Cybersecurity Preparedness of Critical Infrastructure—A National Review

Maryam Roshanaei*

*Assistant Professor of Cybersecurity & IST,
Pennsylvania State University Abington, mur45@psu.edu

Abstract

Critical infrastructures are the foundational pillars of modern society, encompassing essential systems and assets that support our daily lives, economy, and national security. These infrastructures, including transportation networks, power grids, water supplies, telecommunications, and financial systems, play a vital role in ensuring the smooth functioning of governments, businesses, and communities. Safeguarding these critical infrastructures from both physical and cyber threats is of utmost importance in our interconnected world. The global landscape presents various threats that can impact infrastructures, such as the Covid-19 pandemic, the activities of state and non-state hackers, and extreme weather events. Therefore, it is crucial to prioritize the development of resilient infrastructures capable of withstanding crises and maintaining stability. This entails adopting information, communication, and technology (ICT) platforms that leverage emerging and innovative technologies to enhance infrastructure protection. As ICT systems evolve and become more interconnected, collaborative, and holistic strategies are necessary to protect critical infrastructure assets from an ever-increasing number of evolving cyber threats and disruptive cyberattacks. Safeguarding high-risk critical infrastructure assets, which are vital to safety, efficiency, and reliability, presents serious challenges. Recognizing the importance of protecting critical infrastructure from all types of threats and implementing resilient strategies is paramount. This article begins by describing the challenges faced by the United States in protecting critical infrastructure and assessing its Cybersecurity readiness. It then explores strategies for resilience and the urgent need for critical infrastructure protection. Finally, the authors evaluate the resilience and readiness strategies in place for protecting critical infrastructure in the United States.

Keywords: Information, Communication, and Technology (ICT), Critical Infrastructures Protection, Cybersecurity Readiness

 doi: 10.18278/jcip.4.1.4

Introduction

Critical infrastructures are indispensable for the continuous functioning of society. They provide vital services that support economic growth, public safety, and overall well-being. Transportation networks facilitate the movement of goods and people, powering commerce and daily commutes. Power grids supply electricity, enabling industries, hospitals, and homes to operate. Telecommunications systems connect individuals across the globe, facilitating communication, commerce, and emergency services. Water supply systems ensure access to clean water, a fundamental necessity for health and sanitation. Financial systems underpin economic transactions, facilitating trade, investment, and prosperity. Any disruption or failure in these infrastructures can have severe consequences, affecting individuals, businesses, and nations at large. The United States heavily relies on the reliable and functioning critical infrastructure (CIs) for national and economic protection. However, it is crucial to recognize the increased risks associated with this dependency. Today, highly digitized, and interconnected CIs, such as healthcare and energy sectors, face numerous domestic and nation-state-sponsored threats. The cybersecurity readiness in critical infrastructure must ensure the confidentiality, integrity, and availability of assets. This includes protecting the creation, processing, storage, and transmission of assets within the system, preventing persistent, sophisticated, systematic, and well-funded attacks from both internal and external threat actors.

Critical infrastructure operators (Ross, 2018), along with their operational technologies (OT), operate complex industrial control (IC) systems, such as Supervisory Control and Data Acquisition (SCADA). These IC systems and equipment monitor and control devices, processes, and events in sectors like power, water, transportation, manufacturing, and other essential services. SCADA manages programmable systems or equipment that interacts with the physical environment in critical infrastructures. Ensuring the safety of critical infrastructure operators and their OT, as well as recognizing the need for cybersecurity readiness to protect IT infrastructure assets, must be a top priority for critical infrastructure stakeholders. IT assets in critical infrastructure are considered sensitive resources within IT systems and technologies. Addressing system vulnerabilities and effectively responding to attacks is essential for business continuity.

On the other hand, OT assets within critical infrastructure (IEC Technology Report, 2019), specifically power systems, have different security requirements and constraints. These OT power systems include cyber-operational and physical systems, each with specific security needs, such as availability, authentication, authorization, integrity, and safety levels. Disruptive incidents impacting OT assets can harm the safety and reliability of power systems, leading to catastrophic consequences. Safety-related incidents may result in intentional or accidental

mis-operation of OT assets, potentially causing harm or even fatalities, while reliability-related incidents affect the performance of power system components like generators, breakers, transformers, power, and gas lines. Addressing vulnerabilities in OT, including poorly protected operational systems, control systems, and connected devices, has lagged IT infrastructure protection. Table 1 illustrates the priorities and security requirements (confidentiality, integrity, and availability) of critical infrastructure IT and OT systems.

Priority	**C.I.A**	**Description**
IT system	Confidentiality Integrity Availability	Prioritizes confidentiality to protect sensitive and private information
OT system	Availability Integrity Confidentiality	Prioritizes availability for safe and reliable operations

Table 1 – IT and OT C.I.A priorities and security requirement

Information Protection in Critical Infrastructures

The Whitehouse fact sheet (White House Fact Sheet, 2021) reported that the United States of America ranks 13th globally for overall quality of infrastructure protection even though it is considered as the wealthiest country in the world. To support the economy and security interests, it is important to ensure sufficient trustworthiness of systems, products, and services providing Critical Infrastructures Protection (CIP) to strengthen the critical infrastructure operators and their operational technologies. The urgency of protecting critical infrastructures should be recognized against cyber threats, natural disasters, and nation sponsor terrorist activities to avoid direct effect on the security and resilience of numerous sectors that could cause harm with catastrophic consequences.

Providing CIP for critical infrastructure prepare all the sectors to the highest standard for disaster preparedness, response, and recovery. For decades industries and administration (Global Forum on Cyber Expertise Report 2017) prioritized protecting critical infrastructures a range of physical challenges and threats attacks, such as terrorist acts, sabotage, or natural disasters. These events can cause significant damage and disruption to essential services, affecting public safety and economic stability. Additionally, the increasing reliance on technology and interconnected systems has led to the emergence of cyber threats. Cyberattacks targeting critical infrastructures can disrupt operations, compromise sensitive data, and

potentially inflict widespread damage. The ever-evolving nature of these threats necessitates proactive measures to identify vulnerabilities and enhance protection.

Critical Information Infrastructures (CIIs) refer to the systems and networks that are vital to the functioning of a nation, organization, or society. These infrastructures primarily rely on information and communication technologies (ICT) to operate and provide essential services to the public, government, and various sectors of the economy. CIIs are crucial for the functioning of sectors such as energy, transportation, finance, healthcare, telecommunications, and government services. Increasing connectivity is a characteristic of CII that recognizes the growing interconnectedness of systems and devices. This connectivity enables efficient data exchange and integration across various components of the infrastructure, facilitating remote monitoring and management. It is essential to recognize the need for Critical Information Infrastructures Protection (CIIP) in place for effective CIIs. CIIP refers to the policies, strategies, and measures implemented to safeguard and secure critical information infrastructures against cyber threats and attacks. Figure 1 shows the interconnection between CI, CII and ICT infrastructures.

It is crucial for governments, organizations, and stakeholders to collaborate and align their efforts to develop and implement integrated strategies that encompass CIP, CIIP, and Cybersecurity to ensure the security, resilience, and continuity of critical systems and infrastructure in the face of emerging threats and challenges. Elements and concepts of Critical Infrastructure Protection (CIP), Critical Information Infrastructure Protection (CIIP), and Cybersecurity strategies are interrelated and complementary in safeguarding critical systems and assets. Figure 2 shows CIP, CIIP, and Cybersecurity strategies share common goals of protecting critical systems, assets, and information from threats and disruptions.

