Via electronic submission

July 3, 2024

Cybersecurity and Infrastructure Security Agency (CISA)
U.S. Department of Homeland Security
245 Murray Lane, SW
Washington, DC 20528-0380

RE: Submission of Public Comment on the Proposed Rule for the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"), Docket No. CISA-2022-0010, RIN 1670-AA04

Dear Sir or Madam:

The Independent Community Bankers of America ("ICBA")[1] appreciates the opportunity to respond to the Cybersecurity and Infrastructure Security Agency's ("CISA's") notice of proposed rulemaking ("Proposed Rule") to implement the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA").[2] ICBA has a long history of supporting cybersecurity initiatives, including CIRCIA. The nation's community banks understand that sharing advanced threat and attack data across federal agencies and financial sector participants is essential to reducing cyber threats and protecting critical infrastructure. Although the Proposed Rule is a good first step to implement CIRCIA, additional refinement is needed in order to increase efficiency for those reporting cyber incidents, including community banks.

Harmonizing Reporting Requirements

The financial services industry has long been subject to cybersecurity regulations and understands the importance of protecting critical infrastructure. While we support CIRCIA and generally endorse this

[1] *The Independent Community Bankers of America® has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams. For more information, visit ICBA's website at icba.org.*
[2] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644, 23644 (proposed Apr. 4, 2024) (to be codified at 6 C.F.R. pt. 226).

proposed rule, we have concerns that it introduces unnecessary complexities and burdens on community banks, which are already legally obligated to report incident information to numerous governmental agencies, departments, and private organizations following an incident. The proliferation of these reporting requirements underscores the heightened awareness of securing data and critical infrastructure, thereby keeping key stakeholders informed. However, our industry's aspiration is to achieve harmonization of requirements that facilitate efficient reporting of cyber incidents, streamlining processes, and enabling financial institutions to rely as much as possible on existing practices.

Community banks currently report incident information to their primary regulator, to the Financial Crimes Enforcement Network ("FinCEN") through Suspicious Activity Report ("SAR") filings, and share information with the Financial Services Information Sharing and Analysis Center ("FS-ISAC"). Additionally, they report incidents to their financial regulatory agencies where customer data is accessed or systems holding such data are impacted.

While CIRCIA aims to standardize incident reporting requirements across sectors, more effort is needed to leverage the extensive experience and mature regulations of the financial services sector. Requiring community banks to submit duplicative reports to multiple agencies imposes significant burdens. Ideally, reporting should consolidate either through CISA or the appropriate Sector Risk Management Agency ("SRMA"), which can then disseminate reports to other relevant agencies and regulators.

CISA has multiple avenues to achieve harmonization. One approach could involve aligning with current banking sector practices by collaborating with prudential bank regulators to eliminate inconsistencies and redundancies. Another approach could be to exempt community banks from CIRCIA by excluding them from the definition of covered entities. This approach could be implemented with minimal additional risk, leveraging the robust reporting requirements already in place for community banks.

Definition of Covered Entity

The applicability of CIRCIA requirements hinges on defining a "covered entity" and the corresponding "applicability" requirement in §262.2.[3] These definitions exclude large segments of business entities based on size as a proxy for criticality, despite some of these excluded entities being quite sizable by community bank standards and providing critical services, such as hospital care. Similar reasoning for exempting these entities should apply to community banks because they pose no greater risk than other excluded entities.

[3] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644, 23645.

Applying the same regulations to all banks under CIRCIA is incorrect and imposes an undue burden on community banks with minimal overall benefit. CISA has shown recognition of the appropriateness of differentiating industries based on size, as evidenced by exemptions or carve-outs for certain entities.

CIRCIA provides CISA with the flexibility to adjust regulations based on specific criteria outlined in section 681b(c)(1).[4] Section 681b(c)(1)'s criteria requires CISA to assess the consequences a disruption to an entity could have on national security, economic security, or public health and safety; the likelihood that an entity may be targeted by a malicious cyber actor; and the extent to which damage, disruption, or unauthorized access to an entity would likely enable the disruption of the reliable operation of critical infrastructure.[5]

The Proposed Rule defines a covered entity by including entities detailed in the applicability section found in §262.2(b), encompassing all banks regardless of size. While grouping all banks together may seem convenient, smaller banks generally do not pose the same risks to critical infrastructure as larger banks. Additionally, all banks are already subject to comprehensive cybersecurity requirements mandated by their respective prudential regulators. These requirements are sufficiently uniform, and exempting community banks would not introduce additional risk.

