Breaking the Silence in Cyberspace: The Case for a Comprehensive Cyber Incident Reporting Mandate

Justin P'ng*

ABSTRACT

The enactment of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in 2022 has been described as a game-changer for cyber threat management. Its central and innovative feature is requiring covered entities in designated critical infrastructure sectors to report cyber incidents and ransom payments to the Cybersecurity and Infrastructure Security Agency (CISA), which is broadly responsible for upholding national cybersecurity. But like so many other cyber incident reporting requirements before it, CIRCIA falls short of what is ultimately needed to maximize the cyber threat response capabilities of the U.S. government. This Note argues for a more ambitious and comprehensive cyber incident reporting mandate that broadly applies to entities across the private and public sector with reporting jointly made to the Federal Bureau of Investigation (FBI) and CISA. Reforming CIRCIA and expanding its scope with this broader remit would better optimize the threat intelligence and analysis necessary for enhancing law enforcement responses to cyber incidents and improving cybersecurity insights overall.

INTRODUCTION

Nearly a decade after the U.S. government promulgated one of its first private sector cyber incident reporting requirements in 2013 for federal defense contractors,[1] President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) into law in March 2022.[2] Heralded as a "game-changer" that would "fill critical information gaps" in the cyber threat landscape,[3] CIRCIA broadly requires covered entities in designated critical infrastructure sectors to report cyber incidents and ransom payments to the Cybersecurity and

* LL.M., Georgetown University Law Center, 2024; J.D., Osgoode Hall Law School, 2018. Many thanks to Professor Kimberley Raleigh for her guidance and feedback in developing this piece.

1. Under this rule, defense contractors for the Department of Defense are required to report cyber incidents within 72 hours of their discovery. Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 201 1-D039), 78 Fed. Reg. 69,273 at 69,282 (Nov. 18, 2013); *see* Jessica A. Gunzel, *Tackling the Cyber Threat: The Impact of the DOD's Network Penetration Reporting and Contracting for Cloud Services Rule on DOD Contractor Cybersecurity*, 46 PUB. CONT. L.J. 687, 698-99 (2017) (describing the "Incident Reporting" system established by the Department of Defense requiring defense contractors to report cyber incidents).

2. *See generally* 6 U.S.C. §§ 681-681g.

3. Press Release, Jen Easterly, Statement from CISA Director Easterly on the Passage of Cyber Incident Reporting Legislation (Mar. 11, 2022), https://perma.cc/2BWS-WT5R.

Infrastructure Security Agency (CISA), the agency under the Department of Homeland Security responsible for national cybersecurity and infrastructure security.[4] This new mandate capped off several years of dynamic growth in U.S. cyber incident reporting—as of September 2023, there were forty-five active reporting requirements at the federal level distributed between twenty-two agencies across a range of sectors.[5]

CIRCIA is a welcome development in this broader cyber information sharing landscape, but it is also a missed opportunity by being both overinclusive and underinclusive: overinclusive because covered entities in critical infrastructure sectors will broadly include those already subject to existing reporting rules,[6] and underinclusive because it sidelines federal law enforcement and omits wide swathes of cyber incidents that will continue to be chronically underreported.[7] By no means are these new concerns. The metastasizing patchwork of cyber incident reporting rules is, after all, what inspired the establishment of the intergovernmental Cyber Incident Reporting Council (CIRC) under CIRCIA to unravel these tangled threads and work towards reporting harmonization.[8] The under inclusivity concern, however, remains unaddressed by CIRCIA and preserves a significant blind spot to the collective detriment of U.S. cybersecurity stakeholders.[9] Granted, CIRCIA was never intended to comprehensively fill the gaps in cyber incident reporting across the United States. But as one of the more significant efforts to improve national cybersecurity through mandatory cooperation, it unintentionally highlights the limitations of the incremental sectoral approach and the need for a more ambitious framework.

This note argues for a more comprehensive cyber incident reporting mandate that broadly applies to entities across the private and public sector with reporting jointly made to the FBI and CISA.[10] Despite being tasked with leading the federal

4. 6 U.S.C § 681b(a). As the lead authority in this process, CISA has up to 42 months from Mar. 15, 2022, to engage in rulemaking and enumerate these reporting requirements before they take effect. 6 U.S.C. § 681b(b).

5. U.S. DEP'T OF HOMELAND SECURITY, HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 9 (2023), https://perma.cc/8A3S-JAWA [hereinafter CIRC REPORT].

6. *See* 6 U.S.C. § 681(4) ("The term "covered entity" means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director [of CISA]."); Presidential Policy Directive 21, Critical Infrastructure Security and Resilience 10-11 (Feb. 12, 2013), https://perma.cc/A26L-ZMU6 (identifying 16 critical infrastructure sectors including communications, financial services, and healthcare). CISA's rulemaking under CIRCIA is also precluded from superseding the cyber incident reporting requirements of other federal agencies. 6 U.S.C. § 681b(h).

7. See Federal Bureau of Investigation, 2022 Internet Crime Report at 3 (2022) [hereinafter FBI Report] ("While the number of reported ransomware incidents has decreased, we know not everyone who has experienced a ransomware incident has reported to the IC3.").

8. The Cyber Incident Reporting Council was established by CIRCIA to "coordinate, deconflict, and harmonize Federal incident reporting requirements." 6 U.S.C. § 681f(a). *See* CIRC REPORT, *supra* note 5, at 2.

9. FBI REPORT, *supra* note 7, at 2.

10. This Note adopts the definition of "cyber incidents" set out in Presidential Policy Directive 41, *United States Cyber Incident Coordination* (July 26, 2016), https://perma.cc/C9HY-ZXJX ("An event occurring on or conducted through a computer network that actually or imminently jeopardizes the

government's efforts to respond to cyber threats, these two specialized agencies are inadequately served by a largely voluntary patchwork regime that CIRCIA only partly remedies. Unlike other unlawful conduct, cyber incidents carry unique public safety and national security risks that warrant a broad disclosure obligation to maximize intelligence collection for threat response purposes. An improved version of CIRCIA should build on its mechanics and prioritize the integration of law enforcement reporting, while aligning with the CIRC's mission to harmonize existing reporting requirements and reduce the regulatory complexity and burden for victim entities.

Part I of this note sets out the background of the cyber incident reporting landscape, explores the phenomenon of underreporting, and delves into the shortcomings of the current framework even with the inclusion of CIRCIA. Next, Part II explains why mandatory reporting is warranted for cyber incidents due to their interconnected nature as well as their public safety and national security implications. Similar dynamics present themselves in the context of public health surveillance, a well-established framework whose lessons help inform and justify a comprehensive reporting mandate for cyber incidents. Finally, Part III describes how the key pillars of CIRCIA should be repurposed for a broader mandate that ensures effective cyber incident reporting to the FBI and CISA and robustly protects reporting entities from the unwarranted exploitation of their cooperation.

I. THE CYBER INCIDENT REPORTING LANDSCAPE

The rise of cyber incident reporting requirements over the years has been precipitated by a sustained outbreak of malicious cyber activity with impacts of varying severity. Affected entities have responded in evolving ways, with underreporting to federal law enforcement emerging as a consistent trend and an impediment to the federal government's mobilization to respond to cyber threats. While CIRCIA addresses this to some degree, it ultimately falls short in its scope and singular focus on CISA's role.

