February 14, 2025

Via Electronic Submission

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

RE: Docket No. CISA-2024-0037 – Request for Comment on the National Cyber Incident Response Plan Update

To Whom It May Concern:

The Independent Community Bankers of America ("ICBA")[1] welcomes the opportunity to provide comments in response to the Cybersecurity and Infrastructure Security Agency's ("CISA") request for comment on the *National Cyber Incident Response Plan Update*. The plan seeks to outline the strategic national framework for responding to cyber incidents in line with the Presidential Policy Directive 41 (PPD-41). ICBA applauds CISA for its leadership in strengthening the nation's cyber resilience and appreciates its efforts to create a coordinated framework for responding to significant cyber incidents.

The National Cyber Incident Response Plan ("NCIRP") serves as the federal government's blueprint for responding to significant cybersecurity incidents. The current proposed update is intended to refine and enhance the plan by incorporating feedback from stakeholders across critical infrastructure sectors, including financial institutions. This process aims to ensure that incident response coordination, regulatory consistency, and information sharing mechanisms are effective, equitable, and inclusive of all impacted entities. Given the increasing sophistication of cybersecurity threats, it is crucial that community banks, which play a vital role

[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.*

in the financial system, have a voice in shaping the NCIRP's policies and strategies.

Community Banks as Critical Partners

Community banks serve as trusted financial partners to millions of individuals and small businesses across the United States. These banks play a vital role in the economic stability and prosperity of their communities by providing secure and reliable financial services. Given the integral role community banks play in the financial services ecosystem, it is crucial that they are included in communication channels and coordination efforts outlined in the NCIRP.

Inclusion in Communications

The NCIRP emphasizes the importance of coordination among federal, state, and local governments, as well as private-sector partners. However, the plan should explicitly include community banks as key stakeholders in information-sharing efforts and incident response coordination. Community banks rely on timely and actionable intelligence to mitigate the impact of cyber incidents. To enhance the effectiveness of the NCIRP, particularly in the "Phases of Cyber Incident Response Operations" section, CISA should:

- **Ensure Clear Communication Channels:** Establish clear communication channels that directly engage community banks during all phases of incident response, from detection and analysis to recovery.
- **Leverage Existing Frameworks:** Partner with existing industry associations, such as ICBA, to disseminate relevant information and guidance to community banks.
- **Provide Tailored Resources:** Develop resources and tools that address the specific needs and operational constraints of community banks, which often have fewer resources than larger financial institutions.

Admission to the Joint Cyber Defense Collaborative (JCDC)

CISA's Joint Cyber Defense Collaborative ("JCDC") has been instrumental in fostering public-private partnerships to enhance the nation's cybersecurity posture. ICBA strongly encourages CISA to expand access to the JCDC to include community banks. Allowing community banks to participate in the JCDC would address gaps in the "Coordinating Structures" section by:

- **Enhancing Preparedness:** Enable community banks to access real-time threat intelligence and collaborate with other stakeholders to proactively address emerging cyber risks.
- **Facilitating Rapid Response:** Ensure that community banks are better equipped to coordinate with federal partners and industry peers during significant cyber incidents.
- **Promote Equity:** Recognize the critical role of community banks in the financial services sector and ensure they are not disadvantaged compared to larger institutions in receiving critical cybersecurity support.

Harmonization of Regulatory Efforts

Community banks are already subject to extensive cybersecurity regulations and reporting requirements, including those from federal banking regulators. To minimize duplication and regulatory burden, CISA should harmonize the NCIRP's provisions with existing requirements from agencies such as the Federal Reserve, the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC), better aligning with the "Annex C: Voluntary Reporting of Cyber Incidents to the Federal Government" section. Harmonization would:

- Reduce compliance costs and administrative burden for community banks.
- Streamline incident reporting and response efforts.
- Ensure consistent and efficient application of cybersecurity policies across the financial services sector.

Conclusion

ICBA commends CISA for its leadership in enhancing the nation's cybersecurity resilience and appreciates the opportunity to provide input on the NCIRP. Including community banks as key partners in communication efforts and admitting them into the JCDC will strengthen the overall effectiveness of the nation's cyber incident response framework. We look forward to continued collaboration with CISA to ensure the safety and security of the financial services sector.

If you have any questions or would like to discuss our comments in more detail, please contact Anjelica Dortch at Anjelica.Dortch@icba.org or at 202-659-8111.

Sincerely,

/s/

Anjelica Dortch
Vice President, Operational Risk & Cybersecurity Policy