"Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021"

Testimony of Heather Hogsett, Senior Vice President, Technology and Risk Strategy for BITS, the Technology Policy Division of Bank Policy Institute
Before the U.S. House Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation

September 1, 2021

Chairwoman Clarke, Ranking Member Garbarino 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 other leading financial institutions 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.

Executive Summary

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. We were the first sector to form an information sharing and analysis center in 1999 and established a strong sector coordinating council in 2002—both of which have served as leading examples other critical infrastructure sectors have sought to replicate. We are also one of the few critical infrastructure sectors that has had cybersecurity and incident reporting requirements in law and regulation for over 20 years.

We greatly appreciate the Committee's leadership to address the nation's cybersecurity challenges and efforts to improve the resilience of critical infrastructure. We share a mutual commitment to cybersecurity and the value in sharing threat and incident information, and support efforts to fortify CISA as a leader in this space.

As Congress considers legislation to require critical infrastructure entities to report cyber incidents to the federal government, we believe the following elements in the bill—the *Cyber Incident Reporting for Critical Infrastructure Act of 2021*—which are discussed in greater detail below, are vital to achieving our shared goal of protecting the nation's critical infrastructure:

- **Scope** – The scope of required reporting focuses on incidents that could cause actual harm, which will ensure CISA receives accurate and useful data to help achieve its goal of greater situational awareness. Approaches which seek to mandate reporting of "potential" incidents are too broad and would lead to over-reporting that is insufficiently focused on the actual risks.

- **Timeline** – The timeline for reporting of no earlier than 72 hours after confirmation an incident has occurred strikes the right balance to allow sufficient time for investigation and implementation of

mitigation and response measures while reporting timely and useful information to CISA. The initial stages of an incident response require "all-hands-on-deck" and front-line cyber defenders should be focused on response and remediation rather than completing compliance paperwork.

- **Harmonization** – For already regulated critical infrastructure sectors, it is vital to ensure new reporting requirements are harmonized with existing laws and regulations. We appreciate the approach taken in the bill and would recommend continued Congressional focus to ensure implementation avoids unnecessary duplication and establishes a streamlined process for all required reporting.

- **Maintain Protections and Definitions in the Cybersecurity and Information Sharing Act of 2015 (CISA Act)** – We support the Committee clearly incorporating the key definitions and protections already created by the CISA Act for private firms sharing information with government. This bill builds on that, and the consistency for industry is important. Any bill in Congress that seeks to mandate cyber information sharing should incorporate these protections and we appreciate that is clearly defined in the bill.

- **Helping Companies Understand if Their Data has Been Compromised** – The SolarWinds attack targeted several federal agencies but also impacted a much broader swath of entities including critical infrastructure companies. Government agencies who are attacked should be required to notify critical infrastructure entities when their sensitive information may be compromised. We appreciate the language in this bill that seeks to address this important issue.

Working Together on Other Priorities

- There is an additional area that we would like to work on with this Committee and Congress that we believe is essential to improving our cyber defense capabilities, and that is around the need for greatly improved **bi-directional information sharing**. The government should use reported information from critical infrastructure and other government entities to improve the relevancy and speed of alerts and other analyses that can be provided to critical infrastructure. More timely and actionable information being shared with the private sector would benefit our collective security and resilience capabilities.

Background on Existing Financial Services Sector Cybersecurity Efforts

Legal and Regulatory Requirements

The banking/financial services sector is one of the few critical infrastructure sectors that has had mandatory cybersecurity and incident reporting requirements in law and regulation for over 20 years. As a result, we have experienced what is most effective and would emphasize that it is important to ensure that any new requirements are harmonized and align with existing requirements for financial firms.

For example, financial institutions are regularly examined for compliance with the Gramm-Leach-Bliley Act and its implementing regulations, which require cyber incident reporting when unauthorized access to or misuse of customer data occurs. The New York Department of Financial Services Cybersecurity Regulation expanded on these requirements and requires reporting if a cyber incident is likely to cause harm to the financial institution's operations. In the course of ongoing robust oversight from regulatory authorities—such as the Federal Reserve Board, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation, among others— banks are regularly examined for their cybersecurity practices including the use of security controls, third party risk management and senior management and board oversight.