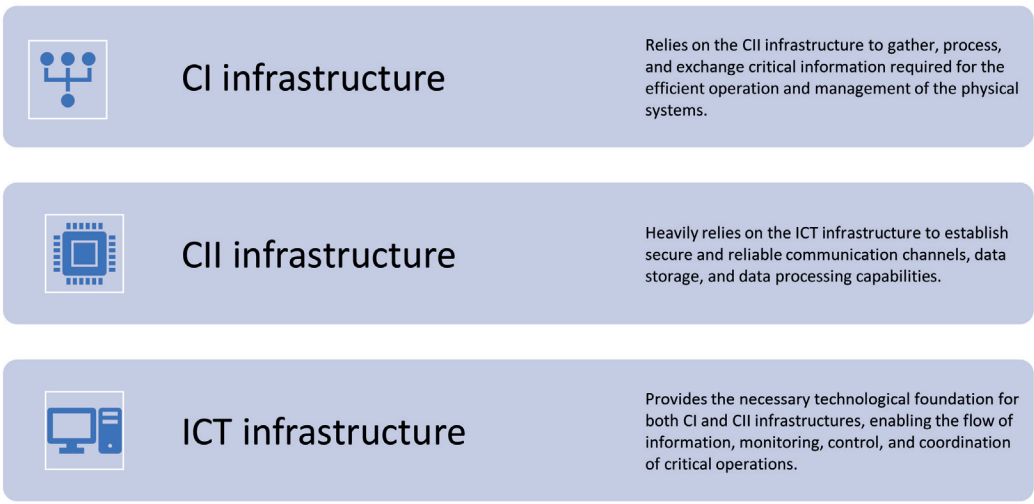

Figure 1 – Interconnection between CI, CII, and ICT infrastructures

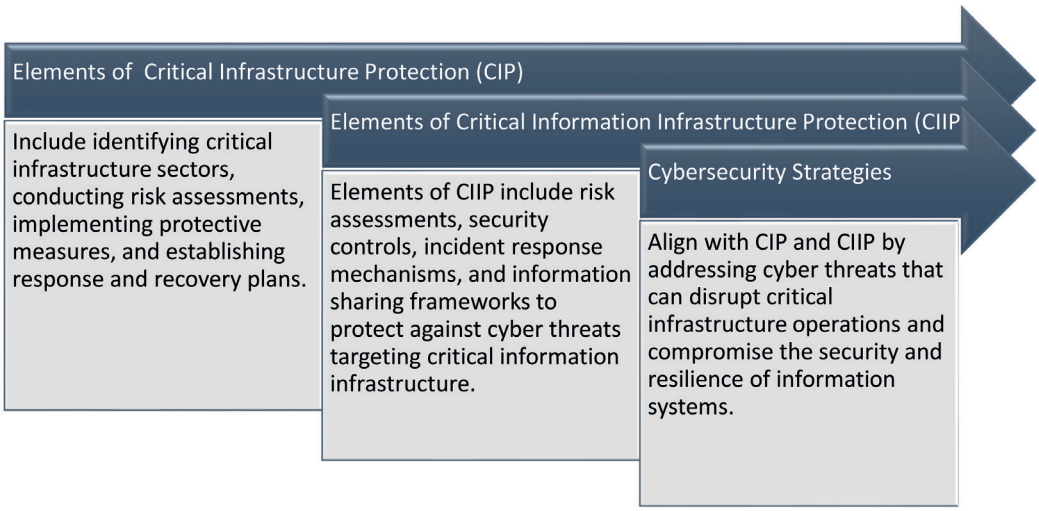

Figure 2 – Perspective on CIP, CIIP, and Cybersecurity strategies how their elements and concepts align

Threats and Risks impacts

Critical infrastructure is susceptible to a range of threats and risks that can have significant consequences for societies and economies. The 2023 global risks report (World Economic Forum Report, 2023) recognized the cybers threats among the top 10 risks. Figure 3 illustrates the threats and risks associated with critical infrastructure.

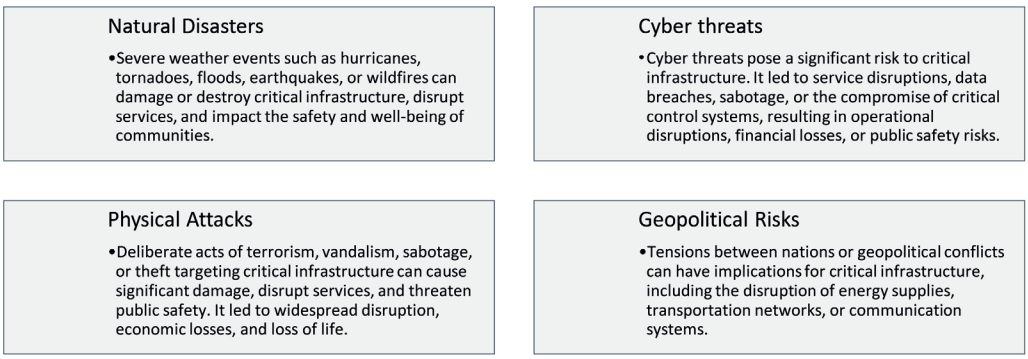

Figure 3 – Ranking threats and risks associated with critical infrastructure 2023

Addressing these threats and risks requires a multi-faceted approach, including risk assessment and management, investment in resilient infrastructure, implementation of robust cybersecurity measures, emergency preparedness and response planning, public-private partnerships, and ongoing monitoring and mitigation efforts. Governments, organizations, and communities must collaborate to

enhance the resilience and security of critical infrastructure to ensure the continued functioning and safety of societies.

Cyber Incidents Timeline

The cyber incidents highlight the increasing sophistication and impact of cyberattacks on critical infrastructure. They underscore the importance of robust cybersecurity readiness, risk assessments, incident response capabilities, and collaboration between public and private sectors to safeguard critical systems and minimize the potential for disruptions. The (Center for Strategic & International Studies, 2023) identified the timeline of significant global cyber incidents since 2006 focusing on state actions, espionage, and cyberattacks. These incidents illustrate the global nature of cyber threats targeting government agencies, defense, and critical infrastructures, highlighting the need for robust cybersecurity measures, readiness, and constant vigilance to protect sensitive information and ensure the resilience of essential systems. Figure 4 shows the substantial global cyber incidents between 2006 to March 2023.

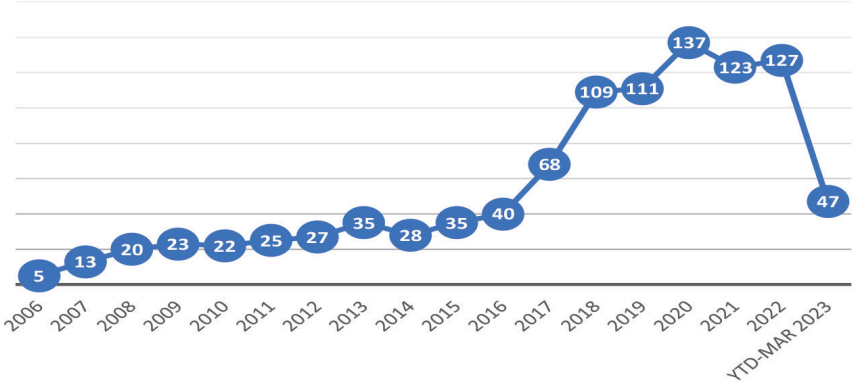

Figure 4 – Timeline of significant global cyber incidents

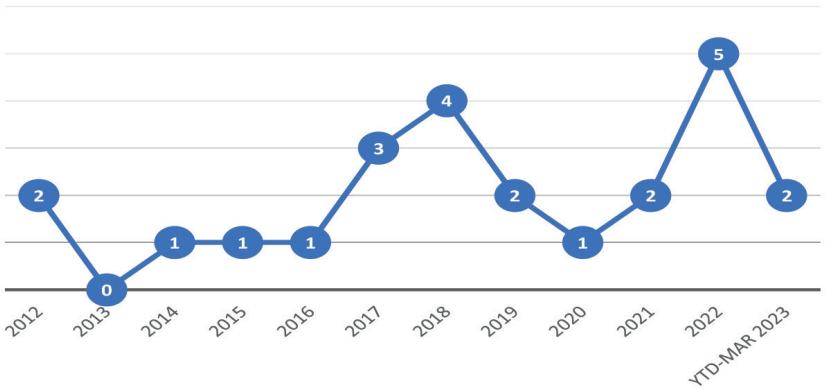

Figure 5 – Timeline of significant global cyber incidents targeting critical infrastructure

Figure 5 shows the substantial global cyber incidents on critical infrastructure between 2006 to March 2023. The incidents highlight the growing sophistication and impact of cyber-attacks on critical infrastructure globally. They underscore the need for robust cybersecurity measures, continuous monitoring, and international collaboration to defend against such threats and protect critical systems. The (Washburn and Sin, 2019) dataset collected significant incidents worldwide, utilizing publicly available information, targeting various domains of critical infrastructures from January 1, 2009, to November 15, 2019. It comprises a total of 130 incidents specifically directed at critical infrastructure sectors. Figure 6 illustrates the notable incidents within different critical infrastructure sectors documented during the period spanning from 2009 to 2019.

