Testimony of Heather Hogsett

Senior Vice President, Technology and Risk Strategy for BITS, the Technology Policy Division of the Bank Policy Institute

Before the U.S. House Subcommittee on Cybersecurity and Infrastructure Protection
"CISA 2025: The State of American Cybersecurity from a Stakeholder Perspective"

March 23, 2023

Chairman Garbarino, Ranking Member Swalwell and Honorable Members of the Subcommittee, thank you for inviting me to testify. I am Heather Hogsett, Senior Vice President of Technology and Risk Strategy for BITS, the technology policy division of the Bank Policy Institute (BPI).

BPI is a nonpartisan policy, research and advocacy organization representing the nation's leading banks. BPI members include universal banks, regional banks and major foreign banks doing business in the United States. BITS, our technology policy division, works with our member banks as well as insurance, card companies and market utilities on cyber risk management and critical infrastructure protection, fraud reduction, regulation and innovation.

I also serve as Co-Chair of the Financial Services Sector Coordinating Council (FSSCC) Policy Committee. The FSSCC coordinates across the financial sector to enhance security and resiliency and to collaborate with government partners such as the U.S. Treasury and the Cybersecurity and Infrastructure Security Agency (CISA), as well as financial regulatory agencies.

Financial Institutions and Cybersecurity

Banks and other financial institutions are increasingly under cyber-attack by foreign nations and criminal groups seeking to disrupt the financial system and undermine the functioning of the U.S. economy. The financial sector takes these risks seriously and has a long history of working across industry and with government partners to address and manage these risks.

As one of 16 critical infrastructure sectors, the financial industry formed and actively participates in the FSSCC[1] and the Financial Services Information Sharing and Analysis Center (FS-ISAC)[2] — both of which have served as leading examples other critical infrastructure sectors have sought to replicate. We also lead cybersecurity and operational resilience collaboration through public-private partnerships with our Sector Risk Management Agency (SRMA) — the U.S. Department of the Treasury — the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the U.S. Secret Service, and importantly with our regulators.

A major part of these industry efforts is focused on in-depth information sharing to accelerate and amplify public-private cooperation. During the nearly two decades of work, we have established exercise programs through the FSSCC and FS-ISAC that have covered a wide range of possible events such as destructive malware, an outage at a large service provider, or a pandemic and addressed

[1] https://fsscc.org/
[2] https://www.fsisac.com/

managing public confidence during a crisis. More than 40 such exercises have been held to date and have included participants from across the industry, third parties, regulators, the U.S. Treasury Department, DHS/CISA and law enforcement agencies.

In addition to Treasury and CISA, we also work closely with financial regulators to address cybersecurity, third-party and supply chain risks and promote operational resilience across the sector. This work occurs with individual firms, through trade associations such as BPI, and via joint efforts between the FSSCC and its government counterpart the Financial and Banking Information Infrastructure Committee (FBIIC), which is chaired by Treasury and includes 17 federal and state regulators.[3]

Experiences with CISA

Since its establishment in 2018 as an operational component of DHS, CISA has taken on an increasingly important role protecting federal civilian agencies and supporting security and resilience across critical infrastructure sectors. Following the important coordination role CISA filled during the COVID-19 pandemic to keep critical infrastructure working for America, there have been notable improvements in faster declassification and sharing of threat information, including a significant increase in publications, alerts and joint advisories with other government agencies such as the FBI and National Security Agency (NSA). These publications have become more frequent, timely and relevant and included recommended mitigation measures to help critical infrastructure entities better protect themselves, particularly midsize and smaller entities where the assistance is needed most. For example, CISA's recommended mitigations and tool kits to help entities protect themselves during the response to Solar Winds, Log4j and the ransomware attack against Colonial Pipeline were welcome for their timeliness and actionable nature. By creating a centralized repository for this information CISA has also made it easier for companies to quickly find and access relevant information and resources.

Its efforts to help raise awareness and promote baseline cybersecurity practices across all critical infrastructure sectors have been a welcome focus that will help reduce risk and improve national resilience. CISA also deserves credit for fostering collaboration and coordination across government entities including the banking industry and other critical infrastructure. Its work to date has built the foundation for trusted relationships and very importantly created resources to support those sectors that are resource constrained and in the earlier stages of building their cyber risk management programs.