The small business exemption is based on the small business size standard set forth in the Small Business Size Regulations, which sets size standards of up to $47 million or up to 1,500 employees.[6] The proposed sector-based criteria for healthcare and public health, defined by §226.2(11)(i), excludes hospitals with fewer than 100 beds from the essential healthcare requirement in public health-related services, including hospitals with 100 or more beds, critical access hospitals, and manufacturers of certain classes of drugs or medical devices.[7]

Nearly all ICBA members employ less than 1,500 employees. In fact, the majority of our members employ fewer than 100 employees, with many employing significantly fewer. ICBA encouraged CISA in a letter[8] dated November 14, 2022, responding to the CIRCIA Request for Information ("RFI") that CISA exclude from the definition of a covered entity a bank as one with $50 billion or more in assets.

---

[4] 6 U.S.C. § 681b(c)(1).
[5] *Id.*
[6] 13 C.F.R. § 121.201 (1996).
[7] § 226.2(11)(i) specifically includes an entity that owns or operates a hospital, as defined by 42 U.S.C. 1395x(e), with 100 or more beds, or a critical access hospital, as defined by 42 U.S.C. 1395x(mm)(1).
[8] Independent Community Bankers of America, "RE: Docket ID CISA-2022-0010 – Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022" (November 14, 2022), https://www.icba.org/docs/default-source/icba/advocacy-documents/letters-to-regulators/comments-on-cyber-incident-reporting.pdf?sfvrsn=62751417_4.

In adopting the requirements for an entity operating more than 100 beds to be covered, CISA states "it is worthwhile to focus on larger hospitals for required reporting, as they are more likely than smaller hospitals to experience substantial impacts if they fall victim to a covered cyber incident…." And that the "same rationale behind CISA's decision to propose an overall size-based criterion based on the SBA small business size standards in the Applicability section (e.g., larger hospitals are more likely hospitals are more likely to have in-house or access to cyber expertise; larger hospitals are likely to be better equipped to simultaneously respond to and report a cyber incident)."[9] Consequently, healthcare size-based logic holds true with community banks health. The important difference between banks and entities with an exemption from the CIRCIA requirements is that banks are already subject to extensive cybersecurity rules and are supervised by federal and state regulators for compliance.

The cyber security and incident notification rules already in place are extensive and nicely layered on a centuries long culture of protecting information. Most relevant to cyber security is the Gramm-Leach-Bliley Act ("GLBA")[10] which has security standards that require banks to implement certain practices to safeguard the information from unauthorized access, use, and disclosure. The Office of the Comptroller of the Currency ("OCC"), the U.S. Department of the Treasury ("Treasury"), the Board of Governors of the Federal Reserve System ("Board"), and the Federal Deposit Insurance Corporation ("FDIC") issued final rule in November 2021 mandating that banking organizations notify their primary Federal regulator of any "computer-security incident" that qualifies as a "notification incident" as soon as possible, but no later than 36 hours after the organization determines that such an incident has occurred.[11] Banking regulators draft rules to implement legal provisions and possess the authority to conduct examinations and oversee institutions within their jurisdiction to enforce compliance with these rules.

As mentioned earlier, cybersecurity threats pose operational, reputational, and potentially systemic risks. These risks are collectively monitored by banking regulators through the Federal Financial Institutions Examination Council ("FFIEC"). Additionally, the Financial Stability Oversight Council ("FSOC") monitors systemic risks to the financial system, including cyber threats. The FFIEC coordinates bank examinations to uphold safety and soundness, compliance, and information technology standards. Therefore, with the current notification regulations and supervisory processes in place, both bank customers and the critical banking infrastructure are well protected. Exempting smaller banks from the definition of covered entities would not relieve them from existing requirements; instead, it would streamline their obligations with minimal impact on the country's critical infrastructure as a whole.