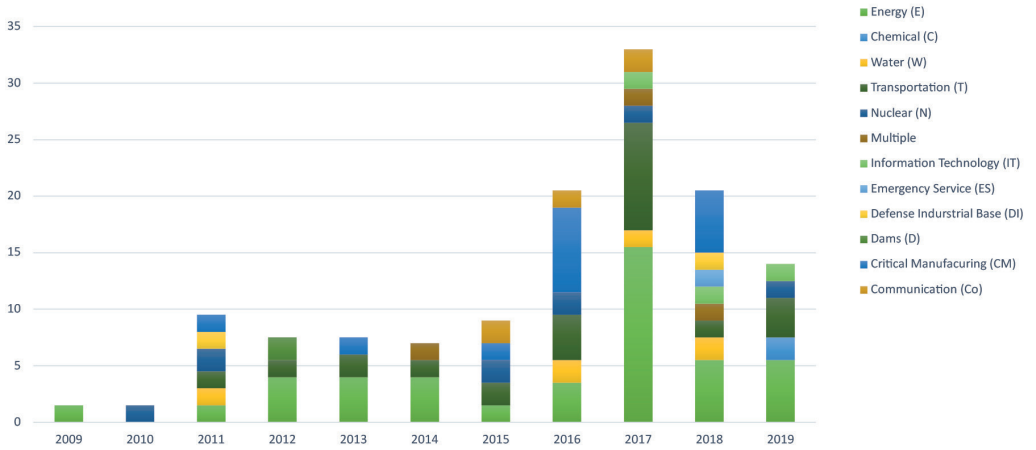

Figure 6 – notable incidents within different critical infrastructure sectors from 2009 to 2019

Based on the graph provided, notable observations can be made regarding the disruption of critical infrastructure sectors, particularly in the Energy and Transportation sectors. These sectors experienced a significant spike in incidents, followed by the critical manufacturing and nuclear sectors, respectively. This spike can be attributed to ransomware attacks like WannaCry and destructive malware such as NotPetya, which occurred in 2017. The dataset encompasses two key factors: disruptive cyber-physical incidents and disruptive cyber-operational incidents. In the case of cyber-physical incidents, malicious activities executed by state or nonstate threat actors have had disruptive effects on operational technology (OT) systems, devices, and processes, thereby compromising Industrial Control (IC) systems. On the other hand, cyber-operational incidents involve threat actors conducting malicious activities that disrupt IT systems connected to ICS or Internet of Things (IoT) systems and devices. These incidents can be aimed at managing inspections, intelligence preparation of the battlefield (IPB), or stealing intellectu-

al property (IP) for economic purposes. Figure 7 displays the cases of disruptive incidents categorized as cyber-physical incidents, cyber-operational incidents, or cases with unknown factors. The data covers the period from January 1, 2009, to November 15, 2019.

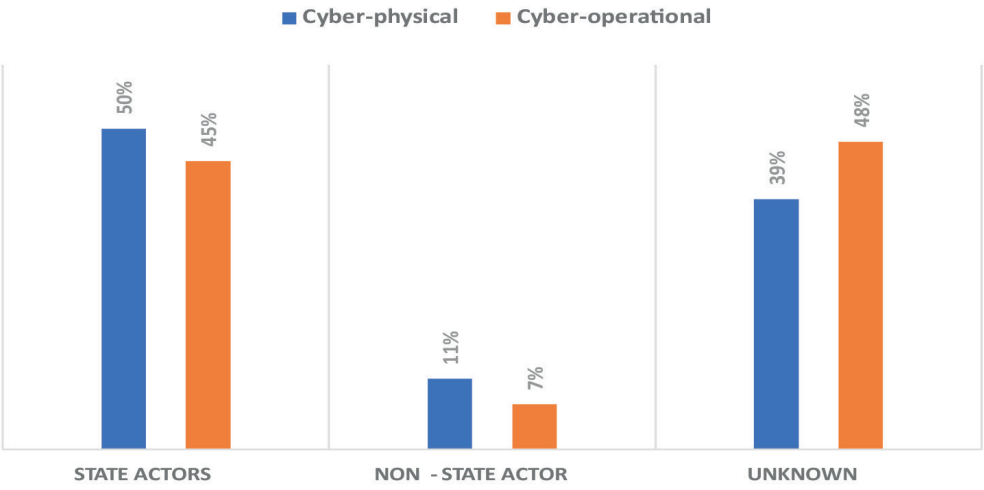

Figure 7 – Disruptive incidents

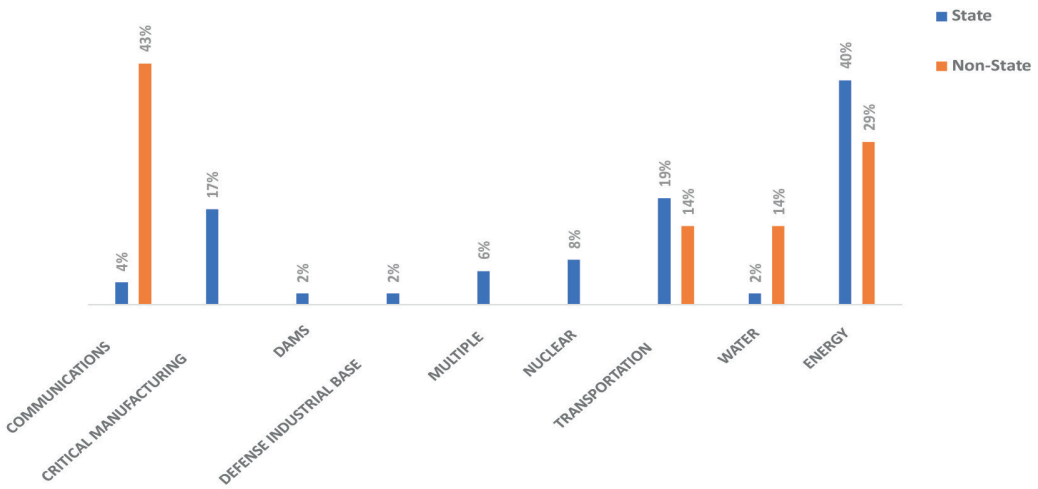

Figure 8 – Critical infrastructure sectors targeted by various threat agents

Based on the data collected, as depicted in Figure 8, it is evident that critical infrastructure sectors have been targeted by various threat agents. The dataset reveals that the number of incidents attributed to state agents is higher compared to non-state agents. This trend can be attributed to the fact that non-state incidents in the cyber domain often remain anonymous, making it challenging to attribute them to specific entities or actors.

Critical Infrastructure Protection (CIP) in the United States

Reliable critical infrastructures serve as a lifeline for the United States, supporting essential aspects of daily life such as access to clean water, power supply, transportation, and communications. The definition of critical infrastructures was redefined under the Patriot Act of 2001 (Patriot Act of 2001) to encompass a wide range of assets, systems, operational technologies, and other vital elements within both the physical and cyber environments. Recognizing the importance of protecting these critical infrastructures, the United States made it a top national priority, leading to the initiation of Executive Order 13636 (Executive Order 13636, 2013) in 2013. This order aimed to enhance the cybersecurity of critical infrastructures by promoting the development and implementation of effective measures. Its policy directive is to bolster the security and resilience of the nation's critical infrastructures while fostering an efficient, innovative, and economically prosperous cyber environment. Additionally, the order emphasizes the importance of maintaining safety, security, business confidentiality, privacy, and civil liberties.

Cybersecurity Enhancement Act 2014 (CEA)

In the United States, critical physical and cyber infrastructures are primarily owned and operated by entities in the private sector, as well as federal, state, or regional governments. In alignment with the directives of Executive Order 13636, the Cybersecurity Enhancement Act 2014 (CEA) (S.1353 -113th Congress, 2014) was enacted. This legislation authorized the National Institute of Standards and Technology (NIST) to lead efforts in developing a framework aimed at reducing risks to critical infrastructures. The CEA focuses on several key areas on in order to enhance the overall cybersecurity posture, collaboration between the public and private sectors is crucial. By encouraging cooperation and information sharing, both sectors can benefit from shared knowledge and resources, leading to improved cyber defense capabilities.

