Analysis of the Cyber Incident Reporting for Critical Infrastructure Act

Danielle Caplinger

Old Dominion University

CYSE 425W

Professor Hiser

Overview

For my policy analysis, I chose to focus on the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). CIRCIA is a federal law establishing reporting requirements when cybersecurity or ransomware incidents occur. When specific criteria are met for such incidents, critical infrastructure organizations are now required to report such an event to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 or 24 hours respectively. Additionally, it allows CISA to take corrective actions if a required entity does not submit the necessary report, including "regulatory enforcement or criminal prosecution" (Clarke, 2021). I chose this policy specifically to analyze because it is a policy-driven response to common cyber incidents and cybercrimes rather than some of its purely technical solution counterparts. It also illustrates a newer shift in US cybersecurity governance from siloed responsibility to a shared endeavor. These characteristics make it an interesting policy from both a cybersecurity and legal perspective.

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) was initially developed in response to a series of high-profile cyber and ransomware attacks against critical infrastructure with the 2021 Colonial Pipeline breach being one of the most significant (Ribeiro, 2025). When the Act was officially signed into law by President Biden in March of 2022, it did so during a time of even more critical infrastructure cyber attacks both in the United States and Ukraine. CIRCIA also coincided with the Biden administration's cybersecurity focus culminating in President Biden's Executive Order on Improving the Nation's Cybersecurity. The Act aims to combat such critical infrastructure attacks by empowering CISA with the time, support, and resources necessary to help respond to such incidents. It also includes an analysis component where CISA can use the gathered information from reports to proactively use trends

to warn potential targets (What is CIRCIA? 2025). In such a rapidly changing environment, this information is extremely valuable and essential to understanding cyber risks, threats, and ways to protect against them.

CIRCIA specifically applies to critical infrastructure "covered entities" which includes public and private businesses in sectors such as communications, defense industrial base, energy, emergency services, healthcare, nuclear, transportation, and water among many others. These entities are then required to report any ransomware attack within 24 hours of a "reasonable belief of incident" and other cyber incidents within 72 hours of that same "reasonable belief" of an incident (CISA, 2022). This "reasonable belief" is established by CISA and organizations are thus required to follow this decision when reporting within the necessary timeframe. These reports must include the systems impacted, information or data impacted, description of the attack, the time of attack, scope of impact, exploited vulnerabilities, attack techniques and tactics, and contact information for the affected organization (What is CIRCIA? 2025). Overall, CIRCIA will allow for an increased awareness of cyber threats by CISA that will allow for increased security across affected industries and the nation as a whole that relies on such services.

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) is not the lone policy aimed at strengthening the nation's cybersecurity posture. CIRCIA supports other policy initiatives including the National Cybersecurity Strategy (NCS) which emphasizes resilience, response, and a collective responsibility between public and private sectors. The enforcement of the reporting aspect also strengthens the NCS's component of cross-sector coordination to incentivize more effective reporting. It also complements similar critical infrastructure initiatives that the Department of Homeland Security and CISA promote across their guidance and work.

As a whole, CIRCIA is a strong policy that reinforces national cybersecurity standards and allows for a proactive response to further critical infrastructure attacks.

Political Implications

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) is a law requiring designated critical infrastructure entities to adhere to strict reporting requirements in the face of cyber incidents and ransomware attacks. By reporting such cyber events to the Cybersecurity and Infrastructure Agency (CISA) and expanding the agency's responsibility , it also reflects national security and regulatory oversight priority shifts in the federal government regarding cybersecurity and the digital world.

The political implications of CIRCIA mainly revolve around the expansion of regulatory authority with the federal government into private sector operations in regards to cybersecurity governance. A major reasoning for such expansion is its role in protecting national security by strengthening defensive measures while centralizing threat intelligence and attack data through swift reporting. With CIRCIA, the federal government reached "forty-five active reporting requirements…distributed between twenty-two agencies across…sectors" (P'ng, 2025). Although there is debate regarding if the scope of the law is far enough to yield significant security advances, it does significantly broaden the regulatory might of the federal government in the data it can collect from private sector cyber incidents. This mandatory reporting shapes how federal oversight of such events can be used to strengthen national security with the hopes of encouraging stronger cybersecurity governance across the critical infrastructure industry (Marotta & Madnick, 2025).

Congress passed CIRCIA with bipartisan support, especially after high-profile critical infrastructure attacks like the Colonial Pipeline ransomware attack. However, there was

significant debate amongst congressmen regarding balancing overregulation with maintaining national security. A chief concern about such overregulation by Senator Peters also emphasized that a strict reporting requirement could actually hinder cybersecurity operations. In particular, in a letter to then CISA Director Jen Easterly, he cited "concerns that the draft rule could require over-reporting of incidents, unnecessarily burdening employees with reporting requirements and pulling them away from important cybersecurity efforts" (Peters, 2024). Both Senator Peters and another developer, Senator Portman, took deliberate steps when drafting the bill to make sure that while reporting was a requirement, it was done so with the intent to help them respond and recover from these incidents. By the time CIRICA was proposed, concerns came from these senators regarding its overbreadth and lack of clarity that could make such purposes convoluted and hard to efficiently carry out. This lack of specificity on a qualifying incident makes the act's potential ramifications to be greater when considering more fleshed-out regulations. Similarly, putting too much emphasis on choices such as timing and scope can also hinder the capacity of cybersecurity professionals, regulators, and the overall ability for all parties involved to fulfill their roles appropriately (Marotta & Madnick, 2023).

