International Journal of Academic Management Science Research (IJAMSR)
ISSN: 2643-900X
Vol. 9 Issue 4 April - 2025, Pages: 38-54

Cybersecurity and Critical Infrastructure: Legal Obligations under the Cyber Incident Reporting for Critical Infrastructure Act, 2022

Chinelo Patience Umeanozie [1] ,Chuma Akana[2] ,Chukwuemezie Charles Emejuo[3]

Abstract: *In response to the increasing frequency and intensity of cyber threats in our international digital space, many countries have instituted laws requiring the mandatory reporting of cyber incidents. All these legislative measures have been put in place for improved resilience both nationally and sectorally. Cyberattacks against very important infrastructure in the United States of America set off the passage of significant legislative measures including the Cybersecurity and Infrastructure Security Agency Act of 2022 (CIRCIA) and the Cyber Incident Reporting for Critical Infrastructure Act. The law was supposed to stop the federal government from lacking sufficient situational awareness on major cyberattacks. This paper will explore the legal obligations imposed by CIRCIA, especially the obligations on covered entities to report significant cyber incidents and any related payments regarding ransomware. In addition to using comparative practices in similar jurisdictions, the analysis assessed relevant jurisprudence, legislative history, regulatory guidance, and statutory provisions using a doctrinal research methodology. It was discovered that CIRCIA established a new federal requirement requiring covered entities to report significant cyber incidents within 72 hours of a reasonable determination and any ransomware payments within 24 hours. Along with protecting submitted reports under statutory confidentiality provisions, the legislation also gave the Cybersecurity and Infrastructure Security Agency (CISA) the authority to issue subpoenas in cases of non-compliance. Ambiguities in the criteria for "covered entities" and the definitional scope of "covered cyber incidents" were noted as possible barriers to successful implementation, despite its progressive intentions. In order to guarantee consistent compliance across industries, the study suggested that CISA's upcoming rulemaking process adopt explicit, sector-specific guidance. Furthermore, it helped to create threat intelligence-sharing systems that support anonymizing and more public and private sector cooperation so that the Act will be successful without compromising private or sensitive commercial data under danger.*

Keywords: CIRCIA, Cyber Incident Reporting, Critical Infrastructure, Ransomware, CISA, and Regulatory Compliance.

1.0 Introduction

The growth of technology, especially information technology, has not only generated a dramatic increase in the prevalence of criminal conduct but has also led to the birth of what seems to be some new sorts of criminal activity[2] that comes under the umbrella of cybercrime. The occurrence and cost of cybercrime are rising year after year. For 2021 alone, it created a worldwide devastation that cost close to $6 trillion.[3] An amount predicted to climb by 15% yearly through the next five years.[4] More and more analysts suggest that this figure is expected to be about $10.5 trillion by 2025, a big increase from $3 trillion recorded in 2015.[5] The worldwide cost of cybercrime reached $8 trillion in 2022.[6] Statistics show that cybercrime will cost the world economy up to 20 trillion U.S. dollars by 2026, with this amount exploding exponentially and crossing $11 trillion in 2023. That is about 1.5 times the unwanted growth compared to statistics for 2022.[7]

Keeping these realities in view, one of the foremost responsibilities with which the modern nation-state is burdened with is national security. This notion of security is not just traditional military threats but includes a complex web of issues such as terrorism,

[1] Chinelo Patience Umeanozie, DipLaw, LL.B, BL, LL.M, MBA; umeanoziechinelo1@gmail.com
[2]Chuma Akana, LL.B, LL.M; akanachuma@gmail.com
[3]Chukwuemezie Charles Emejuo, LLB, BL, LLM; ccemejuo@gmail.com

[2] Ani L, Cyber Crime and National Security: The Role of the Penal and Procedural Law, Law and Security in Nigeria. <http://nials-nigeria.org/pub/lauraani.pdf.> accessed 6th April, 2025

[3] Hernandez J R, What is the Actual Cost of Cybercrime? <https://www.evolvesecurity.com/blog-posts/actual-cost-of-cybercrime#:~:text=The%20global%20cost%20of%20cybercrime%20was%20estimated%20to%20surpass%20%248,beyond%20%2411%20trillion%20in%202023.> accessed 6th April, 2025

[4] *Ibid*

[5] *Ibid*

[6] *Ibid*

[7] *Ibid*

transnational crime, economic stability, environmental sustainability, energy and food security, and, most importantly, cybersecurity.[8] In fact, the relationship between cyber resilience and national security cannot be done without in today's digitalized society.[9] The expanding digital infrastructure upon which societies and economies rely—spanning communication networks, energy grids, transportation systems, and healthcare has rendered cybersecurity a central pillar of national security policy and practice.[10]

The national-critical infrastructures are, at large, both strategically vulnerable yet also operationally essential, which have come to be defined, in broad terms, as facilities and systems — physical, non-physical and cyber — responsible for the functioning of society and economy. Since cyberattacks that threaten critical infrastructure can result in cascading effects across the public welfare, economic systems, and national defense, cyberspace has thus become a matter of national interest in terms of stability, safety, and resilience.[11]

Due to the rising occurrence of cyber threats, there is a corresponding demand for cyber risk intelligence. Following this, various countries have established many kinds of laws and regulations aimed at tackling crimes in cyberspace.[12] Important items include the European Union's General Data Protection Regulation (GDPR) plus the Directive on Security of Network and Information Systems (NIS Directive). Both emphasize the value of speedy breach notification. Such frameworks have acted as basic designs for related domestic strategies.[13] At the same time, the United States passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in 2022, which requires a systematized incident reporting process by entities in critical sectors for such incidents. This will also facilitate strengthening the awareness of cybersecurity threats at the federal level, improving national response capability, as well as building resilience across sectors.

This study sets out to critically examine the legal obligations imposed by the Cyber Incident Reporting for Critical Infrastructure Act, enacted in 2022 (CIRCIA). The investigation is on discerning the thresholds that trigger reporting requirements, the mechanisms designated for enforcement, and the subsequent ramifications for entities subject to this regulation. The analysis is an acknowledgment and exploration of the profound ethical and constitutional questions brought to the fore by governmental initiatives in national cybersecurity. It is therefore, an attending work in the critical assessment of how far the scales will tip in an assurance of public safety against some basic rights such as privacy, autonomy, and freedoms of expression. The end of the analysis is to provide a strong understanding in the converging fields of cybersecurity, infrastructure protection, and compliance under US federal law.

2.0 Critical Infrastructure

Before we can dive into any real talk about critical infrastructure, we've got to zero in on cybersecurity. It's non-negotiable—protecting these vital systems from ever-smarter threats and making sure they can bounce back from potential cyberattacks is a must.

Cybersecurity boils down to spotting, evaluating, and tackling risks that could mess with data security or integrity, whether it's stored or moving through a system. It's also about shielding Critical Infrastructure from dangers that could knock out essential services or operations.[14] It provides protection for nations, institutions, individuals, and ICT assets. The denotation of information security is the guarding of information and information systems against unauthorized access and disclosure, in addition to maintaining integrity

[8]Viganò, E., Loi, M., Yaghmaei, E. Cybersecurity of Critical infrastructure. (2020). In: Christen, M., Gordijn, B., Loi, m.(eds.), The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology (21). Springer. <https://doi.org/10.1007/978-3-030-29053-5_8> accessed 4th April, 2025

[9]*Ibid*

[10]Ecabert, T., Muhly, F. & Zimmermann, V. Implications of cyber incident reporting obligations on multinational organizations headquartered in Switzerland. Int. Cybersecurity. Law Rev. 5, 585–614 (2024). <https://doi.org/10.1365/s43439-024-00129-x> accessed 5th April, 2025

[11] Understanding the Impact of the CISA Critical Infrastructure Cyber Incident Reporting Rules. <https://asimily.com/blog/impact-of-cisa-cyber-incident-reporting-rules/> accessed 7th April, 2025

[12]Ikenna U. Ibe; Justus U. Ijeoma & Chukwubuikem I. Obianyo, (2024) The Dichotomy Between Cybercrimes Act 2015 and Freedom of Expression under Nigeria's 1999 Constitution, COOU Law Journal Volume (9) 1; 46 https://www.journals.ezenwaohaetorc.org/index.php/coou/issue/view/225/showToc > accessed 7th April, 2025

[13]*Ibid*

[14] Adamu Garba, and Aliyu Bade, "The Current State of Cybersecurity Readiness in Nigeria organizations'', (1) *Educational Research (IJMCER*), (2021) (3): 154-162.

and providing accountable continuous access to services.[15] It includes the protection of information systems with data to uphold confidentiality, integrity, and availability, even when there are potential attacks.[16] So, cybersecurity is defending users' information infrastructure from various threats.