Additionally, promoting cybersecurity research and development plays a significant role in strengthening the security of critical infrastructures. This involves advancing technologies, tools, and techniques to stay ahead of evolving threats and vulnerabilities. Another key aspect is education and workforce development. Supporting programs and initiatives aimed at developing a skilled cybersecurity workforce is essential for addressing the growing demand for cybersecurity professionals. By increasing awareness of cybersecurity best practices, individuals and organizations can better protect themselves against cyber threats. Raising public awareness about cybersecurity threats and promoting preparedness measures is also vital. This includes educating the public about common cyber threats, such as phishing and malware, and providing guidance on how to protect personal information and sensitive data. Additionally, fostering an understanding

of the potential impact of cyberattacks can encourage individuals and organizations to take proactive measures to mitigate risks.

Lastly, the advancement of cybersecurity technical standards is crucial for improving the security and resilience of critical infrastructures. By facilitating the development and adoption of technical standards, such as encryption protocols and secure network architectures, we can establish a strong foundation for cybersecurity across various sectors. These standards help ensure interoperability, promote best practices, and foster a more secure digital environment overall. Through the implementation of these initiatives, the CEA aims to enhance the protection of critical infrastructures by fostering collaboration, research, education, preparedness, and the establishment of technical standards in the field of cybersecurity.

The aim is to establish a framework that enables owners and operators of critical infrastructures to effectively address cyber risks in a prioritized, flexible, repeatable, performance-based, and cost-effective manner. This involves implementing information security measures and controls that can be voluntarily adopted. In 2013, Executive Order 13691 (Executive Order 13691, 2013) was issued to promote cybersecurity information sharing and engage the private sector in exchanging information about cybersecurity risks and disruptive incidents.

The United States Critical Infrastructure Sectors

The United States recognizes sixteen critical infrastructure sectors (CISA Year in Review 2022, 2022) that are essential for the functioning of society and the economy. These sectors, as identified by the Cybersecurity and Infrastructure Security Agency (CISA) (H.R.3359-115th Congress, 2018). The critical infrastructure of a nation comprises various sectors, each playing a vital role in the functioning of society.

The Chemical Sector involves facilities engaged in the production, storage, and distribution of chemicals, which are essential for numerous industries. The Commercial Facilities Sector includes shopping malls, sports arenas, and other commercial buildings that provide spaces for business activities and public gatherings. The Communications Sector encompasses the infrastructure and services responsible for transmitting and distributing communication signals, such as telecommunications networks and broadcasting systems. The Critical Manufacturing Sector comprises industries involved in manufacturing essential goods and materials, including automotive, aerospace, and defense. The Dams Sector encompasses dams and related infrastructure, such as reservoirs and levees, which play a crucial role in water management and energy production. The Defense Industrial Base Sector supports defense and military operations by providing the necessary industrial complex. The Emergency Services Sector encompasses organizations involved in providing emergency response and management services, including

law enforcement, fire services, and emergency medical services. The Energy Sector covers the production, transmission, and distribution of energy resources, such as electricity, oil, natural gas, and renewable energy sources. The Financial Services Sector involves institutions engaged in banking, investment, insurance, and other financial activities. The Food and Agriculture Sector plays a critical role in the production, processing, and distribution of food and agricultural products, ensuring food security and supply. The Government Facilities Sector includes facilities and infrastructure that support government operations, such as administrative buildings and public transportation systems. The Healthcare and Public Health Sector comprises healthcare facilities, hospitals, medical supply manufacturers, and public health organizations. The Information Technology Sector involves industries responsible for designing, developing, and maintaining information technology systems and networks, facilitating communication, and data management. The Nuclear Reactors, Materials, and Waste Sector includes nuclear power plants, facilities for handling nuclear materials, and sites for the disposal of radioactive waste. The Transportation Systems Sector encompasses various modes of transportation, including aviation, maritime, rail, and road transportation systems. Lastly, the Water and Wastewater Systems Sector covers facilities involved in water supply, treatment, distribution, and wastewater management, ensuring clean and accessible water resources for communities. These sectors collectively form the critical infrastructure that underpins the functioning and security of a nation, requiring careful attention and protection.

These sectors are interconnected and rely on each other to ensure the reliable operation of critical infrastructure. They represent various industries and infrastructure components that are vital for the functioning of the nation. Each sector has its own unique characteristics, risks, and vulnerabilities. CISA, along with sector-specific agencies and stakeholders, works to enhance the security, resilience, and preparedness of these critical infrastructure sectors. By addressing risks and implementing appropriate protective measures, the aim is to ensure the continued operation and protection of these essential sectors in the face of various threats and hazards. Table 1 presents the sixteen critical infrastructure sectors and their corresponding Sector-Specific Agencies, as outlined in Presidential Policy Directive-21 and the 2013 National Infrastructure Protection Plan (National Infrastructure Protection Plan 2013).

Sector-Specify Agency	Critical infrastructure sectors
Department of Homeland Security (DHS)	Chemical Sector
	Communications Sector
	Dam Sector
	Emergency Services Sector
	Government Facilities Sector
	Information Technology Sector
	Transportation system Sector
	Commercial facilities Sector
	Critical Manufacturing Sector
	Nuclear Reactors, Materials & Waste Sector
Department of Treasury	Financial Services Sector
General Services Administration (GSA)	Government Facilities Sector
Department of Transportation (DOT)	Transportation system Sector
Department of Defense (DOD)	Defense Industrial Base Sector
Department of Energy (DOE)	Energy Sector
Department of Agriculture (USDA)	Food & Agriculture Sector
Department of Health & Human Services (HHS)	Food & Agriculture Sector
Environmental Protection Agency (EFA)	Water & Wastewater systems sector

Table 2 – CISA Critical Infrastructure Sectors

The 16 critical infrastructure sectors in the United States are interconnected and mutually dependent on each other to ensure reliable operations. Consequently, any disruption or loss experienced in one of these critical sectors will directly impact the security and resilience of not only the affected sector but also the operational technologies of other sectors. It is crucial to recognize and comprehend the interdependencies among these sectors in order to assess potential risks and vulnerabilities. Figure 9 provides a visual representation of the interdependencies among the U.S. critical infrastructure sectors.[1]

The private sector is responsible for owning and operating the majority of critical infrastructure sectors in the United States. Establishing strong partnerships between the private and public sectors is crucial to enhance security and resilience through integrated collaboration and interaction. These partnerships play a central role in implementing information sharing and awareness programs, ensuring efficient dissemination of critical threat information, risk mitigation strategies,

1 Critical infrastructure sectors - https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

and other sensitive information from state, local, tribal, territorial governments, and international partners.

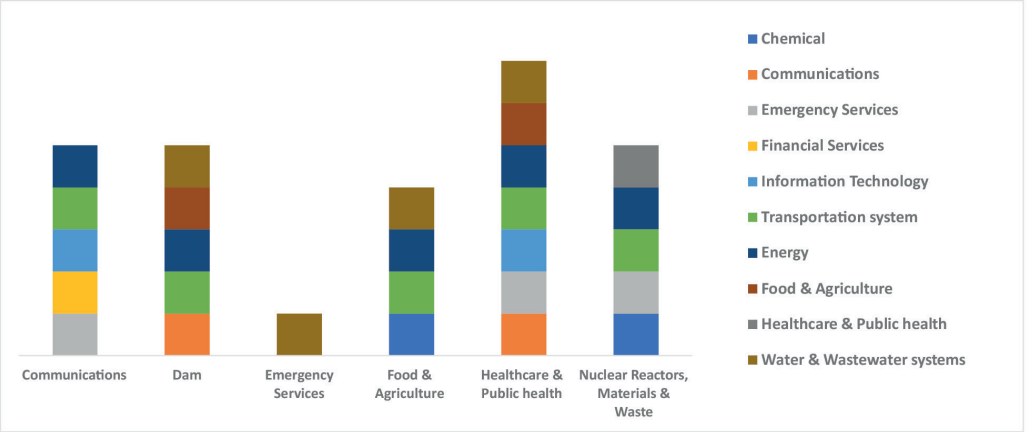

Figure 9 – Critical infrastructure sectors and their Interdependencies

Collaboration Between Public and Private Sector Partners

The Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) actively collaborate with public and private sector partners to effectively manage and safeguard the critical infrastructure of the United States. This collaboration is vital for enhancing the security and resilience of the nation's critical infrastructure. Together, these agencies work closely with stakeholders from both sectors to ensure a comprehensive and coordinated approach to protecting critical infrastructure. To support this unified and coordinated approach, various councils and initiatives play significant roles. They focus on promoting collaboration, information sharing, and efficient resource allocation, all of which contribute to enhancing the overall protection and continuity of critical infrastructures.