A. Background

The ramifications of cyber incidents are legion: based on data submitted to the FBI's Internet Crime Complaint Center (IC3), the potential loss from cybercrime in the United States totaled more than $10.2 billion in 2022.[11] In more grandiose terms, the cumulative loss to cyber incidents, including theft of intellectual property, was famously described by General Keith Alexander as "the greatest transfer of wealth in history."[12] On a global scale, cyber incidents have contributed to

integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.").

11. FBI REPORT, *supra* note 7, at 3. As indicated by the report, this figure is likely an underestimate due to the underreporting of cyber incidents. *Id.*

12. Gen. Keith B. Alexander, Keynote Address at American Enterprise Institute: Cybersecurity and American Power (July 9, 2012), https://perma.cc/3WQX-E2EK. *But see* Peter Maass & Megha

billions of records being misappropriated every year with cascading consequences for the millions of individuals whose sensitive personal data has been compromised.[13] Some of these impacts go beyond monetary harms and trigger life-or-death consequences—cyberattacks on hospitals have reportedly compromised the delivery and quality of healthcare during the post-incident recovery period and contributed to patient deaths.[14]

These accumulating harms have driven the metamorphosis of cyber incident reporting into the current hodgepodge of forty-five active reporting requirements across the federal government covering sectors as varied as financial services, healthcare, transportation, energy, and communications, with several more requirements in development.[15] At the state level, several state utility regulators have promulgated their own cyber incident reporting requirements for critical infrastructure utilities.[16] All fifty states have also enacted breach notification laws requiring that individuals be notified of security breaches involving their personally identifiable information, with some requiring reporting to a designated state agency.[17] The status quo that emerges is a twisted landscape of competing reporting requirements that manages at once to be complex without necessarily being comprehensive.

It is important to acknowledge that cyber incident reporting is only one of several tools that support a cybersecurity strategy, but it is certainly a key trigger and resource for government action.[18] The direct benefits of cyber incident reporting include alerting the government to operational threats or impacts to critical infrastructure and public safety, facilitating the ability of CISA and law enforcement agencies to render assistance, supporting measures to mitigate the harms of data breaches, informing individual remedies for regulatory violations, and equipping law enforcement to prosecute and disrupt cyber threats.[19] In light of these positive contributions, the key question is how to best achieve them through the cyber incident reporting process.

Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012, 12:12 PM), https://perma.cc/C2AS-UZGG (assessing the challenges with accurately estimating losses from cybercrime).

13. Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, THE CONVERSATION (May 13, 2021, 8:33 AM), https://perma.cc/3PZA-2UFP.

14. Maggie Miller, *The mounting death toll of hospital cyberattacks*, POLITICO (Dec. 28, 2022, 4:30 AM), https://perma.cc/R9HL-4QFZ.

15. *See* CIRC REPORT, *supra* note 5, at 9-14 (describing the federal cyber incident reporting requirements and their duplication).

16. *See generally* Hyleah O'Quinn, *Compendium of Cyber Incident Notification Requirements for Critical Infrastructure Utilities by State*, NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS (June 2022), https://perma.cc/63HN-G2X2.

17. *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES, https://perma.cc/AUW4-3CAA.

18. *See* Speech, Lisa O. Monaco, Deputy Attorney General, Keynote Address at International Conference on Cyber Security (ICCS) 2022 (July 19, 2022), https://perma.cc/5BL4-PV5C ("One of the most important steps in disrupting malicious cyber activity is to increase the reporting of cybercrimes by private sector victims or online platforms as soon as those crimes occur.").

19. CIRC REPORT, *supra* note 5, at 4; Mary K. Pratt, *Why reporting an incident only makes the cybersecurity community stronger*, CSO (Apr. 11, 2023), https://perma.cc/9FLG-FREB.

B. Cyber Incidents are Generally Underreported

The consensus among relevant government agencies is that cyber incidents are generally underreported, often due to a perceived risk of public disclosure triggering reputational or other business harms.[20] Victim entities are also averse to shouldering the anticipated procedural burden of supporting the involvement of law enforcement, and for that matter are often not aware of which government agency to engage with or what benefits would be incurred from doing so.[21] Even within law enforcement, there are divisions over which is the appropriate agency to report to depending on the nature of the incident, contributing to a state of affairs that is needlessly complex and presents another reporting hurdle for victim entities.[22] Due to this misalignment of information and incentives, victim entities are more inclined to withhold disclosure of cyber incidents that are not strictly subject to a reporting requirement.[23]

These systemic contributors to underreporting foster the significant gaps in visibility that likely exist when it comes to determining the full scale of cyber incidents.[24] In one rare but illustrative case involving the formerly notorious Hive ransomware group which targeted over 1,500 entities in more than eighty countries,[25] the FBI was able to obtain access to their victim list and discovered that approximately only twenty percent of victims reported to law enforcement.[26] While current reporting does allow for some degree of insight into the extent of cybercrime,[27] it is essentially impossible with current data to precisely estimate the delta between cyber incidents that have occurred and that have been reported, which precludes assessment of the significance of unreported incidents.[28] Based

20. U.S. GOV'T ACCOUNTABILITY OFF., GAO-23-106080, CYBERCRIME: REPORTING MECHANISMS VARY, AND AGENCIES FACE CHALLENGES IN DEVELOPING METRICS 25 (2023), https://perma.cc/L352-7DRC [hereinafter GAO REPORT].

21. *Id. See also* Dan Swinhoe, *Why businesses don't report cybercrimes to law enforcement*, CSO (May 30, 2019), https://perma.cc/6CBB-YX3U.

22. *See Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government*, DEP'T OF HOMELAND SECURITY (Mar. 28, 2023), https://perma.cc/2ATQ-5D85 (explaining that key points of contact in the federal government for cyber incident reporting include the FBI, National Cyber Investigative Joint Task Force, Secret Service, and Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI)).

23. *See, e.g.,* Melanie Evans, *Why Some of the Worst Cyberattacks in Health Care Go Unreported*, WALL STREET JOURNAL (June 18, 2017, 3:30 PM), https://perma.cc/3US9-Y5JS (explaining how hospitals are incentivized to avoid reporting due to the cost of notification obligations that arise from reporting data breaches to HHS).

24. *See* Maass & Rajagopalan, *supra* note 12 ("There is little doubt that a lot of cybercrime, cyberespionage and even acts of cyberwar are occurring, but the exact scale is unclear and the financial costs are difficult to calculate because solid data is hard to get.").

25. Press Release, Department of Justice, U.S. Department of Justice Disrupts Hive Ransomware Variant (Jan. 26, 2023), https://perma.cc/5RK6-G3TL.

26. Chris Way, FBI Director, Director Christopher Wray's Remarks at Press Conference Announcing the Disruption of the Hive Ransomware Group (Jan. 26, 2023), https://perma.cc/U7RD-7PHH.

27. *See generally* FBI REPORT, *supra* note 7.