Critical Infrastructure

Defining critical infrastructure is inherently complex due to its variation across countries. What one nation prioritizes depends on factors like national goals, technological progress, geographic risks, and economic frameworks, which differ elsewhere. In a country where farming is the backbone of life, things like irrigation systems or grain storage might take center stage. But in a place buzzing with tech, high-speed internet and data centers could be what keeps things running. This kind of difference makes it tough to pin down one solid definition of critical infrastructure that works everywhere. Every nation has to tweak what it considers "critical" based on its own quirks and priorities..

To corroborate the above thesis, a 2011 Chatham House report on cybersecurity brought the question:

> what should be considered 'critical' in a modern society; does the spread of information and communication technologies (ICT) also expand the definition of critical national infrastructure? It could be argued convincingly that the criticality of companies such as Google or Amazon to the functioning of a complex modern economy should be acknowledged by governments.[17]

An extended discourse on the issue involves developing a more meaningful understanding of critical infrastructure. It looks at some challenges that interdependence and dependence pose with respect to cyber security and protecting CI. From this, insights were made into these generally broad and oftentimes ambiguous categories, which, in turn, highlighted the need to be much clearer and more specific in defining CI and earmarking investment to address supportive security measures. The report then tackled another sub-question: do increasing cyber complexities and dependencies imply increasing vulnerability? If risks go up, then how does one increase the security response and still justify the economic and social raison d'etre for interconnection? Or are these two goals mutually incompatible?[18]

The aforementioned considerations form the foundation for the development of cybersecurity policies, strategies, and legal frameworks. As critical infrastructure becomes increasingly interconnected and reliant on digital systems, the complexity of securing such systems correspondingly intensifies. This report demonstrates that although greater cyber complexity can amplify vulnerabilities, it does not inherently make resilience and security incompatible with economic and social connectivity. Instead, it underscores the pressing need for clearer conceptual definitions, strategic investments, and adaptive policy measures capable of reconciling security imperatives with the advantages of interdependence.

Answering the call for a more precise definition of CI, the Department of Homeland Security has, in its Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise, defined CI as any physical or virtual information system that controls, processes, transmits, receives, or stores electronic information in any form-including data, voice, or video-that: (1) is vital to the functioning of critical infrastructure; (2) is so vital to the United States that incapacity or destruction of such systems would effect a debilitating impact on national security, national economic security, or national public health or safety; or (3) is owned or operated by-or on behalf of-a State, local, tribal, or territorial government entity.[19]

[15]Ikuero F, Preliminary Review of Cybersecurity Coordination in Nigeria, *Nigerian Journal of Technology* (2022) 41 (3): 521-526

[16] Ikenna U. Ibe; Justus U. Ijeoma & Chukwubuikem I. Obianyo, The Dichotomy Between Cybercrimes Act 2015 and Freedom of Expression under Nigeria's 1999 Constitution, (2024) *COOU Law Journa*l (9) 1; 46

[17] Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, *Cyber Security and the UK's Critical National Infrastructure* (Chatham House, September 2011), p. 2, <http://www.chathamhouse.org/publications/papers/view/178171.> accessed 5th April, 2025

[18] Dave Clemente, *Cyber Security and Global Interdependence: What Is Critical*? (Chatham House, February 2013), p.11

[19] Department of Homeland Security, Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise (2011) Available at <https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf> accessed 6th April, 2025

CI is increasingly dependent on information and communication technologies (ICT).[20] As a result, a country may suffer greatly if such ICT with vital services and functions is disrupted. The Critical Information Infrastructure (CII) is the collection of "all interconnected information and communication infrastructures which are essential for the maintenance of vital societal functions, (health, safety, security, or the economic or social well-being of people), the disruption or destruction of which would have serious consequence."

Closely related to CI is systemically important entities" (SIEs).[21] These organizations have vital infrastructure, and any disruptions or malfunctions would have a major impact on public health and safety, economic security, and national security.[22]

Critical Infrastructure (CI) can be understood at various levels, each with its own scale and complexity. These levels include organizational, local, regional, national, and global.[23]When Critical Infrastructure (CI) is referred to at the national level, it is often termed Critical National Infrastructure (CNI). This refers to various usually interconnected infrastructure which failure or malfunction due to manmade or natural causes may likely result to debilitating effects to national security, economic security, safety and well-being of citizens.[24] Most critical systems are the so-called critical infrastructures: assets, networks and systems, self-sufficient or dependent on other systems, that are essential and stand worth to the functioning of the national. Critical infrastructures need such importance that even a disruption, a degradation or destruction from any cause-natural, accidental, or by a man-made disaster-affects the country's security, economy, public safety and even societal well-being.

Critical National Infrastructure (CNI) covers key areas like energy (think oil, gas, and electricity), water, telecom, transportation, banking, healthcare, and government services. In today's hyper-connected, tech-driven world, these systems don't just stand alone. They're woven into complex webs of social and technical networks, so when one part breaks down, it can set off a chain reaction. Take a long power outage, for example—it could mess with phone lines, banking, water treatment plants, hospitals, and a bunch of other essential services.[25]

The imperative to safeguard Critical National Infrastructure has intensified considerably amid the proliferation of cyber threats, terrorist activities, climate-induced catastrophes, pandemic outbreaks, and geopolitical tensions.[26] These emergent phenomena introduce novel vulnerabilities and obstacles that challenge infrastructural resilience across multiple domains. Consequently, ensuring the security, accessibility, and reliability of CNI constitutes a fundamental prerequisite for preserving national stability and sustaining public confidence in governmental institutions.

The interdependence between infrastructural integrity and societal cohesion underscores the necessity for robust protective frameworks that anticipate and mitigate diverse threat vectors through adaptive governance mechanisms.[27]

This study specifically focuses on this particular subset of critical infrastructure—Critical National Infrastructure—recognizing its strategic significance and the need for robust governance, regulatory frameworks, and risk mitigation strategies.[28] The main goal of this study is to dig into how CIRCIA 2022 shapes the way we identify, safeguard, and manage Critical National Infrastructure (CNI).

---

[20] GFCE Global Good Practices, Critical Information Infrastructure Protection (CIIP)-Global Conference on Cyberspace (2017) p5 <https://thegfce.org/wp-content/uploads/2020/06/CriticalInformationInfrastructureProtectionCIIP.pdf> accessed 5th April, 2025

[21] PwC, Cyber reporting for critical infrastructure. <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-incident-reporting.html#content-free-1-e9b5> accessed 6th April, 2025

[22] *Ibid*

[23] Kim Smith and Ian David Wilson, An Analysis of Definitions of Critical Infrastructures and their Interdependencies (2023) *International Journal of Critical Infrastructures*, (19) 4; 323-339

[24] U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience (2013) <https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf> accessed 6th April, 2025

[25] *Ibid*

[26] Aleem M, Sufyan M, Ameer I, Mustak M. Remote work and the COVID-19 Pandemic: An Artificial Intelligence-Based Topic Modeling and A Future Agenda. J Bus Res. 2023 Jan;154:113303. doi: 10.1016/j.jbusres.2022.113303. Epub 2022 Sep 21. PMID: 36156905; PMCID: PMC9489997.