> *National Infrastructure Protection Plan* (*NIPP*) – (National Infrastructure Protection Plan, 2013) serves as a strategic document, guiding federal, state, local, tribal, and territorial governments, as well as private sector entities, in collaborating and coordinating efforts to protect critical infrastructures. The NIPP emphasizes the importance of partnerships and collaboration as key components of a successful security and resilience strategy. It encourages the formation of public-private partnerships and partnerships between government agencies at all levels to leverage resources, expertise, and information sharing. Additionally, there are several councils that play vital roles in supporting critical infrastructure protection and resilience.

Critical Infrastructures Partnership Advisory Council (*CIPAC*) – (Charter of Critical Infrastructure Protection Advisory Council, 2010) serves as an advisory body, facilitating collaboration and information exchange between public and private sector stakeholders. It helps identify and address cross-sector issues, vulnerabilities, and interdependencies, while supporting the development and implementation of strategies, policies, and programs to enhance the protection, preparedness, response, and recovery capabilities of critical infrastructures.

Critical Infrastructures Cross-Sector Council (*CICSC*) – (Critical Infrastructure Cross Sector Council Charter, 2018) focuses on addressing cross-sector issues and interdependencies among different critical infrastructure sectors. It promotes collaboration and coordination among sector-specific agencies, industry representatives, and other stakeholders to identify and mitigate cross-sector risks and vulnerabilities. Through the exchange of best practices and actionable information, the CICSC contributes to effective risk management, incident response, and recovery capabilities across multiple sectors.

Federal Senior Leadership Council (*FSLC*) – (Federal Senior Leadership Council Charter, 2021) comprises senior officials from federal departments and agencies who provide leadership, coordination, and guidance to enhance the protection and resilience of critical infrastructures at the federal level. The FSLC facilitates collaboration and coordination among federal agencies involved in critical infrastructure protection, aligning efforts, and ensuring effective resource utilization.

State, Local, Tribal, and Territorial Government Coordinating Council (*SLTTGCC*) – (State, Local, Tribal, and Territorial Government Coordinating Council, 2016) serves as a platform for coordination and collaboration among state, local, tribal, and territorial (SLTT) governments. The council enables information sharing, enhances preparedness and response capabilities, and ensures a coordinated and integrated approach to critical infrastructure protection within SLTT jurisdictions.

Regional Consortium Coordinating Council (*RC3)* – (Regional Consortium Coordinating Council Charter, 2018) facilitates coordination and collaboration among regional consortiums, bringing together stakeholders within specific geographic areas. The RC3 supports information sharing, the development of regional strategies, and the integration of regional efforts into the larger framework of critical infrastructure protection and resilience.

Through the collaborative efforts of these councils and initiatives, a unified and coordinated approach is fostered, strengthening the security and resilience of

critical infrastructures. They promote effective communication, resource utilization, and the sharing of best practices, ultimately safeguarding essential services and ensuring the well-being and prosperity of the country.

Information Sharing and Partnerships

Collaborative partnerships, both voluntary and regulatory, along with information sharing facilitation and awareness initiatives, play a pivotal role in safeguarding the security and resilience of critical infrastructures [21]. These programs are essential for establishing a robust knowledge system that enables the exchange and upkeep of critical threat information, risk mitigation strategies, and other sensitive assets. By fostering information sharing, collaboration, and coordination, these programs, and platforms bolster cybersecurity capabilities, fortify the resilience of critical infrastructures and communities, and ensure their enhanced protection.

> *Traffic Light Protocol* (*TLP*) – (Traffic Light Protocol 2.0 User Guide, 2022) provides a standardized framework for classifying and distributing information based on its sensitivity and intended audience. Information is categorized into different levels within the TLP, each serving a specific purpose. TLP Red designates highly sensitive information that should be restricted to individuals with a specific need-to-know within a specific organization or agency. Its distribution is strictly limited to that trusted circle. TLP Amber represents sensitive information that can be shared with a broader audience on a need-to-know basis, especially if it involves specific operational details or potential risks that require limited distribution. TLP Green signifies unclassified information that can be shared more freely within a community or with trusted partners, such as general awareness, best practices, or general threat information. TLP White indicates unclassified information that can be openly shared with the public, including general information, public advisories, or educational resources. By adhering to the TLP, organizations ensure the appropriate handling and control of sensitive information, promoting effective communication, information sharing, and collaboration while maintaining necessary levels of confidentiality and security. The TLP helps prevent unnecessary disclosure and potential risks, enabling organizations and individuals to share sensitive information appropriately.
>
> *Cyber Information Sharing and Collaboration Program* (*CISCP*) – (Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program, 2023) is a program aimed at facilitating the sharing of cyber threat information and promoting collaboration among participating organizations. It provides a structured framework for sharing valuable cyber threat intelligence, including indicators of compromise, attack patterns,

and vulnerability information. By sharing this information in a timely and secure manner, organizations can enhance their situational awareness, improve their cyber defenses, and respond effectively to emerging threats. The program encourages collaboration between public and private sector entities, fostering the exchange of best practices, lessons learned, and technical expertise. It also fosters partnerships between government agencies, industry stakeholders, and other organizations, creating a collaborative ecosystem for addressing cyber threats and improving cybersecurity posture. Participating organizations benefit from access to timely and actionable cyber threat information, enabling them to make informed decisions and take proactive measures to protect their networks and systems. The program also supports the development of standardized processes, tools, and protocols to streamline information sharing and collaboration.

Information Sharing and Analysis Centers (*ISACs*) – (Vijayan, 2022) are industry-specific organizations that facilitate the sharing of cyber threat information and best practices within a particular sector. They serve as trusted hubs for information exchange, collaboration, and coordination among stakeholders to enhance cyber threat awareness and response capabilities. ISACs bring together organizations operating within the same sector, such as companies, government agencies, academic institutions, and non-profit organizations. The primary goal of ISACs is to promote timely and effective sharing of actionable threat intelligence, incident reports, and mitigation strategies. They play a vital role in enhancing sector-wide cybersecurity resilience by fostering collaboration, developing sector-specific incident response plans, and advocating for policy improvements. ISACs also serve as liaisons between their sector and government agencies, enabling information exchange and coordination of cybersecurity efforts.

Information Sharing and Analysis Organizations (*ISAOs*) – (Vijayan, 2022) are entities that facilitate the sharing of cybersecurity information and collaborate with stakeholders to enhance cybersecurity capabilities. They serve as trusted platforms for information exchange, analysis, and coordination among organizations within a specific sector, community, or region. ISAOs encourage the voluntary sharing of cybersecurity-related data, including threat intelligence, incident reports, and best practices. Their primary objective is to foster collaboration and enable members to collectively address cybersecurity challenges. Participating organizations gain access to tailored threat intelligence and analysis, enhancing situational awareness and incident response capabilities. ISAOs also coordinate incident response efforts, share timely alerts and warnings, and provide services such as training and education. They collaborate with government agencies and industry partners to advocate for policy improvements and

promote industry-specific standards and best practices. ISAOs contribute to overall resilience by creating a collective defense environment that strengthens cybersecurity across communities or sectors.

Automated Indicator Sharing (*AIS*) – (Automated Indicator Sharing, 2016) is a system and process that enables organizations to exchange cybersecurity threat indicators in an automated and machine-readable format. It enhances timely detection and response to cyber threats by sharing actionable intelligence such as indicators of compromise (IOCs) with trusted partners. AIS automates the collection, processing, and dissemination of this information, improving the speed and efficiency of sharing. The goal is to proactively detect and respond to cyber incidents by incorporating real-time updates into security systems. AIS operates on trust and compliance with data sharing standards, ensuring privacy and protection of sensitive information. It integrates with existing security infrastructure for correlation and analysis, strengthening collective cyber defense capabilities.

