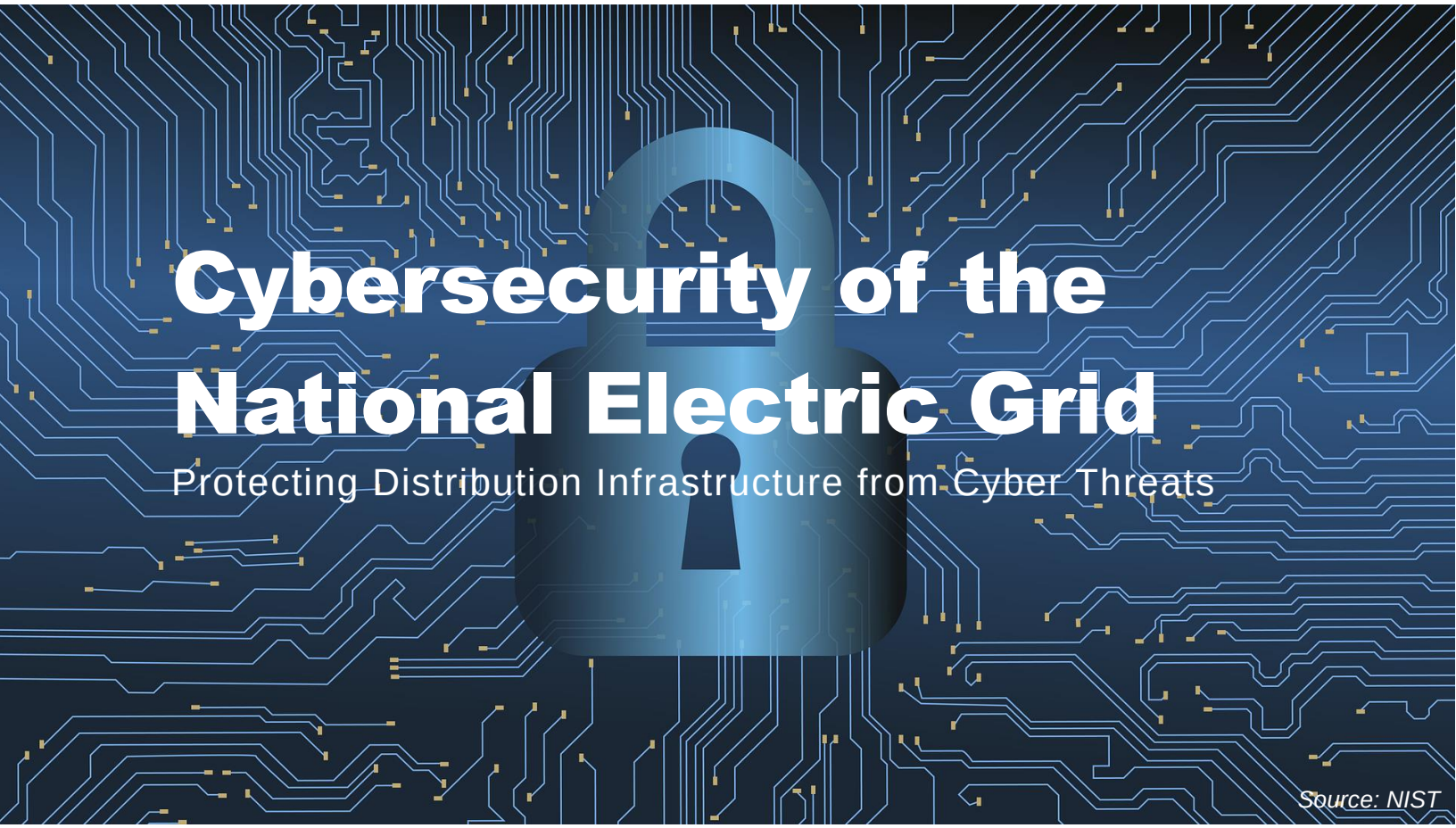
WISE | WASHINGTON INTERNSHIPS for STUDENTS of ENGINEERING

IEEE-USA



Cybersecurity of the National Electric Grid

Protecting Distribution Infrastructure from Cyber Threats

Source: NIST

McKenzy Heavlin

Institute of Electrical and Electronics Engineers

Summer 2022

Table of Contents

Foreword

About the Author

McKenzy Heavlin holds a bachelor's degree in Electrical Engineering with a minor in mathematics from NC State University in Raleigh, North Carolina. He is currently pursuing a master's degree in Electrical Engineering from NC State University. During his academic career, McKenzy has served as a two term Student Body President, Student Body Vice President, and is a member of the NC State chapter of IEEE. McKenzy is passionate about continuing his education through a Ph.D. program in Electrical Engineering focused on technologies aimed at modernizing the national electric grid and security of cyber-physical systems.

About the WISE Program

The Washington Internships for Students of Engineering (WISE) program was founded in 1980 through the collaborative effort of several professional engineering societies. As one of the premier DC internship programs, WISE prepares future engineering leaders to understand and contribute to the intersection of science, technology, and public policy. Over the course of 9-weeks, with the assistance of a faculty mentor in residence, WISE participants research federal laws and regulations to produce an original public policy solution to modern engineering challenges.

About IEEE

The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity. IEEE has over 400,000 members in more than 160 countries, more than 125,000 student members, 39 technical societies, over 1,000 standards, and sponsors more than 1,900 conferences worldwide. IEEE and its members inspire a global community through its highly cited publications, conferences, technology standards, and professional and educational activities.

Acknowledgements

Thank you to those who helped develop my ideas, provide encouragement, and offered their insights to this project. Thanks to Erica Wissolik, Russell Harrison, Aline McNaull, and the entire IEEE-USA team, in addition to the WISE Faculty Member in Residence Dr. Gilbert Brown. A special thanks to Thomas Pierpoint for providing valuable technical and industry support; Dr. Kenneth Lutz for assisting in the early stages of my project; Dr. Paula Gentius, Dr. Laura Bottomley, and Dr. Eddie Grant for their support throughout this program and my academic journey at NC State. Finally, thank you to my WISE cohort for their support throughout this process and making the summer one to remember.

Acronyms

BPS	Bulk Power System
C2M2	Cybersecurity Capability Maturity Model
CESER	Cybersecurity, Energy Security, and Emergency Response
CIE	Cyber-Informed Engineering
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CRISP	Cybersecurity Risk Information Sharing Program
CSF	Cybersecurity Framework
D-ERO	Distribution Electric Reliability Corporation
DHS	Department of Homeland Security
DOE	Department of Energy
E-ISAC	Electricity Information Sharing and Analysis Center
EO	Executive Order
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
IT	Information Technology
NERC	North American Electric Reliability Corporation
NICE	National Initiative on Cybersecurity Education
NIST	National Institute of Standards and Technology
OT	Operational Technology
R&D	Research and Development
RE	Regional Entities

Executive Summary

The electric grid and its supporting infrastructure are fundamental to the American way of life. Disruptions to any component of the grid may lead to widespread blackouts affecting business operations and creating significant challenges for the nation's population. With the increase of digital control systems and smart meters, power companies are turning to new devices and other advances in industrial controls to improve data collection and efficiency of the grid. However, new devices may pose a cybersecurity risk to an industry with an increasingly outdated infrastructure.

Current federal regulations and oversight authority of these systems is limited to transmission and interstate commerce—allowing for a patchwork of solutions to govern distribution infrastructure. There have been increased efforts to close gaps between federal agencies through information sharing, workforce education, and the development of standards and frameworks. These efforts face challenges as they are not enforceable and a variety of approaches to cybersecurity in the distribution industry continues to exist.

To address the ever-growing cyber challenges facing the electric grid and distribution infrastructure, the federal government should pursue the following public policy stances:

1. **Establish a Public-Private Cyber Rotational Program.** Federal agencies should create a rotational workforce program that allows cybersecurity experts from government agencies to rotate through key power companies to assist in the development, implementation, and advancement of local cybersecurity practices.

2. **Implementation of DOE CIE Strategy and other Educational Initiatives.** To continually educate the energy industry and other engineering disciplines, DOE should adopt 3-5 year implementation timelines of the Cyber-Informed Engineering Strategy to mitigate cyber risks and elevate cybersecurity in today's workforce.

3. **Creation of a Distribution Level Reliability Organization.** Congress should authorize FERC to create a new electricity reliability organization focused on electric distribution to ensure new technologies meet a high level of quality and cyber protection, and to protect national security from cyber threats originating in distribution infrastructure.

4. **Greater Focus on International Cyberattacks.** Congress should authorize greater funding for the Federal Bureau of Investigation and Department of Justice to pursue perpetrators of cyberattacks, especially attacks aimed at critical infrastructure of the United State and our allies.

The steps taken in the past decade to strengthen cybersecurity of America's electric grid are notable and a step in the correct direction. However, the Federal government and industry must recognize and act on the increasing cyber threat to distribution infrastructure to ensure security of the national grid.

Introduction

Blackouts and power outages remain a top concern for users and utility companies alike. Even with consistent effort to protect the physical infrastructure from outages, the past few years has seen an increase in the average duration of total annual power interruptions, with 2020 being the highest at just over 8 hours of interruptions per customer [1]. Outages—typically caused by extreme weather events, fallen trees or branches, or wildlife impacts to electric lines—are reported to and tracked by the US Energy Information Administration dating back to 2013. Over this period, there has been an increase in the average duration of annual electric power interruptions [Fig. 1]. These metrics provide valuable information and confirm the increasing need to upgrade our electric infrastructure to better protect from weather and other damage.

With the development of new technology that enables grid operators to better monitor and manage capabilities, the time is right to invest in these upgrades. New technologies, while offering great advantages, also introduce new challenges that the industry must consider. This is particularly true in the case of cybersecurity, which is an increasing concern for governments, industry, and companies. Cyberattacks allow malicious actors to cause chaos, disrupt day-to-day life, and expose private information. Addressing cyber threats used to be limited to information systems and databases, but new internet-enabled technologies now require more robust cybersecurity methods to protect processes and critical machines. The need to prevent these types of cyber threats is high as there are numerous examples of attacks on infrastructure that have significant impact on the daily routine of individuals.

