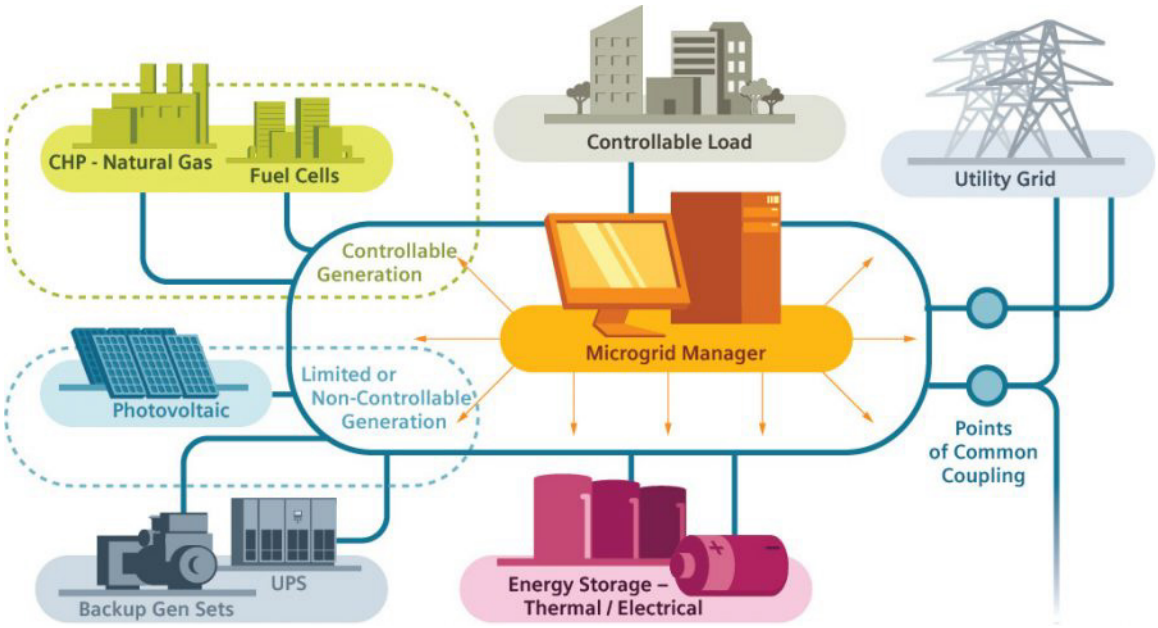

Figure 5. Microgrid Diagram[187]

The microgrid, as depicted above, may be connected to the national grid or disconnected when appropriate. The multiple generation sources, both controllable and not controllable as well as backup generation sources provide a redundancy not typically seen in the larger national grid. Microgrids often do not have a transmission side, eliminating substations and high-voltage requirements.[188] This makes them cheaper and more efficient grid reliability solutions.

Many sources assert the advantages of a distributed system of microgrids to protect energy reliability. A national laboratory has cited microgrids as "a solution for more

[187] Source: "Microgrids," Center for Climate and Energy Solutions, accessed December 12, 2022, https://www.c2es.org/content/microgrids/.

[188] Center for Climate and Energy Solutions.

resilient power."[189] Likewise, the Naval Postgraduate School (NPS) has found microgrids to be highly reliable.[190] Joshua P. Hildebrand declares that the Navy is pursuing microgrids as a solution for dependable electricity.[191] Congressional testimony surrounding grid resilience reinforces that microgrids can increase "local resiliency."[192] Specifically, microgrids offer an option to organizations requiring a "very, very reliable power."[193] The expert cited microgrid use by the Department of Defense and data centers as an answer for reliable electrical service. He concluded that microgrids were "an important element of the future evolving grid."[194] Aminy Ostfeld, Michael Whitmeyer, and Alexandra Von Meier explain that microgrids could provide more reliable service, areas of power during widespread outages, a reduction in cascading failures like those seen in the Northeast Blackout or the 2021 Texas Blackout, and grid recovery assistance when other portions fail.[195] They suggest creating microgrids block by block in cities. Not only would it make the city block resilient, but it would also increase overall grid reliability by reducing power fluxes.[196] Borrego Springs in California installed a microgrid because "they had a lot of issues with the transmission line," implying their leading supplier was unreliable.[197]

Smaller may even be better as regards these grids. One NPS study recommended creating a nanogrid, a tiny microgrid, within a microgrid, which would eradicate electrical interruptions on military installations.[198] It is logical to presume nanogrids are as effective

---

189 Adkisson, "Are Microgrids a Key to Grid Resiliency?"

190 Jones, "Reliability and Resilience Evaluation," 83.

191 Joshua P. Hildebrand, "Estimating the Life Cycle Cost of Microgrid Resilience" (master's thesis, Naval Postgraduate School, 2020), 5, https://hdl.handle.net/10945/66658.

192 H.R., *Lessons Learned from the Texas Blackouts*, 92.

193 H.R., 124.

194 H.R., 124.

195 Aminy Ostfeld, Michael Whitmeyer, and Alexandra Von Meier, "Block-Level Microgrids for Power System Resilience: Scaling and Impacts," in *CIRED Workshop* (Ljubljana, Slovenia, 2018), 1, http://www.cired.net/publications/workshop2018/pdfs/Submission%200322%20-%20Paper%20(ID-21011).pdf.