28. Eileen Decker, *Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score*, 10 J. NAT'L SEC. L. & POL'Y 583, 584 (2020); *see* Maass & Rajagopalan, *supra* note 12.

on what is known about victim reporting behavior, however, a substantial number of cyber incidents is presumably going unreported every year.[29]

C. The Current Cyber Incident Reporting Framework is Inadequate

The inaugural report of the CIRC (the "CIRC Report") highlights many of the inadequacies of the current cyber incident reporting landscape, but mainly from the premise of its existing coverage.[30] In addition to those concerns, there are three major flaws concerning the scope of that coverage and of the government agencies involved. First, the current framework is generally focused on sectors that are already highly regulated and governed by a slew of overlapping incident reporting requirements,[31] or it otherwise imposes a privacy harm threshold that may not be triggered by every cyber incident.[32] CIRCIA potentially expands the overall number of covered entities in critical infrastructure that will be subject to mandatory reporting, but it is ultimately constrained by the four corners of the sixteen designated sectors that can be subject to CISA's rulemaking.[33] It is by no means an oversight to strategically focus information gathering efforts on the sectors of the country that are deemed to be the most vital, but this regulatory precision also forfeits the intelligence and insights that could potentially be obtained from non-covered sectors and unreported incidents.[34]

---

29. *See e.g.,* Decker, *supra* note 28, at 584 (explaining how the FBI believes that self-reported complaints only represent approximately 12% of cybercrime); Zeba Siddiqui, Christopher Bing, & Raphael Satter, *FBI struggled to disrupt dangerous casino hacking gang, cyber responders say*, REUTERS (Nov. 15, 2023, 4:30 AM), https://perma.cc/8U9C-5PZ9 (quoting a former FBI official on underreporting: "What I encountered working on the ransomware stuff is basically nine out of 10 times the company did not want to cooperate"); Gerrit De Vynck, *Many ransomware attacks go unreported. The FBI and Congress want to change that*., WASHINGTON POST (July 27, 2021, 7:32 PM), https://perma.cc/DA44-SP5E (quoting Eric Goldstein, Executive Assistant Director at CISA: "We believe that only about a quarter of ransomware intrusions are actually reported.").

30. *See generally* CIRC REPORT, *supra* note 5.

31. *See id.* at 9-12.

32. The Securities and Exchange Commission's (SEC) formalization of cyber incident reporting requirements for public companies in July 2023 will potentially increase the overall frequency of incident reporting, but by maintaining the existing materiality standard used for other reportable events, it does not necessarily mean there will be an increase to the overall number of reported cyber incidents. *See generally* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 C.F. R. §§ 229.106, 249.308 (2023). For earlier examples of the SEC charging public companies for failing to properly disclose material cyber incidents before the formalization of these reporting rules, see Press Release, Securities and Exchange Commission, SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Aug. 16, 2021), https://perma.cc/JF99-LCBL; Press Release, Securities and Exchange Commission, SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors (Mar. 9, 2023), https://perma.cc/UDH4-3UC9. *But see* Karen Freifeld, *U.S. companies allowed to delay disclosure of data breaches*, REUTERS (Jan. 16, 2014, 2:53 PM), https://perma.cc/4AJ9-3XX6 (quoting Todd Hinnen, a former acting assistant attorney general at the U.S. Justice Department, explaining that after the SEC published guidance in 2011 advising companies to disclose cyber incidents, public companies typically disclosed "generic risk factors" rather than specific incident details).

33. 6 U.S.C. § 681(4); Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* 10-11 (Feb. 12, 2013), https://perma.cc/X7CF-BFLF.

34. *See*, *e.g.*, Evans, *supra* note 23.

The second major flaw is that the current framework otherwise relies on a voluntary approach with inadequate incentives for reporting to non-regulatory agencies, namely the FBI and CISA. This has not necessarily resulted in complete intelligence failure as belied by the IC3's reported receipt of 800,944 complaints concerning cyberattacks and cyber incidents in 2022.[35] However, the FBI estimates that these voluntary complaints only represent a fraction of actual cybercrime events.[36] And while the FBI among others have taken to prominently emphasizing the importance of victim reporting and cooperation in public remarks,[37] skepticism persists among victim entities that engagement will yield meaningful returns.[38]

This touches on a core problem for advocates of voluntary reporting: there may simply be no incentives that would meaningfully increase voluntary reporting without intolerably compromising other public interests. For instance, the key protections offered through CIRCIA, including preservation of privilege and proprietary claims over submitted information,[39] do not immunize the victim entity from regulatory or civil action arising from the cyber incident itself. While this preserves the prospect of accountability being imposed for negligent cybersecurity practices, it trades away a broader regulatory or liability safe harbor that may have served as a stronger incentive for voluntary reporting. And of course, the FBI cannot guarantee involvement in every reported case despite benefitting from the intelligence provided. As a result, the advantages from voluntary reporting are generally tactical and case-specific for which the default amounts to possibly incurring goodwill with regulators, investors, and the public.[40] The 2023 U.S. National Cybersecurity Strategy was notably blunt in recognizing this deficiency by identifying "voluntary approaches to critical infrastructure cybersecurity" as resulting in "inadequate and inconsistent outcomes."[41]

---

35. FBI REPORT, *supra* note 7, at 3.

36. *See* Decker, *supra* note 28, at 584 ("The FBI manages a voluntary self-reporting online database but admits that it captures only about 12% of cybercrime.").

37. *See*, *e.g.*, Monaco, *supra* note 18; Press Release, Department of Justice, Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) (Apr. 6, 2022), https://perma.cc/9VEQ-YUXB.

38. *See* GAO REPORT, *supra* note 20, at 25. This sentiment may be rooted in a history of private sector intelligence sharing not being reciprocated. *See* Jennifer Granick, *The Right Way to Share Information and Improve Cybersecurity*, JUST SEC. (Mar. 26, 2015), https://perma.cc/6W9D-7SDR ("My guess is that the real reason we aren't seeing more robust sharing with DHS is that some sectors of commercial actors don't see that it is worth their while to share with the government. I've been told that the government doesn't share back. . . Any company has to think at least twice about sharing how they are vulnerable with a government that hoards security vulnerabilities and exploits them to conduct massive surveillance.").

39. 6 U.S.C. § 681e(b).

40. This limitation is essentially acknowledged by the U.S. Department of Justice. U.S. DEP'T OF JUSTICE, OFFICE OF THE DEPUTY ATTORNEY GEN., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 88 (2018), https://perma.cc/57ML-WLUV [hereinafter CYBER DIGITAL TASK FORCE REPORT].

41. THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 8 (Mar. 1, 2023), https://perma.cc/X7SB-FSRK.

The third major flaw is that the FBI is not appropriately prioritized under the CIRCIA framework. A previous criticism levelled at CIRCIA during its enactment was the exclusion of dual reporting to the FBI, with CISA ultimately emerging as the sole designated recipient.[42] Although an effort was made to address this by including a requirement for CISA to share reported incident information with designated federal agencies within twenty-four hours,[43] the efficacy of a time-delayed interagency sharing model remains an open question. It is unquestionably important for CISA to receive this information given their mandate as the lead agency for national cybersecurity and critical infrastructure security.[44] Complementing this mission, however, is the designated role for the Department of Justice (DOJ), acting through the FBI and interagency National Cyber Investigative Joint Task Force, as the lead agency for cyber incident "threat response activities."[45] As the operational vehicle for cyber incident response in the national security context, the FBI is uniquely positioned to leverage reporting information for investigation and threat disruption.[46] From a strategic perspective, the absence of a dedicated reporting line to this law enforcement agency is a glaring omission.