At its core, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 is not just a technical reporting requirement but a meaningful turning point for how the US is able to regulate cybersecurity risk in critical infrastructure for national security. By shifting responsibility from that of the private sector to CISA, the federal government is now able to centralize key intelligence data that can be used to analyze, detect, and eventually protect national security assets in private critical infrastructure. Since its initial proposal, CIRCIA had significant changes in many of the specific requirements that potentially change its efficacy and

political implications; however, like many similar laws and the digital industry in general, revisions and language changes in the future are a possibility for improving such concerns.

Ethical Implications

As with any piece of legislation or policy, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) faces tremendous ethical considerations for individuals and private companies. CIRCIA's intention is to create guidelines on when, how, and to whom reports are made regarding cyber incidents or ransomware attacks to the Cybersecurity and Infrastructure Security Agency (CISA). However, in doing so, the line of ethical tension is pulled between advancing collective security while protecting the privacy and autonomy of private industry.

There are many benefits of CIRCIA, but the main ethical considerations for them include its ability to maximize national cyber resilience with a focus on sharing intelligence in such a vital sector. This allows both federal entities and private companies to learn from patterns and analysis done with a much larger dataset that can ultimately reduce the likelihood of future cyberattacks that could adversely affect society as a whole. On the other hand, incident reporting on its own does not have concrete "analyses on its efficacy, implementation, and avenues for improvement…despite its widespread adoption"(Busetti & Scanni, 2024). As such, it is hard to determine if these collective benefits outweigh ethical concerns like compliance burdens, economic impacts, and data privacy. For many companies, stringent incident reporting guidelines have implications beyond their cybersecurity posture but into their financial one including "stakeholder trust, firm performance, cost of capital, innovation, and spillover effects" that put cybersecurity disclosure in direct opposition to market valuation (Amani et al., 2025). This creates an even bigger ethical dilemma for private companies struggling financially who may

feel less inclined to comply with CIRCIA if it could mean negative marketing and eventual profits.

Another key consideration when evaluating the ethical implications of CIRCIA is in its ability to protect individual rights vs limiting them. As previously mentioned, CIRCIA allows for protecting the rights of individuals to public safety and security where they are then able to have reliable, secure critical infrastructure. A further effect of this is that the economy itself can become more stable as financially destabilizing cyber attacks are able to be prevented or mitigated quicker. In contrast to these protected rights, there is concern of potentially limiting rights in the form of corporate privacy, confidentiality, and how reporting can affect personal privacy. Having mandatory reporting requirements takes away much of an organization's control over their own incident response procedures, its internal data, and other cybersecurity operations. As mentioned by Shewale, the increased monitoring and reporting of an organization's systems often has an indirect impact on all entities that may be connected to such a system. This is especially true for high-impact industries like critical infrastructure that will "require extensive monitoring that can infringe on privacy, especially as 93% of modern industrial control systems are connected to external networks, creating additional attack vectors" (Shewale, 2025). This ethical tension is not limited to CIRCIA but is part of a broader debate when it comes to balancing security versus privacy and public safety versus individual intrusion.

As a whole, CIRCIA does not directly infringe on any individual rights but it does have potentially negative consequences for that of private industry operations. As with any piece of legislation, the ethical legitimacy of it will ultimately be based on its proportionality, intent, and effective safeguards. CIRCIA's value must stay focused on protecting public safety and acting as

a centralized information sharing platform that will positively impact national security and citizens' access to critical infrastructure while making sure individual privacy is not neglected.

Social Implications

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) is a piece of legislation that mandates cyber reporting to the Cybersecurity and Infrastructure Security Agency (CISA) for critical infrastructure agencies when certain criteria are met. Guidelines are set forth regarding what constitutes a cyber incident, how to report such activities and with what information, and the timeframe for responsible reporting to avoid fines or other regulatory penalties. CIRCIA itself, however, emerged from a growing societal distrust in the effectiveness of cybersecurity that was shaped by high-profile cyberattacks and American political culture, and continues to carry significant social consequences for privacy and public trust.

As with many pieces of legislation, CIRCIA was enacted in response to a societal need for peace of mind and action in the wake of serious cybersecurity incidents, including the Colonial Pipeline ransomware attack and the SolarWinds attack. According to researchers at the University of Haifa, "the US government's lack of access to cybersecurity information in critical industries wrought havoc on the country's national and economic security," increasing the demands from society for a change to be made (Snider et al., 2021). In that same study, it was seen that the more public exposure to cyber attacks, especially at such great scales, the increased societal pressure for mandatory reforms or legislation.