196 Ostfeld, Whitmeyer, and Von Meier, 2.

197 H.R., *Lessons Learned from the Texas Blackouts*, 124.

198 Alissa R. Kain, "Investigation of Nanogrids for Improved Navy Installation Energy Resilience" (master's thesis, Naval Postgraduate School, 2021), 51, https://hdl.handle.net/10945/67752.

and reliable as the larger microgrid and, therefore, should be considered an efficient path to redundancy, thereby bridging multiple governance gaps.

Some argue microgrids are the single best reliability solution. One study implies that microgrids and redundancy are so crucial to resilience that it proposes the federal government fund microgrids for hospitals and nearby supporting medical facilities.[199] The recommendations include a federal microgrid pilot program to determine whether a nationwide grant option would produce a more resilient healthcare system. The recommended pilot program could have groundbreaking impacts on healthcare resilience for the foreseeable future, as microgrids were the study's solution for the risk of area outages.[200]

Redundant or layered electrical supply systems are resistant to disaster-caused outages. *Applied Energy Journal* determines that many studies support microgrid performance in disaster environments.[201] Studies include recent disasters, including Superstorm Sandy, the Texas Blackout of 2021, and the California wildfires. Superstorm Sandy dropped power to New York City except for New York University (NYU) and Princeton.[202] As Figure 6 demonstrates, NYU created its microgrid capable of detaching from the nation's interconnected grid.

199 Sell, Lien, and Toner, "A Framework for Healthcare Resilience," 22.

200 Sell, Lien, and Toner, 23.

201 Akhtar Hussain, Van-Hai Bui, and Hak-Man Kim, "Microgrids as a Resilience Resource and Strategies Used by Microgrids for Enhancing Resilience," *Applied Energy* 240 (2019): 63, https://doi.org/10.1016/j.apenergy.2019.02.055.

202 Morgan Kelly, "Two Years after Hurricane Sandy, Recognition of Princeton's Microgrid Still Surges," Princeton University, October 23, 2014, https://www.princeton.edu/news/2014/10/23/two-years-after-hurricane-sandy-recognition-princetons-microgrid-still-surges.

Figure 6. NYU Presentation Slide Displaying their Power Following Superstorm Sandy[203]

This layered redundancy allowed NYU's power to stay on and provided a continuity of services unavailable in most of the surrounding area.[204] NYU illustrates that UK's redundancy strategy warrants further consideration because it worked when legacy systems failed. Likewise, Princeton University was a literal shining example of this capability following Superstorm Sandy. While large portions of New Jersey were in the dark, Princeton remained lit, thereby proving its reliability over the larger grid.[205] These

[203] Source: Edward Dodge, "Distributed Energy in New York," *Edward T. Dodge* (blog), October 19, 2014, http://www.edwardtdodge.com/2014/10/19/distributed-energy-in-new-york/.

[204] Deaton, "NYU Microgrid."

[205] Sell, Lien, and Toner, "A Framework for Healthcare Resilience," 19.

established examples of redundancy demonstrate the potential of layered power delivery *despite* a seemingly catastrophic disaster.

Microgrids are proving stable and reliable even in extreme weather conditions, significantly more reliable than the nation's power grid. Such systems in Houston—which also kept the lights on in pockets during the 2021 blackout—have survived hurricanes and other flooding events but were previously untested against extreme cold.[206] Yet, this unknown was addressed when the power remained in those small, localized areas. One microgrid company kept power running for 97.3 percent of the time at 206 different microgrid locations in Texas during a grid failure.[207] This percentage is remarkable in the face of the broader grid status, directly implying a significant reliability rate compared to the broken grid. Further, 130 of these microgrids were feeding electricity into the slowly recovering system, enhancing the overall recovery.[208]

Studies support the resilience and increased electrical capabilities seen in Houston. Mukherjee suggests distributed systems, like microgrids, have the potential to feed electricity into the more extensive system for a black start; a black start is when the grid is completely down and needs to restart with zero energy in the system.[209] Other studies reinforce this thought. For example, focusing on the Puerto Rican power grid, Juan E. Alicea projects that creating microgrids to support the 62 wastewater treatment locations on the island would drastically increase grid resilience following a significant incident.[210] Microgrids may further grid resiliency by ensuring the availability of additional electrical production despite a widespread blackout. Microgrids can supply power to a broken power

206 Joshua Mann, "How Houston's Microgrids Fared Amid Blackouts," *Houston Business Journal*, February 24, 2021, https://www.bizjournals.com/houston/news/2021/02/24/sunnova-enchanted-rock-microgrids-texas-outages.html.

207 Mann.

208 Wood, "Microgrids Help Texas."

209 Srijib Mukherjee, "Applying the Distribution System in Grid Restoration/NERC CIP-014 Risk Assessment," in *2015 IEEE Rural Electric Power Conference* (2015 IEEE Rural Electric Power Conference, IEEE Computer Society, 2015), 104, https://doi.org/10.1109/REPC.2015.21.

210 Juan E Alicea, "Puerto Rico's Homeland Security Readiness: Redesigning the Island's Power Grid to Improve Its Resiliency" (master's thesis, Naval Postgraduate School, 2019), 50, https://hdl.handle.net/10945/62249.

grid, enabling a faster restart.[211] Further, fusing both redundancies and microgrids, Beaton argued that redundant power storage within microgrids enhance resilience.[212] Energy storage allows the grid to deliver power even if the generating plants are offline. These stabilizing components are proving to be a key asset in grid resilience.