II. THE IMPORTANCE OF MANDATORY CYBER INCIDENT REPORTING

The logic in broadly mandating cyber incident reporting flows from two dimensions of these events: (1) their public safety and national security implications, and (2) their interconnected nature. Nominally different incidents can be systemically related by involving shared threat actors, tactics, and vulnerabilities, all of which informs the law enforcement response. As the example of public health surveillance demonstrates, the dynamics of societal threats justifies more intrusive government measures to ensure comprehensive real-time insights are obtained.

A. The Public Safety and National Security Threat of Cyber Incidents

The unique harm of cyber incidents lies in their interconnectedness and symptomatic representation of a broader national security threat. The spectrum of cyber incidents, including cybercrime,[47] cyber espionage, military cyber operations, and

42. *See* Eric Geller and Betsy Woodruff Swan, *DOJ says hack reporting bill 'makes us less safe'*, POLITICO (Mar. 2, 2022, 8:04 PM), https://perma.cc/S56D-ZE34 (quoting Deputy Attorney General Lisa Monaco: "This bill as drafted leaves one of our best tools, the FBI, on the sidelines and makes us less safe at a time when we face unprecedented threats.").

43. 6 U.S.C. § 681a(a)(10) (requires CISA to: "as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report . . . make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies."). The "appropriate Federal agencies" are to be determined by the President. 6 U.S.C. § 681a(b).

44. 6 U.S.C. § 652(c).

45. Presidential Policy Directive 41 (July 26, 2016), https://perma.cc/TE2R-2SAJ.

46. *See generally* Eric Geller, *How DOJ took the malware fight into your computer*, POLITICO (June 13, 2022, 12:25 PM), https://perma.cc/5Q86-2G6Z (describing how the DOJ and FBI have engaged in numerous operations to investigate and disrupt cyber threats and threat actors).

47. *See* GAO REPORT, *supra* note 20, at 1 (explaining that cybercrime "generally includes criminal activities that specifically target a computer or network for damage or infiltration or use computers as tools to conduct criminal activity").

other forms of cyber malfeasance, stems from a vast network of operators ranging from nation-state adversaries to transnational criminal enterprises to rogue actors.[48] As a result of the proliferation and organization of these threat actor networks, a defining characteristic of the cybercrime ecosystem has been their targeting of multiple victims across a range of environments.[49] The mythology of a lone wolf hacker lurking in a basement has gradually been overtaken by an industrialization and specialization that has amplified the impact of cyber incidents to the level of systemic risk in key industries.[50] Moreover, this threat matrix targets a growing victim base of diverse sizes and industries with both individual users and businesses caught in the crossfire.[51]

To take ransomware attacks as an illustrative example, these incidents are perpetrated by a "distributed network of offenders" in which specific aspects of each attack, including the provision of malware, victim infiltration, and extortion process, are managed by different organized entities and affiliates with continually escalating capabilities.[52] While these actors are characteristically organized criminal groups,[53] nation-states have increasingly coopted cybercrime for their own purposes, with North Korea notoriously emerging as a key perpetrator for cybercriminal activities such as ransomware.[54] In many cases, however, even cybercrime activities by private entities are supported to various degrees by foreign states for strategic aims, such as Russia's deliberate cultivation of cybercriminal actors for political warfare by means of disruptive cyber operations.[55] The increasing sophistication of malicious actors in cyberspace and involvement of adversarial nation-states have ultimately transformed cyber incidents into a legitimate threat to national security and public safety.[56]

B. The Value of Aggregate Cyber Incident Reporting

The unique value of cyber incident reporting, as compared to the sharing of computer vulnerabilities and other forms of technical intelligence, lies in its

48. U.S. DEP'T OF JUSTICE, OFFICE OF THE DEPUTY ATTORNEY GEN., COMPREHENSIVE CYBER REVIEW 6 (2022), https://perma.cc/Z68K-2BKG.

49. *See* Press Release, Dep't of Just., Russian National Charged with Ransomware Attacks Against Critical Infrastructure (May 16, 2023), https://perma.cc/SUS8-ADM8 (explaining how a Russian national allegedly deployed ransomware against victim entities in healthcare, law enforcement, government agencies, and other sectors across the U.S. and around the world); *see also* David S. Wall, *Inside a ransomware attack: how dark webs of cybercriminals collaborate to pull them off,* THE CONVERSATION (June 18, 2021, 10:17 AM), https://perma.cc/D3EU-8AW2.

50. Press Release, *supra* note 49; Wall, *supra* note 49.

51. FBI REPORT, *supra* note 7, at 13.

52. Tamas Gaidosch, *The Industrialization of Cybercrime*, FINANCE & DEVELOPMENT (June 2018), https://perma.cc/H8HD-4TAR.

53. *See* DAVID HYLENDER, PHILIPPE LANGLOIS, ALEX PINTO, & SUZANNE WIDUP, VERIZON 2023 DATA BREACH INVESTIGATIONS REPORT 6 (2023), https://perma.cc/2B6K-BPX5.

54. *Guidance on the North Korean Cyber Threat*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (Apr. 15, 2020), https://perma.cc/DUB9-4KAR.

55. Justin Sherman, *Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior*, ATLANTIC COUNCIL 2 (Sept. 19, 2022), https://perma.cc/2RHA-RNJW; *see* THE WHITE HOUSE, *supra* note 41, at 3-4.

56. *See* THE WHITE HOUSE, *supra* note 41, at 3-4.

importance to the federal law enforcement process. The U.S. Attorney General's Cyber-Digital Task Force, an initiative started in 2018 to assess the impact of federal law enforcement in the cyber arena, determined in its inaugural report that cyber incident reporting directly supported the FBI's ability to investigate and neutralize these threats.[57] The logic behind this assessment relies on the capabilities of the FBI, specifically to investigate the incident and connect it to others, make attributions to specific threat actors, better understand their methods and motivations, and ultimately take action by pursuing them through the law enforcement process.[58]

This work is delivered through an array of expert government resources, starting with the FBI's Cyber Division, which specializes in cybercrime and counts over 1,000 dedicated agents and analysts spread across the FBI's field offices with numerous interagency and private sector partnerships.[59] One of those key partnerships is with the DOJ, which has resources and personnel dedicated to prosecuting cybercriminals and national security cyber threats through its National Security Cyber Section and Computer Crimes and Intellectual Property Section.[60] These arrangements and partnerships have netted key successes against threat actors, including 240 arrests, 175 convictions, and 453 threat disruptions in 2021 alone.[61]

Cyber incident reporting has also enabled the FBI to mitigate the impact of cyber threats on victim entities. For instance, timely reporting allowed the FBI to assess whether a zero-day vulnerability was being exploited,[62] identify other affected victims, and coordinate with CISA to proactively render cybersecurity assistance.[63] In another case, incident reporting enabled the FBI to investigate the threat actor's infrastructure and determine which organizations they intended to target next, warn the targeted entities in advance, and protect information from

57. CYBER DIGITAL TASK FORCE REPORT, *supra* note 40, at 88.

58. *Id*. *See also Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats: Hearing Before the H. Comm. On Oversight and Reform*, 117th Cong. 11 (2021) (statement of Bryan A. Vorndran, Assistant Director, Cyber Division, FBI), https://perma.cc/5M7H-ECFN [hereinafter *Vorndran Statement*] ("Each response feeds into our collective efforts to link intrusions to common perpetrators and virtual infrastructure, attribute incidents, and impose risk and consequences on cybercriminals. We need to track and disrupt malicious hackers' activity, infrastructure, and illicit proceeds in as close to real-time as possible.").