[27] *Ibid*

[28] *Ibid*

It considers the rise of new threats and the growing complexity of today's infrastructure systems. Beyond that, the study looks at how well this law can boost the nation's ability to bounce back, sharpen its response skills, and ramp up overall readiness.[29]

3.0 Critical Infrastructure Threat and the Emergence of CIRCIA, 2022

More and more frequently, it seems that the threats directed toward critical infrastructure have undergone increasing sophistication, making ever more urgent a need for strong, coordinated national responses. All these threats, from cyberattacks on energy grids to ransomware incidents crippling healthcare systems, make the vulnerabilities of critical infrastructure systems increasingly visible.[30] In response to this threat landscape, the United States enacted the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in 2022—marking a big step toward enhancing the resilience and security of critical infrastructure nationwide. This section explores the nature of these threats and the reason behind the emergence of CIRCIA as a landmark legislative intervention.

In February 2015, Anthem became the first major healthcare provider to suffer a significant cyberattack when attackers accessed 80 million records belonging to users of Amerigroup and Blue Cross Blue Shield health plans.[31] Just a few months later, in June 2015, hackers breached the Office of Personnel Management (OPM), stealing the personal information of over 20 million individuals in what was, at the time, the largest cyberattack on the U.S. government.[32] The following month, the hacking group known as Impact Team targeted the adultery website Ashley Madison, obtaining its user database in an attempt to blackmail its parent company, Avid Life Media. When their demands were not met, the group publicly released the sensitive data of 37 million users, along with the website's corporate email database.[33]

Ransomware Attacks have been a major concern for U.S. infrastructure. High-profile incidents like the Colonial Pipeline ransomware attack in 2021, along with attacks on local governments, hospitals, and other critical infrastructure, have exposed the vulnerabilities of U.S. systems to cybercrime. These attacks often result in service disruptions, financial losses, and national security risks. Supply Chain Attacks**,** such as the Solar Winds breach in 2020, have demonstrated how cybercriminals can infiltrate U.S. systems through trusted software providers.[34] The SolarWinds incident, which affected a vast range of government and private sector systems, revealed the systemic vulnerabilities within critical infrastructure.[35] These types of attacks can have wide-ranging consequences, affecting entire industries and not just individual organizations.[36]

The Cybersecurity Vulnerabilities in critical sectors, such as the energy sector and healthcare[37] are also pronounced. Attacks targeting electric grids and oil pipelines can cause widespread disruptions, as seen in recent years when attackers attempted to compromise the U.S. power grid.[38] Similarly, the healthcare sector continues to face significant cybersecurity threats, with ransomware attacks

[29] *Ibid*

[30] Kelvin Ovabor et al, Quantum-driven predictive cybersecurity framework for safeguarding Electronic Health Records (EHR) and enhancing patient data privacy in healthcare systems (2025) *World Journal of Advanced Research and Reviews* 25(01):1015-1023

[31] <https://ace-usa.org/blog/research/research-technology/pros-and-cons-of-the-cybersecurity-information-sharing-act-of-2015/> accessed 8th April, 2025

[32] *Ibid*

[33] *Ibid*

[34] Beyond Identity, Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them (3 October, 2021) <https://www.beyondidentity.com/resource/software-supply-chain-attack-methods-behind-solarwinds-kaseya-and-notpetya-and-how-to-prevent-them#:~:text=The%202020%20SolarWinds%20attack%20demonstrated,needed%20to%20protect%20against%20this.> accessed 7th April, 2025

[35] *Ibid*

[36] *Ibid*

[37] Ikechukwu C Obianyo, Solomon V Ater, The Legal Implication of Data Privacy and Protection in the Age of Big Data and the Ever-Emerging Technologies in Nigeria, 3 (2023) Idemili Bar Journal, 3 <https://ezenwaohaetorc.org/journals/index.php/IBJ/article/viewFile/2643/2760> accessed 7th April, 2025

[38] Robert K Knake, A Cyberattack on the US Power Grid: Contingency Planning Memorandum No. 31 (Council on Foreign Relations, April 2017) <https://www.cfr.org/report/cyberattack-us-power-grid> accessed 5th April, 2025

putting lives at risk by disrupting vital healthcare services. These sectors are often reliant on legacy systems, which makes them more vulnerable to sophisticated cyber threats.[39]

Cyberattacks and disinformation campaigns targeting election infrastructure have raised serious concerns about the integrity of democratic processes. The interference in the 2016 and 2020 U.S. elections by foreign actors, including Russia and China, demonstrated how cyberattacks could threaten national security and disrupt electoral processes.[40]

Foreign State-Sponsored Cyberattacks from nations like Russia**,** China**,** and Iran have increasingly targeted U.S. critical infrastructure, particularly in industries such as defense, communications, and transportation.[41] These state-sponsored actors seek to disrupt operations, steal sensitive data, or engage in espionage, posing a significant risk to national security. The Financial Sector remains another high-priority target for cyberattacks.[42] With the potential to disrupt banking services, steal sensitive financial data, or trigger broader economic disruptions, attacks on the financial sector can have severe national and global consequences.

Advanced Persistent Threats (APTs) are long-term, targeted cyberattacks carried out by highly skilled hackers who gain unauthorized access to sensitive systems.[43] These threats have been increasingly targeting U.S. critical infrastructure, and their sophistication and impact have only grown over time. APTs often involve stealthy attacks that allow hackers to monitor and manipulate infrastructure for extended periods, posing a significant risk to national security.

Companies operating in critical infrastructure sectors have continued to face a growing threat from ransomware attacks in recent years. According to the FBI's Internet Crime Complaint Center (IC3), 2023 saw 1,193 reported ransomware incidents targeting 14 of the 16 critical infrastructure sectors—an alarming indicator of the scale and persistence of this threat. The healthcare sector was the most targeted, with 249 reported incidents, followed by critical manufacturing (218 attacks) and government facilities (156 attacks). Notably, the number of ransomware complaints rose by 37% compared to 2022, reflecting a sharp year-over-year increase in both frequency and intensity of these attacks.[44]

The growing complexity and frequency of these attacks demonstrate why CIRCIA 2022 is critical for U.S. infrastructure protection. It enables a proactive and coordinated response to cyber threats, helping to safeguard the nation's most vital systems against increasingly sophisticated and frequent cyberattacks.

4.0 Overview of CIRCIA, 2022 and Legal Obligations

CIRCIA was enacted in March of 2022 by President Joe Biden. It is yet another regulation aiming to enhance federal cybersecurity by requiring critical infrastructure entities to report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA).[45]

---

[39] *Ibid*

[40] Blake, Jedidiah. "Russian Interference In U.S. Elections: How To Protect Critical Election Infrastructure From Foreign Participation." Public Contract Law Journal 49, no. 4 (2020): 709–34. <https://www.jstor.org/stable/27010377.> accessed 5th April, 2025

[41] Industrial Cyber, DHS warns of escalating threats to US critical infrastructure in 2025 Homeland Threat Assessment (4 December, 2024) <https://industrialcyber.co/threat-landscape/dhs-warns-of-escalating-threats-to-us-critical-infrastructure-in-2025-homeland-threat-assessment/.> accessed 5th April, 2025

[42] Fabio Natalucci, Mahvash S Qureshi and Felix Suntheim, 'Rising Cyber Threats Pose Serious Concerns for Financial Stability: Greater Digitalization and Heightened Geopolitical Tensions Imply That the Risk of a Cyberattack with Systemic Consequences Has Risen' (IMF Blog, 9 April 2024) https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability accessed 5th April, 2025

[43] CISA, Nation-State Cyber Actors <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors> accessed 8th April, 2025

[44] Understanding the Impact of the CISA Critical Infrastructure Cyber Incident Reporting Rules. <https://asimily.com/blog/impact-of-cisa-cyber-incident-reporting-rules/> accessed 5th April, 2025

[45] Grayson Taylor, What is the CISA Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)? (Aug 27 2024) <https://www.schellman.com/blog/cybersecurity/what-is-circia#:~:text=Back%20in%20March%202022%2C%20the,Infrastructure%20Security%20Agency%20(CISA).>accessed 6th April, 2025

More particularly, the aim is to improve the government's understanding of cyber threats and enable better incident response and prevention measures for covered critical infrastructure entities.