D. SOLUTION ANALYSIS

Each of these three potential policy solutions offers significant benefits and improvements to grid security, although no single solution fully or adequately addresses current resilience shortfalls. Table 2 compares and contrasts the solutions.

Table 2. Solution Analysis

Solution	Cost	Timeliness	Fully address existing gaps	Proven strategy
Required Redundancy				
Expanding the Scope of Governance				
Microgrids				

Note: Color coding is as follows: Green signifies a superior rating; yellow means the area is unknown, remains to be seen, or signifies neither good nor bad; while red signifies a failing or missing the need.

As Table 2 shows, requiring redundancies for critical nodes or components is likely to be an incredibly expensive and lengthy process. This option potentially duplicates many portions of the grid, a costly venture. Furthermore, building redundant lines and substations could take many years through permitting, easements, and purchasing components in a supply chain-restricted market. Ensuring multiple paths, however, for critical lines and

[211] Teague, Goss, and Weiss, "Applying Risk to Energy Investments," 105.

[212] Daniel T. Beaton, "Testing Whether Distributed Energy Storage Results in Greater Resilience of Microgrids" (master's thesis, Naval Postgraduate School, 2021), 159, https://hdl.handle.net/10945/67104.

critical infrastructure facilities addresses most of the gaps identified within Chapter II, except for systemic threats like cyber vulnerabilities. Physically destroying a single site would not matter if multiple electrical sources step in to fill the gap. A cyber threat, however, could stop the system on an organizational level. Regardless, as demonstrated in the UK, redundant components and systems increases the nation's reliability and resilience.

Expanding the scope of governance to include distribution side components and complying with threat and vulnerability advisories has many unknowns. The cost depends on the expense needed to bring distribution into NERC standards, even if a lower protection threshold were met. Patches to software or upgraded fences may be cheap and fast or expensive and slow. It depends on the threat and the new standard encompassing the distribution side. Since it will expand regulations to areas not currently under protection, the gap analysis remains unknown. Logically, expanded governance would lower outage rates, but the extent to which it will do so, and the question of whether outage reduction will be worth the expense, depends on potential impact, loss of life, consumer insurance claims, economic impacts, and so forth. Also, its effectiveness is unproven at this point. Logically, increasing site protections is a proven strategy; however, the sheer magnitude of distribution components makes a target-rich environment for kinetic attacks. Increasing mandates, as discussed in Chapter II, may not be adequate as a security measure and might hinder the overall resilience of the grid.

Microgrids, on the other hand, address some of these issues and offer more all-around promise as a solution. Microgrids might be the most cost-effective of the three options for the end user. Just as installing solar panels on a house can lower the electrical bill, microgrids may pay for themselves through utility cost savings. If hospitals and other critical infrastructure nodes rely on microgrids' renewable power, they do not have to purchase electricity from the power company. Microgrids are a proven strategy that does address existing gaps outlined in Chapter 2. If a microgrid approach were initiated by starting at critical infrastructure locations and then expanding outward, the nation could see visible results quickly through continuity of power regardless of outages or preventative grid shutdowns.

Time, however, is one drawback of the microgrid strategy. It could take many years to adequately instill resilience in infrastructure systems and the nation through microgrids. Implementation of a nationwide microgrid solution is a significant hurdle.

A blend of all three solutions could bring about the electrical reliability the nation craves. Microgrids could be used as a front-running solution to achieve the redundancy required by newly expanded regulations. To support them, governance could be expanded to require redundant solutions for critical infrastructure sites. Microgrids could be installed in subdivisions, universities, medical facilities, and public safety agency locations. An interim security measure would require immediate threat patching for the rest of the grid. With a more highly protected grid replete with faster threat management and redundant solutions, the nation would be positioned to focus on problems before they happen instead of problems after they occur.

V. CONCLUSION

This chapter outlines the research findings and recommends policy options. Included are implementation limitations and future research suggestions.

A. FINDINGS

Threats to the power grid are dynamic and widespread, and physical attacks which previously debilitated portions of the nation's electrical system. Natural disasters continue to damage or destroy essential components of the system, plunging significant portions and vast areas into darkness. Federal agencies are also aware of the threats and risks of a catastrophically successful cyberattack, yet national protection measures remain inadequate to prevent widespread blackouts. Highlighting these inadequacies and failures of protection mandates are the 45,000 North Carolinians who lost power due to a dual substation attack. It took crews several days to recover the downed portion of the grid, a testament to the fragility of the electrical system.[213]

Increasing regulations in both number and strength in an attempt to secure the grid have, so far, had a limited impact on grid resilience. Physical security regulations are currently in effect following previous physical attacks, yet the low-sophistication attack in North Carolina still succeeded. Regulating risk based only on a downed power grid scenario is an ineffective endeavor in the face of a Category 5 hurricane, a fast-moving wildfire, or a significant earthquake.