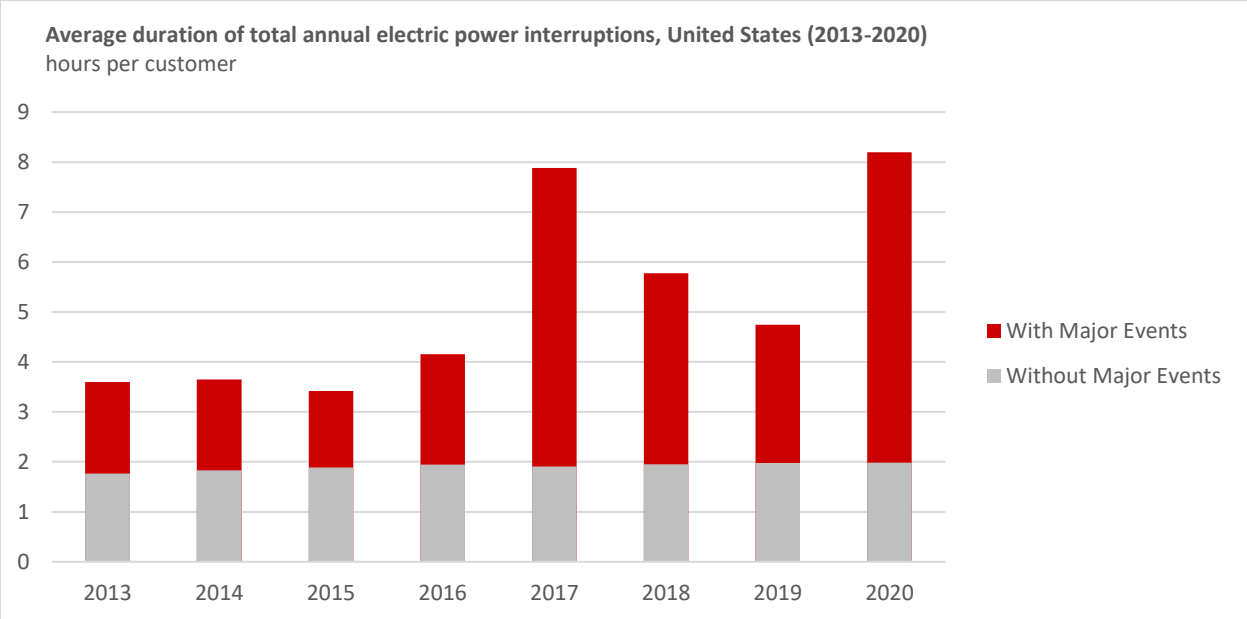


Fig. 1. Duration of Average Annual Electric Service Interruption over the past seven years. The data is reported to the Energy Information Administration through utility companies [52].

In 2021, Colonial Pipeline—which services 14 states and transports 100 million gallons of fuel daily—was the victim of a cyberattack that compromised its IT systems and caused panic. The attack targeted business operations of the company, rather than the pipeline infrastructure, but still caused the company to shut down fuel services until the concern was resolved. The shut off caused gas shortages, fuel outages, and panic buying among customers [2]. Other hackers in 2021 targeted Oldsmar, Florida where they unsuccessfully attempted to introduce deadly concentrations of water treatment chemicals into the public water supply [3]. On the international stage, the Costa Rican government experienced two cyberattacks in the late spring of 2022 that caused mass failure of tax offices, utilities, and public health services [4]. These events highlight the potential significance and impact these attacks can have on modern society.

Another international cyberattack that is demonstrative of the threat posed to American electric utilities is the 2015 Ukrainian power grid hack aimed at three power distribution companies. The attackers gained access through an employee's email and over the course of a few months were able to systematically gain access to critical electrical systems. Once initiated, the attack took only minutes to cause a massive blackout for hundreds of thousands of people and stop electric operators from switching the power back on [5]. This type of attack is not isolated to one country and the question is not if this can happen to America's power grid, but rather when.

Technical and Regulatory Background

The National Electric Grid

The United States' electric grid is often considered one of the largest man-made machines due to its massive scale, complex operating requirements, and the number of users it services.

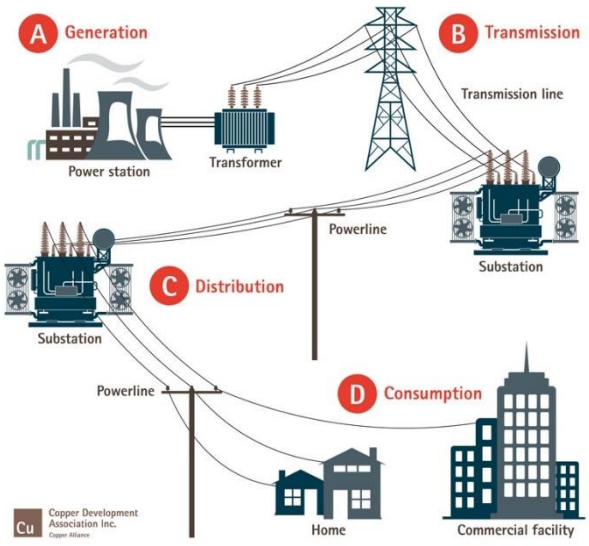


Fig. 2. Graphic of the electrical grid process in the United States—a complex system involving generation, transmission, and distribution [53].

The process of electrifying the United States begins with power generation—as seen to the right [Fig. 2a]. Electricity can be generated from numerous methods, such as hydro facilities, nuclear reactors, or steam turbines powered by natural gas, before it is transmitted across the country. Once generated, the voltage is increased and companies work to ensure efficient transmission to the desired location or substation [Fig. 2b]. From these substations, electricity can be distributed to large industrial plants, cities or towns, and residential houses. This section of the electric grid, and the focus of this paper, is known as the distribution infrastructure [Fig. 2c, Fig. 2d].

The foundation of the grid was built around the start of the 20th century and through continuous projects has developed into a system with “9,200 electric generating units with more than 1 million megawatts of generating capacity connected to more than 300,000 miles of transmission lines” [6] [Fig. 3]. Another technical challenge to managing the grid is the need to operate 24 hours a day for 7 days to ensure the balance of generation output and distribution usage. If the generation and usage become unbalanced for longer than a few minutes, there is a great risk of damaging generation equipment that will cause widespread blackouts in the region.

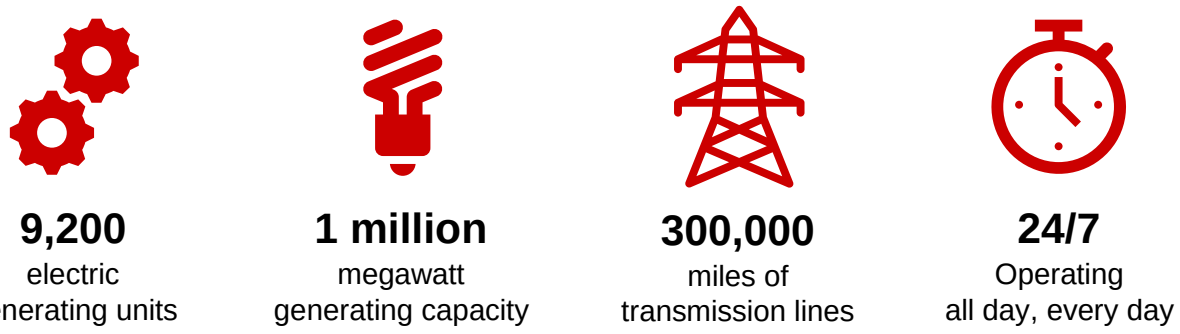


Fig. 3. Duration of Average Annual Electric Service Interruption over the past seven years. The data is reported to the Energy Information Administration through utility companies [52].

To operate within these conditions, the national electric grid is divided into four primary interconnections, the: Eastern Interconnection, Western Interconnection, Texas Interconnection, and Quebec Interconnection. Within these interconnects, shown in Fig. 4, electric utilities are tied together to form one large electric grid; a process which increases system efficiency. This nationwide system is often referred to as the bulk-power system (BPS) and includes “facilities and control systems necessary for operating an interconnected electric energy transmission network…” [7]. Jurisdiction for ensuring reliability of the BPS is given to the North American Electric Corporation (NERC) and Federal Energy Regulatory Commission (FERC). Reliability is defined as “operating elements of the bulk-power system within equipment…limits so that instability, uncontrolled separation, or cascading failures of such system will not occur…” [7]—in other words, reliability means ensuring electricity is available.

NERC can be further broken down into six Regional Entities (RE), the: Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), ReliabilityFirst (RF), SERC Reliability Corporation (SERC), Texas Reliability Entity (Texas RE), and Western Electricity Coordinating Council (WECC). The RE are responsible for assuring reliability of the BPS in their respective regions shown in Fig. 4.

Due to the complexity of each component of electrical infrastructure, RE are further composed of regional reliability coordinators. These coordinators, listed in Fig. 5, closely monitor the distribution components of the grid to ensure reliability and security. Beyond reliability coordinators, there are numerous individuals and companies that have a stake in the electrical distribution grid—such as independent system operators, regional

transmission operators, co-operative groups, public utility commissions, and power companies. These entities can change distribution systems within their jurisdiction to improve efficiency and customer service through a variety of methods, such as upgrading electricity meters, improving factory technologies, and introducing tools that help monitor usage and outages. While beneficial for the bottom line, these solutions pose unique challenges due to a lack of uniformity across the nation and cyber risks created with their implementation.

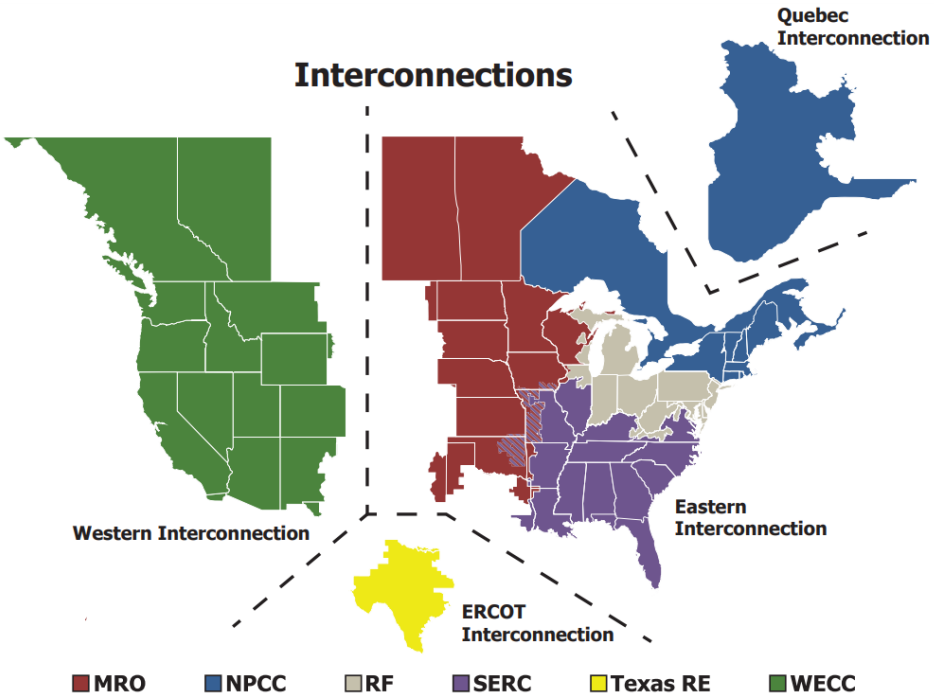


Fig. 4. Four interconnections in the North American electric infrastructure. These interconnections and their reliability are managed by the six regional entities [54].

