STAKEHOLDER PERSPECTIVES ON THE CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2021

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 1, 2021

Serial No. 117–28

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

46–175 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

YVETTE D. CLARKE, New York, *Chairwoman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
ELISSA SLOTKIN, Michigan
KATHLEEN M. RICE, New York
RITCHIE TORRES, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*
ANDREW R. GARBARINO, New York, *Ranking Member*
RALPH NORMAN, South Carolina
DIANA HARSHBARGER, Tennessee
ANDREW CLYDE, Georgia
JAKE LATURNER, Kansas
JOHN KATKO, New York *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
AUSTIN AGRELLA, *Minority Subcommittee Staff Director*
MARIAH HARDING, *Subcommittee Clerk*

CONTENTS

STAKEHOLDER PERSPECTIVES ON THE CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2021

Wednesday, September 1, 2021

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 12 p.m., via Webex, Hon. Yvette D. Clarke [Chairwoman of the subcommittee] presiding.

Present: Representatives Clarke, Jackson Lee, Langevin, Thompson (ex officio), Garbarino, Clyde, and Katko (ex officio).

Ms. CLARKE. The Committee on Cybersecurity, Infrastructure Protection, and Innovation will come to order. The subcommittee is meeting today to receive testimony on "Stakeholder Perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021."

Without objection, the Chair is authorized to declare the committee in recess at any point.

So good afternoon, everyone. I would like to thank the witnesses for participating in today's hearing on the Cyber Incident Reporting for Critical Infrastructure Act of 2021.

Earlier this year, this committee held a joint hearing with the Committee on Oversight and Reform to examine the SolarWinds supply chain attack. Our oversight revealed a number of gaps in Federal authorities, policies, and capabilities that Congress must address to secure its own networks and better serve its private-sector partners. But what stood out to me was how lucky we were that FireEye disclosed that it had been compromised. Where would we be if they had chosen not to?

At this hearing—at the hearing, excuse me, I asked whether we would benefit from implementing a mandatory cyber incident reporting framework. Microsoft President Brad Smith observed that today information is siloed and that we need one entity in a position to scan the entire horizon and connect the dots between all of the attacks or hacks that are taking place.

SolarWinds President Sudhakar Ramakrishna testified having a single entity to which all of us can report will serve the fundamental purpose of building speed and agility and argued that private enterprises, "should be instructed with reporting requirements

and be made part of this community vision where public and private sectors can work together on addressing this issue."

At the same hearing, FireEye CEO Kevin Mandia testified about the importance of centralizing intelligence to improve the speed at which the picture and vision will come together, end quote. That hearing convinced me that Congress must act to ensure the cybersecurity and infrastructure security agency known as CISA receives timely cyber incident information from critical infrastructure owners and operators. Since then, I have worked with Chairman Thompson, Ranking Member Katko to draft legislation to establish a mandatory cyber incident reporting framework at CISA. I would like to thank them both for their support in this effort.

The draft legislation we are discussing today is the product of months of dialog with Government officials and private-sector stakeholders. I want to express my gratitude to those who worked with the committee to provide feedback on various drafts of the legislation. We have worked hard to draft the legislation in a manner that will result in the greatest security impact for both the Federal Government and the private sector, and I am proud of the draft we have developed.

Our bill would direct CISA, after a 270-day period with mandatory windows of stakeholder consultation and comment, to issue an interim final rule describing, No. 1, which critical infrastructure owners and operators are subject to the reporting requirement; No. 2, which cyber incidents need to be reported; No. 3, the mechanism for submitting reports; and, No. 4, other details necessary for implementation.

Importantly, our bill seeks to establish this new mandatory reporting program in a way that sets it apart from CISA's voluntary cyber programs by establishing a new cyber incident review office and tasking this new office with a discrete mission of receiving, aggregating, analyzing, and securing cyber incident reports. The bill also aims to ensure that covered entities benefit from the new reporting requirement in three ways: First, our bill requires CISA to publish quarterly reports with analyzed findings to provide better situational awareness to its partners. Second, it directs CISA to identify any actionable threat intelligence that should be shared rapidly and confidentially with cyber, "first responders," to prevent or respond to other attacks. Third, it requires CISA to notify private-sector entities that may have been impacted by data breaches or intrusions on Federal networks.

I am pleased with the progress we have made on this legislation but want to be clear that our work is on-going. We remain open to additional questions and feedback because it is important to get this right.

In recent days, I have been asked whether we would ask compliance challenges that certain small businesses may have. I want to be clear that we do not expect all critical infrastructure owners and operators to be subject to this reporting requirement. Rather, we expect it to apply only to a subset.

That said, I would be certainly—I would certainly be happy to explore whether we need to add language directing CISA to provide additional compliance assistance to small businesses that are determined to be covered entities.

I look forward to hearing additional stakeholder perspectives on the legislation today.

Before I close and without objection, I would like to include in the record letters of support from Claroty and Accenture, as well as a letter signed by 18 associations, including ITI, the Cyber Threat Alliance, the American Gas Association, Airlines for America, and the Cyber Coalition, among others.

[The information follows:]

LETTER FROM CLAROTY

September 1, 2021.

Rep. YVETTE CLARKE,
Chairwoman, Cybersecurity, Infrastructure Protection & Innovation Subcommittee, House Committee on Homeland Security, Washington, DC 20515.

Rep. JOHN KATKO,
Ranking Member, House Committee on Homeland Security, Washington, DC 20515.

DEAR REPS. CLARKE AND KATKO: On behalf of Claroty, a leading worldwide provider of industrial cyber security solutions with the mission to drive visibility, continuity, and resiliency in the industrial economy, it is my pleasure to send this letter in support of your "Cyber Incident Reporting for Critical Infrastructure Act of 2021". By way of background, Claroty's solutions are deployed in thousands of industrial locations and facilities, in over 50 countries across all seven continents. We serve hundreds of customers, across many industrial verticals in critical infrastructure including energy, water, oil & gas, pipelines, food & beverage, pharmaceuticals, and other areas of critical manufacturing. Claroty's Operational Technology (OT) platform has been selected, tested, and validated by the world's leading industrial automation and cybersecurity vendors, elite system integrators, and Managed Security Service Providers. We are the only OT security provider to be certified by the U.S. Department of Homeland Security's Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act, which was created to encourage the development and deployment of counterterrorism technologies.

We appreciate the opportunity to provide our thoughts and insights on your cyber incident reporting legislation. This bill is a very important step toward building a future where the Federal Government obtains more actionable information from the private sector on cyber incidents so that the Internet ecosystem can be made more secure.

As Claroty reviewed the draft legislation, there were several attributes which led us to the conclusion that this is a measure we should support:

- *Creation of the Cyber Incident Review Office Under CISA is an Important Step to Provide Comprehensive Situational Awareness of Cyber Incidents.*—As part of its creation, the Cybersecurity and Infrastructure Security Agency (CISA) was chartered to provide a wide range of cyber functions and capabilities across Federal Government, agencies, State, local, Tribal, territorial governments agencies, and the private sector. As part of a cyber incident notification bill, we believe that having a single entity responsible for receiving, analyzing, and reporting on all significant cyber incidents would provide a common understanding of cyber situational awareness that could ensure the U.S. National interest are more effectively secured, and accomplished in a more timely and efficient manner. Whether adversaries are sophisticated and targeted, or unsophisticated and opportunistic, having an overarching situational awareness under a single entity of the U.S. Government provides an advantage over fragmented Departmental views of localized hot spots. The attackers play to their strengths of only needing to be right once, while defenders need to right every time. So too does the U.S. Government need to play to our strength by enabling a unified understanding of cyber situational awareness to ensure we can gain insights and provide actionable recommendations. As such, we agree with your legislation's intent that CISA should be provided clear regulatory authority to operate and enforce the cyber incident notification legislation, with full support, cooperation, and coordination with departments and agencies. Additionally, there will clearly need to be an assessment performed regarding resources and funding required to effectively staff the agency and provide capabilities to ensure it can successfully execute on this expanded mission. We stand ready to help you and your colleagues in the Appropriations committee to help in this regard.
- *Conduct cybersecurity reviews in the wake of Significant Cyber Incidents.*—One subtlety overlooked about the Oldsmar water treatment facility breach in Feb-

ruary 2021 was the willingness of law enforcement and plant officials to share details about the attack vector used to gain access to the network, as well as the potential consequences to public safety had controls not been in place to mitigate the attacker's actions. There is tremendous value in these details for peers across industries. Compounding the urgency of this narrative is the news that a California water treatment facility was breached by remote attackers just weeks earlier in January—using the same exact attack technique in February during the Oldsmar attack. Had details about the California attack been disclosed in a timely manner, that Oldsmar incident may have been prevented. Your legislation, by requiring a review of significant cybersecurity incidents is an important step toward making permanent this concept, which will help reduce the number of cyber incidents across U.S. critical infrastructure. If we look at the effectiveness of the National Transportation Safety Board an exemplar, its successes in driving apolitical learnings that have resulted in improved confidence and the reduction of accidents demonstrate that should be replicated in cybersecurity. As you look to continue making improvements in your bill, you might consider adding more content to this section of your bill consistent with Section 5 of Executive Order 14028 (the section which established a Cyber Safety Review Board, with the charter of reviewing and assessing serious incidents against Federal Civilian Executive branch and non-Federal systems).

- *The Scope of the Proposed Legislation Appropriately Calls Out Industrial Economy-Specific Requirements*.—As industrial OT environments such as water treatment facilities and electrical substation are being connected to the IT network, new risks are introduced in the physical world that were not risks in the digital world. We therefore believe that the drafted legislation appropriately calls out not only risks to confidentiality, integrity, and availability of information systems, but also addresses the risks to the safety and resiliency of operational systems and processes. This broader scope will ensure that industrial enterprises take a more expansive view of physical and safety risk—not only to the digital risk affecting IT systems.
- *The Cyber Incident Notification Period of 72 Hours is in-line with Established Standards*.—During the initial hours of a potential cyber incident, a significant amount of fact-finding must occur to validate that the event was truly a malicious cyber incident and determine its potential scope and impact. While large enterprises may be able to accomplish this rapidly, smaller or less well-funded organizations may need to enlist the support of third parties to effectively conduct these activities. Establishing the initial reporting period to 72 hours is the general expectation established from the 2018 European Union's General Data Protection Regulation (GDPR) and would be an effective benchmarking that most organizations are using as a standard. Any shorter of a notification period would run the risk of creating of too many "false positives" which would not be an effective use of Federal Government resources.

As this bill moves through the legislative process, there is one additional area that you might consider when perfecting the text. Specifically, we encourage you to look at how this bill might create disincentives for failure to notify. While the reporting requirements for covered entities are clear in the proposed legislation, we are concerned that given the increasing frequency and impact of cyber attacks, the onus of reporting should be placed on the covered entities for Significant Cyber Incidents and backed with disincentives for a failure to comply. At present, organizations are open to substantial brand and reputational risk for reporting on a cyber incident. The executive decision is therefore tipped all too frequently in favor of not reporting cyber incidents and working to quietly fix them behind the scenes. While focused on privacy, GDPR has driven substantial adoption of its obligations worldwide due to the very high fines for violating (20M or 4 percent of global revenue—whichever is higher) the breach notification provision. Of note, until the financial penalties were enacted in the latest version of GDPR, compliance was halfhearted. At present, many organizations view reporting as having a reputational and brand impact, and without penalties will decide not to report incidents. Claroty believes that given the risk to U.S. National security and interest, we must tip the financial calculus in favor of notification, that must be done through penalties and enforcement for organizations that are clearly in violation. We also believe that this new set of risks will drive Boards of Directors to govern and manage cyber risk, which will drive funding and action through the organization more effectively. By creating effective and material economic disincentives for organizations who do not comply with the expected outcomes, we tip the scale in favor of reporting. To the end, we would encourage you to engage those with experience in GDPR compliance to understand how the financial penalties of that measure have been received, and then decide whether that might be a valuable addition to this bill.

My Claroty colleagues and I stand ready to assist you in your efforts to advance this legislation and look forward to continuing our strong working relationship with your staff to that end.

Sincerely,

GRANT GEYER,
Chief Product Officer, Claroty.

STATEMENT OF ACCENTURE

AUGUST 2021

Accenture supports the Cyber Incident Reporting for Critical Infrastructure Act of 2021 and welcomes the opportunity to provide our feedback on the draft legislation. To improve the Nation's cybersecurity posture, the Federal Government needs to have greater awareness of cybersecurity incidents across critical infrastructure, and this draft legislation would achieve that. Accenture commends the bill drafters for working on a bipartisan basis and for sharing the draft with industry to solicit feedback and collaboration prior to introduction.

Accenture believes the draft legislation:

- Strikes the right balance by requiring narrowly-tailored incident information that can help the Federal Government get a more robust picture of the cyber landscape without overburdening companies with unworkable and overly broad reporting mandates. The legislation strikes this balance by directing CISA to focus on the most critical of critical infrastructure owners and operators and narrowly tailor the definition of a covered cybersecurity incident (and excluding potential incidents). We note that CISA's effort to identify the appropriate covered entities could be done in harmony with proposals for it to identify systemically important critical infrastructure.
- Tailors the incident information required to be provided to CISA, which will help CISA get a broader picture of serious threats to critical infrastructure by focusing on IOCs and TTPs. Information, if available, such as behavioral descriptors, failed/subverted controls or other investigational artifacts can help CISA better protect other critical infrastructure owners and operators by looking for trends and warning others who may be similarly targeted.
- Directs CISA to work to harmonize existing regulatory requirements on incident reporting with the new requirements in this draft bill, and coordinate with regulators that already receive cyber incident reports to streamline processes. As the bill drafters know, not all critical infrastructure sectors are alike. Some sectors such as financial services are far along in their cybersecurity maturity and have existing regulations and practices. For those advanced sectors, it is crucial that CISA examine existing incident notification expectations that are both in regulation and in practice to ensure that the reporting is aligned with the risk profile to the sector as well as the Nation's security. Other sectors' cybersecurity posture such as water and agriculture systems are quite nascent. For the nascent entities, budgeting for, building the capacity for, and implementing the new requirements and maturing their cybersecurity posture will take some time. Still others, such as pipelines within the transportation system and Federal ICT providers subject to the new cyber Executive Order, have new incident notification requirements to comply with. It is imperative that policy makers and CISA take all of this into account when developing the new requirements to reduce confusion, complexity, and duplication.
- Focuses on a "prompt" reporting standard that cannot be shorter than 72 hours, rather than a 24-hour requirement. Once anomalistic activity is identified, it can take some time for a company to verify the intrusion and identify whether it is a serious enough event to warrant reporting. From Accenture's experience in working with many companies across critical infrastructure to respond to such incidents, 72 hours is a reasonable time frame to be able to determine scope, impact, and initial TTPs and IOCs and possibly share malware samples for further analysis. This information would be important to report the initial understanding of an attack with updates as new information is learned. Timing shorter than 72 hours would likely burden CISA with incomplete, unactionable, unhelpful, and inaccurate information. Accenture commends the bill drafters for appropriately balancing the Government's need for information with the affected companies' ability to perform time-sensitive incident response. It may also be helpful to outline a periodic update cycle even if there is no new information, and then a close-out report indicating the incident is contained and remediated and signaling an end to the requirements.

- Incorporates use and liability protections consistent with CISA 2015. (There are a few provisions seemingly not carried over from CISA 2015 and we look forward to further discussion on those items.) While we endorse the regulatory requirement for incident notification, the legislation should seek to structure the Government's role as part of a partnership to improve America's cybersecurity stance, rather than a compliance exercise.

To improve the private/public collaboration that is so central to this legislation, Accenture recommends 4 points for further consideration:

- Require CISA to issue a proposed rule, rather than an interim final rule, to allow for more meaningful industry collaboration which ultimately will result in more engagement and buy-in from the private sector. This significant change to critical infrastructure entities' risk management programs and relationship with CISA warrants fulsome consultation and consideration.
- Companies would like clarification that the information they provided, if shared outside the new office, will be anonymized to protect sensitive information and build companies' confidence that the information sharing will not be used against them.
- Prior to enforcement of the notification provisions, companies would like to understand what protocols will be in place to ensure the security of the information they provide. This will go a long way toward building companies' confidence that the sensitive information provided will be protected.
- Include clear requirements for CISA to promptly share with the private sector the (anonymized) IOCs, TTPs, and threat actor profile (aka SITREP) incident information it receives pursuant to the legislation to improve response by the affected industry and improve resilience across critical infrastructure.

LETTER FROM MULTIPLE ASSOCIATIONS

August 27, 2021.

The Honorable GARY PETERS,
Chairman, Committee on Homeland Security & Government Affairs, U.S. Senate.

The Honorable MARK WARNER,
Chairman, Select Committee on Intelligence, U.S. Senate.

The Honorable BENNIE THOMPSON,
Chairman, Committee on Homeland Security, U.S. House of Representatives.

The Honorable YVETTE CLARKE,
Chairwoman, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, U.S. House of Representatives.

The Honorable ROB PORTMAN,
Ranking Member, Committee on Homeland Security & Government Affairs, U.S. Senate.

The Honorable MARCO RUBIO,
Vice Chairman, Select Committee on Intelligence, U.S. Senate.

The Honorable JOHN KATKO,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives.

The Honorable ANDREW GARBARINO,
Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, U.S. House of Representatives.

DEAR CHAIRS, VICE CHAIRMAN, AND RANKING MEMBERS: The undersigned associations, representing major sectors of the American economy, including the owners, operators, and those that support and maintain the Nation's critical infrastructure, appreciate Congress's on-going focus on cybersecurity incident reporting legislation. Our industries recognize the value of public-private collaboration facilitated by mutual sharing of actionable information on significant cybersecurity incidents and intrusions with Federal agencies. Incident Reporting legislation pending in Congress, when harmonized with the requirements of Section 2 of President Biden's Executive Order on Improving the Nation's Cybersecurity, have the potential to improve the Nation's cybersecurity posture if appropriately developed and implemented.

To ensure an effective incident reporting regime that leverages the limited resources of Federal agencies, enables regulatory compliance, provides liability protections, and advances National cybersecurity interests, we believe that policy makers in Congress should, at a minimum, follow five key principles:

Establish feasible reporting time lines of no less than 72 hours.—Cybersecurity incidents are crisis moments for victim organizations. To ensure that the Cybersecurity and Infrastructure Security Agency (CISA) and its interagency partners receive

actionable information on truly significant incidents, it is essential to give incident responders time to evaluate the intrusion to determine its impact. Shorter time lines also greatly increase the likelihood that the entity will report inaccurate or inadequately contextualized information that will not be helpful, potentially even undermining cybersecurity response and remediation efforts. A formal report on a verified, significant incident should not preclude less-fulsome notifications to CISA on a more flexible time line."

Limit reporting regulations to verified incidents and intrusions.—Incident reporting should focus on verified incidents rather than potential incidents or "near misses." Reporting verified incidents, that have been well-defined and scoped, will avoid a culture of overreporting that will strain limited incident response capacity and capabilities inside and outside the Government. It also can help ensure that information received is useful and actionable.

Limit reporting obligations to the victim organization, rather than third-party vendors or providers.—Any legislation should ensure that the reporting obligation falls only on compromised affected entities. Vendors and third-party service providers should not be required to report cybersecurity incidents to the U.S. Government that have occurred on their customers' networks and vice versa. Such a requirement would pose numerous challenges to normal business operations, including potentially forcing vendors or third parties to disclose business confidential information of that customer or breach their contractual obligations. Requiring third-parties to report incidents could even disincentivize companies from employing outside cybersecurity services to the detriment of those companies' own security and resilience.