Achieving resilient and reliable grid operations requires solutions found in redundancy and microgrids, not just governance changes. Microgrids replicate the nation's interconnected power grid, only in a smaller geographical area. A microgrid may or may not be connected to the bigger grid. Instead of grid components being spread out over hundreds of square miles or multiple states, a microgrid may be dispersed throughout a college campus or a city block. It operates with smaller voltages because long-distance

[213] Bridget Johnson, "'Targeted' N.C. Substation Gun Attack Comes Amid Escalating Critical Infrastructure Threats," *Homeland Security Today* (blog), December 4, 2022, https://www.hstoday.us/featured/targeted-n-c-substation-gun-attack-comes-amid-escalating-critical-infrastructure-threats/.

electricity transmission is unnecessary. Furthermore, protecting their physical footprint over a smaller geographical area is more manageable as many components reside within already protected areas instead of open real estate. Microgrids are the prime example of a layered approach and have proven stable and reliable during critical events such as the Texas 2021 blackout and Superstorm Sandy. Their ability to detach from the primary power grid and operate through various power generation sources lends resilience to a microgrid.[214] Mandating microgrids for specific critical infrastructure will increase the power grid's strength and the nation's.

B. RECOMMENDATIONS

One recommendation is to increase protection requirements (mandates or governance) to include distribution systems, as NERC's 2010 report recommends.[215] Distribution systems, essentially the smaller-voltage neighborhood portions of the grid, account for 78% of the grid, depending on the metric used.[216] Currently, NERC requirements only apply to the bulk electrical grid, not the distribution grid. Congressional hearings, white papers, and joint resilience projects with the National Laboratories will reinforce the criticality of establishing security standards for the distribution portion of the grid. This action is the first step to requiring redundant paths of electrical delivery; including the previously omitted distribution side in federal reliability regulations.

Along the same lines, Congress should create a regulation requiring redundancy, two redundant layers deep, totaling three complete layers of the electrical grid. Microgrids can meet one or two layers depending on the design. This structure mirrors the UK standard and ensures two backup electrical paths should the primary delivery method fail.

Lastly, decrease the 35-day patching requirement to 48 hours, drastically reducing the time vulnerabilities are allowed to remain open. Allowing 35 days to patch vulnerabilities invites considerable risk to the grid.

---

[214] Adkisson, "Are Microgrids a Key to Grid Resiliency?"

[215] North American Electric Reliability Corporation and Department of Energy, *High-Impact, Low-Frequency Event Risk*, 14.

[216] North American Electric Reliability Corporation and Department of Energy, 86.

C. LIMITATIONS TO POLICY IMPLEMENTATION

Supply chain issues are currently a considerable limitation to developing redundant layers. Supply chain limitations span both microgrid components and existing grid components needed for redundant solutions.[217] Expanding NERC regulations, logically increasing costs for grid providers, is unlikely. If Congress creates new legislation, however, it could mandate NERC's compliance, potentially bypassing NERC's consensus-based process to create new regulations. Electrical providers will likely lobby against any initiative that increases expenditures.

D. FURTHER RESEARCH

Determining how best to integrate many microgrids into the existing power system while minimizing vulnerabilities will require further research.[218] This effort would include exploring how to minimize a networked microgrid's increased cyber vulnerabilities.[219] Grant funding or incentivizing the redundancy should be explored, especially concerning critical infrastructure facilities such as hospitals or water treatment facilities.

Additional research is needed to determine how much impact the UK's redundancy requirement has on grid reliability. Furthermore, a study extrapolating from the UK's success in preventing outages through an understanding of causes and the benefits of redundancy would be helpful as the United States continues to improve grid security.

E. CONCLUSION

The current federal regulations have improved the security of the bulk electrical system but falls well short of instilling grid operational reliability. Determined adversaries and natural disasters consistently continue to drop the grid. This thesis has outlined that increased governance is not an efficient or effective path to grid reliability outside of

[217] Jim Thomson et al., "Electric Power Supply Chains: Achieving Security, Sustainability, and Resilience," Deloitte Insights, September 29, 2022, https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/supply-chain-resilience-electric-power-sector.html.

[218] George Baker, "Microgrids – A Watershed Moment," *Insight* 23, no. 2 (June 2020): 32, https://doi.org/10.1002/inst.12295.

[219] William W. Anderson, Jr., "Resilience Assessment of Islanded Renewable Energy Microgrids" (master's thesis, Naval Postgraduate School, 2020), 192, https://hdl.handle.net/10945/66574.

expanding existing governance to include the currently omitted distribution system. Creating redundancy, on the other hand, is a proven path with specific solutions already in use. By pivoting away from legacy regulations and towards redundant systems, the nation can achieve electrical resilience with microgrids.

LIST OF REFERENCES

Adkisson, Kelsey. "Are Microgrids a Key to Grid Resiliency?" Pacific Northwest National Laboratory, December 2, 2021. https://www.pnnl.gov/news-media/are-microgrids-key-grid-resiliency.

Alicea, Juan E. "Puerto Rico's Homeland Security Readiness: Redesigning the Island's Power Grid to Improve Its Resiliency." Master's thesis, Naval Postgraduate School, 2019. https://hdl.handle.net/10945/62249.

Anderson, Jr., William W. "Resilience Assessment of Islanded Renewable Energy Microgrids." Master's thesis, Naval Postgraduate School, 2020. https://hdl.handle.net/10945/66574.

Baggott, Sean S., and Joost R. Santos. "A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid." *Risk Analysis* 40, no. 9 (September 2020): 1744–61. https://doi.org/10.1111/risa.13511.

Baker, George. "Microgrids – A Watershed Moment." *Insight* 23, no. 2 (June 2020): 32–35. https://doi.org/10.1002/inst.12295.