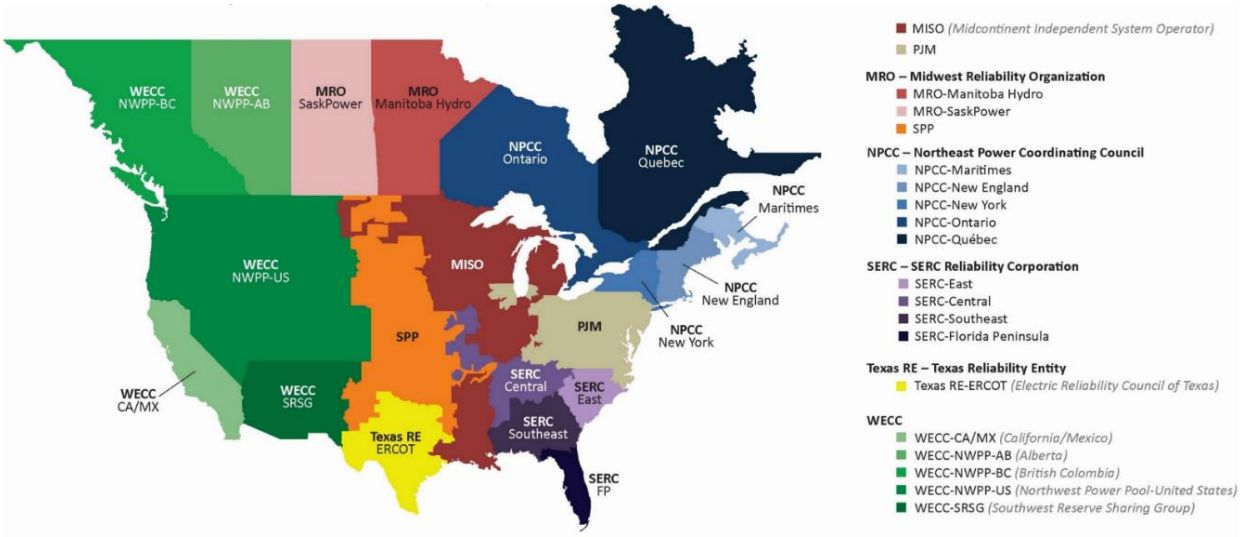


Fig. 5. NERC mapping of the current six regional entities with reliability councils listed on the right. Some RE and reliability councils share jurisdiction at the seams of these groupings. [54].

Cybersecurity Basics

Concerns of cyberattacks and breaches to private information and communication systems can be considered novel when looking at the lifetime of the electrical grid. Modern cyberattacks range from simple methods of attack easily found on the internet to sophisticated attacks perpetrated by enemy nations. Regardless of the attackers, cyber incidents often follow a pattern that can be distilled into five overarching stages: target, survey, deliver, breach, and affect [8] shown in Fig. 6.

Fig. 6. Five high level steps associated with a cyberattack. Advanced models exist for more sophisticated attacks, but the above figure provides an introduction into cyberattack methods [8].

Target – In this stage, attackers identify an entity, business, or corporation to launch a cyberattack. In the electric industry, this may be power companies, specific generation plants, or transmission substations. With new technology and the connectivity of the modern grid, any component (generation, transmission, and distribution) is a potential target for a cyberattack.

Survey – Once the target is identified, the attackers review the target's cybersecurity practices, infrastructure, and digital assets to determine vulnerabilities. Often this information will be protected by the target's cybersecurity practices, so the attackers are looking to exploit individuals who do not strictly follow the target's rules. Once the attacker has identified potential entry points, the attacker moves onto the delivery stage.

Delivery – At this stage, the attackers attempt to deliver malicious software to the identified vulnerability. This stage of cyberattacks may be simple, such as an email with a corrupt attachment from a spam email, or more difficult to identify. Depending on the attacker's eagerness, they could hack a trusted website with lesser cybersecurity measures to deliver the malware to the target.

Breach – Once the attackers have successfully accessed the target's network, if they remain undetected, they can work over days or months to affect the target's systems. This stage of a cyberattack may focus on sensitive business information, private customer data, or physical systems connected to the target's network—all important considerations for power companies and other stakeholders in the electric grid. In extremely malicious cyberattacks, this stage may be utilized to learn as much as possible about the target and plan strategic attacks against their systems.

Affect – Closely related to the breach stage, the affect stage depends on the attacker's motivation and goal. If they need continual access, they may create a "back door" in the target's system to allow for easy access during the next attack. If they gathered the information they were searching for, they may attempt to destroy evidence and files

associated with their attack. However, in most utility industries and certainly the electric industry, any extremely sophisticated attack is likely looking to cause as much damage as possible. To do this, hackers may shut down components, prohibit the control of equipment, or change the operating view of the system to fool operators into shutting down or damaging the system [9].

It is important to note that the stages above are an extremely high-level overview of a cyberattack. More thorough frameworks for understanding cyber threats are readily available for power companies and the electric industry to utilize. For example, MITRE ATT&CK® "is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations" [10] that hosts a complex cybersecurity matrix for industrial control system with 12 stages and numerous techniques associated with each stage. Frameworks like MITRE offer a key distinction that can benefit the electric power industry: they have separate approaches to cybersecurity of operational technology (OT) and information technology (IT).

For general purposes, OT systems can be thought of as systems that have digital control components that elicit a physical response—the software running a machine recognizes an error and instructs the machine to shut down, thus stopping the physical process. On the other hand, IT systems are "a collection of computing and/or communications components and other sources that support one or more functional objectives of an organization…[and] are used in the acquisition, storage, manipulation, display, and/or movement of data" [11].

The difference between OT and IT cybersecurity is another important distinction to make when protecting critical infrastructure like the electric grid, as traditional IT security methods may not translate to OT systems. OT security measures have the tendency to increase latency, the delay of data transfer, in the system which ultimately slows down production and decreases efficiency. IT security measures tend to avoid latency challenges as there are numerous ways to improve the efficiency of a fully digital system.

History of Federal Regulations

The regulatory framework of the electric grid has a complex history tied to system failures. As such, there are numerous stakeholders ensuring the security and reliability of the grid. This section presents the key departments, agencies, and regulatory bodies with authority over aspects of the electric grid. A timeline is shown in Fig. 7.

The Federal Power Act

The earliest effort to establish federal oversight of the electric grid was the Federal Power Act of 1935. This act amended law to create the Federal Power Commission (FPC) with the express purpose of regulating "…the transmission of electric energy in the interstate commerce and the sale of electric energy at wholesale in interstate commerce" [7]. The authority provided to the FPC is narrow and strictly focused on

interstate commerce, or the transmission of electricity, as not to interfere with state regulations of electric power.

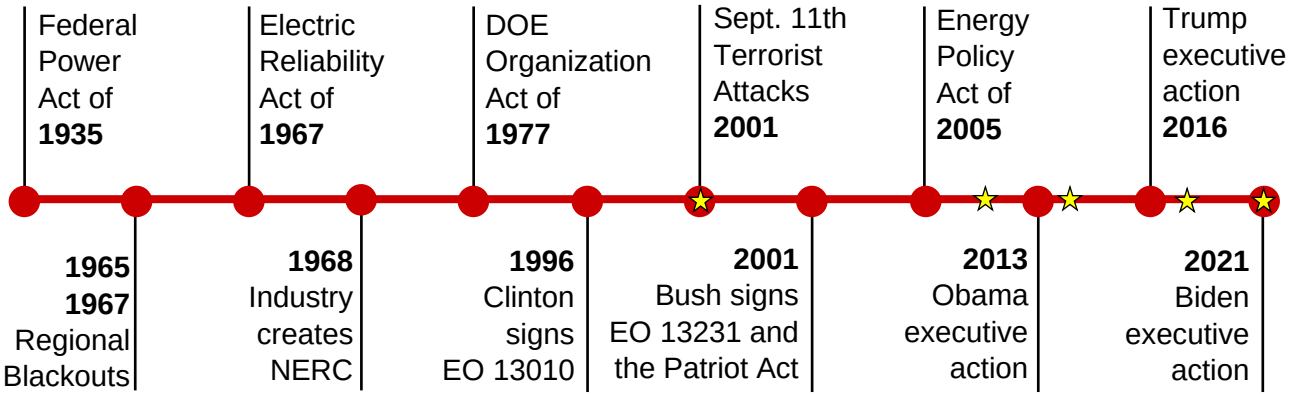


Fig. 7. Timeline showing key Federal actions that shaped the regulatory environment of the electric grid. Stars represent legislation that become public law—these pieces are discussed further in the "Federal Law Related to Cybersecurity and the Grid" box on page 9.

While the Federal Power Act created the regulatory authority for the FPC, there was little initial focus on issues of reliability. However, a significant blackout in the northeast in 1965 and a cascading blackout in 1967 led to the passage of the Electric Power Reliability Act of 1967 [12]. This act expanded FPC's ability to ensure the operability of electricity across the country and solidified the importance of electrical reliability in national policy. After the 1965 blackout, industry leaders understood the need for cooperation and coordination which led to the formation of the National Electric Reliability Council (NERC) in 1968. NERC later changed its name to the North American Reliability Corporation, as Canadian members joined the council and the organization consolidated with other regional entities.

Following the formation of NERC, Congress passed the Department of Energy Organization Act of 1977. This act created the Federal Energy Regulatory Commission (FERC)—an independent agency within DOE [13] with five commissioners appointed by the President. With the reorganization, FERC maintained much of FPC's original responsibilities, and the scope of authority remained strictly focused on "the interstate transmission of electricity, natural gas, and oil" [14].

Over the next few decades, companies and government worked to further determine the best methods for oversight and competition in the electric industry. While these decisions affected how regulatory bodies and businesses responded during this period, their focus remained on the reliability of the electric grid and improving service for the U.S. population.

National Security Concerns

When comparing the origins of federal oversight of electricity infrastructure to current practices, there is one concept that clearly separates the two—national security.

Before the terrorist attacks on September 11, 2001, industry was the primary advocate for protecting the electrical grid and other infrastructure. Government involvement was primarily driven through Presidential Executive Orders, as Congress and legislation were slow. In 1996, President Clinton signed Executive Order 13010, Critical Infrastructure Protection, which established the President's Commission on Critical Infrastructure Protection. The goal of the commission was to provide a comprehensive review and policy proposal of physical and cyber challenges associated with "telecommunications, electrical power systems, gas and oil storage and transportation…and the continuity of government" [15]. President Clinton's EO 13010 was one of the first documents citing the importance of critical infrastructure and the associated cyber concerns with the technology.[1]

Following September 11, 2001, the country intently focused on protecting America from foreign threats and adversaries. In October 2001, President Bush signed EO 13231, Critical Infrastructure Protection in the Information Age, "in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age…" [16]. Order 13231 was closely followed by the USA PATRIOT Act of 2001 which codified the definition of critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [17]. The electric grid is included under this broad definition of critical infrastructure and as such, government and industry's approach to the security of the grid changed significantly.