Harmonize Federal cybersecurity incident reporting requirements.—It is imperative that Congress streamline and normalize Federal reporting requirements to ensure resources are used to combat malicious cyber threat activity, rather than customizing reports on the same incident to multiple agencies. Numerous Federal agencies currently have disparate incident reporting requirements, many of which are just being implemented. Reported information should be aggregated, anonymized, analyzed, and shared, with Government and industry, in a manner to assist in the mitigation and/or prevention of future cyber incidents.

Ensure confidentiality and nondisclosure of incident information provided to the Government.—It is imperative that any legislation have strong and transparent rules about the confidentiality of incident information that is shared with or by Federal agencies. Such rules should govern not only the dissemination of incident information with relevant interagency partners, but should specifically preclude direct or indirect use of such information by the Federal Government. These rules must be crafted to guarantee compliance with existing legal regimes, including contractual, intellectual property, and privacy obligations.

Our industries strongly believe that securing the Nation's digital assets is a shared responsibility requiring collaboration between the private sector and Federal partners. We stand ready to assist policy makers as they develop their proposals on this important National security issue.

Sincerely,

ACT|The App Association
Airlines for America (A4A)
American Fuel & Petrochemical Manufacturers
American Petroleum Institute
American Gas Association
Business Roundtable
BSA|The Software Alliance
The Computing Technology Industry Association
Consumer Technology Association (CTA)
Cyber Coalition
Cyber Threat Alliance
Edison Electric Institute
Electronic Transactions Association
Information Technology Industry Council (ITI)
Internet Association
Software & Information Industry Association
TechNet
Telecommunications Industry Association (TIA).

Ms. CLARKE. Additionally, without objection, I include in the record comments from NTCA, APPA, and NRECA.

[The information follows:]

LETTER FROM NTCA—THE RURAL BROADBAND ASSOCIATION

August 30, 2021.

The Honorable GARY PETERS,
Chairman, Committee on Homeland Security & Government Affairs, U.S. Senate.

The Honorable MARK WARNER,
Chairman, Select Committee on Intelligence, U.S. Senate.

The Honorable BENNIE THOMPSON,
Chairman, Committee on Homeland Security, U.S. House of Representatives.

The Honorable YVETTE CLARKE,
Chairwoman, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, U.S. House of Representatives.

The Honorable ROB PORTMAN,
Ranking Member, Committee on Homeland Security & Government Affairs, U.S. Senate.

The Honorable MARCO RUBIO,
Vice Chairman, Select Committee on Intelligence, U.S. Senate.

The Honorable JOHN KATKO,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives.

The Honorable ANDREW GARBARINO,
Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, U.S. House of Representatives.

DEAR CHAIRS, VICE CHAIRMAN, AND RANKING MEMBERS: Thank you for your leadership to promote the security of our Nation's critical infrastructure. NTCA—The Rural Broadband Association represents over 850 small, rural telecom providers that deliver high-speed broadband and voice service in the most remote areas of the country. These small companies serve areas where it is difficult if not impossible to make the business case for essential broadband network deployment without support from programs such as the Federal universal service fund and financing from the U.S. Department of Agriculture.

Despite their small size and razor-thin operating margins, rural carriers work hard to manage the risk presented by constant cyber attacks against their networks, and several dozen have already joined CyberShare: The Small Broadband Provider ISAC, which NTCA initiated to promote the resiliency and continuity of operation of small network operators across the United States. Nonetheless, because NTCA's members operate on thin margins, because there is presently no program that specifically supports costs incurred from cyber risk management efforts, and because there are no specific mechanisms aimed at helping smaller operators and providers in rural areas attract individuals with cyber expertise, many small carriers (which average only 30 employees overall) have limited resources to devote to such efforts. Indeed, in some cases, rural operators may have only 1–2 staff who work on cybersecurity, and even these individuals may have other functions and responsibilities as well within the enterprise. Therefore, it is essential that these staff are free to focus on securing networks rather than being consumed by the need to comply with reporting requirements.

With this as background, as you work toward passage of cyber incident reporting legislation, please consider making the reports voluntary for small businesses that own or operate critical infrastructure, or at a minimum provide extended compliance deadlines and/or other flexibility to allow small companies to make the necessary preparations. A small business exemption will also benefit those overseeing such compliance by cutting down on the number of reports to review in favor of focusing on the largest networks that are most likely to experience wide-spread cyber threats. And, in the event DHS determines that information relating to a specific cyber incident is necessary to obtain from smaller providers, the agency can always use its subpoena authority to request information from such providers.

Absent a small company exemption, these carriers will benefit at a minimum from more clearly articulated expectations and flexibility for compliance. For example, reports should only be required for verified intrusions that directly and substantially impact operations, providers should have at least five business days to report after confirming an intrusion, and providers should only be required to report intrusions to the network they control as opposed to when they merely serve as a conduit for an attack on a third party. Further, duplicative reporting should be avoided, and providers should be confident that information supplied pursuant to the new requirements will not result in litigation or regulatory action.

Thank you for considering how new cyber incident reporting requirements will impact the wide array of critical infrastructure owners and operators. We look forward to working with you on this important matter as the legislation moves forward.

Sincerely,

SHIRLEY BLOOMFIELD,
Chief Executive Officer, NTCA—The Rural Broadband Association.

STATEMENT OF THE AMERICAN PUBLIC POWER ASSOCIATION (APPA) AND THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION (NRECA)

August 30, 2021.

The Honorable GARY PETERS,
Chairman, Committee on Homeland Security & Government Affairs, U.S. Senate.

The Honorable MARK WARNER,
Chairman, Select Committee on Intelligence, U.S. Senate.

The Honorable BENNIE THOMPSON,
Chairman, Committee on Homeland Security, U.S. House of Representatives.

The Honorable YVETTE CLARKE,
Chairwoman, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, U.S. House of Representatives.

The Honorable ROB PORTMAN,
Ranking Member, Committee on Homeland Security & Government Affairs, U.S. Senate.

The Honorable MARCO RUBIO,
Vice Chairman, Select Committee on Intelligence, U.S. Senate.

The Honorable JOHN KATKO,
Ranking Member, Committee on Homeland Security, U.S. House of Representatives.

The Honorable ANDREW GARBARINO,
Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, U.S. House of Representatives.

DEAR CHAIRS, VICE CHAIRMEN, AND RANKING MEMBERS: We are writing to you regarding several introduced and draft bills that would mandate critical infrastructure sectors to report "cyber incidents" to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA). The American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) do not support additional cyber incident reporting mandates for the electric sector. We believe that the incident reporting mandates currently under discussion would burden electric utilities—especially smaller public power and cooperative utilities—with increased administrative tasks that will not materially increase their, or the country's, cybersecurity posture, but would likely divert limited resources away from securing and defending systems. That said, if Congress chooses to enact broad mandatory cyber incident reporting legislation for critical infrastructure, we agree with the principles laid out in the August 27 letter lead by the Information Technology Industry Council (ITI) and endorsed by numerous other critical infrastructure sector entities and associations.

APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. APPA represents public power before the Federal Government to protect the interests of the more than 49 million people that public power utilities serve, and the 96,000 people they employ. Public power utilities range in size, from very large to very small; approximately 67 percent of public power utilities serve communities of 10,000 people or less. They own, operate, or use generation and transmission infrastructure, as well as distribution infrastructure directly serving homes and businesses.

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power one in eight Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landscape. Electric cooperatives operate at cost and without a profit incentive. NRECA's member cooperatives include 62 generation and transmission (G&T) cooperatives and 831 distribution cooperatives. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, secure, reliable, and affordable electric service.

Combined, the members of our two groups serve close to 30 percent of the American population, which is equivalent to more than twice the population of Canada. Having provisioned such electric service for decades, our members know that a reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans. Electric utilities take very seriously their responsibility to maintain a secure and reliable electric grid. It is the only critical infrastructure sector that has mandatory and enforceable Federal regulatory standards in place for cyber and physical security (collectively known as grid security). These standards include mandatory reporting of specific cyber incidents to the Department of Energy (DOE) via an Electric Emergency Incident and Disturbance Report (OE–417) and to the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC).

Outside of these mandatory reporting standards, all electric utilities, including public power utilities and rural electric cooperatives, participate in robust voluntary information sharing systems such as the Electric Subsector Coordinating Council (ESCC) and the Electricity Information Sharing and Analysis Center (E–ISAC), as well as the Multi-State Information and Sharing Analysis Center (MS–ISAC) for public power. Most recently, electric utilities have worked closely with the National Security Council, DOE, and DHS on the "100 Day Electric Sector Industrial Control Systems Cybersecurity Sprint" to encourage and support utilities' visibility and monitoring of their industrial control system and operational technology networks, as well as automated sharing into government. It is not clear how these bills would impact these existing voluntary channels or existing or planned machine-to-machine sharing.

Our biggest concerns with the various versions of incident reporting legislation currently under discussion can be grouped into two broad categories. The legislation: (1) Treats all critical infrastructure entities as equally impactful to national security—there is no accounting for the wildly differing risk profiles of an electric utility serving millions of customers and a small distribution electric utility without an industrial control system [a type of operational technology] serving 250 customers; and (2) puts the onus on the critical infrastructure entity to share information with multiple government agencies, instead of encouraging and facilitating the sharing of information between and among agencies. While those are the two most significant concerns, we are also concerned that some proposals include heavy financial fines for failure to report within a very short time period. All of our members must be able to focus on the matter at hand in the event of a breach and should be given the flexibility to report once the crisis is understood and being managed. There has also been little discussion on how mandatory reporting requirements would impact long existing and robust voluntary information sharing systems nor on what the government's responsibility is in terms of actionable information sharing and support.

Given the concerns enumerated above, APPA and NRECA do not support including electric utilities in the mandatory cyber incident reporting legislation currently under discussion. However, if Congress chooses to move ahead with the legislation, we urge a careful and deliberative process that takes into account existing reporting mandates, appropriately tailors the mandate commensurate with the risk to national security, and adheres to the principles laid out in ITI's letter. We appreciate the openness that your staff has shown in discussions with our teams and we look forward to continuing our dialog.

Sincerely,

JOY DITTO,
President & CEO, American Public Power Association.

JIM MATHESON,
CEO, National Rural Electric Cooperative Association.

Ms. CLARKE. Again, I thank the witnesses for being here today and look forward to hearing their testimony.

[The statement of Chairwoman Clarke follows:]

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE

AUGUST 30, 2021

Good afternoon. I would like to thank the witnesses for participating in today's hearing on the Cyber Incident Reporting for Critical Infrastructure Act of 2021.

Earlier this year, this committee held a joint hearing with the Committee on Oversight and Reform to examine the SolarWinds supply chain attack.

Our oversight revealed a number of gaps in Federal authorities, policies, and capabilities that Congress must address to secure its own networks and better serve its private-sector partners.

But what stood out to me was how lucky we were that FireEye disclosed that it had been compromised.

Where we would be if they had chosen not to?

At the hearing, I asked whether we would benefit from implementing a mandatory cyber incident reporting framework.

Microsoft President Brad Smith observed that today "information is siloed" and that we need "one entity is in a position to scan the entire horizon and connect the dots between all of the attacks or hacks that are taking place."

SolarWinds President Sudhakar Ramakrishna testified: "[H]aving a single entity to which all of us can report to will serve the fundamental purpose of building speed and agility," and argued that private enterprises "should be instructed with reporting requirements and be made part of this community vision where public and private sectors can work together on addressing this issue."

At the same hearing, FireEye CEO Kevin Mandia testified about the importance of centralizing intelligence to "improve the speed at which that picture and vision will come together."

That hearing convinced me that Congress must act to ensure the Cybersecurity and Infrastructure Security Agency (CISA) receives timely cyber incident information from critical infrastructure owners and operators.

Since then, I have worked with Chairman Thompson and Ranking Member Katko to draft legislation to establish a mandatory cyber incident reporting framework at CISA and I would like to thank them both for their support in this effort.

The draft legislation we are discussing today is the product of months of dialog with Government officials and private-sector stakeholders.

I want to express my gratitude to those who worked with the committee to provide feedback on various drafts of the legislation.

We have worked hard to draft the legislation in a manner that will result in the greatest security impact for both the Federal Government and the private sector, and I am proud of the draft we have developed.

Our bill would direct CISA, after a 270-day period with mandatory windows for stakeholder consultation and comment, to issue an interim final rule describing:

- which critical infrastructure owners and operators are subject to the reporting requirement;
- which cyber incidents need to be reported;
- the mechanism for submitting reports;
- and other details necessary for implementation.

Importantly, our bill seeks to establish this new mandatory reporting program in a way that sets it apart from CISA's voluntary cyber programs by establishing a new Cyber Incident Review Office and tasking this new office with the discrete mission of receiving, aggregating, analyzing, and securing cyber incident reports.

The bill also aims to ensure that covered entities benefit from the new reporting requirement in three ways:

- First, our bill requires CISA to publish quarterly reports with anonymized findings to provide better situational awareness to its partners;
- Second, it directs CISA to identify any actionable threat intelligence that should be shared rapidly and confidentially with cyber 'first responders' to prevent or respond to other attacks; and
- Third, it requires CISA to notify private-sector entities that may have been impacted by data breaches or intrusions on Federal networks.

I am pleased with the progress we have made on this legislation, but want to be clear that our work is on-going.

We remain open to additional questions and feedback because it is important to get this right.

In recent days, I have been asked whether we would consider compliance challenges that certain small businesses may have.

I want to be clear that we do not expect all critical infrastructure owners and operators to be subject to this reporting requirement—rather we expect it to apply only to a subset.

That said, I would certainly be happy to explore whether we need to add language directing CISA to provide additional compliance assistance to small businesses that are determined to be covered entities.

I look forward to hearing additional stakeholder perspectives on the legislation today.

Before I close, I would ask unanimous consent to insert into the record a letter of support from Claroty, as well as a letter signed by 18 associations, including ITI,

the Cyber Threat Alliance, the American Gas Association, Airlines for America, and the Cyber Coalition, among others.

Additionally, I ask to enter into the record comments from Accenture, NTCA, APPA, and NRECA.

Without objection, so ordered.

With that, I thank the witnesses for being here and I yield back the balance of my time.

Ms. CLARKE. The Chair now recognizes the Ranking Member of the subcommittee, the gentleman from New York, Mr. Garbarino, for an opening statement.

Mr. Garbarino.

Mr. GARBARINO. Thank you very much, Chairwoman. I would like to thank Chairwoman Clarke for calling this important hearing today. We have a large panel before us, so, in the interest of time, I will keep my remarks brief.

There should be no question why we are here today. Over the past year, our Nation has been subject to devastating SolarWinds cyber espionage campaign, as well as the Microsoft Exchange and Pulse Secure vulnerabilities, and that is just against the Federal Government.

Our Nation's critical infrastructure has also been under attack, and the American people have begun to feel the impact. Everyone here remembers the ransomware attacks on Colonial Pipeline and JBS Meats, both of which had real-world impacts. The fact of the matter is that something here must change. We cannot allow these devastating attacks on our Nation to continue. We must ensure that CISA has the visibility it needs to help defend our Federal networks and to help our critical infrastructure owners and operators protect themselves.

I have been pleased to see our majority counterparts engage our Members in productive conversations on this, and I hope we can continue the constructive dialog here today. I am particularly interested in learning from our witnesses about how they viewed some of the key provisions of this bill and what, if any, suggestions they have for edits.

Thank you to our witnesses for being here today.

Again, thank you, Chairwoman Clarke, for your leadership on this incredibly important topic.

I yield back.

[The statement of Ranking Member Garbarino follows:]

STATEMENT OF RANKING MEMBER ANDREW GARBARINO

I would like to thank Chairwoman Clarke for calling this important hearing today. We have a large panel before us, so in the interest of time, I will keep my remarks brief.

There should be no question why we are here today: Over the past year, our Nation has been subject to the devastating SolarWinds cyber espionage campaign, as well as the Microsoft Exchange and Pulse Secure vulnerabilities, and that's just against the Federal Government.

Our Nation's critical infrastructure has also been under attack and the American people have begun to feel the impact. Everyone here remembers the ransomware attacks on Colonial Pipeline and JBS Meats, both of which had real-world impacts.

The fact of the matter is that something here must change, we cannot allow these devastating attacks against our Nation to continue.

We must ensure that CISA has the visibility it needs to help defend our Federal networks, and to help our critical infrastructure owners and operators protect themselves. I'm hopeful that this bill will help create a two-way street of information sharing between Government and industry.

I've been pleased to see our majority counterparts engage our Members in productive conversations on this topic and I hope we can continue the constructive dialog here today.

I'm particularly interested in learning from our witnesses about how they view some of the key provisions in this bill, and what, if any, suggestions they have for edits.

Thank you to our witnesses for being here today and again, thank you Chairwoman Clarke for your leadership on this incredibly important topic.

Ms. CLARKE. I thank our Ranking Member for his brevity in his opening remarks. But certainly anything that you have to add, we are all ears. I want to thank Members—to remind Members that the subcommittee will operate according to the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy regarding remote procedures. I don't see our Chairman at this moment, but I do see our Ranking Member. So I want to recognize the Ranking Member of the full committee, the gentleman from New York, Mr. Katko, for an opening statement.

Mr. KATKO. Well, I would like to thank my friend and colleague from New York, Chairwoman Clarke, for convening this important hearing today. This legislative hearing is a fantastic opportunity for our Members to learn directly from industry how they are impacted by specific provisions in the bill as well as any changes they suggest ahead of introduction.

Everyone in this hearing should recognize the urgency and precision with which we need to act. Every single day, entities, large and small, are affected by the scourge of ransomware and cyber crime. From street-level criminal gangs to nation-state actors, like Russia and China, nefarious actors target our private-sector businesses, sting local governments and Federal agencies millions of times per day. Unfortunately, many of these attempts are ultimately successful.

In order to bolster our Nation's collective defense, we must enhance our visibility across both Federal and private networks. I have been pleased with the response we have seen from industry so far. I want to thank our witnesses, not just for being here today but for their diligent work in thinking through this legislative effort.

I hope that everybody here today recognizes that our Nation's cybersecurity cannot simply be a Federal effort or a private effort, but that it is—it is and must be a joint effort. There is no doubt in my mind that cybersecurity is a deep preeminent threat to our country today. Without enhanced collaboration and visibility, we will continue to fall victim to the cowardly actors that target our Nation, our constituents, and all of us on a daily basis.

I have been pleased to work with Chairman Thompson, Chairwoman Clarke, and all our critical industry partners on this bill. I look forward to continue prioritizing major cybersecurity reforms through this committee on a bipartisan basis, including my SICI bill, which is coming up in the next few days. That is the Systemically Important Critical Infrastructure.

One of the things that drew me to this committee other than just my background in law enforcement over 20 years is the fact that there is a spirit of bipartisanship here, and there is a spirit of teamwork here that is manifesting itself again today. I mean, I commend the Chairwoman for that and Mr. Garbarino as well. But

going forward, there is a lot of other things like my Systemically Important Critical Infrastructure bill and many others that are going forward, and I hope we can have the same type of teamwork on that again as well.

So thank you, again, Ms. Clarke, for being here today, and thank you for holding this important hearing.