Beaton, Daniel T. "Testing Whether Distributed Energy Storage Results in Greater Resilience of Microgrids." Master's thesis, Naval Postgraduate School, 2021. https://hdl.handle.net/10945/67104.

Borenius, Seppo, Pavithra Gopalakrishnan, Lina Bertling Tjernberg, and Raimo Kantola. "Expert-Guided Security Risk Assessment of Evolving Power Grids." *Energies* 15, no. 9 (2022): 1–25. https://doi.org/10.3390/en15093237.

Campbell, Richard J. *Electric Grid Cybersecurity*. CRS Report No. R45312. Washington, DC: Congressional Research Service, 2018. https://crsreports.congress.gov/product/pdf/R/R45312/2.

Carter, Chelsea J. "Arkansas Man Charged in Connection with Power Grid Sabotage." CNN, October 12, 2013. https://www.cnn.com/2013/10/08/us/arkansas-grid-attacks/index.html.

Catrantzos, Nicholas. "No Dark Corners: Defending against Insider Threats to Critical Infrastructure." Master's thesis, Naval Postgraduate School, 2009. https://www.hsdl.org/c/abstract/?docid=33503.

Center for Climate and Energy Solutions. "Microgrids." Center for Climate and Energy Solutions. Accessed December 12, 2022. https://www.c2es.org/content/microgrids/.

Civil Contingencies Secretariat. *Keeping the Country Running: Natural Hazards and Infrastructure*. London: Civil Contingencies Secretariat, Cabinet Office, 2011. https://www.gov.uk/government/publications/strategic-framework-and-policy-statement-on-improving-the-resilience-of-critical-infrastructure-to-disruption-from-natural-hazards.

Clarke, Richard A., and Robert K. Knake. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press, 2019.

Clemente, Jason F. "Cyber Security for Critical Energy Infrastructure." Master's thesis, Naval Postgraduate School, 2018. https://hdl.handle.net/10945/60378.

Cybersecurity & Infrastructure Security Agency. "CISA National Cyber Awareness System – Current Activity." Cybersecurity Alerts & Advisories. Accessed January 9, 2023. https://www.cisa.gov/uscert/ncas/current-activity.

Deaton, Jeremy. "Here's Why the Lights Stayed on at NYU While the Rest of Lower Manhattan Went Dark During Hurricane Sandy." *Business Insider*, June 11, 2016. https://www.businessinsider.com/new-york-microgrids-2016-6.

Decker, Debra K., and Kathryn Rauhut. "Incentivizing Good Governance beyond Regulatory Minimums: The Civil Nuclear Sector." *Journal of Critical Infrastructure Policy* 2, no. 2 (Fall 2021): 19–43. https://doi.org/10.18278/jcip.2.2.3.

Defense Science Board (DSB) Task Force on Cyber Deterrence. *Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence*. Washington, DC: Defense Science Board, 2017. https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

Dempsey, Kelley, Nedim Goren, Paul Eavy, and George Moore. *Automation Support for Security Control Assessments: Software Asset Management*. Vol. 3. NISTIR 8011. Gaithersburg, MD: National Institute of Standards and Technology, 2018. https://doi.org/10.6028/NIST.IR.8011-3.

Department of Energy. "Electric Disturbance Events (OE-417) Annual Summaries." Office of Cybersecurity, Energy Security, & Emergency Response. Accessed April 14, 2022. https://www.oe.netl.doe.gov//OE417_annual_summary.aspx.

Department of Homeland Security. *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long Term Power Outage*. Washington, DC: Department of Homeland Security, 2017. https://www.fema.gov/sites/default/files/2020-07/fema_incident-annex_power-outage.pdf.

Dodge, Edward. "Distributed Energy in New York." *Edward T. Dodge* (blog), October 19, 2014. http://www.edwardtdodge.com/2014/10/19/distributed-energy-in-new-york/.

Energy Information Administration. "Canada Week: Integrated Electric Grid Improves Reliability for United States, Canada." Today in Energy, November 27, 2012. https://www.eia.gov/todayinenergy/detail.php?id=8930.

———. "Electric Sales, Revenue, and Average Price." Electricity, October 6, 2022. https://www.eia.gov/electricity/sales_revenue_price/.

Ericson, Sean J., and Daniel R. Olis. *A Comparison of Fuel Choice for Backup Generators*. NREL/TP-6A50-72509. Golden, CO: National Renewable Energy Laboratory, 2019. https://doi.org/10.2172/1505554.

Eto, Joseph H., Kristina H. LaCommare, Heidemarie C. Caswell, and David Till. "Distribution System Versus Bulk Power System: Identifying the Source of Electric Service Interruptions in the Us." *IET Generation, Transmission & Distribution* 13, no. 5 (2019): 717–23. https://doi.org/10.1049/iet-gtd.2018.6452.

Federal Bureau of Investigation. "Attacks on Arkansas Power Grid: Perpetrator Sentenced to 15 Years." FBI News, August 10, 2015. https://www.fbi.gov/news/stories/attacks-on-arkansas-power-grid.

Federal Emergency Management Agency. "Declared Disasters." FEMA Declared Disasters. Accessed February 21, 2023. https://www.fema.gov/disaster/declarations.

Federal Energy Regulatory Commission. "FERC Acts to Boost Grid Reliability against Extreme Weather Conditions." FERC News Releases, June 16, 2022. https://www.ferc.gov/news-events/news/ferc-acts-boost-grid-reliability-against-extreme-weather-conditions.