Modern Regulatory Framework

The current state of regulations for the electricity industry was formalized in mid-2005 with the passage of the Energy Policy Act. This act amended the Federal Power Act to establish improved methods to ensure reliability, encourage technological innovation, and prevent electricity market manipulation. The first key change brought forward by this act was the inclusion of the bulk-power system (BPS) in FERC jurisdiction. This allowed FERC oversight of most of the transmission components of the national grid and supports the security of electrical infrastructure.

The second key change in this bill was the authorization allowing FERC to select an electric reliability organization "…to establish and enforce reliability standards for the bulk-power system" [18]. Previously, industry was responsible for establishing and following reliability standards, as seen by the formation of NERC. However, the Energy Policy Act of 2005 cleared the path for direct federal oversight of industry practices and standards. Following an application process, NERC was selected as the electric reliability organization and charged with creating and enforcing reliability standards

[1] Legislation before 9/11 related to cyber information and protection focused on allocation and appropriation of funds for military and defense purposes.

relating to the transmission of electricity. These standards, known as NERC reliability standards, are approved by FERC and focus on planning and operating the electric grid. With the establishment of NERC as the electric reliability organization, the current federal oversight structure was completed by the late 2000s. Since that time, much of the action taken on the Federal level was focused on R&D and educating the power industry workforce or through presidential executive action. These efforts are summarized below in "Federal Law Related to Cybersecurity and the Grid" [Table 1].

Federal Law Related to Cybersecurity and the Grid

An increasing amount of legislation in the past two decades has focused on general cybersecurity initiatives and cybersecurity of electric infrastructure—a few laws are below.

Cyber Security Research and Development Act (2001) – *Public Law 107-305*
Authorizes and provides funding for the National Science Foundation and NIST to create and lead R&D efforts focused on computer and network security. Focuses on higher education institutions as sources to support information R&D [45].

Energy Independence and Security Act (2007) – *Public Law 110-140*
Omnibus energy bill, however, *Title XIII—Smart Grid* provided clear instruction and support for technologies to modernize the electric grid using smart sensors. Authorized reports, advisory committees, and R&D appropriations to spur grid innovation [46].

Cybersecurity Enhancement Act (2014) – *Public Law 113-274*
Law supporting the development of three key areas of cybersecurity: public-private partnerships, workforce education and development, and advancement of technical standards. Amended the NIST Act (15 U.S.C. 272(c)) to include requirements for continual efforts to assist cybersecurity best practices in critical infrastructure [47].

DOE Research and Innovation Act (2017) – *Public Law 115-246*
Provides guidance and establishes DOE policies for energy research, R&D engagement with industry and academia, and authorizes "energy innovation hubs" focused on numerous topics, including smart grid technologies and cybersecurity [48].

Federal Rotational Cyber Workforce Program Act (2021) – *Public Law 117-149*
Authorizes the establishment of a voluntary, rotational workforce program within select Federal agencies that Federal cyber workers may participate in to broaden and strengthen their technical skillset [49].

Infrastructure Investment and Jobs Act (2021) – *Public Law 117-58*
Division D—Energy, Title I establishes grants to protect electrical equipment, competitive funding for resiliency R&D, and programs to develop transmission lines and technologies to enhance smart grid capabilities. Enhances cybersecurity by establishing a program to test cybersecurity capabilities of new BPS products and technologies, developing implementation methods of standards and frameworks, incentives for cyber investments, cyber grants for rural and municipal utilities, and funding for cyber R&D for the energy sector [50].

Table 1. Federal Law Related to Cybersecurity and the Grid. The table above summarizes pieces of legislation that became public law since 2001 to address cybersecurity.

A key document that provides precedence and authority for executive cybersecurity action is President Obama's 2013 Executive Order 13636, Improving Critical Infrastructure Cybersecurity. This order was the first executive order aimed at improving the cybersecurity protections of critical infrastructure and outlined a detailed course of action to do so [19]. Previous executive actions lacked the technical expertise associated with new technologies or focused on other critical aspects of national security. EO 13636 led to the development of critical frameworks that are utilized today and established the groundwork for future executive actions relating to cybersecurity of the electric grid. President Obama further strengthened this order by releasing EO 13691 which encouraged the creation of sector-specific information sharing groups for industry and allowed for greater participation with the Federal government [20].

President Trump also took executive action through various orders and strategies. Trump released EO 13800, EO 13870, and EO 13920 which, respectively, required Federal agencies to implement the *NIST Framework for Improving Critical Infrastructure Cybersecurity* [21], created a Federal cyber workforce rotation program and an annual cybersecurity competition for Federal employees [22], and declared the threat to the BPS a national emergency and prohibited the acquisition of BPS equipment from foreign adversaries or companies [23].

Federal Cyber Initiatives

Operating within its limited scope, the Federal government has identified a few key methods to assist industry prepare for and respond to a cyberattack. Current Federal cyber initiatives focus on creating frameworks and standards that uphold best practices, enabling information sharing across industry and the government, and workforce development to train new cyber experts.

1. Frameworks and Standards

Frameworks and standards define how the Federal government works with industry to ensure strong cybersecurity. Depending on the agency and component of the grid, industry may be required to adhere to the standard. However, most of the guidance issued by Federal agencies is nonbinding and dependent on whether individual organizations choose to utilize the findings.

1.1 Critical Infrastructure Protection Standards

The Critical Infrastructure Protection (CIP) standards are an example of orders that are enforceable and must be followed by the transmission industry. These standards set forth technical requirements for owners and operators of infrastructure critical to the success of the BPS. CIP standards are developed, updated, clarified, or withdrawn through an open process—allowing for industry engagement at all steps of CIP standards. Once a topic has been identified and accepted by the NERC Reliability Standards staff, the draft will rotate though a process of informal feedback, open comment, and formal stakeholder feedback and voting before being sent to the NERC

Board of Trustees[2]. Once adopted by the Trustees, the standard must be approved by FERC before the standard can be implemented and effective [24].

The first CIP standard was adopted by the NERC Trustees in late 2006, with an effective date of June 2007. In total there have been 98 CIP standards adopted by the NERC Board, with only 65 becoming effective standards and the remaining either being superseded by FERC guidance, another CIP standard, or not being submitted for FERC approval. Some standards also are created with a specific inactive date established in the body, after which the standard can no longer be enforced. To date, there are 13 CIP standards that are subject to enforcement by NERC, with 6 additional standards subject to future enforcement once approved by FERC [25].

Although CIP standards are helpful standards, it is important to note that they are only enforceable on the BPS, not the distribution grid. This is due to how the regulatory framework was developed over the years and the authority of the federal government. With a limited authority, the standards were developed for the transmission sector which means the technical requirements are tailored to transmission equipment and processes. Efforts to apply current CIP standards to distribution cyber systems would be immensely challenging, create a massive burden on the industry, and be met with strong pushback from industry leaders.

1.2 Cybersecurity Capability Maturity Model

The Cybersecurity Capability Maturity Model (C2M2) is a DOE initiative lead by CESER that developed "a free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments" [26]. C2M2 was originally developed in 2012 and subsequent editions were released in 2014 (version 1.1), 2021 (version 2.0), and 2022 (version 2.1). Throughout its development, the tools have provided assistance to energy industry while also supporting non-energy organizations. The goals of C2M2, shown in Fig. 8, are focused on evaluating the current cybersecurity practices of the organization, information sharing, closely tracking company cyber efforts, and prioritizing cybersecurity throughout all aspects of the company.

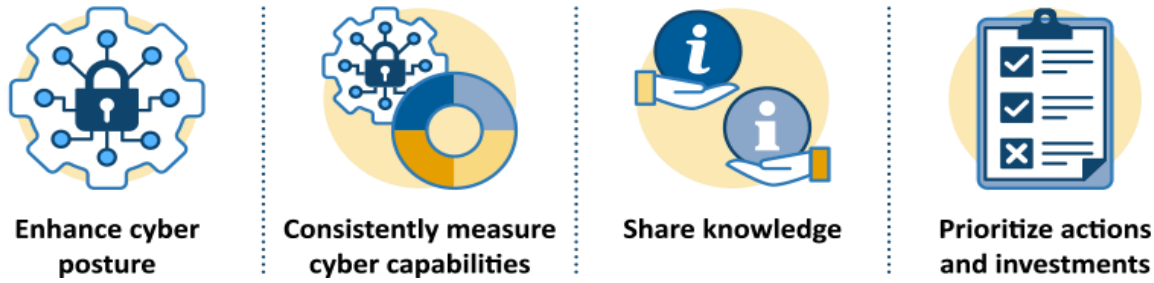


Fig. 8. Goals of DOE's Cybersecurity Capability Maturity Model. The model assists the energy industry evaluating and improving their cybersecurity practices and resources [26].

[2] A more in-depth review of developing NERC Reliability Standards is available at https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

The structure of the model is a complex grouping of cybersecurity practices that are further developed by maturity indicators that help an organization evaluate its cybersecurity standing and set strategic goals. The model contains 10 domains, each with unique approach objectives and management objectives with four different maturity levels for each domain. Overall, there 356 practices that compose the C2M2 model [26]. Fig. 9 provides a structural overview of the model including notes.