The Cybersecurity and Infrastructure Security Agency (CISA) is tasked with developing and enforcing regulations that require designated critical infrastructure entities to report "covered" cybersecurity incidents within 72 hours of their occurrence. Covered incidents may include events such as network breaches or significant disruptions that impair an entity's operational capabilities. In addition, if a ransomware payment is made, it must be reported to CISA within 24 hours—unless the payment is tied to a broader cyber incident, in which case the 72-hour reporting timeline applies.[46]

What Is a Covered Entity Under CIRCIA?

Under the proposed rule outlined in **6 CFR § 226.2**, a **covered entity** is defined based on specific criteria related to critical infrastructure and organizational characteristics. To determine whether an entity qualifies as a covered entity, the following questions must be considered:

1. **Does the entity meet one or more of the 16 sector-based criteria listed in 6 CFR § 226.2?**

The proposed rule defines sector-specific criteria for each of the 16 critical infrastructure sectors.[47]These sectors include**:** Chemical**,** Commercial Facilities**,** Communications**,** Critical Manufacturing**,** Dams**,** Defense Industrial Base**,** Emergency Services**,** Energy**,** Financial Services**,** Food and Agriculture**,** Government Facilities**,** Healthcare and Public Health**,** Information Technology**,** Nuclear Reactors, Materials, and Waste**,** Transportation Systems**,** and Water and Wastewater Systems**.**[48]If an entity engages in activities or performs functions that meet any of these criteria, it may be considered a covered entity—regardless of how it self-identifies or what industry label it uses**.**

2. **Is the entity part of a critical infrastructure sector?**

Even if not explicitly listed, an entity operating within one of the 16 critical infrastructure sectors may fall within the scope if it plays a role essential to national security, economic stability, or public health and safety.

3. **Is the entity a small business, as defined by the Small Business Administration (SBA)?**

Entities that meet the SBA's definition of a small business are exempt from CIRCIA's reporting requirements. However, this exemption does not apply to all businesses across the board. For example, many companies in the Information Technology (IT) sector, especially those that, provide services to the federal government, offer products involving privileged access, operate in operational technology (OT) environments and are linked to domain name services (DNS). They may still be required to report incidents under CIRCIA, regardless of size.

CIRCIA identifies 16 critical infrastructure sectors, and any entity that meets one or more of the proposed criteria is classified as a covered entity—regardless of how the entity identifies its own industry. Small businesses, as defined by the Small Business Administration (SBA), are exempt from these reporting obligations. However, a wide range of IT hardware and software companies will fall under the reporting requirements, especially within the Information Technology sector. This includes companies that work with the Federal government, as well as those whose products or services involve privileged access, are integrated into operational technology (OT) environments, or are connected to domain name services (DNS)—regardless of company size.

[46] Michael Clark, Making Sense of Proposed CIRCIA Incident Reporting Rules (Extrahop, 3 December,2024) <https://www.extrahop.com/blog/circia-cyber-incident-reporting-requirements> accessed 6th April, 2025

[47] The White House, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Washington, D.C.: Feb. 12, 2013).

[48] CISA, Covered Entity Fact Sheet. available at https://www.cisa.gov/resources-tools/resources/covered-entity-fact-sheet

Covered entities are required to report any "substantial cyber incident" they experience. According to CISA, a substantial cyber incident is one that results in any of the following:

- A significant loss of confidentiality, integrity, or availability of the entity's information systems or networks
- A serious impact on the safety or resilience of the entity's operational systems or processes
- A disruption to the entity's ability to conduct business operations, carry out industrial activities, or deliver goods or services
- Unauthorized access to the entity's systems or sensitive, nonpublic information, caused by:
    - A compromise of a cloud service provider, managed service provider, or other third-party data host
    - A supply chain compromise

In addition, covered entities must report any ransomware payments. These payments include the transfer of money, property, or other assets—including virtual currencies such as Bitcoin—made in response to a ransomware attack.[49]

What should be contained in the report?

Under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), covered entities are required to submit detailed reports following a covered cyber incident. These reports must include all relevant and available information that could aid the Cybersecurity and Infrastructure Security Agency (CISA) in assisting the affected organization and preventing similar incidents across other sectors. Critical details may include information identifying the attacker (if known), a description of the nature and scope of the incident, the vulnerabilities exploited, indicators of compromise, and the tactics, techniques, and procedures (TTPs) used by the threat actors. Covered entities must also outline any mitigation efforts or incident response activities they have undertaken.

In cases involving ransomware, the report must contain additional details, such as the amount demanded, payment instructions, and the specifics of any ransom payment made. These elements are vital for understanding the broader threat landscape and informing CISA's strategic response efforts.

Recognizing that new insights often emerge as an investigation unfolds, CIRCIA provides a mechanism for submitting supplemental reports. These follow-up submissions allow covered entities to provide updates that may include newly discovered facts, notification of ransom payments made after the initial report, or confirmation that the incident has been fully resolved.

Furthermore, CIRCIA imposes data retention obligations on covered entities. They must preserve all relevant records and data connected to the cyber incident for a minimum of two years from the date the most recent report was submitted. The preservation timeline begins either on the date the entity reasonably believes the incident occurred or the date a ransom payment was made—whichever comes first. This requirement ensures that critical evidence remains available for future review or investigation, contributing to improved cyber resilience across critical infrastructure sectors.

5.0 Legal and Operational Challenges under the Cyber Incident Reporting for Critical Infrastructure Act, 2022

The critical infrastructure cybersecurity has advanced significantly with the passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). However, a number of practical and legal obstacles stand in the way of its implementation. To guarantee its effectiveness and compliance with current legislation and international regulations, these issues need to be seriously addressed.

5.1 Ambiguity in definitions and thresholds for reporting

The ambiguity of identifying important terminology and thresholds is one of CIRCIA's biggest obstacles. Owners and operators of critical infrastructure face uncertainty as a result of this difficulty. According to CIRCIA, organizations must disclose "substantial incidents" and "covered cyber incidents".[50] However, these words are still unclear. Therefore, it allows for arbitrary interpretation.

[49]Patsakis, C., Politou, E., Alepis, E. et al. Cashing out crypto: state of practice in ransom payments. Int. J. Inf. Secur. 23, 699–712 (2024). <https://doi.org/10.1007/s10207-023-00766-z> accessed 7th April, 2025

[50] Gerard Comizio and others, Combating Ransomware: One Year On, Joint PIJIP/TLS Research Paper Series (2023)

The Act is undefined about what is meant by a "substantial cyber incident". For instance, the word "substantial" is arbitrary and has different meanings in different industries. Because of this, organizations are left wondering if certain incidents, like small-scale ransomware attacks or data breaches, qualify for reporting. Although incidents that result in "substantial disruption"[51] are mentioned by CIRCIA, an objective metric for determining how significant an incident must be is not provided. For instance, is an outage affecting a single facility considered substantial, or must it extend to regional or national levels?

Furthermore, the term covers a wide range of cyber incidents,[52] but organizations are left unsure of what qualifies as a "covered" incident in the absence of clear criteria. For instance, is it appropriate to report ransomware outbreaks or phishing attempts that do not cause serious harm? Confusion results from this ambiguity, especially for operators in industries with disparate cybersecurity standards.

Organizations are required by CIRCIA to notify the Cybersecurity and Infrastructure Security Agency (CISA) of any covered cyber events within 72 hours of their discovery.[53] Determining the precise moment of "discovery" is difficult, though. Determining when the reporting clock begins might be challenging since some situations may change over time.

It is important to note that the Act is ambiguous about whether discovery includes the first identification of suspicious conduct, verification of a breach, or evaluation of its consequences. Cyber incidents frequently happen in phases, and it is very difficult to pinpoint the exact moment of detection.

The Act applies to entities in 16 critical infrastructure sectors, such as energy, healthcare, finance, and telecommunications. Every sector has distinct operating and cybersecurity environments.[54] Nonetheless, the operational environments and cybersecurity threats in these sectors range greatly. A one-size-fits-all approach to reporting thresholds may fail to address sector-specific nuances. It also creates confusion and inconsistent compliance. For example, a cyber incident in the energy sector causing a minor disruption in power delivery may have national security implications, while a similar incident in a small healthcare facility may not. Applying the same reporting standards across diverse sectors fails to account for these differences.