A summary of the main banking/financial services requirements is attached as Appendix A.

Information-Sharing and Collaboration Efforts

In addition to required regulatory reporting, financial firms have made significant investments to protect the industry, developing high-trust collaboration centers to improve resilience at individual firms and across the broader financial system, through digital infrastructure, comprehensive use of security tools, exercise programs and extensive training. They have also created joint initiatives to address systemic challenges such as:

- The **Financial Services Information Sharing and Analysis Center** (FS-ISAC)[1], which shares cyber threat information and best practices for nearly 7,000 members across the globe, including 4,600 U.S. financial institutions. The FS-ISAC was one of the first ISACs created among industry.

- The **Financial Services Sector Coordinating Council** (FSSCC)[2], which strengthens the resiliency of the financial sector against cyber-attacks and other threats by proactively identifying threats, promoting protection, driving preparedness, collaborating with government partners and regulatory authorities and coordinating crisis response.

- The **Analysis and Resilience Center**,[3] which works to mitigate systemic risk to the nation's most critical financial and electric infrastructure, and facilitates operational collaboration between firms, the U.S. government and other key partners.

- **Sheltered Harbor**[4], a secure data repository for consumer bank and securities holdings to protect customers, financial institutions, and public confidence in the event a cyber-attack causes critical systems to fail; and

- The **Cyber Risk Institute's "Cyber Profile"**[5] which is derived from the National Institute of Standards and Technology's Cybersecurity Framework and incorporates financial services regulatory requirements and industry best practices to address one of the industry's most pressing needs to harmonize regulation globally to improve security and resilience.

Discussion Points: Effective Cyber Incident Reporting Model

The recent string of ransomware attacks and supply chain compromises have highlighted the need for more transparency about the nature and depth of cybersecurity attacks affecting the public and private sectors. BPI member banks are committed to improving protections across critical infrastructure sectors and recognize the value in sharing cyber threat and incident information with CISA.

As noted above, banks and other financial institutions already adhere to extensive cybersecurity and regulatory reporting requirements. It must be a priority for Congress to harmonize any new requirements for reporting, oversight and enforcement with existing regulatory requirements to minimize confusion on competing requirements and avoid distracting from response efforts.

Based on the industry's experience with long-standing regulations and requirements, we are encouraged to see that the current draft bill includes the following elements that will help ensure an effective structure for incident reporting for all critical infrastructure sectors:

Scope

The current draft of the legislation appropriately tailors the kinds of incidents to be reported to actual incidents, which will ensure CISA receives accurate, timely and useful information. Other approaches that would collect information on "potential incidents" would create near-constant reporting to CISA by financial services firms based on the number of incidents those firms see on a daily basis. It is unclear what a "potential incident" is, how it would be reported and what value that provides. As the U.S. government seeks to increase its analytical capabilities, it is also critical for it to be able to turn around threat information and share it with all sectors quickly. Collecting information on potential incidents would add noise to the signal of material incidents and thus overwhelm, rather than enhance, CISA's analytical efforts.

[1] https://www.fsisac.com/
[2] https://fsscc.org/
[3] https://systemicrisk.org/
[4] https://www.shelteredharbor.org/
[5] https://cyberriskinstitute.org/

Timeline
The bill's reporting requirement of no earlier than 72 hours after confirmation an incident has occurred, strikes an important balance between allowing an affected entity to implement immediate response measures while ensuring CISA receives timely, useful and accurate information. The initial stages of an incident response require "all-hands-on-deck" to focus immediately on understanding the incident and implementing mitigation and response measures. Other approaches that would require reporting within 24 hours would distract from critical work in the early stages of a response and result in reports that were premature and likely erroneous.

Harmonization
For already regulated critical infrastructure sectors, it is vital to ensure new reporting requirements are harmonized with existing laws and regulations. The bill currently includes helpful provisions to require CISA to coordinate with Sector Risk Management Agencies and regulatory authorities to streamline reporting requirements.