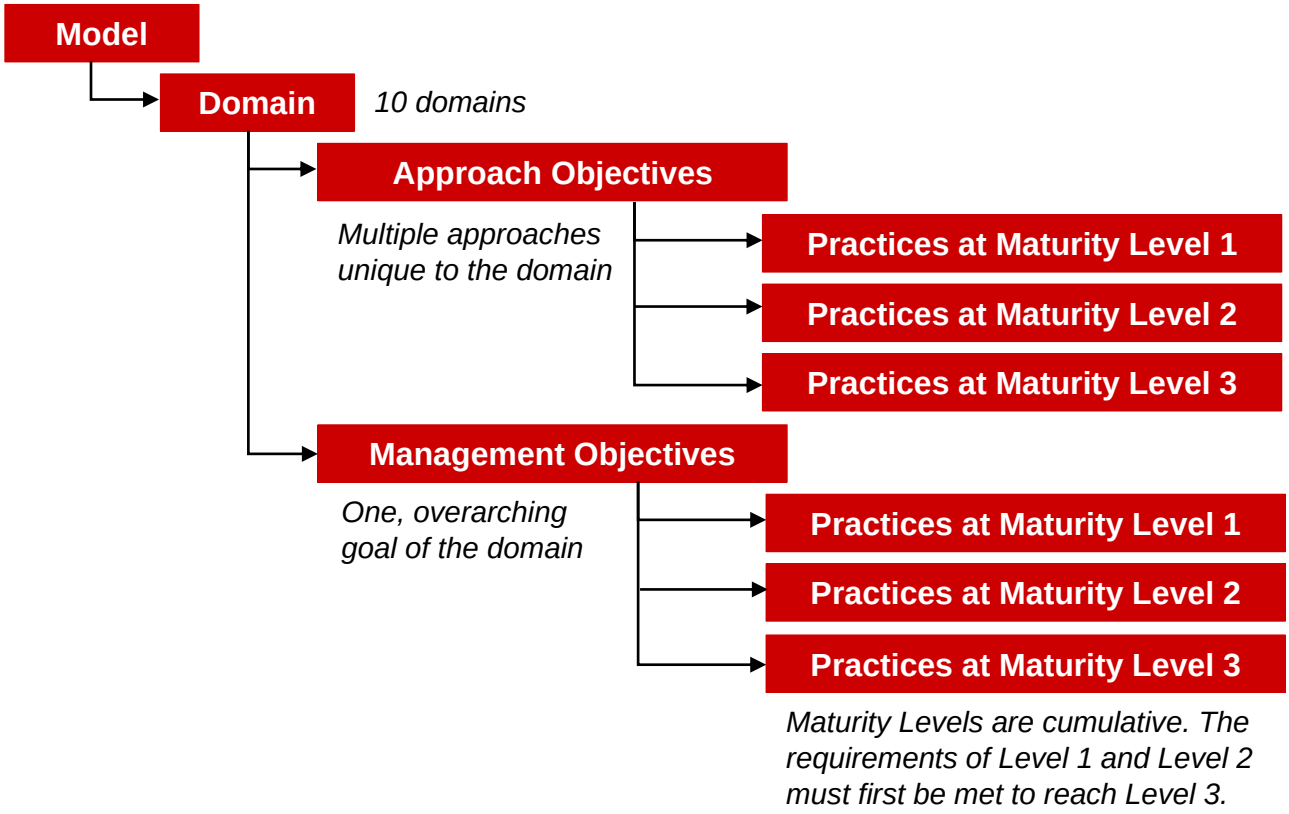


Fig. 9. Composition of the C2M2. This structure is repeated for each domain in the model [26].

The C2M2 model is an example of efforts by the Federal government to address cyber threats and it relies on creating tools and resources that enable sectors to make informed decisions regarding their cyber positioning and potential threats. According to the DOE, they have responded to more than 2,400 requests for the C2M2 from owners and operators in the US critical infrastructure sectors [26]. A sector breakdown is provided in Fig. 10.

A noted strength of the C2M2 model is the distinction between OT and IT systems throughout the domains and objectives—allowing it to apply quickly to new technology and advances in industrial control systems. For the energy sector, this enables owners and operators to install upgrade systems, review the cybersecurity of the new technology, and address any identified gaps. However, these types of resources are only successful if industry sectors recognize the risk to their company, utilize the tool, and provide routine feedback to DOE and CESER.

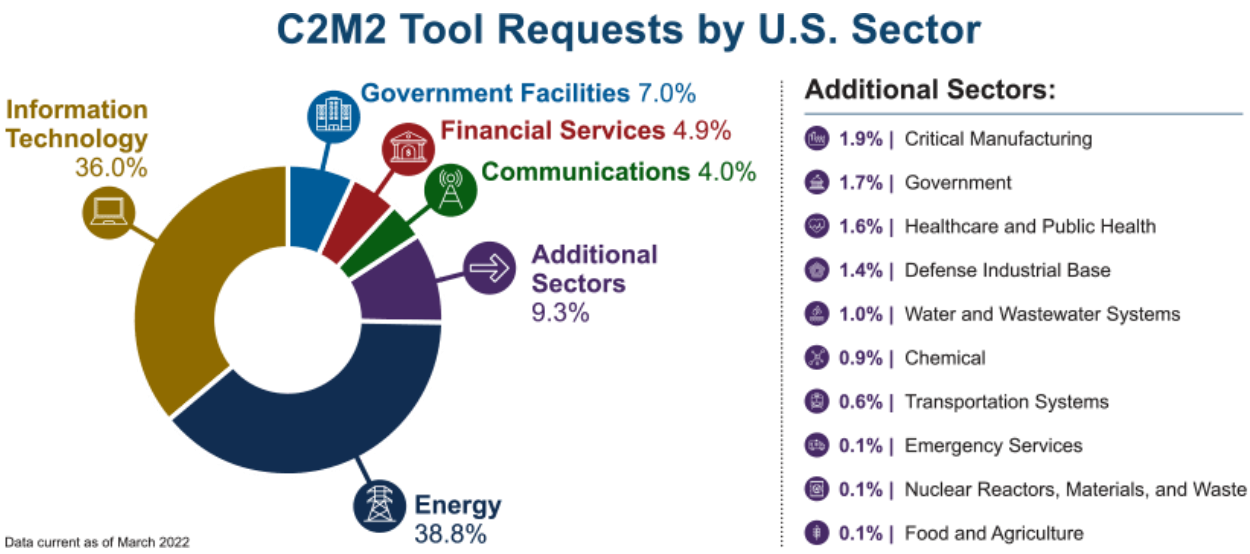


Fig. 10. Requests for the C2M2 by sector [26].

1.3 NIST Cybersecurity Framework

Another initiative established by the Federal government that has seen widespread success due to its flexibility and breadth is the NIST Cybersecurity Framework (CSF) [27]. The CSF was developed over the course of 2013 following President Obama's EO 13636 that instructed NIST to create a framework that included practices to "align policy, business, and technological approaches to address cyber risks" [19].

The CSF is structured to allow for application in any industry but was developed specifically for critical infrastructure sectors. There are three components to the CSF, the: core, tiers, and profile. The core is a list of cybersecurity principles that enable the success of the user. The core is further divided into 5 functions, 23 categories, 108 sub-categories, and numerous informative references per sub-category, as shown in Fig. 11. This breakdown enables a clear path from high-level, abstract cybersecurity topics to specific technical actions that can be taken. As such, one of the key strengths of the CSF is its ability to enable communication and understanding across engineers, managers, and company executives.

The tiers, also known as implementation tiers, allow the user to evaluate the current status of cybersecurity management in the company. The tiers "describe an increasing degree of rigor, and how well integrated cybersecurity risk decisions are into broader risk decision, and the degree to which the organization shares and receives cybersecurity info from external parties" [27]. Unlike the C2M2, the tiers do not exactly represent the maturity of the company's cyber positioning. Finally, the profile portion of the CSF allows a user to understand their cybersecurity risks and priorities in relation to overarching business objectives and strategies. The profile section can assist with the communication of cyber challenges to administrators and provide a path forward.

The CSF is one of the more successful models due to its high flexibility and applicability to companies' current structure and approach to cybersecurity. Since its release, NIST

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Fig. 11. Core of the NIST CSF with 5 high level functions, 23 categories, 108 subcategories, and lists of informative references [27].

has further developed resources to complement the framework and bolster cybersecurity of critical industries. They are currently working on updates to the framework with the goal of releasing version 2.0 of the CSF. The updated model will address a variety of concerns by industry and other stakeholders that are noted in a public feedback document—such as providing guidance for implementing the CSF and ways to evaluate cybersecurity practices and framework success [28].

2. Information Sharing

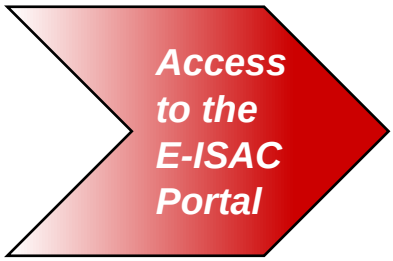
Recognizing the risk that a significant cyberattack may have on the nation, many of the electric utilities participate in voluntary information sharing. These programs allow companies to share specifics about an emerging threat they have detected, the process utilized during a cyberattack, and mitigation plans to prevent future incidents.

2.1 Electricity Information Sharing and Analysis Center

The Electricity Information Sharing and Analysis Center (E-ISAC) was created in 1999 by NERC to provide "the electric industry quality analysis and rapid sharing of security information on how to mitigate complex, constantly evolving threats to the grid" [29]. Membership to E-ISAC is open to any electric owner, operator, or employee in North America. E-ISAC also partners with larger organizations such as state and local governments to support their cybersecurity efforts. The primary benefits of joining E-

ISAC are accessing the information portal and the numerous incident bulletins, security briefings, and white papers only available to members.

E-ISAC also publishes numerous documents to assist industry with the assessment of threats. These include incident bulletins that provide real-time analysis of cyber and physical threats to the grid, security briefings on current concerns, and reports by E-ISAC analysts on emerging cyber threats [51].



The E-ISAC portal allows members to voluntarily share information regarding their cyber systems and processes and enables "users to monitor, mitigate, and respond to emerging and current threats" [51]. The level of information shared on the portal is determined by the user with the option of posting anonymously.

E-ISAC also works to promote the cybersecurity and protection of the grid through conferences and a nationwide security exercise. The annual GridSecCon, co-hosted by NERC, the E-ISAC, and ReliabilityFirst, is the security conference for the electric grid that is open for all general, government, and student attendees. GridSecCon offers the opportunity to learn from experts in topics critical to the success of the grid; the 2022 event will have sessions focused on "cyber or physical security, supply chain issues, diversity and inclusion, human performance, and security policy matters" [30]. Conferences, such as GridSecCon, allows industry and cyber workers to stay up to date on emerging threats, learn about best practices to address cyber concerns, and develop their cybersecurity skills.

GridEx is the second initiative from the E-ISAC that aims to prepare electric owners and operators for security threats. Hosted every two years, GridEx is the largest grid security exercise in North America with "more than 700 planners" participating in 2021 [31]. The exercise tests participants' response and recovery plans to coordinated cyber and physical attacks on the grid. Afterwards, the E-ISAC publishes a report overviewing the lessons learned and recommendations to strengthen industry security practices.

2.2 Cybersecurity Risk Information Sharing Program

The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership that aims to increase the energy sector's ability to constantly monitor their networks and infrastructure using publicly available data, in addition to classified government information. CRISP's unclassified functions are supported by E-ISAC, DOE's Pacific Northwest National Laboratory, and the Argonne National Laboratory while its classified analysis is managed by CESER [32]. CRISP is funded by a shared-cost model which operates partially from Federal funding and a participation fee paid by owners and operators [33]. Due to its structure, CRISP allows the government and the

electric industry a robust understanding of ongoing cyber threats and proposes tangible methods to address the concerns.

CRISP is an ideal process for monitoring an electric utility's cyber space as it does not require any internal changes to the company's cyber practices. Once the company joins as a partner, a passive information sharing device is installed outside the company's firewalls to collect data. The information is gathered, encrypted, and sent to analysts who review the data to identify any anomalies and signs of potential cyber threats. The analysts create a thorough CRISP result, using classified and unclassified data, which is shared with the company along with proposed cyber measures to increase protection. A flowchart of the process is shown below in Fig. 12.