Thank you for the witnesses as well, and thank you, Mr. Garbarino.

I yield back.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

I would like to thank Chairwoman Clarke for convening this important hearing today.

This legislative hearing is a fantastic opportunity for our Members to learn directly from industry how they are impacted by specific provisions in the bill, as well as any changes they suggest ahead of introduction.

Everyone in this hearing should recognize the urgency and precision with which we need to act.

Every single day, entities large and small are affected by the scourge of ransomware and cyber crime.

From street-level criminal gangs to nation-state actors like Russia and China, nefarious actors target our private-sector businesses, State and local governments, and Federal agencies millions of times per day. Unfortunately, many of those attempts are ultimately successful.

In order to bolster our Nation's collective defense, we must enhance our visibility across both Federal and private networks.

I have been pleased with the response we've seen from industry so far, and I want to thank our witnesses, not just for being here today, but for their diligent work in thinking through this legislative effort.

I hope that everyone here today recognizes that our Nation's cybersecurity cannot simply be a Federal effort, or a private effort, but that it must be joint effort.

Without enhanced collaboration and visibility, we will continue to fall victim to the cowardly actors that target our Nation—our constituents—on a daily basis.

I have been pleased to work with Chairwoman Clarke, Chairman Thompson, and all our critical industry partners on this bill. I look forward to continue prioritizing major cybersecurity reforms through this committee on a bipartisan basis, including my SICI bill in the coming days.

Thank you again to our witnesses for being here today, and thank you Chairwoman Clarke for holding this important hearing.

Ms. CLARKE. I thank our Ranking Member for his comments and opening statement, and I am going to then proceed to our witnesses. Should our Chairman join us, we will take a break to hear his comments.

I now welcome our panel of witnesses. First, I would like to welcome Mr. Ronald Bushar, the senior vice president and global government CTO for FireEye Mandiant who works at the intersection of public-private incident response efforts for the types of cyber attacks we are here to discuss today.

Second, we will hear from Ms. Heather Hogsett with the Bank Policy Institute, also known as BPI, a nonpartisan research advocacy group representing the Nation's top banks. Ms. Hogsett is the senior vice president of technology and risk strategy for BITS, the technology policy division of BTI.

Third, we have Mr. John Miller, the senior vice president of policy and general counsel for the Information Technology Industrial Council, also known as ITI, which represents the world's leading information and communication technology companies.

Next, I am pleased to welcome Mr. Robert Mayer back before the subcommittee. Mr. Mayer is the senior vice president for cybersecurity and innovation at the USTelecom and chairs the Communications Sector Coordination Council.

Then, finally, we have Ms. Kimberly Denbow, the managing director of security and operations for the American Gas Association, who also co-chairs the Cybersecurity Working Group for the Pipeline Sector Coordinating Council and the oil and natural gas sector.

Without objection, the witnesses' full statement will be inserted in the record.

I now ask each witness to summarize his or her statement for 5 minutes, beginning with Mr. Bushar.

Mr. Bushar, I believe you may be muted.

STATEMENT OF RONALD BUSHAR, VICE PRESIDENT AND GOVERNMENT CTO, FIRE EYE MANDIANT

Mr. BUSHAR. Always a good start to a hearing. Apologies, Chairwoman.

Thank you, Chairwoman Clarke, Ranking Member Garbarino, and all the Members the subcommittee for the opportunity to talk with you today about this important cyber incident reporting topic.

FireEye Mandiant applauds your efforts to tackle this complex issue and appreciates the open dialog we have enjoyed with you and your staff.

Public-private partnerships are critical to the success of any cyber incident reporting or disclosure program, both in its development and ultimately in its execution. My comments for today's hearing will focus primarily on the major tenets and benefits of the cyber incident reporting framework.

But before I turn to this specific topic, let me share some background on myself and my company to establish context for my narrative and statements today.

I started my career in the United States Air Force as an officer in what was at the time termed information warfare. For more than 20 years, I have worked in cyber defense operations, cybersecurity consulting, and incident response services in both the Government and commercial sectors, including time at the U.S. Department of Justice.

In my current role at FireEye Mandiant, I lead a global team of cyber experts who deliver our capabilities and security functionality and solutions to protect critical missions, infrastructure, and National security interests world-wide.

As I testify today, FireEye Mandiant employees are on the front lines of a cybersecurity battle, really, responding to over 150 active computer intrusions at some of the largest organizations and companies in the world. Over the last 17 years, we have responded to tens of thousands of security incidents. It is unfortunate, but we receive calls almost daily from organizations that have suffered a cybersecurity breach. For each security incident we respond to, it is our objective to determine what happened and what organizations can do to avoid similar incidents in the future. We also maintain over 200 intelligence professionals and analysts located in more than 20 countries, speaking over 30 languages, who pursue attribu-

tion, identification, and more detailed information about threat actors, their motivations, and intents.

FireEye Mandiant is encouraged by the draft legislation the subcommittee has developed to improve cyber incident reporting. The bill is a positive step forward in achieving important, long-term goals of enabling early detection of malicious cyber attacks. It would also enhance the Federal Government situational awareness to better partner with and assist private-sector entities that become cyber attack victims. This whole-of-community approach is critical to increasing capacity and to prevent future cyber attacks as well as to drive ultimately, we believe, deterrence in this space.

Any legislation on this matter should take into consideration the evolving cyber threat landscape; the increasingly sophisticated tactics, techniques, and procedures used by adversaries; and lessons learned from existing voluntary information-sharing models as established by the Cybersecurity Information Sharing Act of 2015. Simply put, any reporting framework must be agile and include opportunities for the Federal Government to pivot or adjust its reporting requirements to keep pace with the threat landscape and actor and adversary actions and activity.

The U.S. Government should consider a Federal incident reporting program that goes beyond voluntary sharing of threat indicators as authorized under the 2015 legislation. It should also include mandatory disclosure requirements for cyber incidents. Major tenets of such a program should safeguard the protection and integrity of electronic and other types of data; ensure confidential sharing; encourage entities to adapt, recognize cybersecurity standards and practices with a minimum threshold; provide greater incentives for private-sector entities, including liability protections and statutory privilege to not be disclosed in civil litigation; protect privacy and civil rights; and provide outreach and technical assistance to entities that do not have cybersecurity expertise or capabilities.

FireEye Mandiant believes that strong cyber community protection is predicated on several key concepts, and lawmakers should consider the following additional components that we believe would constitute a robust and ultimately successful cyber incident reporting program.

No. 1, reporting requirements should account for two key outcomes: Timely and relevant reporting of critical intelligence to relevant Government authorities for assessment, correlation, and decision support; and, No. 2, reasonable latitude for the victim to determine nature, extent, and potential impact of a breach or attack. In the first instance, the timeliness and quality of the data reported to the Government will largely determine how effective the response to and disruption of the attack will ultimately be.

In the second instance, cyber attacks are often complex and require sophisticated analysis to fully understand the scope of compromise. Victims require support from external firms to fully analyze a breach and will likely be dealing with other business impacts and crisis management activities during such activities.

Allowing for a reasonable amount of time to properly assess the situation before requiring reporting will limit false positives and redundant or contradictory information and prevent unnecessary data collection on the part of CISA. FireEye Mandiant encourages

lawmakers to consider harmonizing reporting requirements with existing Federal acquisition regulations and standards to provide for consistent and streamlined regime that simplifies business processes and ultimately encourages and streamlines compliance as well.

Second, FireEye Mandiant strongly believes in the concept of a public-private partner approach to cybersecurity. Unlike most other domains at risk, cyber attacks and cyber crimes are almost always predicated on the use of—use traversal or compromise of privately-owned infrastructure, even when the attacks are focused on Government or National security assets. The private sector, especially critical infrastructure sector businesses, is both a key component over all National cyber resiliency and a key source of intelligence on our adversaries' capability, intent, and activities in cyber space. Over the past decade, many Federal agencies, including CISA, the FBI, the United States Secret Service, and the National Security Agency, have built strong partnerships with key cybersecurity and critical infrastructure organizations through voluntary programs outreach and support.

While we recognize that much more needs to be done, without these efforts and support functions, many private-sector cyber attacks would have likely remained undetected for much longer and would have been much more severe. Under a new cyber incident reporting program, these trusted relationships and partnerships must be strengthened and enhanced to advance our common goals in reducing the frequency and severity of cyber attacks.

No. 3, a reporting program must encourage cooperation and strengthen trust between public and private-sector entities. A regulatory-based approach or a regime that focuses on punitive actions rather than mutual benefits would be counter to the goal of creating a strong National partnership model to counter the increasing cyber threats we are facing.

As previously suggested, although mandatory reporting is necessary, the focus should be on supporting organizations to achieve compliance, not punishment for noncompliance. Fines and other financial or legal punishments do not properly reflect the truth that, barring gross negligence or willful misconduct, organizations that suffer cyber attacks are victims of a crime. Mechanisms to compel collection of critical information, when necessary, such as subpoenas, better align to the general concept of criminal investigation and response.

Fourth, information sharing must be bidirectional. An incident reporting framework should allow for a consistent flow of two-way information sharing between public and private sectors to help maximize the ability to resolve and consider attribution. Organizations that invest significant effort into collecting, analyzing, and sharing cyber attack technical information require feedback on the usefulness and value of what they provided. They also benefit from data that can be only provided by the U.S. Government to enhance their own security posture and to help hone their threat detection in response functions.

Finally, I would like to highlight several clear benefits of broader security incident reporting and bidirectional information sharing. Timely reporting of incidents within and across sectors allow for

early detection of large, sophisticated cyber campaigns that have the potential for significant impacts to critical infrastructure or National security implications. Technical indicators, along with contextual information, provide a more robust data set to conduct faster and more accurate attribution in adversary intent. This type of analysis is critical in formulating the most impactful response to such attacks and to do so in a time frame that has a high probability of successful countermeasures or deterrence.

On behalf of FireEye Mandiant, thank you for the opportunity to testify before the subcommittee today. We are committed to working with our public and private-sector partners to safeguard the Nation from cyber attacks by sharing cyber threat information, lessons learned, and best practices, including through the newly-established Joint Cyber Defense Collaborative at CISA. We stand ready to work with you and other interested parties to devise effective solutions to deter malicious behavior in cyber space and to build a better resiliency into our networks and ultimately improve and enhance the security and well-being of all Americans.

Thank you, and I look forward to your questions today.

[The prepared statement of Mr. Bushar follows:]

PREPARED STATEMENT OF RONALD BUSHAR

SEPTEMBER 1, 2021

INTRODUCTION

Thank you Chairwoman Clarke, Ranking Member Garbarino, and all the Members of the subcommittee, for the opportunity to talk with you today about the importance of cyber incident reporting. FireEye Mandiant applauds your efforts to tackle this complex issue and appreciates the open dialog we have enjoyed with you and your staff—public-private partnerships are critical to the success of any cyber incident reporting or disclosure program—both in its development and execution.

BACKGROUND

My comments for today's hearing will focus primarily on the major tenets and benefits of a cyber incident reporting framework. Before I turn to this specific topic, let me share some background on myself and my company to establish context for my narrative.

I started my career in the United States Air Force as an officer in the Information Warfare Aggressor Squadron. For more than 20 years, I have worked in cyber defense operations, cybersecurity consulting, and incident response services in both the Government and commercial sectors, including the Justice Department. In my current role at FireEye Mandiant, I lead a global team of cyber experts who deliver our unique platform of innovative security program capabilities and solutions to protect critical missions, infrastructure, and National security interests world-wide.

As I testify today, FireEye Mandiant employees are on the front lines of the cyber battle, currently responding to over 150 active computer intrusions at some of the largest companies and organizations in the world. Over the last 17 years, we have responded to tens of thousands of security incidents. It is unfortunate, but we receive calls almost daily from organizations that have suffered a cybersecurity breach. For each security incident we respond to, it is our objective to determine what happened and what organizations can do to avoid similar incidents in the future. We also maintain over 200 intelligence analysts, located in more than 20 countries, speaking over 30 languages, who pursue attribution and identification of the threat actors via research and sources.

INCIDENT REPORTING FRAMEWORK

FireEye Mandiant is encouraged by the draft legislation the subcommittee has developed to improve cyber incident reporting. The "Cyber Incident Reporting for Critical Infrastructure Act of 2021" is a positive step forward in achieving important long-term goals of enabling early detection of malicious cyber attacks. It would also enhance the Federal Government's situational awareness to better partner with and

assist private-sector entities that become cyber attack victims. This "whole-of-community" approach is critical to increasing capacity to prevent and deter future cyber attacks.

Any legislation on this matter should take into consideration the evolving cyber threat landscape; the increasingly sophisticated tactics, techniques, and procedures used by adversaries; and lessons learned from existing voluntary information-sharing models, as established by the "Cybersecurity Information Sharing Act of 2015." Simply put, any reporting framework must be agile and include opportunities for the Federal Government to pivot or adjust its reporting requirements to keep pace with the threat environment and bad actors.

The U.S. Government should consider a Federal incident reporting program that goes beyond voluntary sharing of threat indicators as authorized under the 2015 law—it should also include mandatory disclosure requirements for cyber incidents. Major tenets of such a program should:

- Safeguard the protection and integrity of electronic and other types of data.
- Ensure confidential sharing.
- Encourage entities to adopt recognized cybersecurity standards and practices with a minimum threshold.
- Provide greater incentives for private-sector entities, including liability protections and statutory privilege to not be disclosed in civil litigation (e.g., confidentiality obligations).
- Protect privacy and civil rights.
- Provide outreach and technical assistance to entities that do not have cybersecurity expertise or capabilities.

FireEye Mandiant believes that strong cyber community protection is predicated on several key concepts. Lawmakers should consider the following additional components that we believe would constitute a robust and ultimately successful cyber incident reporting program:

Establish reasonable and effective time lines for reporting.

Reporting requirements should account for two key outcomes: (1) Timely and relevant reporting of critical intelligence to relevant Government authorities for assessment, correlation, and decision support, and (2) reasonable latitude for the victim to determine the nature, extent, and potential impact of a breach. In the first instance, the timeliness and quality of the data reported to the Government will largely determine how effective the response to and disruption of the attack will be. In the second instance, cyber attacks are often complex and require sophisticated analysis to understand the full scope of compromise.

Victims require support from external firms to fully analyze a breach and will likely be dealing with other business impacts and crisis management activities. Allowing for a reasonable amount of time to properly assess the situation before requiring reporting will limit false positives, redundant or contradictory information, and prevent unnecessary data collection.

FireEye Mandiant encourages lawmakers to consider harmonizing reporting requirements with existing Federal acquisition regulations and standards to provide for a consistent and streamlined regime that simplifies business processes and compliance.

Preserve existing trusted relationships and partnerships.

FireEye Mandiant strongly believes in the concept of a public-private partner approach to cybersecurity. Unlike most other domains of risk, cyber attacks and cyber crime are almost always predicated on the use, traversal, or compromise of privately-owned infrastructure, even when the attacks are focused on Government or National security assets. The private sector, especially critical infrastructure sector businesses, is both a key component of overall National cyber resiliency and a key source of intelligence on our adversaries' capabilities, intents, and activities in cyber space.

Over the past decade, many Federal agencies, including the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the U.S. Secret Service, and the National Security Agency have built strong partnerships with key cybersecurity and critical infrastructure organizations through voluntary programs, outreach, and support. While we recognize that much more needs to be done, without these efforts and support functions, many private-sector cyber attacks would have likely remained undetected for much longer and would have been much more severe. Under a new cyber incident reporting program, these trusted relationships and partnerships must be strengthened and enhanced to advance our common goals of reducing the frequency and severity of cyber attacks.

Ensure compliance is non-punitive.

A reporting program must encourage cooperation and strengthen trust between the public and private sector. A regulatory-based approach or a regime that focuses on punitive actions rather than mutual benefits would be counter to the goal of creating a strong National partnership model to counter the increasing cyber threats we are facing.

As previously suggested, although mandatory reporting is necessary, the focus should be on supporting organizations to achieve compliance, not punishment for non-compliance. Fines and other financial or legal punishments do not properly reflect the truth that, barring gross negligence or willful misconduct, organizations that suffer a cyber attack are victims of a crime. Mechanisms to compel collection of critical information when necessary, such as subpoenas, better align to the general concept of criminal investigation and response.

Require information to flow back into the community.

Information sharing must be bi-directional. An incident-reporting framework should allow for a consistent flow of two-way information sharing between the public and private sectors to help maximize the ability to resolve and consider attribution. Organizations that invest significant effort into collecting, analyzing, and sharing cyber attack technical information require feedback on the usefulness and value of what they have provided. They also benefit from data that can only be provided by the Government to enhance their own security posture and help to hone their threat detection and response functions.

BENEFITS

Finally, I would like to highlight several clear benefits to broader cyber incident reporting and bi-directional information sharing. Timely reporting of incidents, within and across sectors, allows for earlier detection of large, sophisticated cyber campaigns that have the potential for significant impacts to critical infrastructure or National security implications.

Technical indicators, along with contextual information related to attacks, provide a more robust dataset to conduct faster and more accurate attribution and adversary intent. This type of analysis is critical in formulating the most impactful response to such attacks and to do so in a time frame that has a higher probability of successful countermeasures or deterrence.

Cyber incident information also allows for cross-correlation and collaboration with international partners, thereby enabling a multilateral response to state-sponsored or state-sanctioned cyber criminals that often originate overseas and travel through an allied nation's infrastructure.

Last, robust and centralized collection of incident information provides the Government with a much more accurate cyber risk picture and enables more effective and efficient investments and support before, during, and after major cyber attacks.

CONCLUSION

On behalf of FireEye Mandiant, thank you for the opportunity to testify before the subcommittee. We are committed to working with our public and private-sector partners to safeguard the Nation from cyber attacks by sharing cyber threat information, lessons learned, and best practices, including through the newly-established Joint Cyber Defense Collaborative at the Cybersecurity and Infrastructure Security Agency.

We stand ready to work with you and other interested parties to devise effective solutions to deter malicious behavior in cyber space and to build better resiliency into our networks. I look forward to your questions.

Ms. CLARKE. All right.

Thank you, Mr. Bushar, for your expert testimony here today.

I would like to acknowledge that we have been joined by the gentleman from Mississippi, the Chairman of our full committee, Mr. Thompson, who will be submitting his opening statement for the record, but I wanted to acknowledge his presence.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

SEPTEMBER 1, 2021

Good afternoon. I want to thank Chairwoman Clarke and Ranking Member Garbarino for holding this important legislative hearing to discuss the Cyber Incident Reporting for Critical Infrastructure Act of 2021.

Establishing a mandatory cyber incident reporting framework at CISA has been a priority for the Homeland Security Committee since last Congress.

I applaud Chairwoman Clarke for engaging with stakeholders and working so hard to get the language right.

I look forward to continuing to work with her as she continues to refine the text.

I would also like to thank Ranking Member Katko for his support of this important legislation.

For a decade and a half, I have served as either Chairman or Ranking Member of this committee.

Over the years, there has been an evolution in thinking about how closely the public and private sector need to collaborate to protect our Nation's critical infrastructure.

I have seen the Federal Government struggle to find the right way for critical infrastructure owners and operators to share security information with the Government and to zero in on how to turn that information into an actionable security product.

The Cybersecurity Information Sharing Act of 2015 was the product of extensive negotiations on the part of both Government and industry.

When the legislation was finally enacted into law, we had high expectations that it would spur timely sharing and enhance our Nation's cybersecurity posture.