Protected Critical Infrastructure Information (*PCII*) – (Protected Critical Infrastructure Information, 2023) refers to sensitive information related to critical infrastructure that is shared with the government and receives certain legal protections. PCII is a designation established by the United States Department of Homeland Security (DHS) under the Critical Infrastructure Information Act of 2002. Its purpose is to encourage private sector entities to voluntarily share sensitive information about their critical infrastructure assets, systems, and operations with the government. PCII includes vulnerabilities, threats, and protective measures. The shared information helps the government understand risks and develop strategies to enhance security and resilience. PCII is protected by law, exempt from public disclosure under the Freedom of Information Act (FOIA). This protection ensures the confidentiality and privacy of shared information and alleviates concerns about legal or competitive consequences. The sharing of PCII follows established channels and processes, prioritizing information protection. Organizations that submit PCII receive certification, recognizing and safeguarding their information. The PCII program fosters a trusted partnership between the government and the private sector, promoting information sharing for critical infrastructure security and resilience. It facilitates the exchange of valuable information, enabling the government to understand the critical infrastructure landscape, mitigate risks, and collaborate effectively with private sector stakeholders to respond to threats.

Homeland Security Information Network (*HSIN*) – (Homeland Security Information Network Annual Report, 2022) is a secure web-based platform operated by the United States Department of Homeland Security (DHS).

It facilitates information sharing and collaboration among homeland security stakeholders, including federal, state, local, tribal, territorial governments, and private sector organizations. HSIN allows authorized users to exchange sensitive but unclassified information, collaborate on operational activities, and access resources for protecting the homeland. It provides a secure environment for sharing situational awareness, threat intelligence, incident reports, and best practices. The platform offers features like discussion boards, file sharing, real-time chat, and notification systems. HSIN supports various homeland security missions and initiatives, serving as a central hub for accessing timely information, coordinating activities, and collaborating on joint projects. Robust security measures ensure the confidentiality, integrity, and availability of shared information, with access restricted to authorized individuals.

National Cyber Awareness System (*NCAS*) – (National Cyber Awareness System, 2023) is a program operated by the United States Department of Homeland Security (DHS). Its main goal is to provide timely and actionable information about cybersecurity threats, vulnerabilities, and best practices. The NCCIC serves as a centralized repository for cybersecurity resources and disseminates alerts, advisories, and notifications to individuals, organizations, and the public. The information is carefully vetted and validated before sharing. The NCCIC offers customizable notifications through various channels and provides educational resources and guidance to improve cybersecurity. Its aim is to empower individuals and organizations to protect their digital assets and contribute to the resilience of the nation's digital infrastructure.

National Information Exchange Model (*NIEM*) – (National Information Exchange Model, 2021) is a framework and set of standards developed by the United States government to facilitate the exchange of information between different organizations and agencies. It provides a common language and structure for data sharing, ensuring interoperability, and consistency. NIEM addresses information sharing challenges across various domains and sectors by promoting standardized data exchange. It includes data standards, exchange specifications, and supporting infrastructure. NIEM streamlines information sharing processes, reduces data translation efforts, and enhances accuracy. It enables disparate systems to exchange data in a consistent manner, fostering efficient collaboration. NIEM is a collaborative effort involving the government, agencies, tribal governments, international partners, and industry stakeholders. It breaks down data silos, improves communication, and supports various government operations.

Threat Information Guidelines

To streamline the exchange of threat information between private and public critical infrastructure sectors, a comprehensive set of guidelines has been implemented. These guidelines serve as a framework that facilitates the sharing of information and expedites its flow among these sectors. The objective is to establish robust information sharing platforms that enhance collaboration and enable swift dissemination of threat intelligence between private and public entities within the critical infrastructure sectors.

Cybersecurity and Infrastructure Security Agency's (*CISA*) *Infrastructure Security Division* – (Infrastructure Security Division, 2023) focuses on protecting and enhancing the security of critical infrastructure in the United States. Its main mission is to collaborate with public and private sector partners to identify, assess, and mitigate risks to critical infrastructure, thereby safeguarding national security and public safety. The division works across multiple sectors, providing services such as risk assessments, incident response coordination, information sharing, and technical assistance. Its responsibilities include conducting thorough risk assessments, coordinating response efforts during incidents, facilitating information sharing among partners, offering technical expertise to infrastructure owners and operators, and establishing partnerships with public and private sector entities. By leveraging its expertise and partnerships, the division works towards enhancing the security and resilience of critical infrastructure, ensuring the availability of essential services, and protecting the well-being of the nation's citizens.

Information sharing tools – promote the sharing of information within and between the various sectors of critical infrastructures, including Homeland Security Information Network - Critical Infrastructures (HSIN-CI) (Homeland Security Information Network - Critical Infrastructures, 2023), Infrastructures Protection Gateway (IP Gateway) (Infrastructures Protection Gateway, 2023), National Infrastructures Coordinating Center (NICC) (National Infrastructures Coordinating Center, 2008), National Risk Management Center (NRMC) (National Risk Management Center, 2023), Protected Critical Infrastructures Information (PCII) Program, Protective Security Advisors (PSAs) (Protective Security Advisors, 2023) and TRIPwire (Technical Resource for Incident Prevention) (TRIPwire, 2023).

Critical Infrastructures Threat Information Sharing Framework and Environment –(Critical Infrastructure Threat Information Sharing Framework, 2016) a structured approach and set of guidelines that facilitate the sharing of threat information related to critical infrastructure. It establishes

policies and procedures, builds trust, standardizes data formats, and utilizes dedicated platforms and tools to enable effective information sharing. The framework includes mechanisms for timely reporting and coordinated response, automation of sharing through technologies like AIS, sector-specific information sharing groups, and continuous improvement and evaluation. By implementing this framework, organizations can enhance their ability to detect, prevent, and respond to threats, ensuring the security and resilience of critical infrastructure. The Sharing Environment is a collaborative effort that enhances the sharing of critical infrastructure information among government agencies, private sector organizations, and stakeholders. It provides a platform for exchanging threat intelligence, best practices, and situational awareness specific to critical infrastructure sectors. It facilitates sector-specific information sharing, develops trusted communities, supports incident reporting and collaboration, offers analytical capabilities, and fosters government-private sector partnerships. It ensures a secure environment for sharing information, maintains confidentiality, and adapts to evolving threats and sector requirements. Participating in this environment enables organizations to access valuable insights, enhance their security posture, and collectively address critical infrastructure challenges for national security and public safety.

Conclusion

Critical infrastructure is a vital requirement for the survival of any society. This article highlights the importance of recognizing security and resilience as critical requirements for effective protection strategies in the United State. It explores various cybersecurity assessment frameworks and strategies with a shared goal of enhancing cybersecurity capacity and effectiveness. These assessments primarily focus on evaluating the level of cybersecurity capabilities by promoting best practices, safeguarding information, guiding cybersecurity activities, and managing risks within organizations. They also contribute to maintaining the desired security posture, assessing the current state of cyber preparedness, and fostering operational resilience. To further enhance the frameworks for protecting critical infrastructure, it is recommended to develop a measurement system that evaluates the capabilities of assessment methods. This system should measure the effectiveness of activities and action plans using meaningful indicators on a shared platform. Moreover, transitioning from voluntary and self-assessment methods to a more consistent and comprehensive approach would be beneficial.

Author Capsule Bio

Maryam Roshanaei, Ph.D. is as an assistant professor specializing in cybersecurity and Information Sciences and Technology at the Pennsylvania State University Abington. She earned her Ph.D. in Computer Networks and Security from University of Kingston London, UK. Before coming to Pennsylvania, she held the position of Associate Professor of Cybersecurity at the University of Greenwich in London, United Kingdom (UK). With over two decades of experience, she is a dedicated and enthusiastic educator, having taught and developed courses at both undergraduate and graduate levels in the fields of Cybersecurity, Information Security, and related subjects in both the USA and UK. She is an active researcher whose areas of expertise encompass various domains including AI for Good, Cyber Trust, Cyber hygiene, Critical Infrastructure Protection, Future Networks (FN), Cybersecurity, Digital Forensics and Crime, Internet privacy, and surveillance. Her involvement extends to esteemed organizations such as the British Standard Institute (BSI), International Standard Organization (ISO), and International Telecommunication Union (ITU) Data Communication standards committees. Within these groups, she serves in significant capacities such as Committee Chair and Principal Expert. Her contributions span standardization and journal publications across a diverse range of applied research projects, including AI for Good, Future Network (FN), Mobility, and Service Composition.