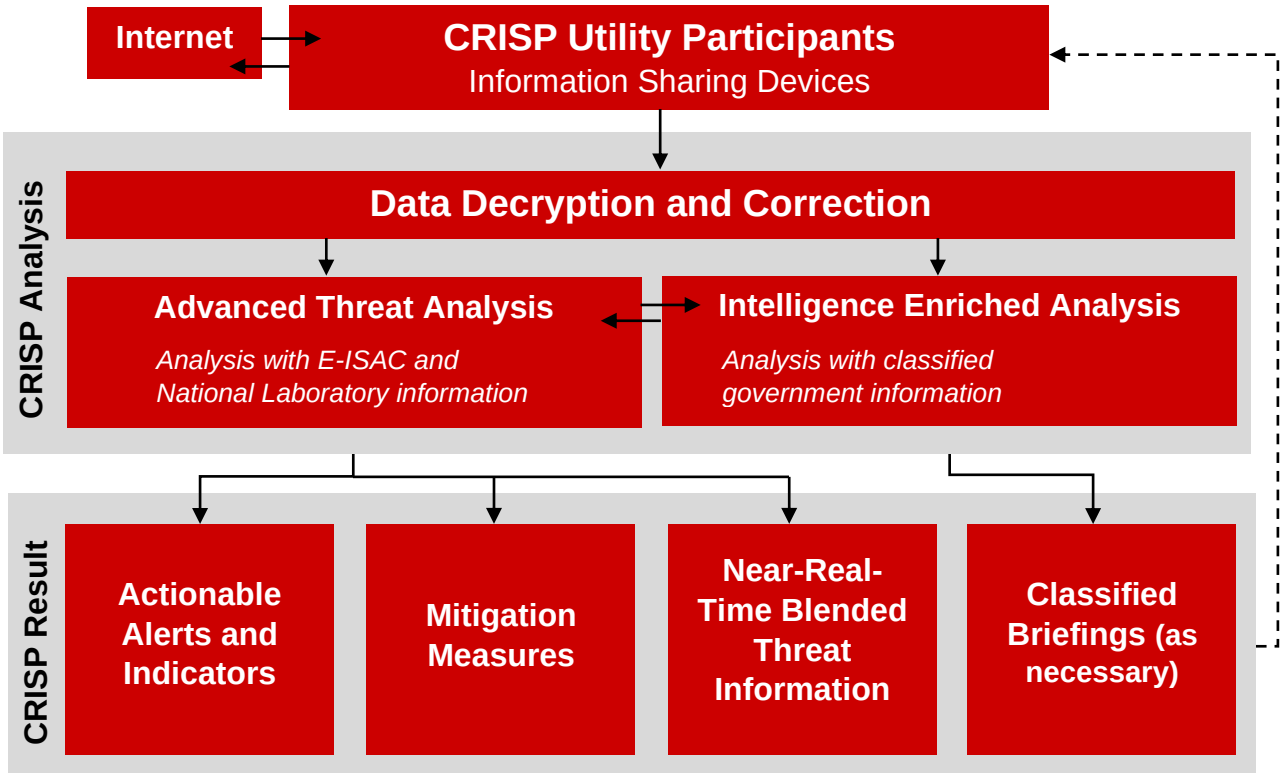


Fig. 12. Flowchart showing the CRISP analysis process and the outcomes associated using unclassified information and classified information [32].

3. Workforce Education

The success of any cyber initiative is dependent on a highly skilled workforce that can implement protection strategies and recognize cyber threats. Although these workers provide critical support to industry, there is currently a shortage of workers who can fill these positions. The U.S. Bureau of Labor Statistics reports that employment of information security analysts is expected to grow 33 percent from 2020 to 2030 [34]. This growth requires the attention of national strategies to teach new cyber experts and instill cybersecurity practices in industry.

3.1 National Initiative on Cybersecurity Education

The National Initiative on Cybersecurity Education (NICE), created and led by the NIST, is one of the prominent federal efforts to educate the workforce and create a pathway for new cybersecurity jobs. NICE is a collaborative initiative between NIST, academia, and private industry aimed to “energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development” [35]. NICE achieves these goals through a variety of methods, but one way is through federal funding for programs and projects. For example, the National Integrated Cyber Education Research Center creates cybersecurity and STEM resources and activities for K-12 teachers to utilize free of charge with the goal of educating the future cyber workforce [36]. NICE also sponsors conferences, workshops, and a National Cybersecurity Awareness Week to highlight the importance of cybersecurity and opportunities to engage with cyber.

The NICE Workforce Framework for Cybersecurity, another key initiative, is more focused on professional workforce development and enables companies to educate and grow their cybersecurity capabilities. The NICE Framework is structured with three main building blocks: tasks, knowledge, and skills; this structure can be used within industry to discuss, evaluate, and expand their cybersecurity job roles. When coupled with the NIST CSF, the pair provide industry robust tools to address the cybersecurity workforce, best practices, and implementation of those practices.

3.2 National Cyber-Informed Engineering Strategy

In June 2022, the DOE released a report regarding the National Cyber-Informed Engineering Strategy that argues the need for a national strategy that couples design and cybersecurity principles. The report was written and compiled by a group of stakeholders from the Federal government, National Laboratories, reliability organizations, and private industries that recognize the need for cyber-informed engineering (CIE) practices. CIE is a method to encourage engineers and system designers to think about critical cybersecurity features at all stages of development rather than the traditional approach—that is adding cybersecurity measures to a system after an identified breach. The difference between these methods is shown in Fig. 13.

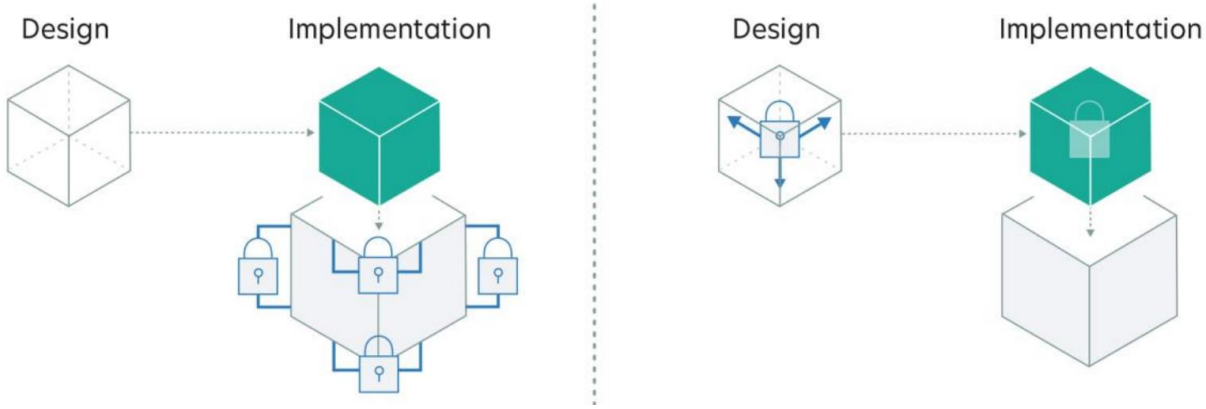


Fig. 13. Graphic showing the conceptual difference between current approach to cybersecurity (left) versus CIE strategy (right) [37].

CIE practices are newly emerging but adhere to design and operational principles that show promise for its use in protecting critical infrastructure. The National CIE Strategy focuses on applying cyber principles when designing the system and its controls; simplifying the system to reduce the potential for an attack; and implementing a layered, active defense to protect the infrastructure. Organizationally, the strategy highlights the importance of instilling a culture of cyber awareness, assessing and protecting sensitive digital and engineering data, and operating under the assumption that a cyberattack will occur [37]. The strategy is composed of five pillars, each with recommended actions to advance the strategy—awareness, education, development, current infrastructure, and future infrastructure. An overview of the pillars is shown in Fig. 14. As the strategy is still being developed, the recommendations within each pillar focus on CIE education, working with industry to identify metrics and technical requirements, policy options to advance CIE, and expanding the CIE tools available to critical infrastructure industries.

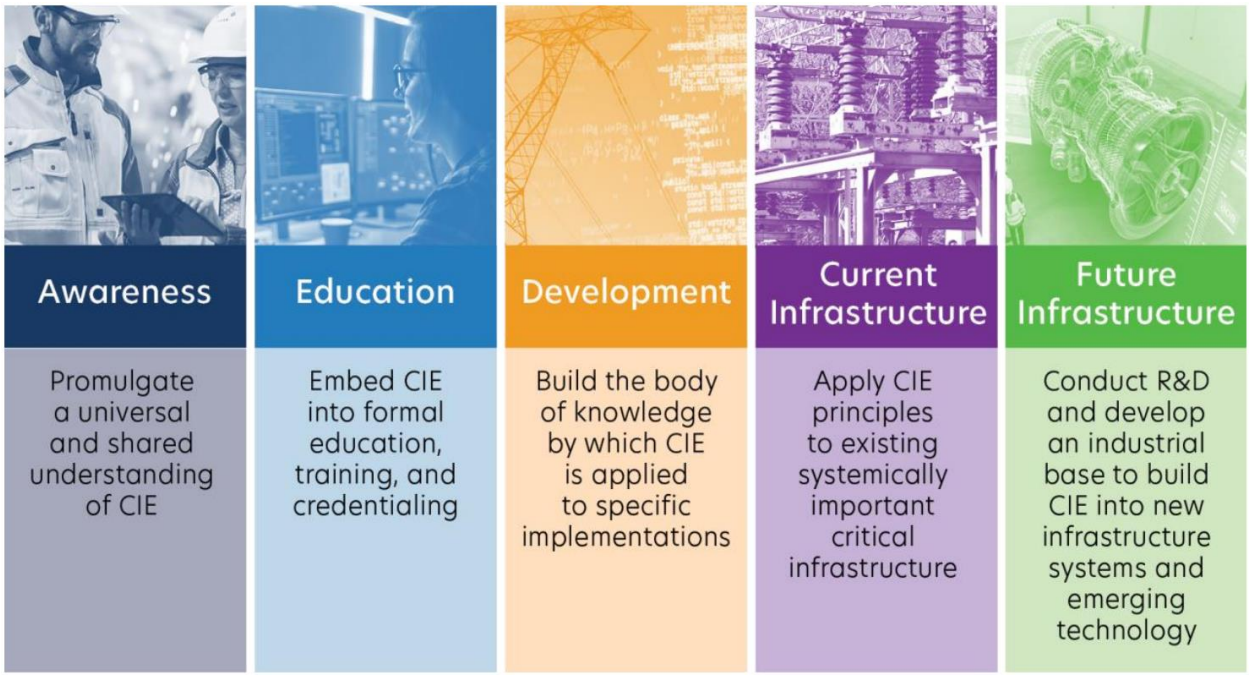


Fig. 14. Pillars and goals of DOE National CIE Strategy [37].

Policy Alternatives

Current efforts to address cybersecurity of the distribution grid are commendable but require additional funding and focus to ensure strong security of the distribution grid. The recommendations presented below were developed to bolster pre-existing initiatives while providing new ideas for the increasing cyber threat facing the nation. As such, recommendations one and two offer solutions based on previous efforts led by DOE or Congress while recommendations three and four present high-level solutions for larger challenges.