But the 2015 bill did not fully deliver.

There was reluctance among many in the private sector to share information with the Department.

And, for its part, the Department struggled to turn what data it did get into something the private sector could use to drive down risk.

It focused too much on the volume of indicators shared and not enough on the quality of the information.

For 6 years, this committee has engaged with the Department and stakeholders to try to correct course, but over time it has become clear that we need a new approach.

Last Congress, former Subcommittee Chair Cedric Richmond offered an amendment to the National Defense Authorization Act that would establish a mandatory cyber incident reporting framework at the Cybersecurity and Infrastructure Security Agency.

It was included in the House-passed package but was stripped during conference negotiations with the Senate.

Since then, a series of high-profile, high-consequences cyber incidents over the past year, have made it clear we need to take urgent action to improve the way the private sector shares information with the Government.

As Chairwoman Clarke said in her opening statement, the text we are discussing today is the product of months of stakeholder engagement and bipartisan negotiations to fine tune the bill.

And we are here today to further refine the legislation to ensure it serves the purposes of the Federal Government and will result in security benefits to covered entities.

I am committed to getting this framework right and across the finish line this Congress.

I thank the witnesses for being here today, and I look forward to their testimony.

Ms. CLARKE. But I now recognize Ms. Hogsett to summarize her statement for 5 minutes.

STATEMENT OF HEATHER HOGSETT, SENIOR VICE PRESIDENT, TECHNOLOGY & RISK STRATEGY FOR BITS, BANK POLICY INSTITUTE

Ms. HOGSETT. Thank you.

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 at the Bank Policy Institute.

BPI is a nonpartisan policy, research, and advocacy organization, representing the Nation's leading banks. Through our technology division, BITS, we work with our member banks as well as other leading financial institutions on cyber risk management and critical infrastructure protection as well as fraud reduction, regulation, and innovation. I also serve as policy committee co-chair for the Financial Services Sector Coordinating Council, which coordinates across the financial sector and with Government partners to enhance security and resiliency.

On behalf of BPI's member firms, we greatly appreciate this committee's leadership on cybersecurity and critical infrastructure protection. We also appreciate the work of the committee on the Cyber Incident Reporting for Critical Infrastructure Act of 2021, which is focused on addressing the urgent need for Government and critical infrastructure to share cyber information to improve awareness of cyber threats and better inform our collective ability to mitigate and respond to them.

Banks and other financial institutions have had legal and regulatory requirements for cybersecurity and incident reporting for more than 20 years. In addition to required regulatory reporting, financial firms have made significant investments to protect the industry, developing high-trust collaboration centers to improve resilience of individual firms and across the broader financial system, through digital infrastructure, comprehensive use of security tools, exercise programs, and extensive training.

Based on past experience, we are encouraged to see that the current draft bill includes five key elements that we believe are vital to achieving our shared goal of protecting the Nation's critical infrastructure. First, the bill appropriately tailors the scope of incidents that should be reported to those that could cause actual harm. This will ensure CISA receives accurate and useful data to help achieve its goal of greater situational awareness.

Second, the time line for reporting of no earlier than 72 hours after confirmation an incident has occurred strikes the right balance to allow a firm sufficient time for investigation and implementation of response measures while reporting timely, accurate, 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 investigation response and remediation, rather than completing compliance paperwork.

Third is the need to ensure harmonization with existing requirements. For already-regulated critical infrastructure sectors, it is vital to ensure new requirements are harmonized with existing laws and regulations. Financial institutions are regularly examined for their cybersecurity operations and compliance with reporting requirements and may be subject to penalties and other enforcement mechanisms for deficiencies or failures to comply.

The bill currently includes helpful provisions to require CISA to coordinate with other agencies and regulatory authorities to streamline reporting requirements.

The bill also builds off the Cybersecurity and Information Sharing Act of 2015. We support the committee clearly incorporating

the key definitions and protections already created by the CISA Act for private firms sharing information with Government. Any bill that seeks to mandate cyber information sharing should incorporate these protections, and we appreciate that you have clearly defined that in your bill.

Finally, the bill addresses the need to help companies understand if their data has been compromised by an attack on a Government system. While the SolarWinds attack targeted several Federal agencies, it also impacted a much broader swath of entities, including critical infrastructure companies.

Financial services firms are required to share sensitive and confidential information with regulators and other Government agencies that, if breached, could pose risks to the institution and its customers. To this end, the bill includes language to address this need for greater transparency.

In closing, I would note that there is an additional area that we would like to continue working with you on, and that is around the need for improvements to bidirectional information sharing and collaboration. Current information sharing is often one-sided from Government—from industry to Government, and the alerts and warnings industry receives from Government are often delayed, limiting their usefulness.

At CISA, along with intelligence from law enforcement agencies, strengthened 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.

Again, thank you for your leadership on cybersecurity and your thoughtful approach to crafting this legislation. We look forward to continuing to work with this committee, and I am happy to answer any questions you may have.

[The prepared statement of Ms. Hogsett follows:]

PREPARED STATEMENT OF HEATHER HOGSETT

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 co-

ordinating 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.
- *Time Line*.—The time line 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 on-going 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 sec-

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

tors 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.

Time Line

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, time lines, 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 on-going 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 Time Line*.—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 on-going 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 Time Line*.—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 on-going regulatory oversight.

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 Time Line*.—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."

---

[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=I5be30d2007-f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&context-Data=(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."

- *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 European Union 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 European Union has both mandatory security mandates on Digital Service Providers and stricter reporting requirements on DSPs.[10] The European Union 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 Time Line*.—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 E.U. 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 Time Line*.—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 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.

Mr. MAYER. Chairwoman, I believe you may be muted.

Ms. CLARKE. I think I was on mute. Did everyone hear me?

Mr. MAYER. No.

Ms. CLARKE. I am sorry about that. They always catch you, don't they?

---

[9] Personal data is under GDPR here: *https://gdpr-info.eu/art-4-gdpr/*.

[10] Essential Services are defined by the European Union 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*.

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

Let me thank Ms. Hogsett for her expert testimony here today. I now recognize Mr. Miller to summarize your statement for 5 minutes.

STATEMENT OF JOHN S. MILLER, SENIOR VICE PRESIDENT OF POLICY, AND GENERAL COUNSEL, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

Mr. MILLER. Thank you.

Chairs Clarke and Thompson, Ranking Members Garbarino and Katko, distinguished Members of the subcommittee, on behalf of the Information Technology Industry Council, or ITI, thank you for the opportunity to testify today on the Cyber Incident Reporting for Critical Infrastructure Act of 2021.

ITI is a global policy and advocacy organization representing 80 of the world's leading ICT companies. I lead ITI's trust data and technology policy team, including our work on cybersecurity globally. As the current vice chair of the Information Technology Sector Coordinating Council and co-chair of the ICT Supply Chain Risk Management Task Force, I have significant experience partnering with CISA on efforts to improve cyber supply chain and critical infrastructure security and welcome your interest on this important topic. I would also like to thank you and your staffs for the thoughtful and collaborative approach you have taken with stakeholders while drafting this legislation.

If narrowly scoped and carefully crafted, we believe that an incident reporting regime can help improve the Nation's cyber resilience and security by increasing situational awareness across Government and critical infrastructure and driving more effective operational collaboration in response to significant incidents.

We commend the subcommittee for its leadership on this issue and commitment to developing an effective and efficient cyber incident reporting regime, and we appreciate the Act leads many of the details to be worked out through a rule-making process prioritizing CISA engagement with stakeholders.

Developing an effective and efficient incident reporting regime while at the same time preserving the partnership and collaborative model that is central to CISA's mission are both important goals. Just last month, ITI published policy principles for cyber incident reporting which are attached to my written testimony and I encourage the subcommittee to consider in full.

ITI also led a multi-association letter to Congress sent last Friday stressing several issues that any incident reporting legislation should address. I will focus the balance of my time on five key recommendations included in both our policy principles and the letter.

First, we recommend any legislation allow for feasible reporting time lines commensurate with incident severity levels but of no less than 72 hours. Ensuring time lines are feasible is important for several reasons, including allowing entities sufficient time to determine what has occurred and ensuring an incident is properly contextualized, upholding cybersecurity while an entity investigates an incident and to align with global best practices. We appreciate the Act makes clear CISA may not require reporting earlier than 72 hours after an entity confirms an incident has occurred.

Second, we recommend any legislation maintain appropriate confidentiality, nondisclosure, and liability protections. We welcome the act's intent to extend liability protections and FOIA exemptions from the CISA 2015 information sharing legislation to reports provided pursuant to the Act but note the language of CISA 2015 may need to be updated to align with the specific categories of incident reporting information that are ultimately required by the pending rule.

Further, the Act should define clear confidentiality and privacy requirements regarding the use of shared information, including to require that any information disseminated to interagency partners is scrubbed of the providing entity's identifying information.

Third, we urge Congress to harmonize existing regulatory reporting requirements to ensure companies are able to efficiently report incidents and not subject to contradictory or duplicative reporting requirements that may hamper notification. We appreciate the Act directs CISA to consider existing regulatory requirements and work with relevant regulatory authorities and recommend adding language clarifying that CISA should leverage existing channels to collect incident information whenever possible, including active interfaces with the FBI, SEC, and financial sector regulators to truly lessen the regulatory burden.

Fourth, we recommend any legislation establish appropriate reporting thresholds and limit reporting to verified incidents. The act's inclusion of minimum thresholds for reporting a covered incident built on a risk-based analytical model and its focus on verified incidents, as opposed to near misses hit the mark. However, there is ambiguity in the minimum threshold language that could be resolved through the concept of an incident categorization matrix which could more accurately determine the severity of actual harm posed by incidents, enabling finer prioritization and more precise reporting.

Finally, we maintain that reporting obligations in any legislation should fall only on impacted entities, not on vendors or third-party service providers. An incident reporting requirement with a broader scope could disrupt normal business operations, including potentially forcing vendors or third parties to disclose business confidential information of impacted customers or breach their contractual obligations and result in flooding CISA with multiple, duplicative reports diverting limited resources away from cyber incident response.

Thank you again for the opportunity to testify today. I look forward to your questions.

[The prepared statement of Mr. Miller follows:]

PREPARED STATEMENT OF JOHN S. MILLER

SEPTEMBER 1, 2021

Chairwoman Clarke, Ranking Member Garbarino, and distinguished Members of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the House Committee on Homeland Security, thank you for the opportunity to testify today. My name is John Miller, senior vice president of policy and general counsel at the Information Technology Industry Council (ITI).[1] I lead ITI's Trust, Data, and Technology team, including our work on cybersecurity policy globally, and I have

[1] See ITI membership list at: *https://www.itic.org/about/membership/iti-members.*

deep experience working on public-private security initiatives in the United States, including currently serving as co-chair of the Cybersecurity and Infrastructure Security Agency (CISA)-sponsored Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM Task Force), and as vice chair of the Information Technology Sector Coordinating Council (ITSCC), the principal IT sector partner to CISA on critical infrastructure protection and cybersecurity policy. I am honored to provide ITI's perspective on the important topic of cyber incident reporting and the legislation the subcommittee is considering today.

ITI represents the world's leading information and communications and technology (ICT) companies. We promote innovation world-wide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, and other internet and technology-enabled companies that rely on ICT to evolve their businesses. Cybersecurity is rightly a priority issue for governments and our industry, and we share the common goals of improving cybersecurity, protecting the privacy of individuals' data, and maintaining strong intellectual property protections. Further, our members service customers across all levels of government and the full range of global industry sectors, such as financial services, health care, and energy. We thus acutely understand the importance of cybersecurity as not only a global business imperative for companies and customers alike, but as critical to our collective security. As a result, our industry has devoted significant resources, including expertise, initiative, and investment in cybersecurity efforts to create a more secure and resilient internet ecosystem.

The SolarWinds compromise and the latest wave of damaging ransomware attacks, along with other recent cyber attacks, serve as an important reminder that the cyber threat landscape is constantly evolving and that we need innovative new policy ideas to help confront the emergence of new threats. We have seen policy makers increasingly consider incident reporting as a potentially appropriate tool to improve Government's ability to leverage its resources toward not only helping victim organizations recover from incidents, but ideally to help protect others from similar threats or vulnerabilities. If narrowly scoped and carefully crafted, we believe that an incident reporting regime can help improve the Nation's digital resilience and security.

We commend the subcommittee for its leadership on this issue and its commitment to developing an effective and efficient cybersecurity incident reporting regime. As a general matter, we appreciate that the Cyber Incident Reporting for Critical Infrastructure Act of 2021 (hereafter "the Act") leaves many of the details to be worked out through a rule-making process in which CISA solicits feedback from stakeholders, as opposed to laying out stringent requirements in statute.

Just last month ITI published our Policy Principles for Cyber Incident Reporting in the United States (hereafter "Policy Principles") to help inform on-going efforts domestically, which is attached as an Appendix to my testimony (see Appendix A). We make ten recommendations to policy makers in the Policy Principles, all of which we encourage the subcommittee to take into account as it considers incident reporting legislation and works on further refinements to the Act. We also led a recent multi-association letter to Congress stressing several key areas aligned with our principles that should be included in any incident reporting legislation.[2]

After briefly providing important context to help inform the current security incident reporting debate, I will focus the bulk of my written testimony on five recommendations that were included in our Policy Principles, as well as the above-referenced multi-association letter, including: (1) Establishing feasible reporting time lines of no less than 72 hours; (2) ensuring appropriate confidentiality, nondisclosure, and liability protections; (3) limiting reporting to the impacted organization, rather than third-party vendors or providers; (4) harmonizing Federal cybersecurity incident reporting requirements; and (5) limiting reporting to verified intrusions and incidents. My testimony concludes by stressing the importance of seizing the opportunity to develop a workable security incident notification regime while preserving CISA's collaborative role with private-sector partners.

I. SECURITY INCIDENT REPORTING IN CONTEXT

Devising a successful cybersecurity incident reporting regime requires an understanding of adjacent and overlapping cybersecurity information sharing and data

[2] Letter available here: *https://www.itic.org/documents/cybersecurity/MultiassnLetter-SecurityIncidentReporting-08.27.2021FINALFINAL.pdf*.

breach notification measures, as well as the evolving global policy debates regarding this issue.

a. Clarifying and Understanding Terms Can Help Efficiently Harmonize Requirements

In thinking about security incident reporting, it is essential that policy makers and other stakeholders recognize that it is distinct from other concepts with which it is often confused: Primarily, data breach notification and cybersecurity threat information sharing. Security incident notification such as that contemplated by the Act requires organizations to report on the details of a cybersecurity incident that has already occurred to help increase visibility into such events; data breach notification requirements are also triggered post-incident but relate specifically to reporting details regarding the unauthorized access to or disclosure of personally identifiable information or other sensitive data for privacy purposes. Importantly, policy makers should consider that in some instances a single incident could trigger both types of notification and reporting requirements and should consider how to reduce potential inefficiencies in reporting. Both of the preceding two concepts are distinct from cyber threat information sharing, which refers to the proactive sharing of threat information to help all entities better understand cybersecurity threats and take steps to prevent future cyber attacks. Given the subcommittee's intent to leverage the Cybersecurity Information Sharing Act of 2015 (CISA 2015) in the security incident reporting context, including to extend CISA 2015's liability protections, it is critical to understand both the differences and similarities between the two concepts. We further elaborate on all three of these concepts in our Policy Principles (see Appendix A).

b. The Global Policy Debate Can Help Inform U.S. Policy

ITI is an active participant in policy conversations on cybersecurity incident reporting globally. Indeed, it is not only the United States that is considering implementing a mandatory incident reporting regime. Europe, in the proposal for a revised Network and Information Systems Directive (NIS 2 Directive), as well as Australia, in their Security Legislation Amendment (Critical Infrastructure) Bill of 2020, which revises the Security of Critical Infrastructure Bill of 2018, are contemplating mandatory incident reporting as a way to increase Government visibility into cybersecurity events.[3] We have similarly encouraged both the European Commission and the Australian Government to adopt the principles discussed in my testimony and referenced in ITI's Policy Principles.[4] These global efforts are relevant and important to consider as Congress seeks to develop legislation that establishes a mandatory incident reporting regime, as the subcommittee acknowledges in the Act by requiring the CISA director to align the reporting requirements CISA develops with international standards.

II. RECOMMENDATIONS FOR A SUCCESSFUL SECURITY INCIDENT NOTIFICATION APPROACH

ITI's Policy Principles set forth ten recommendations that policy makers should incorporate to develop and implement a successful cybersecurity incident notification regime. While all of these recommendations are important, my testimony focuses on five key recommendations below. Please refer to the Policy Principles at annex for the full set of recommendations.

a. Establish Feasible Reporting Time Lines

In our Policy Principles, we recommend that any legislation allow for reasonable reporting time lines commensurate with incident severity levels, but of no less than 72 hours. Ensuring that time lines are feasible is important for a number of reasons, including:

Allowing companies sufficient time to determine what has occurred.—Requiring an entity to report an incident on a shorter time line may be insufficient for companies to determine the nature of the issue—is it a cyber attack or is it merely a network

---

[3] Security Legislation Amendment (Critical Infrastructure) Bill of 2020, first reading text, available here: *https://parlinfo.aph.gov.au/parlinfo/download/legislation/bills/r6657_first-reps/toc_pdf/20182b01.pdf;fileType=application%2Fpdf;* proposal for NIS 2 Directive text, available here: *https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.*

[4] ITI Comments on NIS 2 Directive, available here: *https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems/F2004660_en;* ITI Comments on Security Legislation Amendment Bill of 2020, available here: *https://www.aph.gov.au/DocumentStore.ashx?id=04c36c84-3067-4ffb-bec2-53c780079a02&subId=701444.*

outage? In the early hours following the discovery that something anomalous has occurred, our companies are focused on figuring out what has happened and developing a response plan. Indeed, the primary initial focus for companies should be on identifying and responding to malicious activities, rectifying the problem, and ensuring (or restoring) business continuity.

Upholding cybersecurity while a company investigates the issues.—A shorter time line for reporting may also serve to undermine cybersecurity, in that such a requirement can expose information about an incident before a patch is applied or operations are restored, making operators and their customers vulnerable to additional attacks by hackers.

Ensuring resources are leveraged appropriately and ensuring the incident is properly contextualized.—Requiring reporting on a shorter time line may also divert limited Government resources away from addressing incidents that are actually having a significant impact. If entities are required to report incidents before they have the opportunity to verify what has occurred, an agency such as CISA runs the risk of being inundated with reports that do not offer meaningful information or otherwise lack the appropriate context. It is incredibly difficult to narrow the scope on the back end when an agency is sifting through reports trying to retroactively determine what is important. Instead, the focus should be on only requiring incident reporting of severe and significant attacks that cause actual disruption or loss and that include specific parameters.

Aligning with global best practices.—A 72-hour time line also aligns with global best practices, which we believe is of great importance to facilitating interoperability of approaches. For example, the German IT Security Act and various state-level notification requirements in the United States allow for a reporting window of 72 hours.[5] Article 33 of the EU's General Data Protection Regulation (GDPR) also states that in the case of a personal data breach, impacted companies shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority.