———. "Frequently Asked Questions (FAQs) About FERC." What is FERC?, January 25, 2022. https://www.ferc.gov/about/what-ferc/frequently-asked-questions-faqs/frequently-asked-questions-faqs-about-ferc.

Fetcher, Victoria. "Eastern U.S. Power Grid Orders Cuts, Triggering System-Wide Emergency." *Canada Today*, December 23, 2022, sec. Economy. https://canadatoday.news/ca/eastern-us-power-grid-orders-cuts-triggering-system-wide-emergency-200346/.

Gocke, Alison. "Nodal Governance of the U.S. Electricity Grid." *Duke Environmental Law & Policy Forum* 29, no. 2 (Spring 2019): 205–71. https://scholarship.law.duke.edu/delpf/vol29/iss2/1.

Grether, Nicole, Gloria Pazmino, Hannah Sarisohn, and Tina Burnside. "North Carolina County Announces Curfew as Nearly 40,000 Customers Remain without Power after 2 Substations Damaged by Gunfire." CNN, December 2022. https://www.cnn.com/2022/12/04/us/power-outage-moore-county-criminal-investigation?cid=external-feeds_iluminar_msn.

Heidorn Jr., Rich. "Substation Saboteurs 'No Amateurs.'" RTO Insider, November 15, 2013. https://www.rtoinsider.com/articles/23246-substation-saboteurs-no-amateurs-.

HersterDudley, Marcella R. "Building Resilience within DOD Microgrids by Considering Human Factors in Recovery Procedures." Master's thesis, Naval Postgraduate School, 2021. https://hdl.handle.net/10945/67135.

Hildebrand, Joshua P. "Estimating the Life Cycle Cost of Microgrid Resilience." Master's thesis, Naval Postgraduate School, 2020. https://hdl.handle.net/10945/66658.

Hinchman, David B. *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance*. GAO-22-105103. Washington, DC: Government Accountability Office, 2022. https://www.gao.gov/products/gao-22-105103.

H.R. *Lessons Learned from the Texas Blackouts: Research Needs for a Secure and Resilient Grid*, House of Representatives, 117th Cong., 1st sess. (2021), March 2021, 165. https://www.govinfo.gov/app/details/CHRG-117hhrg43633/CHRG-117hhrg43633/context.

———. *Blackout! Are We Prepared to Manage the Aftermath of a Cyberattack or Other Failure of the Electrical Grid?: Hearing before the Committee on Transportation and Infrastructure*, House of Representatives, 114th Cong., 2nd sess. (2016). Accessed October 6, 2022. https://www.govinfo.gov/app/details/CHRG-114hhrg99931/context.

———. *Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: Joint Hearing*, House of Representatives, 108th Cong., 1st sess. (2003), n.d., 246. https://www.govinfo.gov/app/details/CHRG-108hhrg99793/CHRG-108hhrg99793/context.

Humphreys, Richard. *Critical Infrastructure Security and Resilience: Countering Russian and Other Nation-State Cyber Threats*. CRS Report No. IF12061. Washington, DC: Congressional Research Service, 2022. https://sgp.fas.org/crs/homesec/IF12061.pdf.

Hussain, Akhtar, Van-Hai Bui, and Hak-Man Kim. "Microgrids as a Resilience Resource and Strategies Used by Microgrids for Enhancing Resilience." *Applied Energy* 240 (2019): 56–72. https://doi.org/10.1016/j.apenergy.2019.02.055.

ICF International. *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. Reston, VA: ICF International, 2016. https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf.

Jaksec, Gregory M. "Public-Private-Defense Partnering in Critical Infrastructure Protection." Master's thesis, Naval Postgraduate School, 2006. https://www.hsdl.org/?abstract&did=461639.

Johnson, Bridget. "'Targeted' N.C. Substation Gun Attack Comes Amid Escalating Critical Infrastructure Threats." *Homeland Security Today* (blog), December 4, 2022. https://www.hstoday.us/featured/targeted-n-c-substation-gun-attack-comes-amid-escalating-critical-infrastructure-threats/.

Jones, David O. "Reliability and Resilience Evaluation of a Stand-Alone Mobile Microgrid-Analysis and Experimental Measurements." Master's thesis, Naval Postgraduate School, 2022. https://hdl.handle.net/10945/71070.

Kain, Alissa R. "Investigation of Nanogrids for Improved Navy Installation Energy Resilience." Master's thesis, Naval Postgraduate School, 2021. https://hdl.handle.net/10945/67752.

Kelly, Morgan. "Two Years after Hurricane Sandy, Recognition of Princeton's Microgrid Still Surges." Princeton University, October 23, 2014. https://www.princeton.edu/news/2014/10/23/two-years-after-hurricane-sandy-recognition-princetons-microgrid-still-surges.

Kenward, Alyson, and Urooj Raja. *Blackout: Extreme Weather, Climate Change and Power Outages*. Princeton, NJ: Climate Central, 2014. https://assets.climatecentral.org/pdfs/PowerOutages.pdf.

Keogh, Miles, and Christina Cody. *Resilience in Regulated Utilities*. Washington, DC: National Association of Regulatory Utility Commissioners, 2013. https://pubs.naruc.org/pub/536f07e4-2354-d714-5153-7a80198a436d.