References

Automated Indicator Sharing (AIS). 2016. HDS. Retrieved from https://www.dhs.gov/sites/default/files/publications/privacy_pia_nppd_ais_update_03162016.pdf.

Center for Strategic & International Studies (CSIS). 2023. Significant Cyber Incidents Since 2006.Retrieved from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Charter of Critical Infrastructure Protection Advisory Council. 2010. HDS. Retrieved from https://www.dhs.gov/xlibrary/assets/cipac/cipac_charter.pdf.

CISA Year in Review 2022. CISA. 2022. CISA Year in Review 2022. Retrieved from https://www.cisa.gov/2022-year-review

Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program. 2023. HDS. Retrieved from https://www.cisa.gov/sites/default/files/c3vp/CISCP_20140523.pdf.

Critical Infrastructure Cross Sector Council Charter. 2018. CISA. Retrieved from https://www.cisa.gov/sites/default/files/publications/chartercscapp-508.pdf.

Critical Infrastructure Sector Partnerships. 2023. CISA. Retrieved from https://www.cisa.gov/topics/partnerships-and-collaboration/critical-infrastructure-sector-partnerships-0.

Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community, 2016. DHS. Retrieved from https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf.

Executive Order 13636. 2013. Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

Executive Order 13691.2013—Promoting Private Sector Cybersecurity Information Sharing. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

Federal Senior Leadership Council Charter. 2021. CISA. Retrieved from https://www.cisa.gov/sites/default/files/publications/fslc-charter-2021-508.pdf.

Global Forum on Cyber Expertise Report. 2017. GFCE Global Good Practices Critical Information Infrastructure

Protection (CIIP). Retrieved from https://thegfce.org/wp-content/uploads/2020/06/CriticalInformationInfrastructureProtectionCIIP.pdf.

H.R.3359 — 115th Congress. 2018. Cybersecurity and Infrastructure Security Agency Act of 2018. Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/3359/text

Homeland Security Information Network – Critical Infrastructures (HSIN-CI). 2023. DHS. Retrieved from https://www.dhs.gov/hsin-critical-infrastructure.

Homeland Security Information Network Annual Report, 2022. DHS. Retrieved from https://www.dhs.gov/sites/default/files/2023-05/23_0512_hsin-2022-annual-report-508-version.pdf.

IEC Technology Report. 2019. Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment. Retrieved from www.iec.ch/basecamp/

cyber-security-and-resilience-guidelines-smart-energy-operational-environment.

Infrastructure Security Division. 2023. CISA. Retrieved from https://www.cisa.gov/about/divisions-offices/infrastructure-security-division.

Infrastructures Protection Gateway (IP Gateway), 2023. DHS. Retrieved from https://www.cisa.gov/sites/default/files/publications/ip-gateway-fact-sheet-11-15-508.pdf.

National Cyber Awareness System, 2023. CISA. Retrieved from https://www.cisa.gov/resources-tools/services/national-cyber-awareness-system.

National Information Exchange Model. 2021. NIEM Report. Retrieved from https://www.niem.gov/sites/default/files/2022-02/NIEM_2021AnnualReport%20FINAL.pdf.

National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. Cybersecurity and Infrastructure Security Agency (CISA). Retrieved from https://www.cisa.gov/resources-tools/resources/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

National Infrastructures Coordinating Center (NICC), 2008. DHS. Retrieved from https://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

National Risk Management Center, 2023. CISA. Retrieved from https://www.cisa.gov/sites/default/files/publications/fact_sheet_nrmc_508_1.pdf.

Patriot Act of 2001. Retrieved from https://www.justice.gov/archive/ll/highlights.htm.

Presidential Policy Directive-21. 2013. Critical Infrastructure Security and Resilience. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Protected Critical Infrastructure Information. 2023. CISA. Retrieved from https://www.cisa.gov/sites/default/files/2023-02/pcii-program-fact-sheet-012022_0.pdf.

Protective Security Advisors (PSAs). 2023. CISA. Retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%2520Fact%2520Sheet%2520-%2520PSA%2520Program%2520-%2520508c_IAA%2520Final.19MAR2020.pdf.

Regional Consortium Coordinating Council Charter. 2018. CISA. Retrieved from https://www.cisa.gov/sites/default/files/publications/regional-consortium-coordinating-council-charter-2018-508.pdf.

Ross, Ron. 2018. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Special Publication (NIST SP) No. 800-37r2). National Institute of Standards and Technology. Retrieved from https://doi.org/10.6028/NIST.SP.800-37r2.

S.1353 — 113th Congress. 2014. Cybersecurity Enhancement Act 2014 (CEA). Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

State, Local, Tribal, and Territorial Government Coordinating Council. 2016. HDS. Retrieved from https://www.cisa.gov/sites/default/files/publications/slttgcc-fact-sheet-2017-508.pdf.

Traffic Light Protocol 2.0 User Guide. 2022. CISA. Retrieved from https://www.cisa.gov/sites/default/files/2023-02/tlp-2-0-user-guide_508c.pdf.

TRIPwire (Technical Resource for Incident Prevention), 2023. DHS. Retrieved from https://www.cisa.gov/resources-tools/resources/technical-resource-incident-prevention-tripwire-portal#:~:text=Developed%20and%20maintained%20by%20the,Explosive%20Device%20(IED)%20incidents.

Vijayan, Jaikumar. 2022. "What is an ISAC or ISAO? How this cyber threat information sharing organizations improve security." CSO. Retrieved from https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.

Washburn, Ryan, and Sarah Sin. 2019. Research Brief: Significant Multi-Domain Incidents against Critical Infrastructure (SMICI) Dataset. College Park, MD: START. Retrieved from https://www.start.umd.edu/publication/research-brief-significant-multi-domain-incidents-against-critical-infrastructure-smici.

White House Fact sheet. 2021. The American Jobs Plan. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/fact-sheet-the-american-jobs-plan/.

World Economic Forum Report. 2023. The Global Risks Report 2023. Retrieved from https://www.weforum.org/reports/global-risks-report-2023/.

PJM: Charting the Path to the Grid of the Future

Kenneth Seiler[1]

[1] Senior Vice President – Planning, PJM Interconnection

The electric grid is undergoing a revolutionary transformation—customer preference, corporate clean energy aspirations, and state and federal policy choices are dramatically changing how energy is generated, and the retirement of conventional generators threatens to outpace the construction of new resources.

Technology is offering customers new ways to interact with the system, blurring traditional distinctions between how electricity is generated and transmitted long distances and how it is delivered to homes and businesses. At the same time, the frequency of extreme weather events—and the stresses they put on the system—continues to increase.

All of these forces present challenges for operating the largest and most complex machine on earth for a product that is produced, transported and consumed in an instant.

PJM Interconnection, the grid operator for 65 million people in 13 states and the District of Columbia, along with the many stakeholders with a voice in our operations and policies, is tasked with forging solutions without sacrificing the uninterrupted power supply that allows modern society to function.

As the country's largest regional transmission organization, PJM's No. 1 job is keeping electricity flowing, and doing it cost-effectively, every moment of the day. Affordable, reliable electricity is essential for everything we do as a society—starting with powering the country's critical infrastructure we rely on, from transportation and communication to emergency services and health care.

This responsibility demands that the wholesale electricity market we oversee provides economic incentives to attract the investment needed to build and resources that maintain system reliability, as it has for over 25 years. It also requires us to plan for broader trends and events to make sure the grid is resilient enough to operate through and recover from rare, extreme and high-impact events that PJM has never experienced before.

Reliability Risks on the Horizon

PJM's combined functions of operations, markets and planning have worked together successfully to keep the lights on since 1927, providing up to $4 billion in efficiencies for our customers in the process. But there are working trends on the horizon.

In a recent report, PJM analysis showed that 40 GW of existing genera-

 doi: 10.18278/jcip.4.1.5

tion—mostly coal, gas and oil generators representing 21% of our installed capacity—is at risk of retiring by 2030. Some industry forecasts predict that renewable energy will provide nearly half the power to the country by 2032, but currently those renewable resources are not being built at the rate we need to replace those traditional generators.

As the generation fleet moves to a lower-carbon footprint, reliant on intermittent energy resources (like sun and wind), the planners and operators of the bulk electric system have to plan for a much different kind of system with different physical characteristics—and get it right. Peoples' livelihoods and lives depend on it.