We appreciate that as currently drafted, Subsection (d)(5) of the Act makes clear that the CISA director may not require reporting any earlier than 72 hours after an entity has confirmed that an incident has occurred. We also stress that requiring a formal report on a verified, significant incident should not preclude an impacted organization from voluntarily providing less-fulsome notifications to CISA on a more flexible time line. Indeed, should an entity want to notify CISA of an event before a formal report is finalized and submitted, it should have the ability to do so. Section (f) of the Act seems to contemplate such a layered approach, which would allow for an initial voluntary, preliminary notification to CISA, with more substantial reporting coming once the impacted organization has confirmed that an incident reached the severity metrics established in the IFR called for by the Act.

b. Maintain Appropriate Confidentiality, Nondisclosure, and Liability Protections

In ITI's Policy Principles we also stress the importance of ensuring the confidentiality of information provided in incident reports. It is imperative to have strong and transparent rules about the confidentiality of incident information that is shared with or by Federal agencies in order to cultivate trust in the process and between the private and public sectors. Such rules should govern not only the dissemination of incident information with relevant interagency partners but should specifically preclude direct or indirect regulatory use of such information. Such rules should additionally govern how unclassified information on a specific incident is further shared with the U.S. Government, other governments, and with nongovernmental entities. These rules must be crafted to guarantee compliance with existing legal regimes, including contractual and privacy obligations.

This is an area that we believe could be strengthened in the Act. Indeed, it is our view that the language surrounding how the information provided in an incident report can be used based on the Act's Subsection (e): (1) Does not provide a sufficient level of confidentiality for industry partners. The language lays out broad circumstances where information can be shared (i.e., for a "cybersecurity purpose"), but it does not provide details as to how that information will be protected from disclosure. We believe that the Act should define clear confidentiality and privacy requirements regarding the use of such information and that it should require that any

[5] German IT Security Act 2.0 available here: *https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2021/0301-0400/0324-21.html;* Regarding state-level time lines, see, e.g., New York Department of Financial Services reporting requirements: *https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Newly-Proposed-Cyber-Reporting-Rules-for-Banking-Organizations*.

information that is further disseminated is scrubbed of all identifying information of the entity that provided it.

We also make the point in our Policy Principles that it is important that policy makers ensure that there are appropriate liability protections maintained in incident reporting legislation, so that information provided in a report cannot later be used against an entity. Of course, if there are instances in which entities have engaged in unlawful misconduct, such liability protections would not apply. We also believe that security incident reporting legislation should make clear that cybersecurity incident reports shared with the U.S. Government should be exempt from FOIA requests. Given this recommendation, we welcome the Act's provisions in Section (f) which offer protection to entities that report or provide information under Section 106 of CISA 2015. At the same time—and this is an issue which extends beyond the specific legislation that is being considered at present—we believe that the language in CISA 2015, which is primarily limited to "cyber threat indicators," may well need to be updated to include the categories of incident reporting information that are ultimately required to be included in the reports submitted to CISA under the Act. Adding such definitional clarity to CISA 2015 itself will help to ensure that entities receive liability protection for all relevant information that is shared, whether through voluntary cyber threat indicator sharing, or mandatory or voluntary incident reports provided to CISA under the Act.

c. Limit Reporting to the Impacted Entity

Another question that arises not only in the domestic conversation on incident reporting but in the global conversation as well is who is responsible for reporting an incident to the competent authority (CISA, in the case of the Act). We believe that the reporting obligation should fall only on the impacted entity, and that vendors or third-party service providers should not be required to report cybersecurity incidents to the U.S. Government that have occurred on their customers' networks.

An incident reporting requirement with a broader scope would pose numerous challenges to many organizations' normal business operations, including potentially forcing vendors or third parties to disclose business confidential information of impacted customers or breach their contractual obligations. Such a requirement, if scoped broadly to incorporate third parties and vendors, may also result in duplicative incident reports which, as mentioned previously, could inundate CISA with multiple duplicative reports that they then must sift through, diverting limited resources away from meaningfully addressing significant cybersecurity incidents.

d. Streamline Incident Reporting Requirements

There are currently several different measures that govern Federal cybersecurity incident reporting, making for a complex and often confusing landscape. Numerous Federal agencies currently have disparate incident reporting requirements, many of which are just starting to be implemented. For example, the banking sector is subject to multiple specific notification requirements (see, e.g., 12 CFR part 30, appendix B, supp. A (OCC); 12 CFR part 208, appendix D–2, supp. A, 12 CFR 211.5(l), 12 CFR part 225, appendix F, supp. A (Board); 12 CFR part 364, appendix B, supp. A (FDIC) (italics omitted); NPRM on Computer Security Incident Reporting Requirements for Banking Organizations and their Bank Service Providers) as is the defense industrial base (see 32 CFR § 236.4—Mandatory cyber incident reporting procedures). There are also reporting requirements captured in FISMA (see 44 U.S.C. §§ 3553–54 & associated Binding Operational Directive 16–03); FedRAMP Incident Communications Procedures; NERC Incident Reporting and Response Planning as required by FERC; and the US–CERT Federal Incident Notification Guidelines. Additionally, Section 2 of the President's Executive Order on Improving the Nation's Cybersecurity includes a number of provisions aimed at improving incident reporting on the part of Federal contractors. There may also be interactions with existing privacy reporting requirements or with law enforcement processes. And additionally, as alluded to above, various State laws impose data breach reporting requirements, often stemming from the same incidents.

To alleviate the confusion that is brought about by this complex incident reporting landscape, we urge Congress in our Policy Principles to harmonize existing regulatory reporting requirements to ensure that companies are more efficiently able to report incidents and are not subject to contradictory, duplicative, or otherwise confusing reporting requirements that may serve to hamper the notification process. We also recommend that reported information be aggregated, anonymized, analyzed, and shared in a manner that facilitates the mitigation and/or prevention of future cyber incidents.

All that being said, we appreciate that the Act recognizes in Subsections (d)(7)(A) and (B) that covered entities may be subject to existing regulatory requirements,

and that it directs the CISA director to consider those existing regulatory requirements in establishing reporting requirements for covered entities, including working with other regulatory authorities to see whether and how streamlining is feasible. While we appreciate the inclusion of this provision, the Act currently does little to actually lessen the regulatory burden. We recommend adding language that clarifies that CISA should leverage existing channels to collect incident information whenever possible, including having existing interfaces such as the FBI, SEC, and financial sector regulators provide updates based on engagement with the private sector. This could be accomplished by directing the Office of Management and Budget to issue guidance to Federal regulators and law enforcement requiring agencies to share information related to covered incidents against covered agencies with the Cyber Incident Review Office.

e. Establish Appropriate Reporting Thresholds and Limit Reporting to Verified Incidents

We appreciate that the Act attempts to establish minimum thresholds for reporting a "covered incident" based on a risk-based, analytical model. We consistently encourage policy makers to take a risk-based approach to cybersecurity, and incident reporting is no exception. It is important that the threshold for requiring an incident report is sufficiently narrow and clearly delineated. Reporting requirements should include specific parameters and be mapped to objective criteria, and incident severity levels should be related to identifiable harms, such as to public health and safety, or operational disruption.[6] However, the considerations outlined in the Act's Subsection (4)(A) introduce ambiguity that is not resolved in the minimum threshold language outlined in Subsection (4)(B). Relatedly, providing additional rigor around what constitutes a "significant cyber incident" would be helpful.

In our Policy Principles, we recommend that policy makers explore the idea of an incident categorization matrix, which can represent the severity of an incident more accurately, therefore allowing for prioritization of incidents. We believe that a similar concept would be useful to introduce here and encourage the subcommittee to include language that directs CISA, in conjunction with interagency partners, to develop such an incident categorization matrix. A categorization matrix can be used to help determine the severity of, and potential for, actual harm posed by an incident more accurately, helping to prioritize incidents and ultimately enabling more precise reporting. Focused reporting that is limited to severe incidents that may result in actual harm reduces the burden on information security teams and frees up resources for the essential tasks of examining and remediating incidents and securing an organization's systems.

Similar approaches have been proposed by CISA and have already been adopted by the United Kingdom (UK) and Australia. The United Kingdom's National Cyber Security Center developed a Cyber Attack categorization system, with incidents broken down into six categories, ranging from a category 1 national cyber emergency to a category 6 localized incident. Along with breaking out incidents into categories, the United Kingdom's matrix includes a definition of the type of incident, information about who responds to that incident, and what activities responders should undertake.[7] This approach helps lend additional clarity to determining the severity of an incident and allows for resources to be deployed more efficiently. Australia has developed a similar Cyber Incident Categorization Matrix, which lays out similar categories ranging from 1–6 and provides illustrative examples of the types of incidents and impacted entities that fall in a given category. This matrixed approach allows the Australian Cybersecurity Centre to triage incident reports and respond appropriately based on level of impact.[8]

We applaud the committee's focus on incidents that produce actual harms as established by the minimum thresholds for a "covered cybersecurity incident" as set forth in Subsection (4)(b). This emphasis on incidents that cause disruption of business operations, compromises of the integrity or confidentially of data, and loss of services ensures CISA's limited resources can be effectively and efficiently leveraged. We were pleased to see that the Act focuses on such confirmed incidents, as we have observed a somewhat troubling trend in proposed incident reporting poli-

[6] Currently, the United States approach to categorizing cyber incidents in the National Cyber Incident Response Plan defines a "Significant Cyber Incident" as a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the National security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[7] Overview of NCSC cyber categorization matrix available here: *https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents.*

[8] Matrix available at *https://www.transparency.gov.au/annual-reports/australian-signals-directorate/reporting-year/2019-20-6.*

cies globally which require entities to report "potential" incidents or "near misses." In our view, requiring the reporting of "potential" incidents does little to improve cybersecurity and could inadvertently create an information overload, preventing the competent authority from prioritizing actual, confirmed incidents, and undertaking appropriate action to respond, particularly when it is not clear what would constitute a "potential" incident. As we noted in the multi-association letter and in our Policy Principles, reporting verified or confirmed incidents that have been well-defined and scoped will help to avoid a culture of overreporting that will strain limited incident response capacity and capabilities inside and outside the Government. It will also help ensure that information received is useful and actionable.

III. PRIORITIZING PARTNERSHIP AND COLLABORATION PUTS CISA IN THE BEST POSITION FOR SUCCESS IN CYBER INCIDENT REPORTING

ITI has long advocated that public-private partnerships are essential to improving cybersecurity, and CISA and its predecessor entities at the Department of Homeland Security have been established as key partners to industry on issues such as cybersecurity threat information sharing and supply chain risk management. These partnerships are essential to: (1) Identify potential threats; (2) understand how and to what extent risks can be managed; and (3) determine what actions should be taken to address risks without yielding unintended consequences. The Act we are discussing today acknowledges that Government and industry often have access to unique information sets; this is certainly the case in the context of a security incident, which is why sharing or reporting certain categories of information can help all relevant stakeholders see the complete picture, increasing situational awareness, and driving more effective operational collaboration in response to significant incidents.

The private sector ICT community has not only been foundational in developing the infrastructure of cyber space but, for well over a decade, in providing leadership, innovation, and stewardship in all aspects of cybersecurity, including helping to develop and participating in numerous public-private partnership structures and efforts. For example, global ICT companies have long participated in sector coordinating councils (SCC), self-organized, self-governed councils that allow owners and operators of critical infrastructure to engage on a range of cybersecurity strategies, policies, and activities with CISA and other U.S. Government counterparts, and also participate in the ICT SCRM Task Force launched in 2018. I am pleased to serve as the vice chair of the ITSCC and to work closely with my counterparts in the Communications SCC, as well as CISA and other U.S. Government partners as co-chair of the ICT SCRM Task Force.

We believe that if an incident reporting regime is crafted carefully, it can be a helpful tool to improve Federal agencies' situational awareness into cybersecurity incidents as well as to drive improvements in operational collaboration between CISA and industry. In order to realize such an effort, CISA's role as a trusted and collaborative partner to industry must be preserved, if not strengthened, as it must be able to continue to engage with relevant stakeholders, including critical infrastructure owners and operators, on not just the cybersecurity incident notification and reporting requirements contemplated here but on the array of other important and ongoing cybersecurity and supply chain risk management partnership activities referenced above.

This is an important moment in the history of CISA, still a relatively new agency that has had to adapt itself to meet what seems like a new set of threats and challenges every year. The legislation under consideration by this subcommittee holds the promise of not only developing an effective and efficient cybersecurity incident reporting regime, but in doing so in a way that preserves the partnership and collaborative model that this subcommittee set out when it created CISA 3 years ago. We urge the subcommittee to ultimately adopt legislation that achieves both of these goals.

CONCLUSION

Members of the subcommittee, ITI and our member companies once again commend you for your leadership on this issue. We appreciate your approach to engaging with stakeholders to ensure the partnership model that CISA was founded on will be protected and continue to evolve as it tackles these new threats. We encourage you to keep both the partnership model and goal of improving operational collaboration in mind as you consider how to best refine the Act in order to lend additional clarity to questions around issues including minimum thresholds for incident reporting, confidentiality and liability protections, and conflicting or duplicative reporting requirements.

ITI stands ready to provide the subcommittee with any additional input and assistance as it seeks to develop an approach to cybersecurity incident reporting for critical infrastructure owners and operators. And we reiterate our request that the subcommittee consider our full set of Policy Principles, which, when taken together, will help policy makers to structure a clear, straightforward incident reporting regime that provides actionable, appropriately contextualized information.

I would like to again thank the Chair, Ranking Member, and Members of the subcommittee for inviting me to testify today and for your interest in and examination of this important issue. I look forward to your questions.

Thank you.

APPENDIX A.—ITI POLICY PRINCIPLES FOR SECURITY INCIDENT REPORTING IN THE U.S.

JULY 2021

The SolarWinds compromise has demonstrated how the cyber threat landscape is constantly evolving, resulting in the emergence of new threats. In search of a suitable policy response, policy makers have increasingly turned to incident reporting policy regimes as a potentially appropriate tool. The proposals introduced to date often conflate multiple issues and misunderstand the goals and the applicability of security incident reporting.

ITI recognizes the importance of cybersecurity incident reporting to inform actions to respond to incidents and to contain or prevent further impacts. ITI views the concepts related to security incident reporting as distinct from those of cyber threat information sharing or a data breach notification (see box for details). If a report provides sufficient technical details about the suffered incident, Federal agencies can understand the nature of the attack and take steps to mitigate the associated risk. Likewise, actionable reporting may help Government officials to prioritize incident response assistance to affected organizations, particularly while dealing with an active campaign targeting multiple organizations. This assumes that affected organizations required support and that the principles articulated below have been fully adopted.

As such, if carefully crafted, incident reporting has the potential to be a helpful policy lever. It is through this lens that we offer our recommendations on several key areas that policy makers should consider in developing an effective, efficient security incident reporting regime.

Security incident reporting is distinct from other concepts with which it is often confused: Data breach notification and cyber threat information sharing. While some incidents may blur the line between these concepts, it is important to understand the difference between these terms and what each process is meant to achieve.

Security Incident Reporting focuses on the past because it reports on the details of a cybersecurity incident that has already occurred. This could include the vector of compromise, the systems and information compromised or targeted by the attacker, and any attributes of the attacker's behavior. Reports may focus on the actual or the potential harm caused by an incident. Information conveyed in the reporting highly depends on the reporting time line, reporting purpose (and use) and segment needs.

Data Breach Notification relates specifically to the unauthorized access to or disclosure of personally identifiable information or other sensitive privacy data. In the United States, there are more than 50 State and local laws focused on data breach notification.

Cyberthreat Information Sharing focuses on the future and refers to the proactive sharing of threat information to help all entities understand threats and take steps to prevent successful cyber attacks. Threat information sharing should be voluntary and may include indicators such as anomalous network activity or methods of circumventing security controls.

DEVELOP AND ADOPT AN INCIDENT CATEGORIZATION MATRIX

Policy makers should ensure that the threshold for reporting requirements is mapped to specific objective criteria and specific incident severity levels related to identifiable harms, such as to public health and safety, or operational disruption.[1]

[1] Currently, the U.S. approach to categorizing cyber incidents in the National Cyber Incident Response Plan defines a "Significant Cyber Incident" as a cyber incident that is (or group of related cyber incidents that together are likely to result in demonstrable harm to the National

Continued

Reporting requirements should only focus on severe and significant attacks that cause actual disruption or loss and should include specific parameters. An incident categorization matrix[2] can represent the severity of an incident more accurately which helps with the prioritization of incidents and ultimately supports more precise reporting. Focused reporting that is limited to severe incidents reduces the burden on information security teams and frees resources for the essential tasks of examining and remediating incidents and securing the organization's systems. Moreover, it reduces the likelihood of an informational overload for applicable authorities that would undermine their ability to prioritize responses and divert limited agency resources from critical risk mitigation activities. These considerations are also key in the context of defining the scope and object of reporting (e.g., avoiding the confusion of "incident" with other concepts or expanding to "potential" incident reporting). We recommend policy makers advance the joint understanding of the matrix and severity concept, by facilitating a consensus-driven processes.

ESTABLISH FEASIBLE REPORTING TIME LINES COMMENSURATE WITH INCIDENT SEVERITY LEVEL

Any incident reporting legislation should ensure that time lines are aligned with global best practices. The required time lines should be commensurate with incident severity levels but allow for at least a 72-hour reporting window after an entity has verified the incident. Anything shorter is unnecessarily brief and injects additional complexity at a time when entities are more appropriately focused on the difficult task of understanding, responding to, and remediating a cyber incident. Shorter time lines also greatly increase the likelihood that the entity will report inaccurate or inadequately contextualized information that will not be helpful, potentially even undermining cybersecurity response and remediation efforts.

LIMIT RESPONSIBILITY FOR REPORTING ONLY TO THE COMPROMISED ENTITY

Any legislation should ensure that the reporting obligation falls only on compromised entities. Vendors and third-party service providers should not be required to report cybersecurity incidents to the U.S. Government that have occurred on their customers' networks. Such a requirement would pose numerous challenges to normal business operations, including potentially forcing vendors or third parties to disclose business confidential information of that customer or breach their contractual obligations.

ENSURE CONFIDENTIALITY AND APPROPRIATE PROTECTIONS AROUND SENSITIVE INFORMATION SHARED WITH FEDERAL AGENCIES, INCLUDING AGAINST REGULATORY USE

It is imperative to have strong and transparent rules about the confidentiality of incident information that is shared with or by Federal agencies. Such rules should govern not only the dissemination of incident information with relevant interagency partners but should specifically preclude direct or indirect regulatory use of such information. Such rules should additionally govern how unclassified information on a specific incident is further shared with the U.S. Government, other governments, and with nongovernmental entities. These rules must be crafted to guarantee compliance with existing legal regimes, including contractual and privacy obligations. A designated centralized reporting agency should provide a secure method of communication. This could be as simple as publishing a PGP encryption key or using the Traffic Light Protocol (TLP). Trust is essential.

ESTABLISH TARGETED LIABILITY PROTECTIONS AND APPROPRIATE EXEMPTIONS FROM THE FREEDOM OF INFORMATION ACT (FOIA)

Entities providing incident reports should receive liability protections for providing such information to Federal agencies, including engaging in activities related to monitoring or network awareness of their information systems, other than in instances where entities engage in willful misconduct. Additionally, cybersecurity incident reports shared with the U.S. Government should be exempt from FOIA requests.

---

security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[2] Similar approaches have been proposed by CISA and are already adopted by the United Kingdom and Australia.