59. Mike Elgan, *How the FBI Fights Back Against Worldwide Cyberattacks*, SECURITY INTELLIGENCE (Sept. 19, 2023).

60. U.S. DEP'T JUST., § 9-90.040, JUST. MANUAL (2023) (explaining how the National Security Cyber Section has "primary responsibility for developing the Department's overall strategies for investigating, disrupting, and deterring cyber threats"); *see also* Press Release, Department of Justice, Justice Department Announces New National Security Cyber Section Within the National Security Division (June 20, 2023), https://perma.cc/SHC2-Y3NS.

61. Bryan A. Vorndran, Assistant Director, FBI Cyber Division, Statement Before the House Judiciary Committee (Mar. 29, 2022), https://perma.cc/Z8HU-X299.

62. Computer Security Resource Center, *zero day attack*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://perma.cc/CZU7-5ZBQ (defining a zero day attack as one that "exploits a previously unknown hardware, firmware, or software vulnerability.").

63. Vorndran, *supra* note 61.

exfiltration.[64] Where probable cause and court authorization is required for certain law enforcement powers to investigate and provide assistance, the FBI can also benefit from incident reporting by using the information provided to fulfill these procedural requirements.[65] Based on the interconnected nature of the ecosystem in which cyber incidents take place, information about one incident can shed light on others and lead to collective remedies for multiple victim entities.

C. Applying a Public Health Approach to Cyber Incident Reporting

In many ways, the nature of cyber threats and the capacity for dealing with them reflect the dynamics of how infectious diseases are treated by the U.S. public health system. Information sharing is similarly prized in public health circles due to its importance for two main objectives: advancing population health by tackling the underlying causes of disease; and averting negative health outcomes while upholding individual rights and the environment.[66] A key engine for this system is public health surveillance, which is the "ongoing, systematic collection, analysis, and interpretation of health-related data essential to planning, implementation, and evaluation of public health practice, closely integrated with the timely dissemination of these data to those who need to know."[67] The value of timely, accurate, and comprehensive public health surveillance manifests most strongly in response to an infectious disease—key insights such as symptoms, severity, infection rate, risk factors, and population impacts directly shape policymaking and public health measures as aptly demonstrated by the U.S. government's management of the COVID-19 pandemic.[68]

Underlying these goals is the policy view that a disease capable of impacting the health of others should give rise to a positive reporting duty for the greater well-being of society.[69] These policy rationales have resulted in a federal public health surveillance system in which reporting of certain diseases is mandated for public health practitioners at the state and local level, and from there the Center for Disease Control and Prevention (CDC) receives voluntary state reports of designated nationally notifiable diseases.[70] The fragmentation of disease reporting requirements between and within states guarantees a lack of national consistency akin to the cyber incident reporting landscape,[71] but the historical impact of

64. *Id.*

65. *Id.*

66. Elaine M. Sedenberg & Deirdre K. Mulligan, *Public Health as a Model for Cybersecurity Information Sharing*, 30 BERKELEY TECH. L.J. 1687, 1702 (2015); *see also* Frank L. Smith, III, *Malware and Disease: Lessons from Cyber Intelligence for Public Health Surveillance*, 14(5) HEALTH SECURITY 305, 307 (2016).

67. Richard C. Dicker, *A Brief Review of the Basic Principles of Epidemiology*, *in* FIELD EPIDEMIOLOGY 16, 20-21 (Michael B. Gregg ed. 2008).

68. KAVYA SEKAR & ANGELA NAPILI, CONG. RSCH. SERV., R46588, TRACKING COVID-19: U.S. PUBLIC HEALTH SURVEILLANCE AND DATA 2 (2020).

69. Sedenberg & Mulligan, *supra* note 66, at 1712.

70. *National Notifiable Diseases Surveillance System (NNDSS)*, CENTERS FOR DISEASE CONTROL AND PREVENTION, https://perma.cc/VVH2-9982.

71. *See id.*

previous national epidemics and pandemics has ultimately given rise to a system characterized by regular state reporting of key infectious disease information.[72]

The fundamentals of public health surveillance offer important lessons for cyber incident reporting reforms. The first of these is that information sharing can be a critical mechanism for the protection of "public goods" such as public health, and that cybersecurity as a societal interest warrants this level of treatment.[73] Data forms an integral part of the architecture underpinning the modern economy and government administration,[74] making its protection both a public and national security priority, which in turn magnifies the value of incident reporting.

The second is that more comprehensive information collection can maximize the benefits of government capabilities for the purposes of informing and coordinating a strategic response.[75] Current cyber incident reporting requirements are tailored to reflect the perceived risks implicated by an individual entity, sector, or incident, but this constrictive view fails to adequately account for the interconnected nature of cyber incidents and the informational value that aggregate reporting can offer.[76] The third and closely related lesson is that voluntary reporting is neither reliable nor adequate to address societal problems such as infectious diseases.[77] In the context of cyber incidents, the U.S. public and federal law enforcement apparatus are poorly served by a reporting regime in which pleading for cooperation takes a front-and-center role.[78] The dissatisfactory track record of voluntary cyber incident reporting impels a transition to a mandatory model.[79]

---

72. Joel M. Geiderman & Catherine A. Marco, *Mandatory and Permissive Reporting Laws: Obligations, Challenges, Moral Dilemmas, and Opportunities*, 1 J. AM. COLL. EMERG. PHYSICIANS OPEN. 38, 39-40 (2020).

73. Sedenberg & Mulligan, *supra* note 66, at 1693-95.

74. *See The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://perma.cc/G2JX-RH68; THE WHITE HOUSE, *supra* note 41, at 1.

75. *See* Press Release, Dep't of Health & Hum. Servs., HHS Announces New Laboratory Data Reporting Guidance for COVID-19 Testing (June 4, 2020) (explaining that HHS required more comprehensive laboratory testing results of COVID-19 to formulate a comprehensive response: "Laboratory data serves not only as important information to support decision-making related to the public health emergency, but also as a critical piece to better understanding the impact on socially vulnerable populations. Laboratory testing data, in conjunction with case reports and other data, also provide vital guidance for mitigation and control activities.").

76. *See supra* Parts II (A) and II (B).