Knake, Robert. *A Cyberattack on the U.S. Power Grid*. Washington, DC: Council on Foreign Relations, 2017. https://www.cfr.org/report/cyberattack-us-power-grid.

Ladendorff, Marlene Z. "The Effect of North American Electric Reliability Corporation Critical Infrastructure Protection Standards on Bulk Electric System Reliability." PhD diss., Capella University, 2014. ProQuest.

Leber, Rebecca. "Winter Storms Put the U.S. Power Grid to the Test. It Failed." Vox, December 27, 2022. https://www.vox.com/energy-and-environment/2022/12/27/23527327/winter-storm-power-outages.

Lendvay, Ronald L. "Shadows of Stuxnet: Recommendations for U.S. Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack." Master's thesis, Naval Postgraduate School, 2016. https://www.hsdl.org/?abstract&did=792239.

Luna, Marcy de, and Amanda Drane. "What Went Wrong with the Texas Power Grid?" *Houston Chronicle*, February 16, 2021. https://www.houstonchronicle.com/business/energy/article/Wholesale-power-prices-spiking-across-Texas-15951684.php.

Mann, Joshua. "How Houston's Microgrids Fared Amid Blackouts." *Houston Business Journal*, February 24, 2021. https://www.bizjournals.com/houston/news/2021/02/24/sunnova-enchanted-rock-microgrids-texas-outages.html.

Maynard, Trevor, and Nick Beecroft. *Business Blackout: The Insurance Implications of a Cyber Attack on the U.S. Power Grid*. Lloyd's Emerging Risk Report – 2015. London: Lloyds of London and University of Cambridge, 2015. https://www.lloyds.com/news-and-insights/risk-reports/library/business-blackout.

McCaul, Michael. *Failures of Imagination: The Deadliest Threats to Our Homeland--and How to Thwart Them*. New York: Crown Forum, 2016.

McQuinn, Matthew E. "Energy Regulation Effects on Critical Infrastructure Protection." Master's thesis, Naval Postgraduate School, 2008. https://hdl.handle.net/10945/3753.

Mukherjee, Srijib. "Applying the Distribution System in Grid Restoration/NERC CIP-014 Risk Assessment." In *2015 IEEE Rural Electric Power Conference*, 103–5. IEEE Computer Society, 2015. https://doi.org/10.1109/REPC.2015.21.

National Academies of Sciences, Engineering, and Medicine. *Enhancing the Resilience of the Nation's Electricity System*. Washington, DC: National Academies Press, 2017. https://doi.org/10.17226/24836.

National Park Service. "Electrical Power Transmission and Distribution." Renewable Energy, September 21, 2016. https://www.nps.gov/subjects/renewableenergy/transmission.htm.

Nevius, David. *The History of the North American Electric Reliability Corporation*. Washington, DC: North American Electric Reliability Corporation, 2020. https://www.nerc.com/AboutNERC/Resource%20Documents/NERCHistoryBook.pdf.

North American Electric Reliability Corporation. "ERO Enterprise | Regional Entities." About NERC – Key Players. Accessed December 30, 2022. https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx.

———. *Extreme Cold Weather Preparedness and Operations*. Draft 1 of EOP-012-1. Atlanta, GA: North American Electric Reliability Corporation, 2022. https://www.nerc.com/pa/Stand/Project202107ExtremeColdWeatherDL/2021-07%20Initial%20Ballot_EOP-012-1_clean_051922.pdf.

———. *Glossary of Terms Used in NERC Reliability Standards*. Atlanta, GA: North American Electric Reliability Corporation, 2022. https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

———. *Implementation Plan: Project 2021–07 Extreme Cold Weather Grid Operations, Preparedness, and Coordination Reliability Standards EOP-011-3 and EOP-012-1*. Atlanta, GA: North American Electric Reliability Corporation, 2022. https://www.nerc.com/pa/Stand/Project202107ExtremeColdWeatherDL/2021-07%20Implementation%20Plan_second%20posting_082022.pdf.

———. *NERC Frequently Asked Questions*. Atlanta, GA: North American Electric Reliability Corporation, 2013. https://www.nerc.com/AboutNERC/Documents/NERC%20FAQs%20AUG13.pdf.

———. *Physical Security*. CIP Reliability Standards, CIP-014-1. Atlanta, GA: North American Electric Reliability Corporation, 2014. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

———. "Project 2014–04 Physical Security." NERC Standards, May 7, 2015. https://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx.

———. "Project 2016–02 Modifications to CIP Standards." NERC Standards. Accessed December 29, 2022. https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx.

———. "Reliability Guidelines, Security Guidelines, Technical Reference Documents, and White Papers." North American Electric Reliability Corporation. Accessed November 30, 2022. https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx.

———. *Reliability Standards for the Bulk Electric Systems of North America*. Atlanta, GA: North American Electric Reliability Corporation, 2022. https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf.

———. "US Reliability Standards." NERC Standards, November 28, 2022. https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx.

North American Electric Reliability Corporation, and Department of Energy. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. Washington, DC: Department of Energy, 2010.

Office of Electricity Delivery and Energy Reliability. *United States Electricity Industry Primer*. DOE/OE-0017. Washington, DC: Department of Energy, 2015. https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf.

Office of Personnel Management. "Approaches to Calculating Performance-Based Cash Awards." Policy, Data, Oversight: Performance Management. Accessed January 11, 2023. https://www.opm.gov/policy-data-oversight/performance-management/performance-management-cycle/rewarding/approaches-to-calculating-performance-based-cash-awards/.