HARMONIZE FEDERAL CYBERSECURITY INCIDENT REPORTING REQUIREMENTS

There are currently several different measures that govern Federal cybersecurity incident reporting, making for a complex and oftentimes confusing landscape.[3] To alleviate such confusion, Congress should consider harmonizing existing regulatory reporting requirements to ensure the efficient sharing of covered cybersecurity incidents.

DESIGNATE A SINGLE POINT OF CONTACT FOR COMPANIES TO REPORT SECURITY INCIDENTS TO WITHIN THE GOVERNMENT

Incident response and recovery resources are in short supply. To effectuate the efficient use of limited resources, the Federal Government should designate, and adequately fund, a single point of contact for all companies that need to report an incident. If existing reporting requirements have not been harmonized and sector-specific reporting requirements remain in place, impacted organizations should not be required to report an incident twice. All future legislative proposals should designate CISA as the single point of contact where no sector-specific regulator exists, and appropriate resources should be allocated for that purpose.

DEFINE AN APPROPRIATE AND FLEXIBLE REPORTING TEMPLATE

All incident reports should follow a standardized template to ensure consistent reporting across agencies and industries. Consensus-driven processes are needed to refine the elements of such a template to ensure consistency with existing frameworks, like MITRE ATT&CK or VERIS, and international industry best practices, as well as to ensure that the template fits the needs and existing practices of a particular sector. Reporting entities can use such a template to report the most relevant information where available. By way of example, the template may include appropriate and reasonably obtained information on: (1) The attack vector or vectors that led to the compromise; (2) the indicators of compromise; information on the affected systems, devices, or networks; (3) information relevant to the identification of the threat actor or actors involved; (4) a point of contact from the affected entity; and (5) impact, earliest known time, and duration of compromise.[4] Entities should have the option to report additional types of information on cybersecurity incidents to help to identify emerging trends or otherwise preempt attacks. Entities should also not be penalized for or precluded from reporting an incident if all information, including the information proposed in this list, is not available.

ALIGN REPORTING PROCESSES AND MECHANISMS TO ENSURE CONSISTENCY WITH INDUSTRY BEST PRACTICES AND ALLOW FOR BI-DIRECTIONAL INFORMATION SHARING

The protocols and mechanisms of reporting an incident should be consistent with existing frameworks, recognized sectoral, international, and industry best practices. To ensure incident information is shared quickly and continuously, sections 2.f and 2.g of Executive Order 14028 direct improvements to the inter-agency sharing of incident information. In addition to these provisions, Federal agencies also need to streamline legal agreements involving industry partners to allow for bi-directional sharing of incident information.

BUILD AGENCY CAPABILITY TO ACT ON SECURITY INCIDENT REPORTS

Security incident reporting will be of limited utility if the designated recipient agency does not have the capacity to ingest and act on the information it receives. A manual-intensive approach will quickly max out resources and elevate the risk that important alerts are inadvertently missed. Before a security incident reporting

[3] See, for example, banking sector notification requirements: 12 CFR part 30, appendix B, supp. A (OCC); 12 CFR part 208, appendix D–2, supp. A, 12 CFR 211.5(l), 12 CFR part 225, appendix F, supp. A (Board); 12 CFR part 364, appendix B, supp. A (FDIC) (italics omitted); NPRM on Computer Security Incident Reporting Requirements for Banking Organizations and their Bank Service Providers; defense industrial base mandatory reporting requirements: 32 CFR § 236.4—Mandatory cyber incident reporting procedures; FISMA reporting requirements: 44 U.S.C. §§ 3553–54 & associated Binding Operational Directive 16–03; FedRAMP Incident Communications Procedures; NERC Incident Reporting and Response Planning as required by FERC; and US–CERT Federal Incident Notification Guidelines.

[4] This initial list is based on the following CISA documents: *https://www.cisa.gov/sites/default/files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015__1.pdf;* other resources are available: *https://us-cert.cisa.gov/sites/default/files/publications/Federal__Incident__Notification__Guide- lines.pdf.*

scheme is established, the designated recipient agency should have the capability to automate data collection so that internal data can be cross-referenced with externally available data. This will inform and improve the orchestration of incident response actions.

Ms. CLARKE. We thank you for your expert testimony here today, Mr. Miller.

I now recognize Mr. Mayer to summarize his statement for 5 minutes.

STATEMENT OF ROBERT MAYER, SENIOR VICE PRESIDENT, CYBERSECURITY, USTELECOM

Mr. MAYER. Good afternoon, Ranking Member Garbarino, Chairwoman Thompson, and Ranking Member Katko, and other distinguished Members of the committee, thank you for the opportunity to testify at today's hearing to express our industry support for the provisions included in the Cyber Incident Reporting for Critical Infrastructure Act of 2021.

My name is Robert Mayer, and I am the senior vice president for Cybersecurity and Innovation at USTelecom, the broadband association representing broadband providers, suppliers, and innovators connecting our families, communities, and enterprises. My diverse membership ranges from large publicly-traded global communications providers, manufacturers, and technology enterprises to local companies and cooperatives, all providing advanced communication services to markets, urban and rural, and everything in between.

I also serve as the chair of the Communications Sector Coordinating Council, which represents five communication segments: Broadcast, cable, satellite, wireless, and wire line and as co-chair of the Department of Homeland Security Information and Communications Technology Supply Chain Risk Management Task Force. In all of these roles, I have seen first-hand how the cybersecurity threats we face are real and growing.

On an almost daily basis, we learn of attacks by nation-state adversaries and global criminal enterprises that disrupt or exploit access to functions that support our daily lives. We in industry recognize the core interest of Government in enhancing the Nation's cybersecurity and the key role of Government-industry partnership in doing so, including through more robust and coordinated information sharing and incident reporting and response. We also recognize the unique resources the Government has available to aid private-sector organizations when responding to a major cybersecurity crisis.

For these reasons, I am here today to express our industry support for legislation that would establish cyber incident-reporting capabilities within CISA. We believe that the following elements are critical success factors in any incident reporting regime, and we are encouraged to see that they are included in the current proposal.

First, when a cybersecurity incident occurs, impacted organizations need time to investigate the incident, determine whether reporting criteria have been met, and comply with applicable best practices. The proposed legislation provides for a reporting window that is flexible and large enough for industry to triage the incident.

Second, defining reporting thresholds is a highly technical exercise that requires extensive subject-matter expertise. The thresh-

olds need to be specific enough to avoid ambiguity so that industry knows exactly how to comply. The legislation under consideration directs Federal agency experts to define thresholds in consultation with industry. Moreover, to avoid undermining the system with overreporting, only confirmed cybersecurity incidents that will be reported, not potential or unverified incidents. This grounds the thresholds and criteria that are verifiable, attributable, and actionable.

Third, the legislation strives to protect the Government's industry partners when they are victims of cyber attacks. By building upon liability protections afforded in the Cybersecurity Information Sharing Act of 2015, the stage is set for strong, legal, and conceptual foundation for such protections.

Fourth, when the Government collects sensitive information from industry partners, it has a responsibility to protect that information. To that end, the legislation includes provisions to ensure data from incident reports is not shared inappropriately or leaked once it is provided to CISA.

Fifth, any policy requiring ISPs to report customers' incidents would be cause for concern on a number of grounds, including public policy and privacy concerns, disruptions to business relationships, and operations and possible legal issues associated with those kinds of disclosures. The reporting obligations in the proposed legislation reside with the victims of cyber attacks and not intermediaries or third parties.

In addition to the above critical success factors that are included in the bill, we are further encouraged by the following aspects of the proposed legislation. Cyber incident reporting is best enforced with subpoenas rather than fines. The legislation under consideration today wisely relies on subpoenas rather than fines as an enforcement mechanism for cybersecurity reporting.

CISA should serve as a central hub for information sharing and incident reporting. This legislation appropriately directs CISA to shape and maintain this reporting and information-sharing program. CISA is uniquely well-suited to serve as a central hub for cybersecurity information sharing and incident reporting. While CISA has a central role to play, a new reporting concert should take into account that other Federal agencies will consider to be engaged with the private sector.

Recognizing that cybersecurity is a shared responsibility across the ecosystem, we appreciate that the legislation requires the U.S. Government to take its obligations to report and share cybersecurity information seriously, just as industry takes its own obligations seriously. USTelecom and the communications sector stand ready to work with the committee to advance this legislation and will continue to collaborate in partnership with CISA to continuously advance our Nation's cybersecurity, risk management, management, and response capabilities.

Thank you for your leadership and for prioritizing this critical issue. I look forward to your questions.

[The prepared statement of Mr. Mayer follows:]

PREPARED STATEMENT OF ROBERT MAYER

WEDNESDAY, SEPTEMBER 1, 2021

Chairwoman Clarke, Ranking Member Garbarino, Chairman Thompson, and Ranking Member Katko and other distinguished Members of the committee, thank you for the opportunity to testify at today's hearing to express our industry's support for the provisions currently included in the Cyber Incident Reporting for Critical Infrastructure Act of 2021.

My name is Robert Mayer, and I am the senior vice president for cybersecurity & innovation at USTelecom—The Broadband Association, representing broadband providers, suppliers, and innovators connecting our families, communities, and enterprises. Our diverse membership ranges from publicly-traded global communications providers, manufacturers, and technology enterprises, to local Main Street companies and heartland cooperatives—all providing advanced communications services to markets, both urban and rural, and everything in between.[1]

I also serve as the chair of the Communications Sector Coordinating Council and as co-chair of the Department of Homeland Security (DHS) Information and Communications Technology (ICT) Supply Chain Risk Management Task Force.[2]

In all of these roles, I've seen first-hand how the cybersecurity threats we face are real and growing. On an almost daily basis, we learn of attacks by nation-state adversaries and global criminal enterprises to disrupt or exploit access to functions that support our daily lives. Some of these attacks—such as those mounted against SolarWinds and its Government and private-sector customers, and the attack against Colonial Pipeline that had the effect of gas price spikes and gas shortages down the East Coast—target critical functions that enable the basic activities of commerce and consumers' lives. We now have actual experience with a significant disruption to critical infrastructure, highlighting the importance of securing all 16 critical infrastructure sectors including water, transportation, energy, finance, information technology, and communications.

We in industry recognize the core interest of the Government in enhancing the Nation's cybersecurity, and the key role of Government-industry partnership in doing so—including through more robust and coordinated information sharing and incident reporting and response. We also recognize the unique resources the Government has available to aid private-sector organizations when responding to a major cyber crisis.

The Council to Secure the Digital Economy (CSDE), founded by USTelecom and other key industry partners, described the necessary foundations for this coordination in its 2019 Cyber Crisis Report, noting that in the midst of a cybersecurity crisis, Government and industry must be prepared to mobilize together rapidly and collaborate with relevant responders.[3] This means building close working relationships with the companies whose diverse leadership, assets, and operational experience within the digital ecosystem provide unique value in the global fight against cyber threats.

We've seen this partnership work, perhaps most significantly in recent years in the context of the COVID–19 pandemic's unprecedented demands on IT and communications systems to keep us connected, learning, and working, just as threat actors used our increased reliance on connected technology to find new avenues to exploit. Throughout the pandemic, the Communications Sector has worked hand-in-hand with DHS's Cybersecurity and Infrastructure Security Agency (CISA), the National Telecommunications and Information Administration (NTIA), the Federal Communications Commission (FCC), and other Government agencies to allocate and deliver resources, establish access for critical workers, maintain services, and address threats.

This collaboration was not a response to top-down regulatory directives, but rather an operationalization of trusted partnerships cultivated over decades between Government and industry and across diverse members of the ICT sector. It worked—together, we kept the Nation connected through the pandemic, and this successful experience in communications security and reliability is a model to follow in the years ahead.

---

[1] USTelecom The Broadband Association, *www.ustelecom.org.*

[2] Communications Sector Coordinating Council, *www.comms-scc.org;* ICT Supply Chain Risk Management Task Force, *https://www.cisa.gov/ict-scrm-task-force.*

[3] Council to Secure the Digital Economy, *Cyber Crisis: Foundations of Multi-Stakeholder Coordination (2019), https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_CyberCrisis-Report_2019-FINAL.pdf.*

We have also seen the benefit of this engagement in the DHS ICT Supply Chain Risk Management Task Force over the past 2 years. When I last had an opportunity to testify before this committee, the Chair and Ranking Member expressed interest in addressing the essential segment of small and medium-sized businesses (SMBs). The IT and Communications Sectors have similarly recognized the unique set of challenges SMBs face and that these challenges constitute a National security imperative as U.S. critical infrastructure relies on the defensive posture of these individual, yet highly-connected organizations. This year, USTelecom produced a survey examining these challenges and found that critical infrastructure SMBs are distinctly vulnerable to breaches that can take longer to detect and from which to recover.[4] As we enter the Task Force's third year, we plan to continue focus on the critical element of SMBs and how we can further leverage cross-sector and Government-industry partnership to provide greater support.

For these reasons, I am here today to express our industry's support for the committee's efforts to facilitate establishing cyber incident reporting and analysis capabilities within CISA rooted in the foundational information-sharing framework of the 2015 Cybersecurity Information Sharing Act. In the context of this hearing, we see the Cyber Incident Reporting for Critical Infrastructure Act of 2021 as another foundational building block in the growing whole-of-Nation collaboration across industry and Government.

To support our collective interest in leveraging trusted partnerships to enhance cybersecurity, information sharing and incident reporting must be done effectively and efficiently. With this in mind, we believe that the following elements are critical success factors in any incident reporting regime, and we are encouraged that many of these are included in the current legislation proposed by Chairwoman Clarke and Ranking Member Katko:

1. The reporting window should be large enough for industry to triage the incident.—When a cyber incident occurs, impacted organizations need time to investigate the incident, determine whether reporting criteria have been met, and comply with applicable best practices. The committee should consider giving CISA discretion to establish reporting windows within reasonable parameters and with appropriate flexibility afforded to meet the unique needs of a given situation. If the mandatory reporting window is too short, CISA will likely receive an overwhelming quantity of "false alarm" reports that do not merit reporting, which could strain Government resources and undermine the value of the reporting program.

2. Thresholds for incidents that merit reporting should be clearly defined by subject-matter experts, and only confirmed incidents should be reported.—Defining reporting thresholds is a highly technical exercise that requires extensive subject-matter expertise. The thresholds need to be specific enough to avoid ambiguity, so that industry knows exactly how to comply. Given these complexities, the committee should consider directing Federal agency experts to define thresholds in consultation with industry, rather than attempting to include thresholds in legislation itself. Moreover, to avoid undermining the system with over-reporting, only confirmed cyber incidents should be reported—not potential or unverified incidents. The thresholds must be grounded in criteria that are verifiable, attributable, and actionable.

3. Legislation should protect the Government's industry partners when they are victims of cyber attacks.—There are numerous operational benefits to affording protection to entities that report cyber incidents. The Cybersecurity Information Sharing Act of 2015 provides a strong legal and conceptual foundation for such protections, but the committee should also consider ways it and CISA can leverage consultation with stakeholders to refine these protections in the incident reporting context. Different organizations may provide unique insights into how incident reporting affects them legally and operationally.

4. The Government must safeguard the sensitive information it collects.—When the Government collects sensitive information from industry partners, it has a responsibility to protect that information. To that end, the committee should consider provisions to ensure data from incident reports is not shared inappropriately or leaked once it is provided to CISA. We must ensure that the victim names reported to CISA are not shared outside the agency. This is essential to ensuring the information is safeguarded appropriately and not misused.

5. Reporting obligations should reside with the victims of cyber attacks and not intermediaries or third parties.—Any policy requiring Internet Service Providers (ISPs) to report customers' incidents would be cause for concern on a number

[4] USTelecom, *USTelecom 2021 Cybersecurity Survey: Critical Infrastructure Small & Medium-Sized Businesses,* at 6, *www.ustelecom.org/cybersurvey.*

of grounds, including public policy and privacy concerns, disruptions to business relationships and operations, and possible legal issues associated with those kinds of disclosures.

In addition to the above critical success factors that are included in the bill, we are further encouraged by the following aspects of the proposed legislation:

- Cyber incident reporting is best enforced with subpoenas rather than fines. The legislation under consideration today wisely relies on subpoenas rather than fines as an enforcement mechanism for cybersecurity reporting. Where fines are inherently punitive—and may in some cases actually punish entities that aim to report cyber incidents in good faith—subpoenas enable the Government access to the information it seeks and also inform industry more specifically about the Government's interests and priorities. This will enable the overall information-sharing regime to improve with the benefit of experience over time.
- CISA should serve as a hub for information sharing and incident reporting, but must work with its partner agencies. This legislation also directs CISA to shape and maintain this reporting and information-sharing program. Since the agency's statutory establishment in 2018, CISA is well-suited to serve as a hub for cybersecurity information sharing and incident reporting. CISA's expertise and on-going relationships will enable it to build an effective information-sharing framework that will be nimble enough to keep pace with cybersecurity innovation over time. However, any new mandatory reporting requirements should not overlook the extensive collaboration that industry currently has with the broader Federal Government. While CISA has a critical role to play and can serve as a central location for reporting, other Federal agencies will continue to be engaged with the private sector. Indeed, consistent with the Federal Government's recommendation, many companies will contact law enforcement if they have a cyber incident. If a company has a significant intrusion, its first reaction may be to reach out to the FBI, for example, who could take any appropriate criminal action (e.g., seize back some of the ransom payment). Policy makers should ensure that a new reporting construct takes into consideration this dynamic and does not inadvertently punish a private entity for heeding the Government's advice and/or put the entity in the middle of two competing Government agencies in the wake of an attack.
- Information-sharing obligations should be reciprocal between Government and industry partners. We also appreciate that the proposed legislation places expectations on Government stakeholders to report cyber incidents and share cybersecurity risk information. Recognizing that cybersecurity is a shared responsibility across the ecosystem, we appreciate that the legislation would require the U.S. Government to take its obligations to report and share cybersecurity information seriously, just as industry takes its own obligations seriously.

USTelecom—The Broadband Association and the Communications Sector stand ready to work with the committee to advance this legislation and will continue to collaborate in partnership with CISA to continuously advance our Nation's cybersecurity risk management and response capabilities.

Thank you for your leadership and for prioritizing this critical issue. I look forward to your questions.

Ms. CLARKE. We thank you for your expert testimony here today, Mr. Mayer.

I now recognize Ms. Denbow to summarize her statement for 5 minutes.

STATEMENT OF KIMBERLY DENBOW, MANAGING DIRECTOR, SECURITY AND OPERATIONS, AMERICAN GAS ASSOCIATION

Ms. DENBOW. Thank you. Thank you, Chairwoman Clarke, Ranking Member Garbarino, and Members of the subcommittee. I am Kimberly Denbow, managing director of security and operation of the American Gas Association, AGA. I have led AGA's Security Policy and Technical Program for nearly two decades. I am a former member—voting member—former voting member of the TSA Surface Transportation Security Advisory Committee and co-chaired the Cybersecurity Subcommittee. I presently co-chair the Cybersecurity Working Group for both the Oil and Natural Gas Sector Coordinating Council and the Pipeline Sector Coordinating Council.

Thank you for inviting me to share my perspective on the Cybersecurity Incident Reporting for Critical Infrastructure Act of 2021 and sharing AGA's general approach to cybersecurity.

AGA represents more than 200 local energy companies that deliver clean and affordable natural gas to 95 percent of natural gas customers in the United States. AGA supports the provisions necessary for a workable incident reporting framework, as laid out in the Cyber Incident Reporting for Critical Infrastructure Act of 2021.