77. *See* Sedenberg & Mulligan, *supra* note 66, at 1712 ("In this context, relying on voluntary participation or even offering an "opt-out" would undermine the health of society as a whole, so privacy loss is tolerated, but mitigated."); Press Release, Dep't of Health & Hum. Servs., *supra* note 75 (quoting Alex Azar, U.S. Department of Health and Human Services Secretary, expressing concern that laboratory testing data of COVID-19 infections at that point in time was not adequate to inform public health policymaking: "HHS and the entire Trump Administration are deeply concerned that COVID-19 is having a disproportionate impact on certain demographics, including racial minorities and older Americans. High quality data is at the core of any effective public health response, and standardized, comprehensive reporting of testing information will give our public health experts better data to guide decisions at all levels throughout the crisis.").

78. *See* Sam Sabin, *FBI wants more ransomware victims to report attacks*, AXIOS (Jan. 31, 2023), https://perma.cc/KL8M-CPFF (explaining why the FBI struggles to persuade victims of ransomware attacks to come forward).

79. *See supra* Parts I (B) and I (C).

It is worth highlighting the auxiliary advantages such a regime would potentially deliver. Normalizing cyber incident reporting by mandating and standardizing it across the board would create the conditions for increased victim cooperation by collectively demonstrating to victim entities that their fears of being overwhelmed and swept up by law enforcement investigations are overblown.[80] Formalizing reporting as the default would similarly help reduce the stigma of being the victim of a cyber incident to the extent this remains a lingering concern for organizations.[81] To reciprocate the assistance from victim entities and illustrate the value of aggregate cyber incident information collection, the government could also share this data back with the public in the form of anonymized insights that would help improve the risk assessment and management strategies of organizations, leading to better public cybersecurity overall.[82]

III. KEY CONSIDERATIONS FOR COMPREHENSIVE MANDATORY CYBER INCIDENT REPORTING

To achieve its most useful form, CIRCIA must be transformed into a comprehensive mandate that broadly covers all entities across the private and public sector pursuant to Congress's national security lawmaking powers. Its key features would include joint reporting to the FBI and CISA, streamlined reporting that incorporates the deconfliction recommendations of the CIRC, and robust legal protections for reporting entities to facilitate their cooperation.

A. Legal and Constitutional Considerations

To obtain the foregoing advantages of aggregate cyber incident reporting, a comprehensive cyber incident reporting mandate would need to cover the broadest possible scope of entities irrespective of their size, sector, and interstate presence. In addition to capturing entities in critical infrastructure and other sectors already subject to regulatory reporting obligations, the framework should broadly encompass any private or public entity at the federal, state, and local level that experiences a defined cyber incident.

---

80. *See* Mike Buchwald & Sean Newell, *Encouraging the Private Sector to Report Cyber Incidents to Law Enforcement*, 67 DEP'T OF JUST. J. FED. L. & PRAC. 215, 222-24 (2019) (explaining that the FBI's priority is to conduct cyber incident investigations in a discrete manner that avoids "re-victimizing" the victim); Sabin, *supra* note 78.

81. *See* Peter Apps, *Stigma puts many firms off reporting cyber attacks*, REUTERS (June 6, 2011, 8:45 AM). *Cf.* Geiderman & Catherine A. Marco, *supra* note 72, at 40 (explaining how mandatory reporting of HIV infections and the launch of public awareness campaigns helped reduce the stigma associated with the disease).

82. *See* Rachelle Blair-Frasier, *Experts weigh in on CIRCIA one year later*, SECURITY (Mar. 31, 2023), https://perma.cc/ENM5-52ER (quoting a cybersecurity engineer on the impact of CIRCIA: "By sharing information, even sanitized and redacted information, about security events we can analyze the attacks and improve our defenses overall."); Andrew J. Grotto, Christos Makridis, *Publicly Reported Data Breaches: A Measure of Our Ignorance?*, LAWFARE (July 11, 2018, 9:13 AM), https://perma.cc/73RD-ZSW3 ("Better data would help executives to more effectively manage the cyber risks facing their enterprises, guide investment decisions, enable the insurance industry to develop innovative insurance products, and inform U.S. government efforts to craft proportional and tough responses to cyber incidents perpetrated by foreign adversaries.").

The constitutional basis for this scope of application naturally flows from the "power of Congress to make laws necessary and proper" to national security.[83] This recognition is tethered to Congress's enumerated authority to "provide for the common defense and general welfare of the United States"[84] and is supported by the Necessary and Proper Clause,[85] which broadly empowers Congress to enact legislation that is "useful" or "conducive" to a grant of legislative authority in the sense of being "rationally related to [its] implementation."[86]

A comprehensive cyber incident reporting mandate whose primary objective is enhancing the federal government's strategic threat response is an obvious suitor for this category of congressional authority.[87] The insights from aggregate cyber incident reporting would directly support and improve law enforcement operations and strategic cybersecurity planning aimed at threat actors that pose ongoing national security and public safety threats against the U.S. writ large.[88] In light of this reality and the numerous law enforcement affirmations of the need for greater information collection on cyber incidents to maximize threat response activities,[89] there is a robust and rational policy connection between a comprehensive reporting mandate and the national security lawmaking powers of Congress.[90]

To preempt the legal challenges that may be mounted against this mandate by the business community, state governments, and other stakeholders who may be opposed to a comprehensive federal reporting requirement, it is critical that the mechanism be designed in a way to minimize the viability of such challenges. To

83. *See* United States v. Farhane, 634 F.3d 127, 137 (2d Cir. 2011), quoting Lambert v. Yellowley, 272 U.S. at 596 (1926); *see also* Aptheker v. Sec'y of State, 378 U.S. 500, 509 (1964) ("That Congress under the Constitution has power to safeguard our Nation's security is obvious and unarguable.").

84. U.S. Const. art. I, § 8, cl. 1 ("The Congress shall have power to. . .provide for the common defense and general welfare of the United States.").

85. U.S. Const. art. I, § 8, cl. 18 (authorizes Congress to "make all laws which shall be necessary and proper for carrying into execution the foregoing powers, and all other powers vested by this Constitution in the government of the United States, or in any department or officer thereof.").

86. United States v. Comstock, 560 U.S. 126, 133–34 (2010).

87. *See supra* Part II.

88. *Id.*

89. *See e.g.*, *Vorndran Statement*, *supra* note 61 ("However, we are troubled that all legislation being considered on mandatory cyber incident reporting does not explicitly account for the essential role that federal law enforcement, and notably the Department of Justice and the FBI, plays in receiving cyber incident reporting and actioning the information to assist victims and impose risk and consequences on cybercriminals.").

90. Another potential source of authority would be the Commerce Clause, which authorizes Congress to "regulate commerce. . . among the several states." U.S. Const. art. I, § 8., cl. 3. The Supreme Court has interpreted the Commerce Clause as addressing three main areas, namely the use of "channels of interstate or foreign commerce," the "protection of the instrumentalities of interstate commerce," and intrastate activities that "substantially affect interstate commerce." Perez v. United States, 402 U.S. 146, 150 (1971); United States v. Lopez, 514 U.S. 549, 559 (1995). Under this theory of constitutional authority, cyber incident reporting for threat response purposes is rationally related to facilitating use of the Internet as a channel of interstate and foreign commerce, protecting use of the internet as an instrumentality of interstate commerce, and addressing a problem that substantially affects interstate commerce. However, efforts to mandate activity based on prior inactivity pursuant to the Commerce Clause, as opposed to regulating existing activity, have been previously rejected. *See* Nat'l Fed'n of Indep. Bus. v. Sebelius, 567 U.S. 519, 552 (2012).

reduce legal disputes based on state jurisdiction, the requirement should set a minimum reporting standard that is broadly applicable but does not otherwise preempt comparable state laws on cybersecurity incident reporting. As discussed further below, the mandate should avoid claims of self-incrimination by including protections for reporting entities to ensure reported information is not subsequently used for regulatory enforcement, prosecution, or civil discovery unless legitimately obtained elsewhere.