1. Public-Private Cybersecurity Workforce Rotational Program

The importance of a large and knowledgeable cyber workforce can mean the difference between a successful and unsuccessful cyberattack. With the current lack of cyber experts and the anticipated growth in need over the next ten years, Congress and the Federal government have a responsibility to create systems that protect the critical infrastructure, provide support to industry until the workforce demand is met, and continuously work with the energy sector on cybersecurity education.

1.1 Authorize the creation of a public-private rotational program for cybersecurity of distribution infrastructure.

To assist industry cyber capabilities, Congress should authorize the Office of Personnel Management to create a rotational program where cybersecurity workers within identified Federal agencies work with electric utilities for a select period of time. The recently passed Federal Rotational Cyber Workforce Program Act of 2021 (Cyber Workforce Act) can serve as a model for this program. Under this model, DOE would submit to the Office of Personnel Management a list of identified distribution owners and operators that may benefit from increased cybersecurity and support from the Federal government. At the same time, agency heads would determine potential Federal employees to participate in the program. Once the distribution entity has officially partnered with the government, the Office of Personnel Management assigns the Federal employee to a rotation at the utility for a period of not less than 180 days and not more than 1 year.

While cyber experts from public offices may have a more robust knowledge of Federal cyber initiatives, they may lack the practical experience to readily integrate the security measures into unique systems. This challenge is remedied by utilizing the full-time engineers at the company, as they will have a thorough understanding of the system and current security measures to protect it. The proposed duration of rotation, which could be extended, offers the ideal amount of time to review current cyber practices, work with the utility to make urgent changes, and propose additional steps to improve their security. To ensure effectiveness of the rotational workforce, participating Federal employees should be required to review and stay updated on current electric grid cybersecurity efforts lead by DOE, DHS, and NIST.

1.2 The program should adopt a cost-shared model.

Ensuring industry participation is critical to the success of the program and the authorization act should consider methods to ensure strong industry engagement. The funding model for the program should differ from the Cyber Workforce Act, as the electric industry is directly involved in the coordination and operation of the program. The best way to do this is to create a funding model that shares the salary and expenses of the workers.

The program would be most accessible to varying electric entities by utilizing a tiered, cost-shared model that accounts for the total number of customers served, the company's annual budget, a rough estimate of the current spending on cyber initiatives, and a current cyber threat level. Smaller companies with less access to cyber resources, who are experiencing a continued cyber threat should be expected to pay the least for the program. An example of a potential funding matrix is shown below.

Tiered, Cost-Shared Funding Model for a Public-Private Cybersecurity Workforce Program

Number of Ultimate Customers (in millions)	Percentage of Total Annual Budget Spent on Cyber Initiatives					Identified Risk Level
	0 - 5%	5 - 10%	10 - 15%	15 - 20%	> 20%	
< 1	70 - 30	65 - 35	60 - 40	55 - 45	50 - 50	Low
	75 - 25	70 - 30	65 - 35	60 - 40	60 - 40	High
1 - 2.5	65 - 35	65 - 35	60 - 40	55 - 45	50 - 50	Low
	70 - 30	70 - 30	65 - 35	60 - 40	50 - 50	High
2.5 - 5	60 - 40	60 - 40	55 - 45	55 - 45	50 - 50	Low
	70 - 30	65 - 35	60 - 40	60 - 40	50 - 50	High
> 5	50 - 50	50 - 50	50 - 50	50 - 50	50 - 50	Low
	60 - 40	60 - 40	50 - 50	50 - 50	50 - 50	High

In this example, the number of ultimate customers is estimated using data from the "2020 Electric Power Annual" report, published by the Energy Information Administration, Table 2.11 [38]; the percentage of total annual budget spent on cyber initiatives was estimated from "A SANS 2021 Survey: OT/ICS Cybersecurity" [39]; and identified risk levels would be determined by a select industry risk framework. The values inside individual cells represent the percentage of the program that the Federal government would cover, followed by the percentage of the program that the electric utility would pay. Using this example, if an electric company services 2.7 million end users, spends 5-10% of their total annual budget on cyber initiatives, and their identified risk level is 'low', the Federal government would cover 60% of the cost to send a federal employee to the company and the company would cover the remaining 40%.

Ultimately, the finer details required to implement such a cost-shared program would require more discussion to reach a reasonable solution for both government and industry. The shared-cost model has been utilized in other public-private partnerships (CRISP, for example) and has a well-established pathway for implementation. This tested model would allow for quick implementation of a solution to the industry's cyber workforce shortage.

2. Implementation of DOE CIE Strategy and other Educational Initiatives

As cybersecurity becomes an increasingly important aspect of the electric grid, the government, academia, and industry must work together to ensure that new engineers, technicians, and employees possess proper cybersecurity skills. By not training the workforce, the nation is allowing itself to be defenseless and unprepared for a potentially devastating national security event. There is an opportunity to strengthen our national response by adopting aggressive timelines for the DOE National Cyber-Informed Engineering Strategy and similar cyber-educational materials. The education efforts presented previously in the paper show a path forward, but there is currently a slow effort to implement these items. The nation would greatly benefit from a targeted advancement of the proposed strategies and initiatives.

2.1 DOE should work academia to roll out the CIE strategy over the next 3 years.

The work completed by DOE with the CIE national strategy presents an opportunity to strengthen cybersecurity education from an early stage in engineering education. To ensure a successful implementation, DOE should identify key partner institutions within the nation to integrate CIE into the engineering coursework. The effort should focus on engineering curriculum at all levels of higher education programs and become more advanced as the student progress. As academia processes vary from institution to institution, DOE should aim for the material to be taught at the majority of the identified institutions within three years. Adhering to rapid timelines ensures that the next generation of engineers who work on the electric grid are informed about the cyber threat and can take steps to protect equipment.

DOE should also target institutions with strong entrepreneurship programs, especially with engineering schools, and work with program staff to implement the strategy. As new technologies are being explored for the distribution grid, there is an opportunity for engineers and entrepreneurs to create innovative products for the market. By including the strategy into these fundamental entrepreneurship courses, DOE can work to promote general cybersecurity in all aspects, but especially promote cyber innovation for the electric grid.

2.2 DOE should work with industry to formalize a process for educating career engineers on the CIE strategy and principles over the next 3 years.

While the next generation of engineers are learning the CIE strategy, it is important to educate lifelong engineers on the ideas of the strategy so the workforce can begin immediate work to protect the electric grid. To increase the number of cybersecurity experts and engineers who know about the CIE strategy, DOE should partner with key

electric companies to offer workshops and presentations to employees over the next three years. Partner companies should be encouraged to identify key workers and managers who could implement the strategy into daily workplace functions and offer incentives for these individuals to attend the CIE workshops.

DOE should also work with state level engineering licensing boards to encourage the adoption of the national CIE strategy for continued education activities for Professional Engineers (PE). As each state has its own rules governing the licensure of professional engineers with varying requirements for continuing professional competency, DOE should review each state's requirements and tailor a CIE program that meets each state's rules for continuing education courses. This implementation effort should be a focus for the CIE strategy over the next five years was electrical engineers with a PE license are responsible for the design and approval of electrical systems. With the knowledge of the CIE strategy, the PE could design systems that enable the CIE principles and protect critical distribution infrastructure.

2.3 DOE should work with NIST to include CIE in NICE.

America's youth will become the next generation's cybersecurity experts and need a strong skillset to address the challenges they will face. To help introduce young students to the cyber world and the importance of cybersecurity, DOE should partner with NIST's NICE program to implement the CIE at appropriate levels for K-12 students over the next ten years. Working with NICE allows DOE to utilize existing structures of cybersecurity education which strengthens interagency relations, reduces duplicative efforts, and ensures strategic allocation of resources. The partnership also gives the opportunity for students to learn about the importance of security in a way that will spark a life-long interest in engineering and science, while setting the foundation for future careers.

3. Distribution Level Electric Reliability Organization

With the growing concerns of cyber threats to the distribution grid, there is a growing need for a centralized entity to organize the distribution industry and respond to these attacks. However, current regulatory organizations and their standards were not established to apply to the distribution owners and operators—making it extremely difficult to expand NERC's jurisdiction without significant challenges with implementation. To avail these challenges and to prepare the distribution entities for the upcoming decades, a Distribution Electric Reliability Organization (D-ERO) should be established. Recognizing the significant challenges and potential pushback from industry and states, steady and purposeful actions are required to pursue this policy recommendation and are detailed below.

3.1 Congress should authorize FERC to lead an in-depth reliability study of the physical and cyber security of distribution infrastructure.

As prescribed by the Federal Power Act and subsequent amendments, FERC does not have jurisdiction of the distribution infrastructure of the grid. To initiate this policy solution, Congress should authorize FERC to research and report on the current

reliability of physical and cyber systems on the distribution grid. The basis for establishing such a study exists and has been reported on numerous times over the past decade. In 2018, the Congressional Research Service released a report titled “The Smart Grid: Status and Outlook” focused on the deployment of new meters with advanced sensors and a cost analysis of the implementation [40]. The National Academies published “The Future of Electric Power in the United States” in 2021, in which the authors discuss future technologies, regulations, and recommendations for advancing the nation’s grid [41]. The DOE also contributed substantial reports regarding the distribution grid—such as the “2020 Smart Grid System Report” [42] which included additional key recommendations for industry and research.

With an abundance of research available, Congress should seize the opportunity to advance a consolidated national report on distribution infrastructure. The authorization bill should be explicit in what the report should cover including but not limited to a list of key stakeholders to engage, industry opinion on the creation of a D-ERO, a proposed timeline for selecting the D-ERO, and a proposed funding model for the organization.

3.2 Congress should authorize FERC to establish a second ERO focused on critical infrastructure of the distribution grid.

Following successful completion of the distribution reliability study by FERC, Congress should use the report’s findings to authorize the creation of a D-ERO. While it is generally expected that industry will push back on the effort and additional Federal regulation, the authorization should be clear that the scope will be focused. The authority for the organization should be strictly related to aspects of the distribution grid that are found to be critical to the nation’s electric grid and should readily address the concerns presented by industry. Limited authority ensures that the industry is protected from cyber threats while not stifling innovation in distribution technologies and other advancements.

The D-ERO should have the ability to set and enforce reliability standards for identified distribution owners and operators and their equipment—similar to NERC’s jurisdiction, but at the distribution scale. The D-ERO authorization should also consolidate regulatory authority of the distribution grid to one group as it is currently split between state regulatory agencies and non-regulated groups (for example, rural cooperatives). Consolidating reliability efforts into a single group will better support electric users and improve the reliability of the grid.

The reliability study and authorization bill should discuss the ability to regulate new smart meters and emerging technologies that increase the number of entry points to critical distribution infrastructure. Proactive discussions regarding these new devices will enable industry and companies to utilize the requirements and bolster the security of their devices before implementing them in the market.