As noted above, financial institutions comply with a multitude of reporting requirements which establish key definitions, timelines, and reporting thresholds, as well as oversight and enforcement mechanisms which may include fines and other penalties. There is value in reporting to CISA, but it is important to ensure government agencies and regulators work together quickly to develop a common reporting form that would be good for all government entities requiring incident reporting. Otherwise, still more time will be spent by first responders working with firms' legal and compliance teams to ensure that each agency's nuanced requirement is met, rather than reporting uniformly and allowing more time for protecting critical infrastructure.

Maintain Protections of the Cybersecurity and Information Sharing Act of 2015
The bill incorporates existing definitions and protections from the CISA Act, which will provide helpful continuity for industry. These measures, which include privacy and liability protections, serve as instrumental building blocks to greater sharing and collaboration between the public and private sectors, and should be continued as Congress expands the information firms are required to submit to CISA.

Helping Companies Understand if Their Data has Been Compromised
Financial services companies are required to share sensitive and confidential information, including operational and customer data, with regulators and other government agencies that, if breached, could pose risks to the institution and its customers. The current draft of the bill recognizes the importance of ensuring that government agencies are also required to provide greater transparency and alert critical infrastructure companies if their sensitive data is affected by a breach at a federal agency. Such notification would allow the firm to take proactive measures to mitigate risks, helping protect the firm, its customers and potentially the broader sector.

Future Work Together
Recent disruptive ransomware attacks on critical infrastructure are a stark reminder of the threats we face and the urgent need to rethink how government and industry work together to protect against national security threats. Expanding CISA's awareness of cyber incidents affecting critical infrastructure through required reporting will help improve the quality of cyber threat analysis that can be shared more broadly across the public and private sectors. We appreciate the Committee's thoughtful approach and efforts to take input from critical infrastructure sectors in crafting this important legislation and look forward to continued collaboration.

We also look forward to working with the Committee on other opportunities to improve public-private collaboration to address cybersecurity threats. As CISA and other government agencies increasingly receive incident data and other threat information, they should be required to improve the quality, timeliness and actionable nature of the information that can be provided to critical infrastructure. Current information sharing is often one-sided from industry to government and the alerts and warnings industry receives from government are often delayed, limiting their usefulness. As CISA, along with intelligence and law enforcement agencies, strengthen

coordination and collaboration with the private sector, we urge Congress to ensure government agencies are improving the speed and quality of information provided back to critical infrastructure.

I appreciate the opportunity to testify today and look forward to any questions.

APPENDIX A

The following is a snapshot of the main banking/financial services cybersecurity incident notification and reporting requirements, a myriad of others exist as well.

Gramm-Leach-Bliley Act (GLBA). Under the GLBA and its implementing regulations[6], cyber incident reporting is triggered when a financial institution becomes aware of unauthorized access to sensitive customer information that is, or is likely to be, a misuse of the customer's information. Notification to regulators is required as soon as possible after the institution determines that misuse of customer data has occurred or is reasonably possible (*e.g.* at the start of an investigation to determine the likelihood that the information has been or could be misused). To ensure adherence to these requirements, regulators conduct ongoing and rigorous reviews of institutions' operating and governance processes, including data security and data handling processes and third-party risk management measures. Failure to report incidents and adhere to these requirements could result in serious enforcement measures including mandatory corrective action directives, restrictions on activities, and fines.

- **Reporting Timeline –** as soon as possible once the institution determines unauthorized access occurred.
- **Definitions –** A *cyber incident* is defined as unauthorized access to sensitive customer information.
- **Scope of Reporting –** Covers non-public customer information such as personally identifiable financial information, financial transaction information, income, and credit rating data, etc.
- **Reporting Mechanism –** Report provided to regulators; information becomes part of ongoing regulatory oversight/examinations.

New York Department of Financial Services (NYDFS) Cybersecurity Regulation. The NYDFS regulations[7] became effective on March 1, 2017 and add another layer of mandatory cybersecurity reporting requirements for financial services companies. A financial institution must notify NYDFS when a cyber event triggers reporting to any other government body, regulatory or self-regulatory agency. Notification is also triggered if there is a reasonable likelihood of material harm to the institution's operations. Once a triggering event has occurred, notification must occur as promptly as possible, but not later than 72 hours from the determination that a cybersecurity event has occurred.