These provisions include report timing of 72 hours after confirmation of the incident, clarity provided around supplemental reporting, harmonization of new reporting rules with preexisting reporting requirements, leveraging the information sharing and analysis centers, and operator liability, information, and regulatory protections.

Properly framed cybersecurity incident reporting can help counter adversaries and minimize impact. With slight alterations, particularly regarding private-sector involvement, this bill can be even stronger. Suggested improvements include specified outreach to sector coordinating councils in development of the interim final role; ensure flexibility and regular updates to the list of covered entities; ensure CISA has the staffing and sector-specific expertise necessary to coordinate and communicate with operators; and limit CISA director discretion to ensure any disclosure of reported information is nonattributional.

Cybersecurity management is an endless evolution. For nearly two decades, AGA operators worked within a structured oversight model, conceived by TSA, our pipeline security authority. This unconventional and nonregulatory model achieved something the traditional stick-and-carrot approach could not. Constructive information exchange at a level of confidence and cooperation not typically available to regulators. TSA Surface Transportation has always done more with less and on a shoestring budget.

For instance, to develop the TSA pipeline security guideline, the mechanism that underpins pipeline security and has advanced pipeline security by orders of magnitude, TSA collaborated with pipeline operators, CISA, and other entities. The quality output from TSA has been the result of the dedication of TSA staff in partnership with pipeline operators toward a shared common goal: Pipeline security. That said, when done right, regulations can be beneficial.

For example, through the collaboration of nearly 70 organizations, including TSA, CISA, trade associations, and pipeline operators, the consensus-based standard API 1164 Version 3 Pipeline Control Systems Cybersecurity was developed as a tool to help operators manage cyber risks and control system environments and at critical connection points along the supply chain.

As TSA transitions from the structured oversight model to more traditional regulation, API 1146 Version 3 will be the most efficient way to put effective pipeline cyber regulations in place.

In a similar manner, this cyber incident reporting legislation has the potential to advance constructive reporting requirements. The key to meeting this potential lies with CISA and its commitment to the partnership. The AGA board of directors supports an indus-

try-wide cybersecurity commitment and recently agreed to support reasonable cybersecurity regulations. While there is no single cybersecurity solution for absolute system protection, vigilance, technological capability, and leadership commitment will continue to keep America's natural gas delivery system safe, secure, and reliable.

Thank you for the opportunity to testify. I look forward to the exchange of ideas.

[The prepared statement of Ms. Denbow follows:]

PREPARED STATEMENT OF KIMBERLY DENBOW

SEPTEMBER 1, 2021

Chairwoman Clarke, Ranking Member Garbarino, and Members of the subcommittee, I am Kimberly Denbow, managing director of security & operations, of the American Gas Association (AGA). I have led AGA's security policy and technical program for nearly 2 decades. Also relevant to this hearing, I am a former voting member of the Transportation Security Administration (TSA) Surface Transportation Security Advisory Committee for which I helped stand up and co-chaired the Cybersecurity Subcommittee. I also helped stand up and presently co-chair the Cybersecurity Working Group for both the Oil & Natural Gas Sector Coordinating Council and the Pipeline Sector Coordinating Council. Thank you for inviting me to share my perspectives on the Cyber Incident Reporting for Critical Infrastructure Act of 2021 and AGA's general approach to cybersecurity.

Founded in 1918, AGA represents more than 200 local energy companies that deliver clean and affordable natural gas throughout the United States. There are more than 76 million residential, commercial, and industrial natural gas customers in the United States, of which 95 percent—more than 72 million customers—receive their gas from AGA member utilities. Natural gas is a necessary fuel for a clean and secure energy future, providing benefits for the economy, our environment, and our energy security. Alongside the economic and environmental benefits and opportunities natural gas offers our country comes the great responsibility to protect our distribution pipeline system network from cyber compromise.

Technological advances over the last 30 years have made natural gas utilities more cost-effective, safer, and better able to serve our customers via web-based programs and tools. Unfortunately, the opportunity cost of a more connected and more efficient industry is that we have grown to be an attractive target for increasingly sophisticated cyber criminals and terrorists. The cyber threat landscape is evolving at an alarming rate comparable to biological virus mutations. This said, America's investor-owned natural gas utilities are meeting the threat daily via skilled personnel, robust cybersecurity system protections, an industry commitment to security, and a successful on-going cybersecurity partnership with the Federal Government.

Safety and security are core values for America's natural gas utilities. AGA and its member companies are committed to investing in leading security technologies, utilizing best practices and training, and promoting an industry-wide vigilant security culture to help fortify our security defenses.

CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2021

Effective cybersecurity incident reporting is essential to dampening wide-spread cybersecurity compromise. AGA supports the Cyber Incident Reporting for Critical Infrastructure Act of 2021, which establishes the criteria AGA members argue is necessary for a workable incident reporting framework. A few provisions of particular interest and which have industry's support include report timing, supplemental reporting clarity, recognition of existing reporting requirements, Information Sharing & Analysis Centers (ISACs), and liability protections. Additional details are outlined below:

- *Incident Report Timing*.—Providing covered entities 72 hours after confirmation to report on cybersecurity incidents appropriately recognizes that owners/operators need a reasonable amount of time to not just identify but also to verify the validity of a cybersecurity incident before reporting. This minimizes the reporting of non-credible incidents, which can be excessive and resource-intensive with negligible value-add.
- *Supplemental Reporting*.—The latest draft of this legislation helpfully clarifies what qualifies as supplemental reporting and offers the Department of Home-

land Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) director (and covered entities) the useful option of a flexible reporting time line so as not to specifically "prioritize incident response efforts over compliance." This synchronizes the efforts of CISA with the operator, ensures incident investigation is prioritized, and eliminates unnecessary supplemental information submission.

- *Information Sharing and Analysis Organizations*.—We appreciate the latest draft bill's increased reliance on industry Information Sharing & Analysis Centers (ISACs) for Government-private-sector outreach as well as incident reporting. Permitting owners/operators to leverage existing mechanisms through third parties, such as AGA's Downstream Natural Gas ISAC, strengthens the function of these entities to the benefit of all stakeholders, since such organizations have sector-specific threat analysts who can provide additional perspectives to CISA.
- *Harmonizing Reporting Requirements*.—AGA's member natural gas utilities are among the most regulated in the country at the State, Federal, and local level. Complicating matters, well over 50 percent of AGA members are combination natural gas-electric utilities with separate electric sector requirements. As such, we appreciate efforts to reduce potential conflicting mandates by harmonizing the cyber incident reporting requirements with preexisting cyber reporting requirements.
- *Industry Legal Protections*.—We appreciate the inclusion of reasonable information disclosure rules, liability protections for reporting entities (familiar to industry as they mirror those in the Cybersecurity Act of 2015), and regulatory protections in the legislation. Without these provisions, it would be hard to imagine the sort-of streamlined and trusted public-private incident reporting partnership this legislation contemplates.

While the draft legislation sets a strong foundation for moving forward, there are a few policy areas where we recommend some expansion and/or clarification. Not surprisingly, most of our suggestions surround additional private-sector involvement in the overall process, per below:

- *Rulemaking Detail [SEC .2220A(d)(1) In General]*.—This section outlines the incident reporting rule making process. While we appreciate that "appropriate stakeholders" will be able to comment on the interim final rule, we strongly recommend greater specific outreach to critical infrastructure organizations (Sector Coordinating Councils, ISACs, individual covered entities, industry organizations, etc.) in developing the rule. Private-sector engagement from the beginning will ensure the rule will be reasonable, credible, and based on vital critical infrastructure experience and operational capabilities.
- *Who are the Covered Entities? [SEC .2220A(d)(2) Covered Entities]*.—The list of covered entities should be flexible and updated regularly (or as necessary) as companies change operations. DHS should be able to accommodate such changes. To help determine covered entities, we recommend: (1) Consulting with the private sector, (2) utilizing preexisting Government lists that identify critical facilities, (3) a periodic review and update of covered entities, and (4) a process that allows critical infrastructure entities to appeal their inclusion on the list.
- *Ensuring CISA has the Tools it Needs. [SEC .2220A(d)(6) Responsibilities of Covered Entities]*.—This subsection focuses on industry's coordination with CISA personnel. This coordination will only be effective and efficient if CISA has the staffing and sector-specific cybersecurity expertise necessary to communicate with private companies in vastly different business sectors. As such, we recommend adding language to ensure that "CISA will coordinate with SRMAs" (or similar).
- *Director Authority [SEC .2220A(e)(1) Authorized Activities]*.—This subsection lists the exceptions under which the director may disclose information provided to the Office. The discretion allotted the director in the first two exceptions (A and B) are overly broad, which could lead to literally ANY "cybersecurity purpose" as a reason to disclose sensitive company information. AGA recommends adding clarifying language to each exception (A) and (B) specifying "to circumvent national security or national economic harm."

Cybersecurity incident reporting, framed properly, can be the difference between pivoting against our adversaries in an effective manner and minimizing impact, or fumbling to our adversaries' advantage. Cyber Incident Reporting for Critical Infrastructure Act of 2021 provides the structure while also delivering agility. With slight alterations, it can be even stronger.

NATURAL GAS UTILITY CYBERSECURITY MANAGEMENT: AN ENDLESS EVOLUTION

America's natural gas delivery system is the safest, most reliable energy delivery system in the world. This said, industry operators recognize there are inherent cyber vulnerabilities with employing web-based applications for industrial control and business operating systems. Gas utilities employ multiple mechanisms to support a robust cybersecurity program, including participating in an array of Government and industry cybersecurity initiatives. The most important resource is the existing cybersecurity partnership between the Federal Government and industry operators. This partnership fosters the exchange of vital cybersecurity information which helps stakeholders adapt quickly to dynamic cybersecurity risks. That partnership should continue to be supported by Congress.

THE IMMEASURABLE VALUE OF AUTHENTIC PARTNERSHIP

For nearly two decades, AGA favored effective partnership above cybersecurity regulations, which we felt served as a ceiling that stifled robust cybersecurity management. We valued the structured oversight model conceived by TSA, our Federal regulator for pipeline security. Though the model was unconventional by Federal Government standards, it achieved something the traditional "stick-and-carrot" approach could not—constructive information exchange and at a level of confidence and cooperation not typically available to regulators. The TSA "Pipeline Security Guidelines"[1] (Guidelines) coupled with the trust fostered between industry and Government advanced pipeline security by orders of magnitude over the years. Whereas regulations serve as a ceiling to which operators rise but are not incentivized to exceed, Guidelines serve as the floor upon which an operator's program may be built and continuously improved based on the operator's system-specific risks and applicable counter measures.

A SHARED COMMON GOAL

Some have suggested cyber compromise in the pipeline industry is a direct consequence of the structured oversight model. TSA has been criticized for not doing more prior to the recent issuance of the pipeline security directives. For the record, TSA Surface Transportation did more with less and on a shoestring budget. The TSA Pipeline Group has been the epitome of innovation—leveraging the infrastructure subject-matter expertise of pipeline operators, partnering with CISA and Idaho National Labs for in-house industrial control system cybersecurity knowledge, and collaborating with the Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) on cybersecurity reviews of control centers. AGA helped champion the CISA/TSA Pipeline Cybersecurity Initiative[2] and promoted effortlessly the Pipeline Validated Architectural Design Reviews.[3] The quality output has been the result of the dedication of TSA and CISA staff, in partnership with pipeline operators, toward a shared common goal—pipeline security.

DRIVING CHANGE

Over the past few years, more than 70 organizations, including TSA, CISA, PHMSA, the Department of Energy (DOE), Federal Energy Regulatory Commission, National Institute of Standards & Technology (NIST), trade associations, and numerous pipeline operators, worked on revising a standard managed by the American Petroleum Institute (API) for control system cybersecurity. The revision was designed to align with existing cybersecurity guidelines, the NIST Cyber Security Framework,[4] and prominent industry cyber standards. This recently-updated consensus-based standard, API 1164 version 3, "Pipeline Control Systems Cybersecurity"[5] (API 1164 version 3), helps the operator manage cyber risks associated with control system cybersecurity environments by providing requirements and guidance for proper isolation of control system environments from non-control system environments. It also addresses enhanced protections at critical connection points along the supply chain.

Walking the Talk

The AGA Board of Directors continues to be forward-leaning on multiple fronts—with security at the forefront. Actions and activities include:

---

[1] *https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.*
[2] *https://www.cisa.gov/pipeline-cybersecurity-initiative.*
[3] *https://us-cert.cisa.gov/resources/ncats#Validated%20Architecture%20Design%20Review-%20(VADR).*
[4] *https://www.nist.gov/cyberframework.*
[5] API Standard 1164, 3d edition.

- Creation of the Downstream Natural Gas ISAC, which facilitates the sharing of threat information within the natural gas industry and across sectors by providing analysis, coordination, and summarization of threat indicators and other relevant information to its members—a community of nearly 100 percent of our Nation's natural gas utilities and transmission companies;
- Membership-wide adoption of the AGA Commitment to Cyber and Physical Security[6] to demonstrate dedication to ensuring the natural gas pipeline infrastructure remains resilient to the growing and dynamic cyber and physical security threats; and
- Development of a three-point Cybersecurity Action Plan which encompasses enhancing cyber standards for gas utility operations, collaborating with CISA for the enhancement of a cybersecurity verification tool, and developing an operator accountability mechanism. The roadmap includes the progression from guidelines to regulations.

Recently, the AGA Board passed a resolution in support of reasonable cybersecurity regulations. Such regulations would be characterized by four critical components:

1. a risk-based methodology,
2. a framework organized by the functions Identify, Protect, Detect, Respond, and Recover,
3. operator flexibility to pivot to a constantly-evolving cyber threat landscape, and
4. alignment with natural gas industry cybersecurity guidelines and standards for operational technology.

These four critical components are satisfied by API 1164 version 3.

An Effective & Timely Transition

As TSA, in collaboration with CISA, transitions from issuing pipeline security directives to issuing cybersecurity regulations, the Federal Government is encouraged to leverage API 1164 version 3 which reflects practical, attainable, sustainable, and measurable state-of-the-art cybersecurity protections tailored specifically to pipeline operations. Given the imminent threat that prompted issuance of the pipeline security directives, incorporating this standard by reference will be the Federal Government's most efficient way to put effective pipeline cyber regulations in place.

A Commitment to America—A Commitment to the Communities We Serve

America's natural gas utilities are cognizant of enduring cyber threats and the continued need for vigilance through cybersecurity protection, detection, and mitigation mechanisms. There is no single solution for absolute system protection. Through a combination of cybersecurity processes and timely and credible information sharing amongst the Government intelligence community and industry operators, America's natural gas delivery system remains protected, safe, and reliable, and will remain so well into the future.

Ms. CLARKE. Ms. Denbow, I want to thank you for your expert testimony here today.

I thank all of our witnesses for testifying.

I will remind the subcommittee that we will each have 5 minutes to question the panel.

I will now recognize myself for questions.

This first question is to all of our witnesses today. For the past several months, I have worked with stakeholders to craft legislation that, No. 1, gives CISA the visibility it needs to be a more effective partner to the private sector; and, No. 2, informs our understanding of cyber threats in a way that supports long-term systemic improvement to the cybersecurity ecosystem. Many of the questions about how to do this effectively are questions of scope, defining what information CISA needs to be bringing in and setting clear expectations about what CISA needs to be putting out.

What specific information does CISA need about a cyber incident in order to detect cyber campaigns early and help other owners and

[6] *https://www.aga.org/sites/default/files/sites/default/files/media/commitment__to__cyber__and__physical__security__sep2016.pdf.*

operators defend themselves? Is this the same information CISA needs in order to understand threats over time and help owners and operators buy down the risks?

Mr. BUSHAR. So I can start, Chairwoman, answering that question.

Ms. CLARKE. Thank you.

Mr. BUSHAR. So I believe, you know, generally speaking, that CISA will require what we often term technical indicators of compromise, or IOCs, as part of any analysis function and collection effort on their behalf. So what we often recommend is the ability for the victims and the covered entities to be able to provide technical indicators of compromise, which can include things such as IP addresses, domain names, tools, pieces of malware software that are being used in the attack, along with techniques, not necessarily software, but behavioral-based techniques that the victims are observing the attackers taking, such as phishing, lures, or email, and things of that nature.

That sort of information, when correlated across sectors or across industries or even within several organizations, can often increase the rapidity and accuracy of attribution of threat actors.

The additional context that CISA may require related to strategic analysis would have to do with things such as targeting. What I mean by that, that would be information more related to what sort of data or information systems appear to be targeted by the threat actor, what data was confirmed to be taken out of the environment, if that is known, what sort of people or personas attempted to be compromised during the attack, whether that is, you know, positioned—executive positions in the organization, other sorts of key leadership inside the organization. Those can all be useful information—points of information for analysis of threat actor intent and where they would likely see similar sorts of attacks and behavior emerging again across sectors or within sectors. So those two broad categories of information we feel are valuable to CISA to collect and understand, again, in a nonattributional way, wherever possible, or at least in a anonymized way for each victim.

Ms. CLARKE. So, if the other panelists agree with Mr. Bushar, let me ask what information and intelligence do your industries need from CISA in order to defend against threats today and in the future? What makes information actionable for your purposes?

Mr. BUSHAR. Yes, that is great question, Chairwoman. It is very similar to the answer in the direction of CISA, and frankly. So, when the Government has access to that sort of indicator information, again, in a nonvictim attribution model, we in the private sector can often make use of that information in similar ways by correlating information, by comparing that information to what we are seeing across our customer set, and to deconflict or to understand where these threat actors may be operating that we don't have perfect visibility.

It is really completing, you know, that fuller picture for everyone in the community to understand where threat actors are acting and how they are behaving and how to catch them as well. So that data is extremely valuable to commercial companies to put into detection tools, to software, to drive more rapid again detection and, ideally, prevention, right? So the ultimate goal in feeding informa-

tion back from the Government to the private sector would be to inoculate. To use kind-of a comparison, it would be an inoculation. So we saw the first victim. We understand what happened there. Now, I can take that vaccine of information and apply it to all my other clients. Now if that same threat actor tries to use that exact same capability against other victims, it won't work; they are protected.

Ms. CLARKE. Thank you, Mr. Bushar.

My time has elapsed.

I now recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Garbarino, for his questions at this time.

Mr. GARBARINO. Thank you, Chairwoman. Actually, I want to follow up—I wasn't aware I was going to start, but I wanted to follow up on what you were just talking about with what should be reported. My question to witnesses is, on a covered incident—and we have different groups on here, telecom and banks and energy—it shouldn't be a one-size-fits-all approach, right? How do we determine—is this something we set out legislatively in the actual text, or are we going to have to do this in rule making? Or how do we make sure it is done right in the rule making?

Ms. Denbow, I will start with you. I saw you raise your hand real quick.

Ms. DENBOW. Thank you. This is something that is very near and dear to my heart. I believe that the quickest way to get to an effective solution is, again, to consult with the Sector Management Risk Agencies and the Sector Coordinating Councils. That is where you are able to bring together the communities that have the subject-matter expertise in the various critical infrastructure sectors already there. So you already have that learning curve taken care of, and you are diving right into the middle of the pool, so to speak.

Mr. GARBARINO. Mr. Mayer, you wanted to add onto that?

Mr. MAYER. Yes, I do. Thank you. So I think definitely it is not about putting legislative language in that becomes very prescriptive in terms of how to characterize an incident because incidents are evolving, and we need the flexibility to take in the information, relevant information associated with different attacks.