The preparation and response to the Russian invasion of Ukraine highlight a number of these accomplishments. As tensions rose and the U.S. prepared for Russian aggression and the potential for retaliatory attacks, CISA's senior leadership, along with senior leaders at Treasury, DHS and the FBI, was in regular communications with financial institutions and organizations like the FSSCC, FS-ISAC and the Analysis and Resilience Center for Systemic Risk (ARC). CISA created the "Shields Up" campaign to raise awareness and urge critical infrastructure companies to shore up their defenses and actively share suspicious information with the government to provide an early warning of attacks. During this time, CISA created a new bi-directional communication mechanism to provide for near real-time information sharing among trusted partners in both industry and government that had never previously been done. This coordination role was invaluable for our industry and others and provided a streamlined mechanism to exchange threat information and share timely updates to those operating some of the nation's most critical infrastructure.

[3] www.fbiic.gov

Evolving for the Future

Looking ahead, it will be important for CISA to establish a clear path for maturing and scaling its operations, including ensuring these programs and initiatives have stakeholder input and will continue despite future changes in leadership. A number of the efforts to date have been in response to current cyber threats, which was and continues to be important, but CISA is also uniquely positioned to address longer-term strategic planning and cross-sector risk mitigation that will be particularly valuable for mature sectors. As CISA continues to evolve, we encourage a focus on the following areas:

- ***Cyber Incident Reporting and Harmonization – Supporting Response and Recovery***
  Last year, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022, requiring critical infrastructure companies to report ransomware payments and cyber incidents to CISA. BPI supported this legislation which we believe will help improve national cyber defense by providing CISA and other government agencies with timely and relevant information to assess and analyze cyber threats across sectors, improve the alerts and security services CISA provides and ultimately provide earlier warning of potential attacks so companies can better defend themselves. Under the law, CISA must conduct a rulemaking process, seek input from stakeholders, and develop the necessary systems and processes to collect, analyze and share reported information while ensuring strong data security and protection measures are in place.

  As CISA crafts rules under CIRCIA, it is also required to harmonize the new requirements with existing regulatory reporting to avoid conflicting, duplicative or burdensome requirements. Given the comprehensive set of cybersecurity and incident notification rules[4] that financial institutions already comply with, harmonizing and aligning the new rules will be important to ensure cyber defenders can maintain focus on protecting the firm rather than complying with multiple government reporting requirements.

  This is a significant undertaking that CISA must get right from the outset and will require extensive coordination with critical infrastructure entities, SRMAs, other government agencies and independent regulators. As a critical infrastructure sector that has had mandatory cyber reporting requirements for more than 20 years and has invested significant time and resources into harmonizing and driving toward regulatory convergence, this is a key area of focus. CISA should ensure that definitions, timelines, thresholds and required incident information are aligned with existing requirements and designed to avoid interfering with response and mitigation at an affected firm.

  BPI recommends that CISA build a streamlined reporting system that accomplishes the following: 1) allows an impacted firm to report incident information once and have it shared, as appropriate, with SRMAs, regulators and law enforcement agencies; 2) provides CISA with timely and relevant information useful to assessing trends, improving analysis, and the development of alerts, tools and services that can be provided to critical infrastructure companies; and 3) maintains its role as a trusted channel for information and communications, preserving privacy and confidentiality while supporting the response and recovery of an impacted entity.

[4] https://staging4.bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/

- ***Identification and Prioritization of National Systemic Risks***
  Identifying critical infrastructure assets that are most important to our national security would help prioritize resources and guide public-private collaboration to prevent or mitigate threats and prepare for potential response and recovery needs.

  Financial institutions have existing designations such as the Systemically Important Financial Institution designation that stems from the Dodd-Frank Act of 2010 and 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 DHS, 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."

  Similarly, in 2019, CISA created a list of 55 National Critical Functions that are functions "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[5] CISA is in the process of working with SRMAs to decompose or analyze these further. At the same time, CISA is developing a new designation for Systemically Important Entities (SIEs) and was appropriated an increase of $1.9 million for the creation of an SIE Program Office.