Office of Technology Assessment. *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*. Washington, DC: U.S. Government Printing Office, 1990. https://ota.fas.org/reports/9034.pdf.

Ostfeld, Aminy, Michael Whitmeyer, and Alexandra Von Meier. "Block-Level Microgrids for Power System Resilience: Scaling and Impacts." In *CIRED Workshop*, 1–4. Ljubljana, Slovenia, 2018. http://www.cired.net/publications/workshop2018/pdfs/Submission%200322%20-%20Paper%20(ID-21011).pdf.

Parfomak, Paul. *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?* CRS Report No. R45135. Washington, DC: Congressional Research Service, 2018. https://sgp.fas.org/crs/homesec/R45135.pdf.

———. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*. CRS report No. R43604. Washington, DC: Congressional Research Service, 2014.

Pena, Ivonne, Michael Ingram, and Maurice Martin. *States of Cybersecurity: Electricity Distribution System Discussions*. NREL/TP-5C00-67198. Golden, CO: National Renewable Energy Laboratory, 2017. https://doi.org/10.2172/1347682.

Petri, Clark. "Assessing the Operational Resilience of Electrical Distribution Systems." Master's thesis, Naval Postgraduate School, 2017. https://hdl.handle.net/10945/56166.

Popik, Thomas, and Richard Humphreys. "The 2021 Texas Blackouts: Causes, Consequences, and Cures." *Journal of Critical Infrastructure Policy* 2, no. 1 (Spring 2021): 47–73. https://doi.org/10.18278/jcip.2.1.6.

Rose, Robert W. "Defending Electrical Power Grids." Master's thesis, Naval Postgraduate School, 2007. https://hdl.handle.net/10945/3677.

Rusco, Frank. *Electricity Grid: DOE Should Address Lessons Learned from Previous Disasters to Enhance Resilience, Report to Congressional Committees*. GAO-22-105093. Washington, DC: Government Accountability Office, 2022. https://www.hsdl.org/?abstract&did=868221.

Rusco, Frank, and Nick Marinos. *Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*. GAO-21-81. Washington, DC: Government Accountability Office, 2021. https://www.gao.gov/assets/gao-21-81.pdf.

S. *Electric Power Reliability: Hearing before the Committee on Commerce*, Senate, 90th Cong., 1st sess. (1967). Accessed April 13, 2022. ProQuest.

Schaefer, Michael L. "Operating in Uncertainty; Growing Resilient Critical Infrastructure Organizations." Master's thesis, Naval Postgraduate School, 2011. https://www.hsdl.org/?abstract&did=5540.

Scott, Christina. *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*. London: Cabinet Office, Civil Contingencies Secretariat, 2010. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf.

Sell, Tara Kirk, Onora Lien, and Eric Toner. "A Framework for Healthcare Resilience during Widespread Electrical Power Loss." *Journal of Critical Infrastructure Policy* 1, no. 1 (Spring 2020): 13–26. https://doi.org/10.18278/jcip.1.1.3.

Sherman, Tina Won. *Critical Infrastructure Protection: DHS Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure*. GAO-22-105973. Washington, DC: Government Accountability Office, 2022. https://www.gao.gov/products/gao-22-105973.

Taleb, Nassim. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2007.

Teague, Brendan, TJ Goss, and Mark Weiss. "Applying Risk and Resilience Metrics to Energy Investments." MBA professional report, Naval Postgraduate School, 2015. https://hdl.handle.net/10945/47883.

Tesla. "Powerwall." Tesla. Accessed March 15, 2022. https://www.tesla.com/powerwall.

Thomson, Jim, Marlene Motyka, Kate Hardin, and Jaya Nagdeo. "Electric Power Supply Chains: Achieving Security, Sustainability, and Resilience." Deloitte Insights, September 29, 2022. https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/supply-chain-resilience-electric-power-sector.html.

Weiss, Matthew, and Martin Weiss. "An Assessment of Threats to the American Power Grid." *Energy, Sustainability and Society* 9, no. 1 (2019): 1–9. https://doi.org/10.1186/s13705-019-0199-y.

Willson, Miranda. "North Carolina Substation Attack Exposes Grid Risks." *Energywire*, December 7, 2022. https://www.eenews.net/articles/n-c-substation-attack-exposes-grid-risks/.

Wood, Elisa. "Microgrids Help Texas as It's Forced to Undertake Rolling Blackouts." Microgrid Knowledge, February 16, 2021. https://microgridknowledge.com/microgrids-texas-blackouts/.

Young, Charles P. "Method or Madness: Federal Oversight Structures for Critical Infrastructure Protection." Master's thesis, Naval Postgraduate School, 2007. https://hdl.handle.net/10945/3022.

Young, Chuck. *Federal Electrical Emergency Preparedness Is Inadequate*. EMD-81-50. Washington, DC: Government Accounting Office, 1981. https://www.gao.gov/assets/emd-81-50.pdf.

Zhang, Zhen. "Environmental Review & Case Study: NERC's Cybersecurity Standards for the Electric Grid: Fulfilling Its Reliability Day Job and Moonlighting as a Cybersecurity Model." *Environmental Practice* 13, no. 3 (September 2011): 250–64. https://doi.org/10.1017/S1466046611000275.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California