This means PJM and its stakeholders have been hard at work crafting a reliable path forward through our core functions of planning, markets and operations.

We have synthesized these efforts into our Ensuring a Reliable Energy Transition initiative, dedicated to finding answers to reliability challenges through intensive, data-driven research and analysis and collaboration across government and industry.

New Fuel Mix Challenges Reliability

The story of this energy transition is told in our New Services Queue, where generation projects come to interconnect with the PJM system. More than 97 percent of the resources requesting to join the PJM system are wind, solar or batteries, or a hybrid of both.

These smaller, weather-dependent resources generate energy in a whole different way than traditional thermal generators powered by coal, oil, gas or nuclear, introducing a new set of physical dynamics and characteristics.

Underlying the new reality of grid operations is the fact that intermittent and limited-duration resources like batteries do not replace "1 for 1," but rather require multiple megawatts to replace 1 MW of dispatchable generation due to their limited availability in certain hours of the day and seasons of the year.

As generators increasingly rely on renewable energy sources like wind and solar, PJM has identified trends that could realize a shortage of generating resources as early as 2027:

- The demand for power is growing with the electrification of transportation, industrial and building sectors, along with the development of energy-intensive data centers—driven in part by the increase in artificial intelligence and machine learning processes—at an unprecedented rate.

- At the same time, fossil fuel generators that balance the grid today are retiring at a significant rate.

- Replacement generation is made up of primarily intermittent and limited-duration resources that require multiple megawatts to replace 1 MW of dispatchable generation.

- Renewable resources that have passed through PJM's vetting process are not being built at the pace required to replace these resources, through factors beyond PJM's control, like supply chain issues, cost of capital and permitting.

The related analysis is detailed in our most recent paper in the Energy Transition in PJM series.

New Planning Process Begins

Critical to getting generation online, PJM this summer began transitioning to a new "first-ready, first-served" interconnection process that improves project cost certainty for network upgrades and significantly improves the overall process by which new and upgraded generation resources are studied and introduced onto the electrical grid.

In the transition period to our new interconnection process, we will study enough interconnection requests to replace the entire generation fleet of nearly 200 GW and far more than make up for retiring coal, oil and gas generators.

The key question is: Will the new generation actually come online?

Right now, we have more than 40,000 MW of projects that have completed PJM's study process and should be moving to construction.

Yet in 2022, we saw just 2,000 MW in projects built, and only 700 MW of those were renewables. So far in 2023, we have seen 620 MW of solar, 285 MW of wind, and 41 MW of storage come online, along with 3,100 MW of natural gas.

Many projects coming through the queue are not being built because of siting, financing or supply chain issues. These factors are out of PJM's control.

PJM is not alone in having stalled projects. This same issue is happening across the country. But we are leading the pack in clearing our queue. A recent S&P Global Market Intelligence analysis of U.S. interconnection queues found that PJM has the shortest project turnaround time of all grid operators in the country.

Reliability-First Policies

These reliability concerns are not unique to the PJM grid. As this year's North American Electric Reliability Corporation's (NERC) summer assessment showed, roughly two-thirds of the U.S. (but not the PJM region) already faced increased resource adequacy risk this past summer.

However, we believe this risk is avoidable. How? Through policies that accelerate the rate of entry of new generation (such as through permitting reform)

and slow the exit of the traditional thermal generation we use to balance the grid today. This will give time for replacement generation to be installed and operating at the required scale.

In addition, PJM advocates an approach to policymaking that expressly considers reliability impacts in the development phase of the policy—not after the fact.

We continue to work with both state and federal policymakers to ensure that reliability considerations are built into all environmental and renewable generation policies.

PJM Steps Up as Independent Industry Leader

The energy transition presents a broad set of challenges and opportunities, and PJM is making headway in a number of areas, including:

- Enacted major interconnection reform, which is expected to result in the processing of over 250 GW of new generation requests in the next three years and produce a more predictable, streamlined process for new generators to connect with the system
- Filed with FERC a set of proposals to better recognize the relative contribution of all generation resources in meeting reliability needs
- Engaged stakeholders in developing a long-range transmission planning protocol that will enable us to analyze the longer-term needs of the system under multiple long-range scenarios to optimize a set of solutions based on the changing fleet and electrification
- Developed new rules to remove barriers to renewable resources participating in PJM's capacity market
- Performed groundbreaking work with the state of New Jersey to advance the buildout of its ambitious offshore wind program—a model that is being considered by other states

Our Ensuring a Reliable Energy Transition initiative proposes an initial set of actions to support reliability that PJM can take with its stakeholders, government and industry over the immediate, near-term and upcoming time frames to keep pace with these trends:

- **Immediate**: Ensuring the performance of existing generation resources
- **Near Term**: Maintaining adequate generation resources and deliverable megawatts to meet electricity demand

- **Upcoming**: Attracting and maintaining (as needed) resources that have essential reliability services

Essential reliability services are defined by NERC as the ability of a generation resource to provide services such as voltage control, frequency support, and ramping capability to balance the electrical grid and maintain the reliable delivery of electricity.

PJM has documented in its research that the more we depend on intermittent resources, the more we will need to share electricity with our neighboring systems to account for fluctuations in supply. PJM is already a leader in this area and regularly exports and imports electricity to adjoining systems; we are currently working both internally and externally to determine just how much of that interregional transfer capability we will need to build.

Helping States Achieve Their Goals

Another action we're taking as part of our reliability initiative is offering states a way to incorporate their policy goals into our Regional Transmission Expansion Plan (RTEP).

The first state to do this was New Jersey. In October 2022, the New Jersey Board of Public Utilities (NJBPU) selected a package of onshore transmission solutions that, in conjunction with prior action, will enable the injection of 7,500 MW of offshore wind capacity by 2035.

The NJBPU order was informed by technical analysis performed by PJM staff under the State Agreement Approach (SAA), through which states can access PJM's expertise and existing planning process to cost-effectively develop and optimize the transmission improvements necessary to support the reliable interconnection of certain desirable resources.

The SAA enables a state or group of states to propose a project that could potentially realize public policy requirements as long as the state (or states) agrees to pay all costs of the state-selected buildout included in the RTEP.

The first engagement of the SAA was so successful, New Jersey returned to PJM in April and requested to partner on a second stage to enable an additional 3,500 MW of offshore wind energy. New Jersey's experience can serve as a template for PJM's other coastal states.

Together, We Will Find Solutions

PJM has sufficient generation to meet the needs of our system today. However, as we look further out, we are concerned by the trends we see.

Despite PJM's healthy reserve margins, recent winter storms have provided a sobering reminder of the critical role that resource adequacy will play through

the energy transition. For the first time in recent history, PJM could be at risk of facing resource adequacy challenges.

Decarbonizing the grid will be a challenge, for all of us, but it will happen. We're all going to have to work together to find solutions, including state and federal policymakers.

The solutions are there; this country has proven that time and time again, it simply requires dedicated resources and brainpower. PJM will find those solutions but will need all stakeholders at the table to do so.

Author Capsule Bio

Kenneth Seiler leads PJM's System Planning Division. He is responsible for all activities related to resource adequacy, generation interconnection, interregional planning and transmission planning, including the development of the Regional Transmission Expansion Plan. Previously, Seiler was the executive director of System Operations and was responsible for the reliable operation and coordination of the bulk power system, including PJM's real-time dispatch operations and near-term reliability studies. Seiler oversaw the dispatcher training and certification functions, as well as the markets coordination function, to ensure the efficient and most cost-effective dispatch of the generation fleet.

Seiler is on the board of directors of ReliabilityFirst, one of the eight Federal Energy Regulatory Commission-designated regional entities responsible for ensuring the reliability of the North American bulk power system. He is also on the board of PJM Environmental Information Services Inc. In addition, he is an instructor for the Mayfly Project, a national organization that uses fly fishing as a catalyst to mentor and support children in foster care and introduce them to their local water ecosystems, with a hope that connecting them to a rewarding hobby will provide an opportunity for foster children to have fun, build confidence and develop a meaningful connection.

Prior to joining PJM, Seiler was employed by Metropolitan Edison Company/GPU Energy for nearly 14 years. He held the positions of operations manager, transmission engineering manager, relay protection and control engineer, and substation/transmission construction and maintenance engineer. He earned a Bachelor of Science in electrical engineering from The Pennsylvania State University and a Master of Business Administration from Lebanon Valley College.