Without sector-specific limits, organizations also find it difficult to decide whether an occurrence qualifies for reporting. For instance, what is considered a serious disruption in the transportation industry (such as a service outage impacting air traffic control) may be very different from what is considered a significant interruption in the financial sector (such as a brief stock market malfunction).

CIRCIA does not authorize person or agency the authority to decide what is and is not substantial.[55] This ambiguity will probably cause covered companies to report more or less, which will have an impact on the final quality and usefulness of the data that CISA receives.[56] The SEC has mandated disclosure of certain "material" cybersecurity threats by publicly traded corporations for more than ten years.[57] The SEC suggested new cybersecurity risk disclosure rules for public corporations one week prior to the enactment of CIRCIA.[58] According to the SEC's recently proposed rule, public corporations must report a "material" cyber event on a publicly available 8-K form within four days, citing "growing concerns" that material cyber incidents are underreported and that reporting may not be prompt enough.[59]

Therefore, the ambiguity in definitions and thresholds risks overreporting (leading to unnecessary administrative burdens) or underreporting (leaving critical incidents undetected). These undermines the Act's intent of timely and effective incident response. Without clear definitions, enforcement of reporting requirements becomes inconsistent and potentially arbitrary. Organizations may

[51] § 226.1 CISA-2022

[52] CIRCIA, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet. <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia> accessed 7th April, 2025

[53] Defense Federal Acquisition Regulation Supplement, 252.204-7012 (Oct. 28, 2022).

[54] Bright Ojo, Justine ChilenovuOgborigbo and Maureen Oluchukwuamaka Okafo, 'Innovative Solutions for critical infrastructure resilience against cyber-physical attacks', *World Journal of Advanced Research and Reviews*, 2024, 22(03), 1651–1674

[55] Kaitlyn Holmecki, Comments of the American Trucking Associations (2024). <https://downloads.regulations.gov/CISA-2022-0010-0364/attachment_1.pdf> accessed 8th April, 2025

[56] Ibid.

[57] CF Disclosure Guidance, Topic No. 2 Cybersecurity, SEC DIVISION OF CORPORATION FINANCE (2011)

[58] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 C.F.R. 229, 232, 239, 240, & 249 (proposed Mar. 9, 2022)

[59] Ibid.

face penalties for failing to report incidents they did not believe met the threshold, leading to legal disputes and eroding trust in the regulatory framework.

5.2 Balancing transparency with confidentiality and reputational risk

CIRCIA's reporting requirements aim to increase transparency and information-sharing[60] between the private sector and the government to combat cyber threats[61]. However, organisations face challenges in balancing this transparency with confidentiality and reputational risk. There is concern on how this information will be handled and protected. Although CIRCIA has provisions to protect sensitive information, including exemptions from public disclosure (e.g., under FOIA - Freedom of Information Act)[62], the risk of leaks or inadvertent exposure remains. CIRCIA mandates reporting of significant cyber incidents to CISA[63] enhance national cybersecurity resilience. However, this requirement raises concerns about several issues. Reporting cyber incidents to CISA involves sharing sensitive data about vulnerabilities, breaches, and mitigation efforts. Organizations may worry that such information may be inadvertently disclosed, either through government leaks or public records requests, exposing them to further cyberattacks or litigation. Although CISA is required to protect sensitive information, the risk of inadvertent disclosure remains.

Also, public awareness of a cyber-incident, even if properly reported, may damage an organization's reputation and erode stakeholder trust. This is particularly concerning for entities in sectors such as finance, healthcare,[64] and energy, where customer confidence is paramount. According to CIRCIA, information and reports provided in response to a subpoena should not be subject to the protections of civil liberties and privacy. They should not be subject to liability protections.[65] Despite the possibility of liability protections for reported information, organizations may still be afraid of regulatory enforcement or lawsuits resulting from event disclosures, particularly when negligence may be assumed. Furthermore, for multinational organizations, sharing incident details with U.S. authorities may create conflicts with global data protection regulations (e.g., GDPR in the EU, which limits cross-border data sharing). This adds complexity to compliance and confidentiality.

5.3 Legal tension with other federal/state cybersecurity laws and global data protection regulations

CIRCIA interacts with a complex web of existing cybersecurity and data protection regulations. There is no unified, national cybersecurity regulation in the United States. Instead, cybersecurity is addressed in a sector- or jurisdiction-specific way by a number of overlapping regulatory regimes at the federal and state levels. Critical infrastructure operators face operating difficulties and perhaps disputes as a result of this difficulty. There is no unified, national cybersecurity regulation in the United States. Instead, cybersecurity is addressed in a sector- or jurisdiction-specific way by a number of overlapping regulatory regimes at the federal and state levels.[66] Critical infrastructure operators face operating difficulties and perhaps disputes as a result of this difficulty.

At the federal level, many critical infrastructure sectors are already subject to cybersecurity requirements under laws such as the Health Insurance Portability and Accountability Act (HIPAA)[67] for healthcare or the Gramm-Leach-Bliley Act (GLBA)[68] for financial institutions. CIRCIA's reporting mandates duplicate or conflict with these existing obligations. The effect of this is that it leads to regulatory fatigue and inefficiencies.

---

[60] Michael Clark, Making Sense of Proposed CIRCIA Incident Reporting Rules, ExtraHop (2024) <https://www.extrahop.com/blog/circia-cyber-incident-reporting-requirements> accessed 6th April, 2025

[61] Beth George, Timothy Howard, Brock Dahl and Megan Kayo, Cybersecurity 2025, Chambers and Partners (2025). <https://practiceguides.chambers.com/practice-guides/comparison/971/15677/24449-24453-24458-24465-24468-24470> accessed 7th April, 2025

[62] Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 Federal Register 23723-23724, (2024).

[63] Gerard (n 47)

[64]Ikechukwu C Obianyo, Solomon V Ater, The Legal Implication of Data Privacy andProtection in the Age of Big Data and the Ever-Emerging Technologies in Nigeria, 3 (2023)Idemili Bar Journal, 3 <https://ezenwaohaetorc.org/journals/index.php/IBJ/article/viewFile/2643/2760> accessed 7th April, 2025

[65] 89 Fed. Reg. 23774- 23775

[66] Michael (n 56)

[67] PF Edemekong, P Annamaraju, M Afzal M, Health Insurance Portability and Accountability Act (HIPAA) Compliance. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025. Available at: <https://www.ncbi.nlm.nih.gov/books/NBK500019/> accessed 7th April, 2025

[68] Ojo (n 50)

Moreover, several states have their own cybersecurity incident reporting requirements (e.g., New York's SHIELD Act, Virginia Consumer Data Protection Act, California's Consumer Privacy Act).[69] The California Consumer Privacy Act is complicated to comply with, much like the GDPR. The Act influences other states while requiring companies to modify their data practices. Because there is not a federal statute, different states may have different privacy laws. [70] The federal provisions of CIRCIA could not be in line with state legislation. Organizations are forced to manage several, occasionally conflicting, reporting frameworks as a result.

In addition, multinational organizations operating critical infrastructure may face legal tension between CIRCIA and international data protection laws, such as the European Union's General Data Protection Regulation (GDPR). For instance, sharing cyber incident data with CISA might violate GDPR's strict data transfer and privacy rules, exposing organizations to significant penalties.