  Financial institutions are very supportive of efforts to better identify and prioritize cross-sector risks; however, the current approach appears disjointed and opaque, making it challenging for industry to provide input or information that might be helpful. Past proposals to create an SIE or Systemically Important Critical Infrastructure (SICI) designation would have duplicated existing designations and requirements on financial institutions, diverting resources from defending against threats to regulatory compliance.

  As CISA continues this work, we encourage greater transparency and clarity in the approach, what it intends to accomplish, and how an SIE designation fits with related areas of work such as the Section 9 list, NCFs and sector-specific systemic risk designations such as SIFI. CISA should not only avoid duplication or overlap with other systemic designations and their requirements but also leverage work that has already been done in the more mature critical infrastructure sectors. Financial institutions have worked through the ARC to analyze financial sector systemic risks and are ready to work with CISA to develop a framework for assessing risks and critical dependencies across sectors.

- ***Fostering Cross-Sector Coordination and Operational Collaboration***
  CISA's role as national coordinator for critical infrastructure security puts it in a unique position to support collaboration among more mature sectors and the government to reduce risk and disrupt threats. Since 2017, the financial, energy and communications sectors have conducted joint planning and exercises to address cyber threats that could impact or cascade across the three sectors. CISA supported the creation of the "tri-sector" working group which is a good example of fostering and enabling collaborative efforts.

[5] https://www.cisa.gov/national-critical-functions

CISA's Joint Cyber Defense Collaborative (JCDC) was helpful in bringing together industry and government partners to improve visibility and communication in response to geopolitical tensions and the Russian invasion of Ukraine. This response-oriented focus, however, has not fulfilled the need for longer-term strategic planning across government agencies and the private sector. As originally authorized by Congress,[6] CISA was charged with creating a Joint Cyber Planning Office (JCPO) to develop plans for cyber defense operations and coordinated actions that public and private sector entities could take to protect, mitigate, or defend against malicious cyber-attacks. To date, we have not seen the JCDC engage in the type of planning directed by Congress but continue to believe this would be beneficial for financial institutions and other more mature sectors.

The recently released National Cybersecurity Strategy recognizes that the private sector has growing visibility into adversary activity and calls for enhancing public-private operational collaboration to disrupt adversaries.[7] Through our relationship with Treasury as our SRMA, we have robust partnership and dialogue. Treasury is establishing a cyber collaboration center to facilitate greater opportunity for firms to exchange classified and unclassified information and facilitate discussion around threat actor activity and vulnerabilities. Other parts of government have created similar centers such as the NSA's Cybersecurity Collaboration Center. Plans to create a cross-sector equivalent or otherwise foster collaboration and exchange among these efforts would be valuable and CISA could play a helpful role.

Sustaining Progress and Building Capabilities

We are at a defining juncture in CISA's development, similar to any startup at this stage, where achieving scale matters. As Congress intended and supported with funding, CISA must refine its focus and apply resources carefully to be successful. Now that CISA has established its presence, developed communications and outreach capabilities, and designed tools and services to improve near-term resilience, it should shift its approach to expand management capabilities, add operational expertise and establish processes that will be the foundation for sustained leadership on immediate tactical response matters as well as longer-term, proactive planning and support that will benefit even the most cyber-mature sectors like financial services.

Successful implementation of CIRCIA, including harmonizing its reporting requirements to optimize protection and response and streamline coordination, will serve as a cornerstone for the future of public-private partnerships and should be a top priority. Similarly, developing the means to identify and prioritize the highest risks by sector and across sectors will refine CISA's focus and support more secure and resilient outcomes for the nation.

This is no small task and requires CISA to focus on building organizational consistency and rigor, hiring and retaining experienced staff, and sourcing support from sectors that have well-established security, resilience and, in the financial services case, regulatory standards that can be leveraged.

We are committed to working with CISA to support its continued development and look forward to the opportunity to engage in future national risk mitigation efforts.

[6] *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*. P.L. 116-283, Sec 1715.
[7] National Cybersecurity Strategy, March 2023, p. 15