3.3 Encourage the use of the NIST CSF to establish requirements and distribution standards.

Once established, the D-ERO should review the NIST CSF to determine aspects to incorporate into their initial distribution reliability standards. Utilizing the CSF allows for a comprehensive review of the status of cybersecurity of the distribution grid and the ability to create high level priorities for the D-ERO. These priorities may also highlight areas for strategic partnerships with other Federal agencies and initiatives or provoke industry leaders to act on an issue.

The D-ERO should also be encouraged to apply relevant NERC standards but must ensure that NERC standards are approved through the D-ERO governance structure rather than adopted through other means. As NERC standards were crafted with specific technologies in mind, the applicability of the standard to distribution infrastructure is not guaranteed. However, as the standards have been developed using an extensive process they can provide guidance of potential areas for D-ERO oversight.

4. Greater Focus on International Cyberattacks

The threat of a debilitating cyberattack is a concern for every nation. An attack on electric infrastructure would cripple supply chains, create societal chaos, and potentially be met with an equal, if not greater, reaction from the target nation—mutually assured destruction of modern infrastructure.

4.1 Fund the FBI to Investigate Cyberattacks on the Electric Grid

The ability to investigate those who perpetrate cyberattacks is a growing function of the Federal Bureau of Investigation (FBI). This is confirmed by the 2023 fiscal year budget request for the FBI that "includes an additional 137 positions…and $52 million to enhance cyber information-sharing abilities and increase cyber tools and capabilities" [43]. To assist with the FBI's ability to operate successfully, Congress should authorize additional funding and provide a clear directive to pursue individuals and groups that perform cyberattacks.

The directive should specifically request that the FBI investigate cyberattacks against the electric grid and other critical infrastructure sectors to ensure an up-to-date understanding of the threat facing the country. The investigation should include a review of cyberattacks against other country's critical infrastructure with a focus on how the intruder gained access to the systems and the scale of the damage. The results of the investigation should be reported, at least, to Congress, DHS, and DOE to ensure relevant bodies are aware of the threat.

4.2 Reaffirm a Strong International Stance on Cyberattacks

One of the greatest challenges associated with cyberattacks is the fact that they are easily perpetrated and require few resources. This ease of access increases the number of individuals who could launch an attack on our electric grid and makes it significantly more difficult to limit access. One of the best ways to protect the United States from cyber threats is to ensure good international relations with countries around

the world. Maintaining strong relations with countries will enable the federal government to investigate and pursue attackers—limiting the number of safe locations for cyber criminals that may target our electric grid and other infrastructure.

While there are numerous ways to improve international relations, the federal government, primarily the Executive Office of the President and its Departments, should assist countries experiencing cyber attacks with its resources and expertise. Providing this aid will help the country respond to an attack, stabilize governments around the world, and potentially limit the number of attacks. Supporting countries during these attacks—like the attack against Costa Rica [44] —would significantly improve our relationship which ensures they are willing to cooperate during future events. In addition, these deals could assist the FBI in understanding attack patterns, key perpetrators, and other information critical to investigating and stopping future cyber threats.

5. Update Current Cyber Initiatives

Many of the current cybersecurity initiatives focused on the electric grid have been sporadically updated over the past decade. To ensure these systems are addressing current grid cyber threats, the following programs should review their funding models, implementation strategies, and feedback from industry partners. Once complete, the responsible agency should update the models accordingly and create future review plans.

- **The CRISP funding model should be updated to allow greater access.** The current model relies on direct industry buy-in which limits participation to companies who have a large budget or prioritize cybersecurity. This model has the potential to leave out numerous distribution entities who have other budget priorities which could result in an increased cyber threat for the grid. To mitigate this challenge, the CRISP funding model should be updated to address budgetary constraints of smaller distribution owners and operators. This may be done in any manner of ways and methods—such as the tiered system proposed above for the cyber workforce rotational program or a model that allows the participation cost to be split amongst multiple groups.
- **The CSF should include example metrics for successful implementation and evaluation.** In 2013, the CSF was purposefully developed with no metrics or guidance regarding implementation, as each user was able to choose the metrics that best suited their situation. The recent review of NIST's request for information regarding updates to the CSF noted that "the lack of specificity may result in inconsistent interpretation and implementation of the CSF. They reflected a desire for more implementation guidance…" [28]. In concert with the feedback, the framework should include metrics for implementation and evaluation. These metrics are important to build upon the success of the framework, as it increases the accessibility of the framework to a wider audience

and increases the opportunity for companies with limited cyber resources to track implementation progress.

- **Upon release of NIST CSF version 2, the CIP Standards should be mapped to the new framework and gaps addressed.** One of the tools available to the electric industry is the mapping of the CSF to CIP standards and vice versa. It allows industry to use the tangible examples of the framework to meet potentially vague directives from FERC and NERC. As such, upon the release of version 2.0 of the CSF, NERC should partner with NIST to map its reliability standards to the new framework and identify any shortcomings within its standards. These shortcomings should be addressed by NERC to ensure comprehensive protection of the electric grid.

Final Notes

Cybersecurity of distribution infrastructure is an increasing challenge for the electric industry that will require a coordinated and aggressive response. While direct federal oversight of distribution systems does not exist, the current initiatives discussed herein recommends the following: educating the workforce, sharing important information across the industry, and creating frameworks for industry to utilize to protect their infrastructure. The ideas presented offer an approach to ensure the federal government is fulfilling its role in protecting critical electric infrastructure from devastating attacks. These initiatives can promote a viable policy solution to protect national security and our electrical distribution networks, encourage innovation, and create the cyber experts of tomorrow.

References

[1] US Energy Information Administration, "US electricity customers experienced eight hours of power interruptions in 2020," November 2021. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=50316.

[2] C. Thorbecke, *Gas hits highest prices in 6 years, fuel outages persist despite Colonial Pipeline restart,* ABC News, 2021.

[3] B. Fung and A. Marquardt, *Hacked Florida water plant reused passwords and had aging Windows installations,* CNN, 2021.

[4] A. Suderman and B. Fox, *Costa Rica chaos a warning that ransomware threat remains,* AP News, 2022.

[5] P. Bock, J.-P. Hauet, R. Francoise and R. Foley, *Lessons Learned From a Forensic Analysis of the Ukrainian Power Grid Cyberattack,* ISA Interchange.

[6] US Department of Energy, *The Smart Grid,* Office of Electricity, 2022.

[7] "The Federal Power Act", *16 U.S.C. 12 § 824.(b)(1),* 1935.

[8] National Cyber Security Centre, "How cyber attacks work," 23 June 2016. [Online]. Available: https://www.ncsc.gov.uk/information/how-cyber-attacks-work.

[9] MITRE ATT&CK®, "Impact Techniques," 6 May 2022. [Online]. Available: https://attack.mitre.org/tactics/TA0105/.

[10] MITRE ATT&CK®, "MITRE ATT&CK® Homepage," 2022. [Online]. Available: https://attack.mitre.org/.

[11] D. E. deZafra, S. I. Pitcher, J. D. Tressler and J. B. Ippolito, *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* National Institute of Standards and Technology, 1998.

[12] D. Nevius, "The History of the North American Electric Reliability Corporation," North American Electric Corporation, 2020.

[13] Federal Register, *Federal Energy Regulatory Commission,* 2022.

[14] Federal Energy Regulatory Commission, *What FERC Does,* 2022.

[15] President Clinton, "Executive Order 13010 Critical Infrastructure Protection," 1996.

[16] President Bush, "Executive Order 13231 Critical Infrastructure Protection in the Information Age," 2001.

[17] "The USA PATRIOT Act", *42 U.S.C § 5195.(c),* 2001.

[18] "The Energy Policy Act", *16 U.S.C. § 824.(o),* 2005.

[19] President Obama, *Executive Order 13636 - Improving Critical Infrastructure Cybersecurity,* 2013.

[20] President Obama, *Executive Order 13691 - Promoting Private Sector Cybersecurity Information Sharing,* 2015.

[21] President Trump, *Executive Order 13800,* 2017.

[22] President Trump, *Executive Order 13870,* 2019.

[23] President Trump, *Executive Order 13920,* 2020.

[24] NERC, "Standard Processes Manual," 2019.

[25] NERC, "US Reliability Standards: All Reliability Standards," 2022.

[26] Department of Energy, "Cybersecurity Capability Maturity Model (C2M2)," 2022.

[27] National Institute of Standards and Technology, *An Introduction to the Components of the Framework,* 2021.

[28] National Institute of Standards and Technology, *Initial Summary Analysis of Responses to the Request for Information (RFI) Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management,* 2022.

[29] Electricity Information Sharing and Analysis Center, *About the E-ISAC,* 2022.

[30] Electricity Information Sharing and Analysis Center, *GridSecCon 2022,* 2022.

[31] Electricity Information Sharing and Analysis Center, *GridEx,* 2022.

[32] US Department of Energy, *Cybersecurity Risk Information Sharing Program (CRISP),* 2022.

[33] Electricity Information Sharing and Analysis Center, *Cybersecurity Risk Information Sharing Program (CRISP),* 2022.

[34] Bureau of Labor Statistics, US Department of Labor, *Occupational Outlook Handbook, Information Security Analysts,* 2022.

[35] National Institute of Standards and Technology, *National Initiative for Cybersecurity Education,* 2022.

[36] National Initiative for Cybersecurity Education (NICE), *NICE Brochure,* 2022.

[37] US Department of Energy, *National Cyber-Informed Engineering Strategy,* 2022.

[38] Energy Infromation Administration, *Table 2.11. Number of Ultimate Customers by Sector,* 2020.

[39] M. Bristow, "A SANS 2021 Survey: OT/ICS Cybersecurity," Nozomi Networks, 2021.

[40] Congressional Research Service, "The Smart Grid: Status and Outlook," 2018.

[41] National Academies of Sciences, Engineering, and Medicine, "The Future of Electric Power in the United States," The National Academies Press, 2021.

[42] DOE, "2020 Smart Grid System Report," 2022.

[43] C. Wray, *Federal Bureau of Investigation Budget Request for Fiscal Year 2023,* FBI News, 2022.

[44] A. Suderman and B. Fox, "Costa Rica chaos a warning that ransomware threat remains," AP News, 2022.

[45] Congressional Research Service, *HR 3394 - Cyber Security Research and Development Act,* 2002.

[46] Energy Independence and Security Act Title XIII, *15 U.S.C. 17381,* 2007.

[47] Cybersecurity Enhancement Act, *15 U.S.C. 7421,* 2014.

[48] DOE Research and Innovation Act, *42 U.S.C. 18601,* 2017.

[49] Federal Rotational Cyber Workforce Program Act, *5 U.S.C. 3341,* 2021.

[50] The Infrastructure Investment and Jobs Act, *42 U.S.C. 18701,* 2021.

[51] Electricity Information Sharing and Analysis Center, *Join the E-ISAC,* 2022.

[52] U.S. Energy Information Administration, *Form EIA-861,* Annual Electric Power Industry Report.

[53] Copper Development Association, Inc., *Grid Infrastructure,* Copper Alliance.

[54] North American Electric Reliability Corporation, *2022 Summer Reliability Assessment,* 2022.