6.0 Comparative Legal Frameworks

6.1 European Union: NIS2 Directive and CIRCIA

The European Union introduced the NIS2 Directive (Directive on Security of Network and Information Systems) in 2022[71] the updated cybersecurity rules for critical infrastructure build on the foundation of the 2016 NIS Directive, strengthening protections for key sectors.[72] The new law ramps up cybersecurity demands and tightens rules for reporting incidents, with a consistent approach across the board. It covers a broad range of 18 sectors, from energy and healthcare to banking, transportation, IT services, and public administration.[73] A key obligation requires organizations to report significant cyber incidents to a designated national authority, such as a CSIRT, within 24 hours of discovery.[74]. For comparison, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in the United States addresses entities within 16 critical infrastructure sectors, among them energy, healthcare, finance, and telecommunications.[75]

The NIS2 Directive covers companies outside the EU that offer key or essential services in EU countries, no matter where they're based. If a non-EU business operates in NIS2-regulated industries in Europe or has a big digital footprint in the EU, they've got to follow NIS2 rules. For companies with a global reach, making sure they comply is a top priority. [76]

The NIS2 streamlines reporting obligations, it is more precise than its predecessor (NIS) in providing precise provisions relating to reporting, report content and timeframes.[77] Essential and relevant organizations must notify the 'competent authority' or the "Computer Security Incident Response Team" (CSIRT) of the Member State about any occurrence that jeopardizes the services offered, or the personnel utilizing the services. This includes an incident that have caused to disrupted business operations, or may incur a significant fiscal damaging loss. This also encompasses potentially dangerous cybersecurity threats that may have inflicted serious harm.[78] While certain businesses are required by the CIRCIA to notify the federal government of cyber-attacks, the majority are not. Defense contractors must report cyber issues, for instance, within 72 hours of being discovered.[79]

---

[69] Edward R. McNicholas and Frances E. Faircloth, Cybersecurity Laws and Regulations USA 2025, International Comparative Legal Guides (ICLG) (2024) <https://www.google.com/amp/s/iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa/amp>

[70]Okunade BAand others, 'Community-Based Mental Health Interventions In Africa: A Review And Its Implications For Us Healthcare Practices', *International Medical Science Research Journal* (2023) 3(3), 68-91.

[71] Niels Vandezande, Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor, Computer Law & Security Review (2024) Volume 52, 105890. <https://doi.org/10.1016/j.clsr.2023.105890>accessed 8th April, 2025.

[72]*Ibid*.

[73] C Singh, The European approach to cybersecurity in 2023: A review of the changes brought in by the network and information security 2 (nis2) directive 2022/2555, *International Company and Commercial Law Review* (2023) 5, 251-261.

[74] *Ibid.*

[75] Ojo. (n 5)

[76]PrivaLex Advisory, Beyond Borders: What Non-EU Companies Need To Know About The New NIS2 Cybersecurity Directive, Mondaq(2024) <https://www.mondaq.com/nigeria/security/1547478/beyond-borders-what-non-eu-companies-need-to-know-about-the-new-nis2-cybersecurity-directive> accessed 8th April , 2025

[77]*Ibid*.

[78]*Ibid*.

[79] Defense Federal Acquisition Regulation Supplement, 252.204-7012 (2022).

Within an hour of learning of a cyber issue, cloud service providers that operate systems for federal agencies must notify the U.S.-CERT and impacted clients.[80] Owners and operators of critical pipelines must notify CISA of any proven or suspected cybersecurity issues.[81] Public businesses are likewise subject to certain disclosure requirements when it comes to significant cybersecurity events.[82]

NIS2 contains additional sectors and entrants compared to CIRCIA, which is limited to particular critical infrastructure sectors. What is more, NIS2's 24-hour initial reporting deadline is more stringent than CIRCIA 's 72-hour requirement. In NIS2, organizations must submit a full report within 72 hours of the incident, outlining the cause, scope and impact of the breach as well as any mitigation measures taken. NIS2 brings uniformity across the whole of the EU, while CIRCIA serves alongside a fragmented patchwork of federal and state laws in the U.S., leading sometimes to conflicts.[83].

6.2 United Kingdom: NIS Regulations and CIRCIA

The UK's NIS Regulations, rolled out in 2018[84] were built on the EU's original NIS Directive but tweaked after Brexit to fit the UK's own system. They're all about keeping critical service providers and digital companies safe from cyber threats.[85] Businesses have to dig into their risks and put solid technical and organizational steps in place to fend off dangers.[86] Unlike CIRCIA, which zeros in on reporting incidents after they happen, the UK pushes hard for upfront risk checks. Each sector—like telecom or energy—gets its own regulator, such as Ofcom or Ofgem, to offer custom guidance.[87]f a major disruption hits, companies need to report it to the right authority within 72 hours. The UK's approach, with its sector-specific watchdogs, gives tailored oversight, while CIRCIA funnels everything through CISA without diving into industry-specific details.[88]

Under the UK NIS Regulations, the Operators of Essential Services (OESs) must report any incidents where the interruption or reduction in services exceeds the threshold value set for that OES, as determined by the relevant Competent Authority[89]. As outlined in the European Commission Implementing Regulation, for Digital Service Providers (DSPs), the incident reporting criteria are set at a harmonized threshold across Europe.[90] Both frameworks have a 72-hour reporting window, but the UK's regulators often require more detailed risk assessments upfront.

6.3 Australia: Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 and CIRCIA

Australia's Critical Infrastructure Protection (CIP) Act focuses on staying ahead of cyber threats with strong security measures and government support to safeguard vital infrastructure[91]. Entities must identify and mitigate risks through mandatory "Risk Management Programs" (RMPs)[92]. Cyber incidents must be reported to the Australian Cyber Security Centre (ACSC) within 12

[80] FEDRAMP INCIDENT COMMUNICATIONS PROCEDURES, FEDRAMP 6 (2021)

[81] DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, DEP'T OF HOMELAND SECURITY (2021)

[82] CF Disclosure Guidance, Topic No. 2 Cybersecurity, SEC DIVISION OF CORPORATION FINANCE(Oct. 13, 2011).

[83]*Ibid*.

[84] Department for Digital, Culture, Media, and Sport, The NIS Regulations 2018 (2018). Available at: <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018> accessed 7th April, 2025

[85] Department for Digital, Culture, Media & Sport, The NIS Regulations 2018 (2018) <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018> accessed 8th April, 2025

[86] Department of Health and Social Care, The Network and Information Systems Regulations 2018: guide for the health sector in England (2023)<https://www.gov.uk/government/publications/network-and-information-systems-regulations-2018-health-sector-guide/the-network-and-information-systems-regulations-2018-guide-for-the-health-sector-in-england> accessed 7th April, 2025

[87] Department for Digital, Culture, Media & Sport, Security of Network and Information Systems (2018). <https://assets.publishing.service.gov.uk/media/5ad87a14ed915d32a65dbe9b/NIS_-_Guidance_for_Competent_Authorities.pdf> accessed 8th April, 2025

[88]*Ibid*.

[89] Section 2.4, UK NIS Regulations

[90] Michael (n 56)

[91] Department of Home Affairs, Security Legislation Amendment (Critical Infrastructure Protection) Act 2022. <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022>accessed 8th April, 2025

[92] Susanne Lloyd-Jones and Kayleen Manwaring, First Steps to Quantum Resilience: Identifying 'Broken Concepts' In Australia's National Security Laws, *Australian National University Journal of Law and Technology* Vol 5(1) 2024

hours if they pose a significant threat to critical operations.[93] Lesser incidents must be reported within 72 hours.[94] Australia's Critical Infrastructure Protection (CIP) Act doesn't mess around—it demands that serious cyber threats get reported within 12 hours, way tougher than CIRCIA's 72-hour rule. Where CIRCIA stops short, Australia's law goes big: the government can jump in and tell companies what to do, or even take over operations if things get dire. The CIP Act casts a wide net, pulling in supply chain vendors and others to keep risks in check across the system. Like the UK, Australia's all about staying ahead of trouble with proactive planning, while CIRCIA's more about dealing with the fallout after something goes wrong.