Another challenge may be based on First Amendment grounds on the theory that the degree of reporting required is unconstitutionally compelled disclosure whose means are not appropriately tailored to a sufficiently important objective.[91] While cyber incident reporting is likely not traditional commercial speech that would attract a less stringent standard of constitutional scrutiny for compelled speech,[92] the ultimate standard is not necessarily determinative given the overall justification for the mandate. For the reasons set out in this note, the government interest engaged is a national security and public safety priority whose importance is more than sufficient.[93] Based on the history and impact of systemic underreporting of cyber incidents,[94] compelling the disclosure of incident information on an aggregate basis represents a narrowly tailored means for achieving this objective.

It is worth noting that such a mandate would also not be the first legal instrument to impose affirmative obligations to assist law enforcement for this type of policy rationale. Financial institutions subject to the Bank Secrecy Act are required to report known or suspected criminal transactions to federal law enforcement to help counter the national security and public safety risks of money laundering and terrorist financing activities.[95] In a similar vein, the Communications Assistance for Law Enforcement Act effectively mandates law enforcement assistance for national security and public safety reasons by requiring telecommunications providers to ensure their equipment, facilities, and services are designed to enable authorized electronic surveillance by law enforcement authorities.[96] Whereas a comprehensive cyber incident reporting mandate would entail a much broader multisector scope of application, its purpose and obligations would not be legislatively unprecedented.

---

91. *See* VALERIE C. BRANNON & VICTORIA L. KILLION, CONG. RSCH. SERV., IF12388, FIRST AMENDMENT LIMITATIONS ON DISCLOSURE REQUIREMENTS 1 (2023).

92. *Id.*

93. *See supra* Part II.

94. *See supra* Part I (B).

95. 12 C.F.R. § 353.3 (2020)*; see* U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-105242, BANK SECRECY ACT: ACTION NEEDED TO IMPROVE DOJ STATISTICS ON USE OF REPORTS ON SUSPICIOUS FINANCIAL TRANSACTIONS 1 (2022), https://perma.cc/3BKX-GWVM ("Illicit finance activity, such as fundraising by terrorist groups and money laundering by drug-trafficking organizations, can pose threats to national security, the well-being of citizens, and the integrity of the U.S. financial system.").

96. 47 U.S.C. § 1002(a)*; see CALEA*, NATIONAL DOMESTIC COMMUNICATIONS ASSISTANCE CENTER (last visited Nov. 22, 2023) ("In October 1994, Congress took action to protect public safety and ensure national security by enacting the Communications Assistance for Law Enforcement Act of 1994 (CALEA)... The objective of CALEA implementation is to preserve law enforcement's ability to conduct lawfully authorized electronic surveillance while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness.").

B. Reporting Requirements

The specialized roles of the FBI and CISA warrant prioritizing informational access for both agencies in the form of dual reporting. Of course, there is also operational value in ensuring that cyber incident information is shared with other federal government actors, namely the Department of Defense (DoD) as well as the broader intelligence community. While the DoD does not enjoy the same lead agency status as the FBI for threat response activities, it also plays a key role in "defense forward" operations through actors such as U.S. Cyber Command to proactively disrupt cyber threat actors and generate threat intelligence.[97] These complementary roles warrant relatively prompt access to the information gathered from cyber incident reporting to help develop a strategy for such activities. However, prioritization of the FBI and CISA in the information flow for cyber incident reporting is merited given the FBI's "first responder" mandate, and the recognized legal authority of CISA to store and distribute such information within the federal government.[98] Based on these respective authorities, a more straightforward approach would be to direct reporting to the two lead agencies in the threat response process and leverage information sharing mechanisms to diffuse intelligence where it is also needed.

The design of the reporting process is similarly essential. The content reporting requirements should broadly reflect the input of the FBI and CISA and be actionable for their respective mandates and capabilities, which may include details of the incident, the provision of a ransom payment, and the evidence and analysis arising from any forensic investigation.[99] In keeping with the intent of CIRCIA, reporting entities in critical infrastructure sectors should be required to designate their sectoral status to ensure prioritization in the threat response process. For operational efficiency, the reporting mandate should also procedurally align with the reporting harmonization recommendations of the CIRC to the extent practicable. These include the substantial adoption of a shared model definition for reportable cyber incidents,[100] a reporting timeline of up to seventy-two hours with shorter periods prescribed for incidents with particularly significant impact,[101] and the use of a

97. *See* THE WHITE HOUSE, *supra* note 41, at 14-15; DEPARTMENT OF DEFENSE, 2023 CYBER STRATEGY SUMMARY 1-2, 6-7 (2023).

98. ANDREW NOLAN, CONG. RSCH. SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES AND SOLUTIONS LEGISLATIVE ATTORNEY 6-10 (2015).

99. *See* Daniel Schwarcz, Josephine Wolff & Daniel W. Woods, *How Privilege Undermines Cybersecurity*, 36 HARV. J. L. & TECH. 421, 453-54 (2022) (describing the benefits of post-incident forensic investigation reports).

100. CIRC REPORT, *supra* note 5, at 26 ("A reportable cyber incident is a cyber incident that leads to, or, if still under the covered entity's investigation, could reasonably lead to any of the following: (1) a substantial loss of confidentiality, integrity, or availability of a covered information system, network, or operational technology; (2) a disruption or significant adverse impact on the covered entity's ability to engage in business operations or deliver goods, or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death; (3) disclosure or unauthorized access directly or indirectly to non-public personal information of a significant number of individuals; or (4) potential operational disruption to other critical infrastructure systems or assets.").

101. *Id.* at 27.

model reporting form with a process for reporting updates and interagency sharing to standardize the reporting process.[102]

That third recommendation is particularly critical for systematizing threat information collection and analysis, untangling the web of cyber incident reporting requirements, and ensuring that a new reporting mandate will not be unnecessarily duplicative and burdensome. While CIRCIA exempts reporting to CISA where a covered entity has reported to a regulatory agency that has an information sharing agreement in place with CISA,[103] this opt-out should not be carried over to the FBI under a broader reporting mandate given the time-sensitive nature of incident response needs and the uncertainties that may arise from relying on the expediency of interagency information sharing. Unless and until an effective centralized reporting mechanism can be instituted,[104] there should be a direct line of reporting to the FBI and CISA, with other government actors such as the DoD and intelligence community agencies relying on interagency information sharing. Regulators would accordingly maintain visibility and oversight in this redesigned information flow, subject to prioritization of those two agencies and the threat response process.

