November 14, 2022

Via Electronic Submission

Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

RE: Docket ID CISA-2022-0010 – Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

Dear Sir or Madam:

On behalf of the Independent Community Bankers of America ("ICBA"),[1] we appreciate the opportunity to provide comments to the Cybersecurity and Infrastructure Security Agency ("CISA") which is requesting information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 to collect diverse perspectives on approaches to incident reporting, requirements, and associated definitions.

Recommendations

ICBA frequently engages its members to explore how to best secure the Financial Services Sector and to keep customer information and data safe. This includes the topics of incident reporting and harmonization of overlapping regulations. ICBA encourages CISA, now and in the

[1] *The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services.*

With nearly 50,000 locations nationwide, community banks constitute 99 percent of all banks, employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding more than $5.8 trillion in assets, over $4.9 trillion in deposits, and more than $3.5 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org

WASHINGTON, DC
1615 L Street NW
Suite 900
Washington, DC 20036

SAUK CENTRE, MN
518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

866-843-4222
www.icba.org

future, to work with the National Institute of Standards and Technology ("NIST") when establishing industry acceptable definitions and work with federal banking regulators and the Financial Crimes Enforcement Network ("FinCEN") to harmonize incident notification regulations and reporting requirements. ICBA also suggests that CISA produce resource materials and share information with critical information operators.

Definitions in General

ICBA suggests that CISA utilize definitions that are already in place and considered industry and governmental standards, such as those produced by NIST. NIST's portfolio of services for measurements, standards, and legal metrology provides solutions that ensure traceability, enable quality assurance, and harmonize documentary standards and regulatory practices. Where a definition is missing or in need of clarification in the Cyber Incident Reporting for Critical Infrastructure Act of 2022, ICBA suggests that CISA first and foremost work with NIST to co-develop private and public sector acceptable definitions rather than engaging in a separate body of work to clarify definitions as the current RFI is seeking to do.

Covered Entity

Systemic risk is the possibility that an event at the company level could trigger severe instability or collapse of an entire industry or economy.[2] When considering what size of business should be considered in the definition of a covered entity, ICBA suggests that CISA considers only systemically important critical infrastructure operators such as Large financial institutions. To help define what that is, the United States has three primary Federal banking regulators, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the "Agencies"). In compliance with the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018[3] the Agencies sets the threshold for a large financial institution as an institution with $50 billion or more in assets.

The definition of a covered entity, for the Financial Services Sector, should only include banks with $50 billion or more in assets. This would align with existing definitions of systemically important financial institutions. What's more, all banks have existing cyber incident reporting requirements to their primary federal banking regulator.[4] ICBA suggests that banks with $50 billion or more in assets should report cyber incidents to their banking regulator and CISA, while banks under $50 billion in assets should continue to report cyber incidents only to the Agencies. Additionally, the threshold for banks to notify their federal banking regulator is 36 hours. This

[2] Systemic Risk Definition (investopedia.com). Accessed October 4, 2022.
[3] Economic Growth, Regulatory Relief, and Consumer Protection Act | Congress.gov | Library of Congress
[4] Federal Register: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers. Accessed October 4, 2022.

would enable CISA to retrieve incident information from the federal banking regulator within CISA's Cyber Incident notification window of 72 hours. This would also reduce the reporting burden on community banks during a cyber incident.

Harmonization

In general, ICBA suggests that CISA harmonize CISA's incident reporting regulations with existing regulatory guidance provided by the Agencies. Specifically, ICBA suggests that CISA standardize its definitions of a "substantial cyber incident" and a "covered incident" with the Agencies' definitions of a "computer-security incident" and a "notification incident."

The Agencies define a "'computer-security incident'' as an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.

The Agencies define a ''notification incident'' as a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's—

- Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

- Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or

- Operations, including associated services, functions, and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

Cyber Incident and Ransomware Report Submission

In addition to the regulatory requirement for banks to notify the Agencies of incidents, including cyber breaches and ransomware attacks, banks are subject to the reporting requirements of the Bank Secrecy Act (BSA) and its implementing regulations. Financial institutions are required to file a Suspicious Activity Report ("SAR") with FinCEN when they detect a known or suspected criminal violation of federal law which includes cyber breaches, ransomware, and other cyber incidents.

ICBA suggests that as CISA develops incident reporting fields and report submission requirements that CISA should reference the standards outlined in FinCEN SAR filing advisories.[5]

Information Preservation

A Bank's Information Security Programs, including incident management, and incident response plans are covered by the Federal Financial Institutions Examination Council's Information Security booklet.[6] The Agencies also encourage banks to establish evidence-gathering and handling procedures aimed at preserving evidence of an incident and aiding in prosecution activities as part of their incident response plan.

ICBA suggests that information and data preservation techniques and durations not be regulated. During an incident, the preservation of evidence should be based on the best efforts of the financial institution. The primary goal of a financial institution is to recover systems and provide services to its customers in as quick of a timeframe as possible, this is sometimes done at the expense of evidence preservation. Additionally, depending on the specifics of an incident, evidence preservation may not be possible, such is the case with servers that are encrypted and then subsequently wiped by cybercriminals.

Information Sharing

ICBA suggests that CISA set up an information-sharing mechanism between CISA and the Agencies, the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), federal law enforcement, FinCEN, and the Financial Services Information Sharing and Analysis Center (FS-ISAC)[7]. ICBA also suggests that CISA produce and make available anonymized reports on incident case studies, incident trends, and successful mitigating strategies.

Conclusion

ICBA greatly appreciates the opportunity to provide comments in response to this request, and ICBA asks that CISA carefully consider our comments and suggestions as they work to develop final rules for the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

If you have any questions, please do not hesitate to contact me at Joel.Williquette@icba.org or (202) 821-4454.

---

[5] FinCEN Advisory, FIN-2016-A005, October 25, 2016 and FinCEN Advisory, FIN-2021-A004, November 8, 2021.
[6] FFIEC IT Examination Handbook InfoBase - III.D Incident Response. Accessed October 6, 2022.
[7] Financial Services Information Sharing and Analysis Center (fsisac.com). Accessed October 6, 2022.

Sincerely,

/s/

Joel Williquette
Senior Vice President, Operational Risk Policy

WASHINGTON, DC
1615 L Street NW
Suite 900
Washington, DC 20036

SAUK CENTRE, MN
518 Lincoln Road
P.O. Box 267
Sauk Centre, MN 56378

866-843-4222
www.icba.org