6.4 Lessons Learned and Best Practices from Other Jurisdictions

1. Broaden the Scope of Covered Entities: Both NIS2 and Australia's CIP Act cover medium and large organizations across all sorts of sectors, including supply chain vendors. If CIRCIA followed suit and included these groups, it could tackle bigger, system-wide risks and boost overall security. CIRCIA could take a page from their book and use a tiered system—let smaller companies deal with simpler rules while hitting the big players with tougher requirements.
2. Harmonization of Cybersecurity Standards: The EU's harmonized approach under NIS2 makes regulatory fragmentation reduce. This ensures consistency across member states. In contrast, in the U.S. there is a lot of problems arising from conflicting federal and state cybersecurity laws. CIRCIA should work toward harmonizing federal, state, and sector-specific laws to reduce compliance burdens and get a unified national strategy.
3. Stricter Incident Reporting Timelines: NIS2 gives you just 24 hours to report issues, and Australia's CIP Act is even tougher—12 hours for critical cyber threats—compared to CIRCIA's more relaxed 72-hour window. Those tight deadlines push regulators to move fast and curb risks before they spiral. CIRCIA could keep its 72-hour rule for detailed reports but maybe add a quick 24-hour heads-up for major incidents to speed things up.
4. Emphasis on Proactive Risk Management: The UK and Australia require organizations to implement proactive risk management programs. This helps prevents incidents before they occur. CIRCIA focuses primarily on post-incident reporting, leaving a gap in proactive measures. CIRCIA could mandate risk assessments and mitigation plans as part of its framework, aligning with global best practices.
5. Sector-Specific Oversight: The UK's sector-specific regulators provide specific guidance for different industries. This increases compliance and addresses unique sectoral risks. CIRCIA's centralized approach through CISA might overlook the distinction of individual sectors. CIRCIA could designate sector-specific oversight bodies to work alongside CISA. CIRCIA may also provide customized support to pivotal infrastructure sectors.
6. Anonymized Threat Intelligence Sharing: The EU and Australia emphasize anonymized information-sharing to protect the reputation of reporting entities to allow collective learning. CISA could focus on sharing anonymized, aggregated threat intelligence to allow collaboration without exposing specific organizations.

7.0 Conclusion and Recommendations

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) marks a big change in how the U.S. tackles cybersecurity for the nation. By requiring certain organizations to quickly report cyber incidents, the law aims to boost awareness, speed up the government's response, and strengthen overall defenses against cyber threats. This study shows that CIRCIA plugs a major gap in the government's ability to spot critical cyber incidents, giving them a solid legal tool to gather real-time threat data affecting national infrastructure.

That said, the analysis points out some legal and practical gray areas that could trip up CIRCIA's goals. For starters, the definitions of "covered cyber incidents" and "covered entities" are murky, which might lead to confusion over compliance and inconsistent enforcement. While CIRCIA's confidentiality protections and subpoena powers add muscle and credibility, there's still a pressing need for clearer rules and better guidance.

Based on these insights, the study suggests the following steps forward:

1. **Regulatory Clarification and Sector-Specific Guidance**: CISA's forthcoming rulemaking should prioritize the development of sector-specific criteria and illustrative examples to define "covered cyber incidents" and "covered entities." This would reduce interpretive ambiguities and foster consistent compliance across industries.

[93] Department of Home Affairs, Cyber Security Incident Reporting. <https://www.cisc.gov.au/resources-subsite/Documents/cyber-security-incident-reporting.pdf> accessed 8th April, 2025
[94] *Ibid*.

2. **Enhanced Public-Private Collaboration**: Establishing robust engagement channels between CISA and private sector stakeholders will be vital. Mechanisms such as advisory committees, industry consultations, and pilot programs could facilitate mutual understanding and trust in the implementation process.
3. **Threat Intelligence Sharing and Anonymization Protocols**: To balance the need for actionable intelligence with concerns over confidentiality and commercial sensitivity, CISA should implement frameworks that allow for the anonymized aggregation and dissemination of threat data. This would promote sector-wide situational awareness without exposing proprietary information.
4. **Compliance Support and Capacity Building**: Particularly for small and medium-sized enterprises (SMEs) that may lack sophisticated cybersecurity infrastructure, the federal government should consider offering technical assistance, compliance toolkits, and financial incentives to facilitate adherence to reporting obligations.
5. **Periodic Review and Adaptive Governance**: Finally, CIRCIA's implementation should be subject to regular evaluation to ensure that it remains responsive to the evolving threat landscape. Feedback loops, audits, and legislative refinement mechanisms should be embedded into its regulatory architecture.

References

Adamu Garba, and Aliyu Bade, "The Current State of Cybersecurity Readiness in Nigeria organizations'', (1) *Educational Research (IJMCER*), (2021) (3): 154-162.

Aleem M, Sufyan M, Ameer I, Mustak M. Remote work and the COVID-19 Pandemic: An Artificial Intelligence-Based Topic Modeling and A Future Agenda. J Bus Res. 2023 Jan;154:113303. doi: 10.1016/j.jbusres.2022.113303. Epub 2022 Sep 21. PMID: 36156905; PMCID: PMC9489997.

Ani L, Cyber Crime and National Security: The Role of the Penal and Procedural Law, Law and Security in Nigeria. <http://nials-nigeria.org/pub/lauraani.pdf.> accessed 6th April, 2025

Beth George, Timothy Howard, Brock Dahl and Megan Kayo, Cybersecurity 2025, Chambers and Partners (2025). <https://practiceguides.chambers.com/practice-guides/comparison/971/15677/24449-24453-24458-24465-24468-24470> accessed 7th April, 2025

Beyond Identity, Software Supply Chain Attack Methods Behind Solarwinds, Kaseya, and Notpetya and How to Prevent Them (3 October, 2021) <https://www.beyondidentity.com/resource/software-supply-chain-attack-methods-behind-solarwinds-kaseya-and-notpetya-and-how-to-prevent-them#:~:text=The%202020%20SolarWinds%20attack%20demonstrated,needed%20to%20protect%20against%20this.> accessed 7th April, 2025

Blake, Jedidiah. "Russian Interference In U.S. Elections: How To Protect Critical Election Infrastructure From Foreign Participation." Public Contract Law Journal 49, no. 4 (2020): 709–34. <https://www.jstor.org/stable/27010377.> accessed 5th April, 2025

Bright Ojo, Justine Chilenovu Ogborigbo and Maureen Oluchukwuamaka Okafo, 'Innovative Solutions for critical infrastructure resilience against cyber-physical attacks', *World Journal of Advanced Research and Reviews*, 2024, 22(03), 1651–1674

C Singh, The european approach to cybersecurity in 2023: A review of the changes brought in by the network and information security 2 (nis2) directive 2022/2555, *International Company and Commercial Law Review* (2023) 5, 251-261.

CF Disclosure Guidance, Topic No. 2 Cybersecurity, SEC DIVISION OF CORPORATION FINANCE (2011)

CF Disclosure Guidance, Topic No. 2 Cybersecurity, SEC DIVISION OF CORPORATION FINANCE(Oct. 13, 2011).

CIRCIA, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet. <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia> accessed 7th April, 2025

CISA, Covered Entity Fact Sheet. available at https://www.cisa.gov/resources-tools/resources/covered-entity-fact-sheet

CISA, Nation-State Cyber Actors <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors> accessed 8th April, 2025

Cybersecurity and Infrastructure Security Agency, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 Federal Register 23723-23724, (2024).

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 C.F.R. 229, 232, 239, 240, & 249 (proposed Mar. 9, 2022)

Dave Clemente, *Cyber Security and Global Interdependence: What Is Critical*? (Chatham House, February 2013), p.11

Defense Federal Acquisition Regulation Supplement, 252.204-7012 (Oct. 28, 2022).

Defense Federal Acquisition Regulation Supplement, 252.204-7012 (2022).