- **Reporting Timeline –** 72 hours from the determination that a cyber event has occurred.
- **Definitions –** A *cyber event* is defined as any act or attempt to gain unauthorized access to, disrupt, or misuse an information system or information stored on an information system.
- **Scope of Reporting –** Covers non-public customer information and information technology systems[8]
- **Reporting Mechanism –** Report provided to NYDFS; information becomes part of ongoing regulatory oversight

[6] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. See https://www.federalregister.gov/documents/2005/03/29/05-5980/interagency-guidance-on-response-programs-for-unauthorized-access-to-customer-information-and

[7] See New York Codes, Rules and Regulations (23 NYCRR 500). https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)

[8] Defined as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems."

European Union General Data Protection Regulation (GDPR). In the case of a personal data breach, notification is required without undue delay and, where feasible, not later than 72 hours after having become aware of it. GDPR sets specific privacy parameters for use, data security, and handling of consumer data.

- **Reporting Timeline –** 72 hours
- **Definitions –** A "data breach" is defined as "the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
- **Scope of Reporting** – Personal data[9]
- **Reporting Mechanism –** Entities report to the agency designated by each Member state, which then notifies other Member states as needed.

European Union NIS Directive 1.0: In 2016, the EU mandated cyber incident reporting for all sectors defined under the term Essential Services which is like the U.S. term of Critical Infrastructure. However, the EU has both mandatory security mandates on Digital Service Providers and stricter reporting requirements on DSPs[10]. The EU is in the midst of updating the NIS Directive 2.0 where notification must occur with any event compromising the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or of the related services offered by, or accessible via, network and information systems.

- **Reporting Timeline –** 24 hours from when an entity is aware of an incident, and then a report 30 days later.
- **Definitions –** An *incident* means any event having an actual adverse effect on the security of network and information systems.[11]
- **Scope of Reporting –** The Directive does not define the threshold of what is a significant incident requiring notification to the relevant EU Member state national authority and defines 3 parameters for reporting: number of users affected; duration of incident; geographic spread. DSPs have 5 requirements that are broader.
- **Reporting Mechanism** –Entities report to the agency designated by each Member state.

Notice of Proposed Rulemaking (NPR) from OCC/Federal Reserve/FDIC. On Jan. 12, 2021, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), and the Federal Deposit Insurance Corporation (FDIC) published a proposed rule on "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers." Under the proposal, incident notification would be triggered after the determination by a banking organization that a computer-security incident has occurred that the bank believes in good faith could cause significant disruption to the institution's operations and ability to deliver products and services to a significant portion of its customers or could pose a risk to the financial stability of the United States. Upon determining that an event has reached the notification incident threshold, a banking organization would be required to notify as soon as possible but no later than 36 hours.

- **Reporting Timeline –** 36 hours after a 'good faith' determination of an incident.
- **Definitions** – A *computer security incident* is defined as an occurrence that jeopardizes confidentiality, integrity or availability of an information system or the information a system processes, stores, or transmits[12]; a *notification incident* is defined as a significant computer security incident that could jeopardize the viability of the operations of a financial institution, prevent customers from accessing their

[9] Personal data is under GDPR here: https://gdpr-info.eu/art-4-gdpr/
[10] Essential Services are defined by the EU in the NIS Directive and was implemented in 2016. See: https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[11] For definition of "incident," see https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[12] This definition is taken from NIST which states a computer security incident is "an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. See NIST, Computer Security Resource Center, Glossary https://csrc.nist.gov/glossary/term/Computer_Security_Incident

deposit and other accounts, or impact the stability of the financial sector.

- **Scope of Reporting –** covers non-public customer information and information technology systems[13].
- **Reporting Mechanism –** Notification to be provided to primary federal regulator; intended to provide early awareness of emerging threats to individual institutions and potentially the broader financial system.

[13] The NPR does not define information technology systems.