C. Protections for Reporting Entities

The expansive breadth of this proposed reporting mandate engages legitimate concerns regarding the legal implications of affected entities disclosing potentially sensitive information about cyber incidents. Fortunately, the key protections stipulated under CIRCIA already provide a robust framework for managing these risks and should be adopted with targeted improvements. Chief among these protections is a safe harbor provision for both regulatory and civil litigation against a reporting entity based on their compliant submission of a mandatory report,[105] which appropriately carves out the reporting process without precluding liability for other conduct related to the incident itself. In related fashion, CIRCIA also precludes regulatory enforcement from being based on information solely submitted through its reporting process.[106]

Protecting the reported information is of course integral to upholding a safe harbor, which implicates two dimensions of protection: technical and procedural. Robust technical security safeguards are vital for shielding a vast trove of incident

102. *Id*. at 30-31.

103. 6 U.S.C. § 681b(a)(5).

104. *See generally* CIRC REPORT, *supra* note 5, at 31 ("The Federal Government should assess how reporting entities may best provide cyber incident information to the Federal Government, how relevant agencies should receive the information, and how such information can be shared across the Federal Government with those agencies that need it. Such a study could assess the feasibility of establishing a single portal or network of interconnected portals (an information technology system or multiple interconnected systems) to allow the entity to submit key information to appropriate agencies in an efficient manner.").

105. 6 U.S.C. § 681e(c). The exception to this safe harbor provision is noncompliance with cyber incident reporting requirements, which may result in federal government action against the reporting entity. CIRC REPORT, *supra* note 5, at 31.

106. 6 U.S.C. §§ 681e(a)(5).

information that could easily be misused in the wrong hands, a point addressed in CIRCIA by requiring the use of federal information system standards.[107] Procedural safeguards must also be implemented to ensure that information disclosed in confidence to the FBI and CISA is not overshared with other agencies except to the extent regulatorily required. This requires a delicate balancing act between the three goals of facilitating the reporting of useful and detailed cyber incident information, assuring reporting entities that their submissions will not be taken advantage of by unrelated regulatory agencies, and streamlining the reporting process by enabling interagency information sharing.

Whereas CIRCIA threads this needle by restricting CISA's information sharing to specific purposes, including defined exigent circumstances and for identifying cyber threats and vulnerabilities,[108] a voluntary sharing mechanism should be incorporated that would enable reporting entities to opt in to providing reported information to other agencies. To achieve this under a centralized reporting process, the intake process should be designed with input from the FBI and CISA to reflect a more modular approach in which both agencies receive the fullest version of the report, but agencies downstream may receive different or more limited information depending on their regulatory priorities and requirements. The reporting mandate would then largely be able to preserve the firewalls instituted by CIRCIA between CISA and regulatory agencies.

It goes without saying that a comprehensive reporting mandate must contain robust safeguards for claims of legal privilege and confidentiality to ensure reporting entities are not being compelled to engage in disclosures that would undermine legal protections or expose them to legal liability.[109] Formalizing this would be relatively straightforward by adopting the applicable CIRCIA provisions to deem reported information as confidential and proprietary when so designated by the reporting entity, categorically exempting them from freedom of information laws nationwide, and declaring that reporting does not waive any applicable trade secret protection or legal privilege.[110] To further crystallize the safeguard for legal privilege, this provision should explicitly include protection for applicable evidentiary and common law privileges.[111] Likewise, mandated

107. 6 U.S.C. § 681e(a)(4) ("The Agency shall ensure that reports submitted to the Agency pursuant to section 2242, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.").

108. 6 U.S.C. § 681e(a)(1).

109. *See generally* HOMELAND SECURITY PROJECT, CYBER SECURITY TASK FORCE: PUBLIC-PRIVATE INFORMATION SHARING, 9 (2012), https://perma.cc/WWL9-F8F9 ("Corporations often are reluctant to share cyber vulnerability information with the government because they consider their system vulnerabilities to be sensitive information and do not want proprietary documents and information to be disclosed to the public and competitors. Stakeholders worry that such disclosures could result in reputational harm, competitive disadvantage, lost profits and shareholder derivative actions or other lawsuits.").

110. *See* 6 U.S.C. § 681e(b).

111. *See* Steve Stransky, *The 2022 Cyber Incident Reporting Law: Key Issues to Watch*, LAWFARE (Mar. 25, 2022), https://perma.cc/YR8T-2SCJ ("As part of its implementing regulations, CISA may

reports and information solely used to prepare such reports should be broadly exempted from the evidentiary process in any proceeding to definitively close off any airgaps in the information supply chain.[112] While reporting entities themselves should be responsible for, and are in the best position for, removing personally identifiable information from their submissions except as necessary to facilitate follow-up contact, other sensitive information should benefit from legislative protections.

D. A Moderate Approach to Enforcement

As critical as the objectives of mandatory reporting are, it is also important to take a moderate approach to enforcement that recognizes the challenges faced by reporting entities based on the impact of the incident and their respective capabilities. A severe cyber incident for any organization can lead to reduced capacity across all lines of business and hamper their functionality for compliance matters such as reporting.[113] Small-to-medium-sized businesses are likely to be especially incumbered by the need to engage in a new compliance process on top of prioritizing incident response and recovery.[114] It would be a dangerous policy choice to allow a tool for assisting cyberattack victims to be weaponized against them. As CISA Director Jen Easterly famously said when describing her agency's approach to assisting victim entities, it was to help them and not to "stab the wounded."[115]

Weighing these interests against the imperative of comprehensive information collection to improve collective remedies for a large-scale problem, the focus should be on promoting compliance generally and targeted regulatory enforcement against larger organizations and designated critical infrastructure entities. The ability for CISA to subpoena noncompliant entities and refer violations to the Attorney General to bring civil actions would add indispensable teeth to this mandate,[116] but consideration for the size and sector of a noncompliant entity should be explicitly formalized in regulation or operational guidelines to govern enforcement action. From a public engagement perspective, this reporting mandate should be seen as a cooperative partnership rather than another regulatory burden.

IV. CONCLUSION

The cyber landscape is increasingly pockmarked with the artillery of cyber incidents and corresponding regulatory reporting requirements. Organizations

consider adopting guidance issued in other information sharing contexts and clarify that this protection applies in all circumstances where federal or state legal and evidentiary privileges may be invoked, and is interpreted to include protections recognized under common law, such as the attorney-client and work product privileges.").

112. *See* 6 U.S.C. § 681e(c).

113. *See* Mike Szczesny, *Understanding the impact of cyberattacks on small businesses*, SECURITY (Aug. 14, 2023), https://perma.cc/Q543-GJNJ.

114. *See id.*

115. Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency, Remarks at Center for Strategic & International Studies: Next Steps in Critical Infrastructure Protection: Challenges for CISA and Congress (Oct. 29, 2021), https://perma.cc/G25U-4FDT.

116. *See* 6 U.S.C. § 681d.

beset by a diverse ecosystem of cyber threat actors are inadequately served by a reporting regime that largely serves regulatory interests and by the collective silence of other victims caught in the crossfire. As a necessary first step, this collective action problem can be substantially remedied through a comprehensive cyber incident reporting mandate that expands the framework introduced by CIRCIA across all sectors and integrates the threat response role of federal law enforcement. By bringing more cyber incidents into the light, those government capabilities can be more fully exercised against the raging threats in cyberspace.