Department for Digital, Culture, Media & Sport, Security of Network and Information Systems (2018). <https://assets.publishing.service.gov.uk/media/5ad87a14ed915d32a65dbe9b/NIS_-_Guidance_for_Competent_Authorities.pdf> accessed 8th April, 2025

Department for Digital, Culture, Media & Sport, The NIS Regulations 2018 (2018) <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018> accessed 8th April, 2025

Department for Digital, Culture, Media, and Sport, The NIS Regulations 2018 (2018). Available at: <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018> accessed 7th April, 2025

Department of Health and Social Care, The Network and Information Systems Regulations 2018: guide for the health sector in England (2023)<https://www.gov.uk/government/publications/network-and-information-systems-regulations-2018-health-sector-guide/the-network-and-information-systems-regulations-2018-guide-for-the-health-sector-in-england> accessed 7th April, 2025

Department of Home Affairs, Cyber Security Incident Reporting. <https://www.cisc.gov.au/resources-subsite/Documents/cyber-security-incident-reporting.pdf> accessed 8th April, 2025

Department of Home Affairs, Security Legislation Amendment (Critical Infrastructure Protection) Act 2022. <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022>accessed 8th April, 2025

Department of Homeland Security, Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise (2011) Available at <https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf> accessed 6th April, 2025

DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, DEP'T OF HOMELAND SECURITY (2021)

Ecabert, T., Muhly, F. & Zimmermann, V. Implications of cyber incident reporting obligations on multinational organizations headquartered in Switzerland. Int. Cybersecurity. Law Rev. 5, 585–614 (2024). <https://doi.org/10.1365/s43439-024-00129-x> accessed 5th April, 2025

Edward R. McNicholas and Frances E. Faircloth, Cybersecurity Laws and Regulations USA 2025, International Comparative Legal Guides (ICLG) (2024) <https://www.google.com/amp/s/iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa/amp>

European Commission, NIS2 Directive: new rules on cybersecurity of network and information systems. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> accessed 8th April , 2025

Fabio Natalucci, Mahvash S Qureshi and Felix Suntheim, 'Rising Cyber Threats Pose Serious Concerns for Financial Stability: Greater Digitalization and Heightened Geopolitical Tensions Imply That the Risk of a Cyberattack with Systemic Consequences Has Risen' (IMF Blog, 9 April 2024) https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability accessed 5th April, 2025

FEDRAMP INCIDENT COMMUNICATIONS PROCEDURES, FEDRAMP 6 (2021)

Gerard Comizio and others, Combating Ransomware: One Year On, Joint PIJIP/TLS Research Paper Series (2023)

GFCE Global Good Practices, Critical Information Infrastructure Protection (CIIP)-Global Conference on Cyberspace (2017) p5 <https://thegfce.org/wp-content/uploads/2020/06/CriticalInformationInfrastructureProtectionCIIP.pdf> accessed 5th April, 2025

Grayson Taylor, What is the CISA Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)? (Aug 27 2024) <https://www.schellman.com/blog/cybersecurity/what-is-circia#:~:text=Back%20in%20March%202022%2C%20the,Infrastructure%20Security%20Agency%20(CISA).>accessed 6th April, 2025

Hernandez J R, What is the Actual Cost of Cybercrime? <https://www.evolvesecurity.com/blog-posts/actual-cost-of-cybercrime#:~:text=The%20global%20cost%20of%20cybercrime%20was%20estimated%20to%20surpass%20%248,beyond%20%2411%20trillion%20in%202023.> accessed 6th April, 2025

https://ace-usa.org/blog/research/research-technology/pros-and-cons-of-the-cybersecurity-information-sharing-act-of-2015/> accessed 8th April, 2025

Ikechukwu C Obianyo, Solomon V Ater, The Legal Implication of Data Privacy and Protection in the Age of Big Data and the Ever-Emerging Technologies in Nigeria, 3 (2023) Idemili Bar Journal, 3 <https://ezenwaohaetorc.org/journals/index.php/IBJ/article/viewFile/2643/2760> accessed 7th April, 2025

Ikenna U. Ibe; Justus U. Ijeoma & Chukwubuikem I. Obianyo, (2024) The Dichotomy Between Cybercrimes Act 2015 and Freedom of Expression under Nigeria's 1999 Constitution, COOU Law Journal Volume (9) 1; 46 < https://www.journals.ezenwaohaetorc.org/index.php/coou/issue/view/225/showToc > accessed 7th April, 2025

Ikuero F, Preliminary Review of Cybersecurity Coordination in Nigeria, *Nigerian Journal of Technology* (2022) 41 (3): 521-526

Industrial Cyber, DHS warns of escalating threats to US critical infrastructure in 2025 Homeland Threat Assessment (4 December, 2024) <https://industrialcyber.co/threat-landscape/dhs-warns-of-escalating-threats-to-us-critical-infrastructure-in-2025-homeland-threat-assessment/.> accessed 5th April, 2025

Kaitlyn Holmecki, Comments of the American Trucking Associations (2024). <https://downloads.regulations.gov/CISA-2022-0010-0364/attachment_1.pdf> accessed 8th April, 2025

Kelvin Ovabor et al, Quantum-driven predictive cybersecurity framework for safeguarding Electronic Health Records (EHR) and enhancing patient data privacy in healthcare systems (2025) *World Journal of Advanced Research and Reviews* 25(01):1015-1023

Kim Smith and Ian David Wilson, An Analysis of Definitions of Critical Infrastructures and their Interdependencies (2023) *International Journal of Critical Infrastructures*, (19) 4; 323-339

Michael Clark, Making Sense of Proposed CIRCIA Incident Reporting Rules (Extrahop, 3 December,2024) <https://www.extrahop.com/blog/circia-cyber-incident-reporting-requirements> accessed 6th April, 2025

Michael Clark, Making Sense of Proposed CIRCIA Incident Reporting Rules, ExtraHop (2024) <https://www.extrahop.com/blog/circia-cyber-incident-reporting-requirements> accessed 6th April, 2025

Niels Vandezande, Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor, Computer Law & Security Review (2024) Volume 52, 105890. <https://doi.org/10.1016/j.clsr.2023.105890>accessed 8th April, 2025.

Okunade BAand others, 'Community-Based Mental Health Interventions In Africa: A Review And Its Implications For Us Healthcare Practices', *International Medical Science Research Journal* (2023) 3(3), 68-91.

Patsakis, C., Politou, E., Alepis, E. et al. Cashing out crypto: state of practice in ransom payments. Int. J. Inf. Secur. 23, 699–712 (2024). <https://doi.org/10.1007/s10207-023-00766-z> accessed 7th April, 2025

Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, *Cyber Security and the UK's Critical National Infrastructure* (Chatham House, September 2011), p. 2, <http://www.chathamhouse.org/publications/papers/view/178171.> accessed 5th April, 2025

PF Edemekong, P Annamaraju, M Afzal M, Health Insurance Portability and Accountability Act (HIPAA) Compliance. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025. Available at: <https://www.ncbi.nlm.nih.gov/books/NBK500019/> accessed 7th April, 2025

PrivaLex Advisory, Beyond Borders: What Non-EU Companies Need To Know About The New NIS2 Cybersecurity Directive, Mondaq(2024) <https://www.mondaq.com/nigeria/security/1547478/beyond-borders-what-non-eu-companies-need-to-know-about-the-new-nis2-cybersecurity-directive> accessed 8th April , 2025

PwC, Cyber reporting for critical infrastructure. <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-incident-reporting.html#content-free-1-e9b5> accessed 6th April, 2025

Robert K Knake, A Cyberattack on the US Power Grid: Contingency Planning Memorandum No. 31 (Council on Foreign Relations, April 2017) <https://www.cfr.org/report/cyberattack-us-power-grid> accessed 5th April, 2025

Susanne Lloyd-Jones and Kayleen Manwaring, First Steps to Quantum Resilience: Identifying 'Broken Concepts' In Australia's National Security Laws, *Australian National University Journal of Law and Technology* Vol 5(1) 2024

The White House, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Washington, D.C.: Feb. 12, 2013).

U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience (2013) <https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf > accessed 6th April, 2025

Understanding the Impact of the CISA Critical Infrastructure Cyber Incident Reporting Rules. <https://asimily.com/blog/impact-of-cisa-cyber-incident-reporting-rules/> accessed 7th April, 2025

Understanding the Impact of the CISA Critical Infrastructure Cyber Incident Reporting Rules. <https://asimily.com/blog/impact-of-cisa-cyber-incident-reporting-rules/> accessed 5th April, 2025

Viganò, E., Loi, M., Yaghmaei, E. Cybersecurity of Critical infrastructure. (2020). In: Christen, M., Gordijn, B., Loi, m.(eds.), The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology (21). Springer. <https://doi.org/10.1007/978-3-030-29053-5_8> accessed 4th April, 2025