July 29, 2022

U.S. Senate Committee on Homeland Security & Governmental Affairs
340 Dirksen Senate Office Building
Washington, D.C. 20510

U.S. Senate Committee on Armed Services
228 Russell Senate Office Building
Washington, D.C. 20510

Dear Chairman Peters, Ranking Member Portman, Chairman Reed and Ranking Member Inhofe:

As the Senate considers the National Defense Authorization Act for Fiscal Year 2023, we urge you to oppose language creating a designation for Systemically Important Entities (SIEs) that was added to the House bill as floor amendment 554. Financial institutions are supportive of efforts to improve the identification and risk assessment of critical infrastructure but believe the provision, as written, would duplicate existing designations without addressing gaps in government efforts to help protect private critical infrastructure from national security threats. While some critical infrastructure sectors are not captured by similar designation programs and may warrant additional oversight, financial institutions are already subject to extensive cybersecurity risk management and incident reporting frameworks that require reviews of security controls and data protection measures, the security of vendors and suppliers, governance processes, and incident notification and reporting. Adding yet another layer of reporting to a different set of agencies with different standards would detract significantly from financial institutions' essential work defending against cyber threats. We welcome efforts to mature how the government assesses risk and improve the private-public partnership; however, this provision requires discussion with industry and other Congressional Committees to ensure it meets these objectives.

We encourage efforts to mature CISA's capabilities and refine risk assessment models, but the SIE provision is problematic for several reasons, including:

- *Duplication with existing systemic designations and requirements* – Financial institutions are already subject to several designations intended to recognize their heightened importance to national security. The Systemically Important Financial Institution (SIFI) designation, which stems from the Dodd-Frank Act of 2010, requires firms to adopt enhanced measures for security and resilience and includes additional oversight and examination by financial regulators. Many of these firms are also included in the Section 9 process, established by Executive Order 13636 in 2013 and managed by the Department of Homeland Security, which recognizes firms where a cyber incident could result in "catastrophic regional or national effects on public health or safety, economic security or national security."

The SIE provision proposes to harmonize reporting requirements by allowing CISA to accept reports from regulators. Given the nature of financial regulations and the information CISA would require, however, a financial firm would have to prepare completely different reports to CISA. We would welcome a dialogue on how we can continue to inform CISA's risk analysis efforts, but legislation should exempt regulated financial institutions from new reporting requirements.

- *Requirements to share sensitive information that could increase risk to firms* – The information firms would be required to submit to CISA is sensitive and extensive. For example, providing CISA with details of supply chain risk management practices and "identifying critical assets, systems, suppliers, technologies, software, services, processes, or other dependencies" could expose firms to risk if it is inappropriately disclosed or stolen in a breach. This information would be highly valuable to malicious actors because it would provide a roadmap for how to attack a firm or disrupt a critical system or service. The legislation also does not specify what CISA would do with such information, nor how it would be shared or protected against disclosure.

- *Insufficient support for operational collaboration between firms and intelligence agencies* – The Section 9 program was originally envisioned not only to identify critical infrastructure of importance to national security, but also to prioritize these firms for government support and enhanced cyber threat information sharing. Thus far, financial institutions have received limited government support, and would welcome greater opportunity for operational collaboration, not only with CISA but also with intelligence agencies. Any legislation addressing national systemic risks should institutionalize operational collaboration on national security threats between firms and intelligence agencies, including clear legal authorities, guiding policies, and corresponding resourcing to support the protection of critical infrastructure. Congress should address these issues and encourage opportunities for greater direct engagement at both strategic and tactical levels.

Banks and other financial institutions meet daily challenges from nation-state actors and sophisticated cyber criminals seeking to disrupt our economy. Firms have made significant investments individually and collectively through organizations like the Financial Services Information Sharing and Analysis Center, the Financial Services Sector Coordinating Council, and the Analysis and Resilience Center for Systemic Risk—organizations that work to improve information sharing and readiness across financial firms and between critical infrastructure sectors. We firmly support sharing information and collaborating with government partners to address cybersecurity threats and we supported the recent passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

Financial institutions also have decades of experience meeting the requirements of existing systemic designations and have complied with rigorous legal and regulatory requirements for the security and resilience of their operations for decades. As noted above, we have significant concerns with the SIE provision and encourage much greater dialogue and consideration of its impact on financial institutions given the complexities of our sector and myriad regulatory requirements. Legislation this important merits full consideration by relevant committees, including hearings and debate.

Thank you for your leadership on these important issues. We look forward to continuing to work with you to protect critical infrastructure and defend against cybersecurity threats.

Sincerely,
American Bankers Association
Bank Policy Institute