---

[9] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. at 23694.
[10] 15 U.S.C. § 6801.
[11] 12 C.F.R. § 304.23 (2021).

Sector Risk Management Agency Reporting

Although ICBA favors reporting to community banks' prudential regulators, we understand the importance of sharing information with the financial sector's SRMA, the Treasury Department. To fulfill its role effectively, the SRMA needs access to information in the most frictionless manner possible. The financial sector frequently engages with the Treasury on issues such as physical threats, third-party risks, resilience, and cyber threats. The Treasury also plays a key role in developing and testing sector incident response plans.

Given the Treasury's critical involvement in the initial stages of working with firms, regulators, and other government agencies to assess incident impacts and potential downstream effects, it is essential that CISA provides the Treasury with timely access to information regarding the financial sector. Establishing a well-defined process for this information sharing will further CIRCIA's key objective of limiting downstream harm, as the Treasury can leverage its established relationships with financial firms to disseminate information more quickly.

Protect Reported Information

Under CIRCIA, covered entities will confidentially provide CISA with highly sensitive incident information, including details on ongoing incidents. This information will be of significant interest to cyber adversaries and, if not properly protected, could be used to inflict further damage on critical infrastructure.

CIRCIA mandates that CISA protect reported information "at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199." As CISA develops the final rule, it should also leverage the Financial Services Sector Coordinating Council's joint work with the regulatory agencies of the Financial and Banking Information Infrastructure Committee to enhance data security protections for sensitive information submitted to Federal agencies. In particular, CISA should designate all agency systems containing CIRCIA reports as High Value Assets, in accordance with Office of Management and Budget guidance. This designation provides a consistent way to protect this information commensurate with the risk environment.

Substantial Cyber Incident

CIRCIA requires CISA to define a "covered cyber incident" as one that is "substantial."[12] The Proposed Rule defines a covered cyber incident as a "substantial cyber incident experienced by a covered entity."[13] This means that covered entities only need to determine if a cyber incident is substantial to know if it must be reported. A substantial cyber incident is defined as one that leads to any of the following results:

- Substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
- Serious impact on the safety and resilience of a covered entity's operational systems and processes;
- Disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; and
- Unauthorized access to a covered entity's information system or network, or any nonpublic information contained within, facilitated through or caused by a compromise of a cloud service provider, other third-party data hosting provider, or supply chain compromise.[14]

CISA provides guidance on when an incident might meet any of these impact thresholds. However, we find the criterion "disruption of a covered entity's ability to engage in business or industrial operations" to be vague and potentially overly broad. This criterion could encompass a wide range of issues that may not typically be critical and could lead to incidents being reported that do not meet the intended threshold.

In the final rule, we encourage CISA to reconsider this requirement and establish clearer parameters. This would ensure that covered entities have a better understanding of when incidents should be reported, reducing the risk of overreporting incidents that do not meet the necessary criteria.

Conclusion

CISA should aim to simplify cyber incident reporting to ensure that community banks are not burdened by duplicative requirements. It should leverage the existing cybersecurity regulations and reporting processes already in place for these banks. Given their small size, limited share of financial sector assets, and very low probability of causing national disruption, community banks should not be considered covered entities.

---

[12] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. at 23660.
[13] *Id.* at 23660.
[14] *Id.* at 23661.

Community banks invest significantly in cybersecurity and are supervised by bank regulators. CISA should utilize the current reporting processes for community banks instead of requiring them to follow additional, redundant procedures. ICBA supports CISA and generally is supportive of enhancing cybersecurity and operational resiliency across all sectors of the country, thus affirming ICBA's position that the requirements are right sized for the risks at hand. As provided more fully above, additional work is needed to ensure that the requirements in the proposed rule are efficient and effective for community banks.

Thank you for considering these recommendations. Please do not hesitate to contact me at Lance.Noggle@icba.org or (202)821-4311.

Best regards,

/s/

Lance Noggle
Senior Vice President, Senior Regulatory Counsel