With such massive new reporting guidelines came a shift in responsibility to private companies in their reporting requirements in the wake of such precarious cyber incidents. As such, hundreds of thousands of organizations across the critical infrastructure industry must now face the consequence of not meeting the necessary regulatory standards. In addition, privacy

concerns were once again being discussed as a line to balance between organizational privacy versus national security. However, studies showed that "as a result of exposure to cyberattacks, respondents were willing to forfeit civil liberties and privacy in exchange for more security" (Snider et al., 2021). There was an even bigger societal shift in the wake of regulations like CIRCIA in the form of how cybersecurity and cyber threats are discussed. Incidents that prompted CIRCIA also shifted related discussions from "the realm of tech professionals and government agencies" to "the forefront of national discourse, making it a key issue" (Wood, 2023).

In years past, there was a societal culture that tended to favor minimal government regulation when it came to cybersecurity and technological innovation. However, the breadth of impact that came from critical infrastructure cyberattacks that led to CIRCIA's enactment fundamentally changed this perspective. It moved a decentralized culture into one of inter-industry cooperation that would benefit society as a whole. Additionally, analyzing weak spots in cybersecurity norms, as Clare in a study by Dwyer et al. noted, brings up if vulnerabilities are equal for all groups or if some vulnerabilities are "more worrying or relatable for some national cultures or groups" (Dwyer et al., 2022). What marks all of these cultures and groups together, though, is their dependence on critical infrastructure, and as such, the need to keep them confidently secure.

As a whole, the Cyber Incident Reporting for Critical Infrastructure Act ultimately reflects the broader societal shift from loosely regulating how highly targeted industries respond to cyber threats into a more centralized model. A new shared responsibility matrix allows for a collective, strengthened cyber posture that protects society as a whole and keeps critical services safe. CIRCIA allows for a new culture of accountability and collaboration across the public and

private sectors in order to truly bring resilience to an industry, and society, that relies so heavily on it.

References

Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity Risks and Incidents Disclosure: A Literature Review. *Accounting Perspectives*. https://doi.org/10.1111/1911-3838.12411

Busetti, S., & Scanni, F. M. (2024). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly, 42*(1), 102000–102000. https://doi.org/10.1016/j.giq.2024.102000

CISA, D. (2022). *Cyber Incident Reporting For Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet*. CISA. https://www.cisa.gov/sites/default/files/2023-01/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf.

Clarke, Y. D. (2021, September 30). *H.R.5440 - 117th Congress (2021-2022): Cyber Incident Reporting for Critical Infrastructure Act of 2021*. Congress. https://www.congress.gov/bill/117th-congress/house-bill/5440.

Dwyer, A. C., Stevens, C., Pijnenburg Muller, L., Dunn Cavelty, M., Coles-Kemp, L., & Thornton, P. (2022). What can a critical cybersecurity do? *International Political Sociology*, 16(3), Article olac013. https://doi.org/10.1093/ips/olac013

Marotta, A., & Madnick, S. (2025). Analyzing and Categorizing Emerging Cybersecurity Regulations. *ACM Computing Surveys*. https://doi.org/10.1145/3757318

Marotta, A., & Madnick, S. (2023). Regulating Cyber Incidents: A Review of Recent Reporting Requirements. *Proceedings of the 20th International Conference on Security and Cryptography*. https://doi.org/10.5220/0012086000003555

Peters Expresses Concerns on CISA Plan to Implement Rule on Cyber Incident Reporting - Committee on Homeland Security & Governmental Affairs. (2024, July 10). Committee

on Homeland Security & Governmental Affairs. https://www.hsgac.senate.gov/media/dems/peters-expresses-concerns-on-cisa-plan-to-implement-rule-on-cyber-incident-reporting/

P'ng, J. (2025, September 24). *Breaking the Silence in Cyberspace: The Case for a Comprehensive Cyber Incident Reporting Mandate*. Georgetown Law ; Journal of National Security law & Policy. https://nationalsecurity.law.georgetown.edu/journal/2025/09/24/breaking-the-silence-in-cyberspace-the-case-for-acomprehensive-cyber-incident-reporting-mandate.

Ribeiro, A. (2025, September 10). *CISA moves to finalize CIRCIA rules by 2026, eyes streamlined cyber reporting*. Industrial Cyber. https://industrialcyber.co/cisa/cisa-moves-to-finalize-circia-rules-by-2026-eyes-streamlined-cyber-reporting/.

Shewale, V.. (2025). The Ethics of Cybersecurity: Balancing Security and Privacy in the Digital Age. *European Journal of Computer Science and Information Technology*, 13(15), 11–20. https://doi.org/10.37745/ejcsit.2013/vol13n151120

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity, 7*(1), tyab019. https://doi.org/10.1093/cybsec/tyab019

What is CIRCIA? How This Law May Affect Your Business (2025, July 1). UpGuard. https://www.upguard.com/blog/circia.

Wood, K. (2023, March 7). Cybersecurity policy responses to the Colonial Pipeline ransomware attack. *Georgetown Environmental Law Review*.

https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/