One of the things that, I think, speaks relative to legislation is you have already identified some considerations that would be considered. So, for example, how sophisticated is the attack? Is this a novel attack, something, though, we haven't seen before? Who is going to be affected by the attack? What is the potential impacts of cascading effects? Does it impact industrial control systems, skaters, different systems? How does that work? I think that we can work within those parameters. As I fully anticipate, we will have an opportunity to engage CISA in the interim rules and then the final rules, is to bring subject-matter experts—sector-specific subject-matter experts, because what works, involves our networks and our systems is different than what Kimberly's systems look like or what the banking systems look like.

We really need—and this is something where I think industry makes a very significant contribution, is we bring subject-matter experts to the discussion to the partnership with CISA. These are front-line workers, so there are some limitations in terms of how

much we can demand from them, but we really can't go forward in making these kind of decisions around how to define a covered incident without that kind of industry-specific input.

Mr. GARBARINO. I actually appreciate that both of your answers because I think it is great idea, Ms. Denbow, that we deal specifically with the 16 different critical infrastructure subgroups there are now. I think DHS should—maybe there is something we can put in that maybe they set up different requirements for different ones, but they deal specifically with those agencies. I think that is a great idea.

Another question I have is about the quarterly reporting. Mr. Mayer, you just talked about how these things happen very quickly. Is CISA releasing a report every quarter? Is that good enough? I mean, and the reason why is 3 months later it might not mean anything anymore? I mean, things move very quickly.

Mr. MAYER. Yes, so I tell you, I credit CISA—they are not going to wait 3 months. The 3 months, as I understand it, in the context of the legislation is designed to encapsulate what they learned, aggregate the information, and anonymize it, and push it out.

CISA has been incredibly responsive and timely in pushing out information about threats. We send them information on all types of malware, on ransomware. In some instances, they have affiliated with NSA in pushing out information, affiliated with the FBI. They are not sitting on the information. Then we engage with CISA I would say pretty much on a daily basis when it comes to receiving alerts and what—you know, sharing what we have discovered in our systems, what they are observing either on the Federal agency. So the dialog is already taking place. I think the benefit of this is there is going to be a virtual cycle because, as these incidents evolve, there are going to be new PTPs, new tactics and techniques and procedures that are going to require different ways of responding to them. CISA is going to have the benefit of more data and information, and they are going take those lessons learned, I believe, and deliver them in an un-Classified way to the critical infrastructure sector. So I think it is a balance, and I think it is accretive in terms of its value.

Mr. GARBARINO. Right, Ms. Denbow, did you just want to add something real quick? I saw you raise your hand.

Ms. DENBOW. I actually—thank you. I actually do. With respect to working with CISA and our various sector risk-management agencies and their intel groups, it is very important that the intelligence community comes together with the operators to be able to determine what is worse, downgrading from this Top Secret level to that next level so that they are not spending time trying to reclassify something that really is of no use to the operator.

For example, we are still waiting on a threat briefing in response to the issuance of the secured—pipeline security directive. The challenge there—and it is not on the staff at TSA or CISA because they are doing the best that they can—is trying to downgrade that information to a level that is valuable to the operators. What would be great if we could get subject-matter experts from the field sitting in with CISA and TSA to say, "You know what, that is what needs to be downgraded; not that. That wastes your time. That wastes our time. Just give us this."

Mr. GARBARINO. I appreciate that. I am out of time, but I appreciate those answers. Thank you.

I yield back, Madam Chairwoman.

Ms. CLARKE. Thank you, Ranking Member.

I now recognize the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for his questions at this time.

Mr. THOMPSON. Thank you very much, Madam Chair. I apologize for being a little late. I was on a call with the FEMA administrator. We are managing Hurricane Ida down in my State right now.

As you have indicated, I have a statement for the record.

I am glad to hear from the witnesses their interest in your legislation. One of the things we are trying to do is to get it right. Stakeholder engagement is absolutely important. As you know, this might be our 2.0 initiative, because we tried a similar effort in our Cyber Act of 2015 to incentivize volunteer public, private information sharing and, unfortunately, no one has gotten out of what they bargained for.

So what I would like to get from our witnesses, starting with Mr. Bushar, is, how do you—how can we make sure this cyber incident reporting legislation is crafted in a way that brings real security value so we aren't having the same conversation 6 years from now?

Mr. BUSHAR. Yes, sir. Thank you for that question. I think it goes to what I—what I stated in my opening statement, as well as some of the other witnesses here today, there has to be some flexibility in the rule-making process. I think what we have learned in the interceding 6 years between the legislation being drafted in 2015 and today is, you know, there is certainly some limitations to voluntary regimes. Let's be honest, right? I think you are only going to get so much, you know, cooperation there. I think it has been tremendous, but maybe there are certain groups or certain, you know, commercial entities that just aren't incentivized to share that data today.

The other factor I believe that comes into play, is really important in terms of getting this legislation correct, is the flexibility in the process because, as we stated, the threats change and rapidly evolve, and that is not only on the capabilities of the adversaries we are dealing with; it is also the technology and the underlying capabilities of the companies using IT infrastructure and the way that that becomes more critical to their operations and business over time.

So we have to be able to adjust what is important from an information collection and sharing regime over time. There has to be an ability for, you know, regulated but also cohesiveness in the way that information is collected and used. As I stated in my testimony, I think that two-ways communication information sharing has to be effective, timely, and relevant to the sector partners participating as well.

Whether it is mandatory or voluntary, I think the more collaboration that occurs over time will strengthen that information sharing and collaboration environment in such a way that you will be much better positioned to defend our critical infrastructure over time.

Mr. THOMPSON. All right.

Ms. HOGSETT. Mr. Chairman——

Mr. THOMPSON. Thank you.

Ms. HOGSETT [continuing]. May I—may I add to that?

Mr. THOMPSON. Yes, please.

Ms. HOGSETT. Thank you. That is a really important question that you asked, and so I want to just focus on two things. I think, first, this is why the scope, as you have put it in the bill, is so important to get right.

If you are seeking to sort-of boil the ocean and get information on a lot of things out there, you are going to wind up with a situation where CISA is deluged with information that is not helpful to them, it is not useful, and they also get bogged down with information that isn't really the actual threat and the highest risks that we want them and everyone else to focus on.

So I think through the rule-making process, that will allow the opportunity for engagement with sector-specific—excuse me—sector risk management agencies, our Sector Coordinating Councils, to talk about those risks that we all believe from our vantage point are important.

So beyond the scope, I think also, then again, you know, setting up a process where there is a regular feedback loop so CISA is also regularly getting feedback from owners and operators of critical infrastructure about what they are finding valuable.

I think if we can—that has often been missing. So if we can kind-of close that so that CISA then also has real-time, you know, valuable information for them to help improve their operations, those would be, I think, a couple of key pieces. It is set up, the way the bill is drafted, to allow for that. But I think your role, of course, helping oversee that as it is implemented would also be a critical thing that we would highlight.

Mr. THOMPSON. Thank you.

Would any other witness like to comment?

Mr. MAYER. Real quickly, if I may, you know, there is a concept that Tony Sager, who led a big team at NSA, talks about, which is the fog of more. When you are in a situation like this and where you are in triage mode, what you don't want to do is you don't want to put so much information out there to CISA that you are putting information that is extraneous, that is noise, that is not focused. So you want some time, and that is why we think the 72 hours from a confirmed event is an important period of time to put in place, and the flexibility to engage in conversations after that.

I think what you are setting up, Chairman, is what I consider to be a virtuous cycle, where—you talk about 6 years down the road. We know that the attacks are going to be probably very different than they are right now. We are going to have different types of networks, more software. We are going to be certainly in AI—in a world of AI, where systems are working with very complex algorithms.

What we need to do is we need to build information up so that we can look at the attacks; they actually become an opportunity for us to understand what our adversaries are doing to see where we are failing, to see what is working, and build that into—going forward—into the kinds of expectations we will have for refining the reporting, refining the information that comes back, and, most im-

portantly, I think, for collaborating with CISA, collaborating with the intelligence community, collaborating with, you know, organizations that are looking at criminal activities.

What—the beauty of this legislation in my mind is you are building the opportunities for a broader and more effective partnership in the context of a mandatory requirement. I think, you know, credit to the committee for recognizing the value of maintaining the partnership—the best parts of the partnership, but also on insisting on accountability and incenting companies to participate in this process. I think that is the big story.

Mr. THOMPSON. Thank you.

Madam Chair, I yield back. Again, thank you for this very thoughtful legislation, and I look forward to its approval. I yield back.

Ms. CLARKE. I thank you, Mr. Chairman.

The Chair will now recognize the other Members of the subcommittee for questions they may wish to ask the witnesses.

In accordance with the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy, I will recognize Members in order of seniority, alternating between the Majority and Minority.

Members are also reminded to unmute themselves and turn on their cameras when recognized for questioning.

The Chair recognizes for 5 minutes the gentleman from Georgia, Mr. Clyde, at this time.

Mr. Clyde.

OK. I am going to go forward, then, and have the Chair recognize for 5 minutes the gentleman from Rhode Island, Mr. Langevin, for his questions at this time.

Mr. LANGEVIN. Thank you, Madam Chair. I want to thank our witnesses for their testimony today.

Mr. Mayer, if I could start with you. In your testimony, you recommended that only confirmed incidents should be covered by this bill, not potential or universal incidents. I want to explore that idea.

The SolarWinds breach has brought new attention to the issue of incident reporting, and for good reason. It took FireEye stepping forward and confirming that they had been compromised for the revelations of the largest SolarWinds campaign to come to light.

So let's say that, in the future, a nation-state is conducting a similar espionage campaign against a U.S. critical infrastructure sector. So if critical infrastructure operators in this sector are not obligated to report suspicious network activity to CISA and they are only obligated to report once they have discovered a breach of confidentiality, integrity, or ability, how would we be meaningfully better positioned to proactively identify and mitigate this hypothetical espionage campaign than we are right now?

Mr. MAYER. So I think, sir, that is—that is an important question. So when I—when we say "confirmed," does that mean you are going to have every aspect confirmed, that you are going to have attribution confirmed, that you are going to know every system that is impacted? No. That is going to take some time. In fact, if you look at SolarWinds, I believe it took months—8 months or so to even detect it.

I think, in my mind, if you have a significant cyber incident that has the kind of impact on confidentiality, integrity, and availability, you are going to know it—you are going to know it when you see it. It is going to be a very obvious impact on a pretty significant system, on a pretty significant function.

U.S. Government, then CISA more likely than not is going to be aware of these types of events. They are going to affect Federal systems. They are going to be observable in some cases.

So I think, you know, in the spirit of this legislation here, once a company realizes that it has been hit in a very significant way and has some visibility into that attack at some level and is maybe beyond the initial hours and days of triage, I would have every expectation, certainly in my sector, that there would be a conversation with CISA.

Of course, there are provisions here that, if companies are not responsive, there are mechanisms in place to apply a stick that I think would be very painful and incent companies to come forward.

Mr. BUSHAR. If I may, sir, can I add to that testimony briefly?

Mr. LANGEVIN. Sure.

Mr. BUSHAR. So, actually speaking directly to, you know, the experience that we had during SolarWinds, I think the way to think about your question is this way.

So in the early days of our analysis of what was happening inside of our own organization, we had some information that looked suspicious, but, you know, early, early on, we weren't quite sure if that was misbehavior potentially by an employee or just anomalous or something, you know, unusual happening with our technology inside the organization.

Once we had confirmation that there was, in fact, a significant compromise, we actually—that is when we came forward and made the voluntary notifications to Government agencies.

I think the point here is that, not that you would never disclose or you would wait until you had all the information available, but simply that, you know, in many cases in our experience, you could have situations where initial indicators aren't indicative of an actual true compromise, and you want to allow organizations time to fully analyze what is happening in their environment and determine that there is, in fact, a real impact, and then have the qualifying event to report to CISA.

That speaks to the relative value and taking the noise out of the data that we talked about earlier.

Mr. LANGEVIN. Yes. You know, I think, first of all, you know, we should ask FireEye when they think they would have reported under this bill. You know, Mandia has testified that he put hundreds of people on it for weeks before the disclosure, not 72 hours. It was weeks. You know, and those were weeks where Russia was stealing data.

Any comment on that?

Mr. BUSHAR. Yes, sir. I mean, again, that is a great point. It is—I think it is a reason why we are actually endorsing, you know, a named time line. It is, you know—we are—at the time and still to this day, organizations, when it is the—the breach is not affecting covered data, privacy data, HIPAA data, et cetera, it is really

under your own recognizance to determine the appropriate time line and agencies and authorities to report to.

I think, by providing guidelines and actual criteria, you are providing us, you know, a very clear structure for organizations to report within. I think it is—there is something to keep in mind here, and I think it is captured inside the bill already, which is 72 hours gets that initial window, and it gives some reasonable balance between analysis time and getting first indicators and warnings, you know, of the hurricane, let's call it, coming, to CISA.

But I—you know, I can say with assurance to you that that information is likely to change, adapt, and evolve beyond the 72 hours. So I think, in the bill, the way it is captured in terms of updating that information is also critically important. It can't just be that first reporting. There has to be information updates as more is learned throughout the investigation and analysis. I think——

Mr. LANGEVIN. Yes.

Mr. BUSHAR [continuing]. That speaks to your question regarding Mr. Mandia's testimony.

Mr. LANGEVIN. So, just so I am clarifying, so you don't think that FireEye testified—you don't think that FireEye reported early enough? Just to be clear, that is your testimony?

Mr. BUSHAR. No. Not—I wouldn't say it that way, sir. I think we did the best we could under—and under, you know, voluntary analysis and trying to understand what was the appropriate, again, timeliness and reporting authorities under a stressful situation.

I do—we believe strongly that a reasonable period of time, you know, within that 72-hour window, does make sense for most entities, at least for an initial reporting requirement.

Mr. LANGEVIN. Well, OK. I know that my time is—you know, is close to end. Let me just say that, Madam Chair, you know, as I am highlighting here, I am a bit concerned about the gap I see between the amount of information CISA needs to meaningfully improve the cybersecurity of our critical infrastructure sectors and the amount of information that CISA would receive would—only to be notified of—for confirmed cyber incidents.

You know, further illustrate this concern with the second example. Let's say that there is a threat actor who is deploying destructive ransomware across critical infrastructure providers, but it has not yet activated—activated it yet. This is not unusual behavior. Once a confirmed cyber incident occurs, threat actors know that news will spread quickly and they will have a limited opportunity to act before cyber defenders close off the vulnerability and root out their malware.

This means threat actors are likely to start encrypting the files of all of the targets they have compromised as fast as possible. By the time that CISA learns of this first ransomware attack, it could be too late for it to take any meaningful action and mitigate the threat to other entities in the sector, or, importantly, in other sectors which are vulnerable to the same malware.

So, you know, Madam Chair, as we continue to consider this bill, I hope that we are going to continue to explore what definition of cyber incident will best ensure that CISA is able to do a job proactively when—job and proactively warn critical infrastructure providers of threats.

I know my time has expired, so I will yield back, Madam Chair.

Ms. CLARKE. Thank you very much, Mr. Langevin. Point well taken.

Wanted to just make sure that everyone is aware we will probably do a second round of questioning after we hear the questions posed by the gentleman from Georgia, Mr. Clyde, for 5 minutes at this time.

Mr. CLYDE. Thank you, Chairwoman Clarke, for holding this very important hearing with Ranking Member Garbarino.

As previously stated by my colleagues, cyber attacks are one of the biggest national security challenges that our nations face. I am dedicated to working with all of you in finding solutions that mitigate these threats.

I think one of the biggest challenges in addressing and understanding cyber attacks is encouraging entities to come out of the shadows and report these incidents to CISA.

There seems to be a fear that these stakeholders, that they could be unfairly blamed for these attacks. As a society, I think we do not blame the store clerk when a business is robbed by a gunman. We blame the perpetrator, and we work to bring them to justice. So I think our society must take the same approach when organizations report cyber instances and stop blaming victims for taking the correct actions to address these attacks.

So I have got some questions. I want to follow up on something that Mr. Bushar said, and—but I will get to that.

The Federal Information Security Modernization Act of 2014 requires the OMB to define a major incident, and directs agencies to report major incidents to Congress within 7 days of identification. The legislation we are discussing today would require the director to determine the time frames, but no earlier than 72 hours. I think there is a disconnect between the way the Federal Government and the private sector report.

So what I would like to know is whether this 72 hours or this 7 days is the appropriate period, and if—or is it something else in between? I think, Mr. Bushar, you said that 72 hours was probably sufficient. But, Mr. Miller, if I could get your input on that. I would also actually like to hear from each of the witnesses what their thoughts are on that time frame. What should the appropriate time frame be? Thank you.

If I could go in with Mr. Miller first, and then alphabetically, Ms. Hogsett, Mr. Mayer, and Ms. Denbow.

Mr. MILLER. Thanks very much for the question, Representative Clyde.

Yes. Well, as we say in our written testimony and as our policy principals indicated and as I think we have heard from several other witnesses today already, it does seem like 72 hours does hit the—kind-of the sweet spot, if you will, for a variety of different reasons.

You know, I don't want to be duplicative of some of the other points that were made here, but, you know, just to put a fine point on something, you know, whether we are talking about the Cybersecurity Information Sharing Act of 2015 and the information sharing under that act, or if we are talking about incident reporting requirements here, you know, the—the goal of these—hopefully of

these bills and laws is not to share the information or just, you know, provide an avalanche of information or as much as possible. Really do need to report information in a way that is going to be usable, not only by CISA, but by critical infrastructure, by other companies, such as FireEye, that are working, you know, on the front lines of these incidents.

So 72 hours seems to be the amount of time that many cybersecurity professionals say is sufficient to determine what has occurred and to provide some of that additional contextual information that is needed, you know, to conduct the investigations, to actually make sure that, you know, cybersecurity—that you are actually also paying attention to trying to shore up your systems and avoid further damage.

Also, it does seem to be in line with kind-of a global standard, if you will, in the 72 hours time frame——

Mr. CLYDE. Well, thank you.

Ms. Hogsett, do you concur with that?

Ms. HOGSETT. Sure. I think what we are all trying to do is we recognize the benefit and the value of providing more information into a central place in the Government—in this case, CISA—to help everybody else sort-of avoid attacks if it hasn't already hit them instant.

So what you note around FISMA and the 7-day, I would have to go back and look specifically at when that time line kicks in, because we have often found in industry, when the clock starts ticking can be very different. We believe, as structured in this legislation, it does allow, as John noted, a reasonable time period for a firm to do initial investigation without interfering with that important work that needs to happen, while still providing then useful information that could benefit others.

I think the larger point that you highlight, though, is that we do have already in place varying different standards, and there is a need to ensure that there is harmonization. Industry certainly faces this. We have it with our existing regulations. Government agencies are likely also now, as you highlight, you know, to have to face that.

So this is something that we would encourage and would love to continue working with you and Congress on to help ensure that there is more of a standardized baseline and that everyone has a clear time line and a clear set of expectations around reporting.

Mr. CLYDE. OK. Thank you very much.

Mr. Mayer.

Mr. MAYER. Yes. So I will be quick here just to add. I think—I am looking for the language. I can't find it right now. But two things.

One is the legislation recognizes that there is a balance between the agency's desire to get situational awareness and to get information out that could be useful, and the desire of a company to have—feel that they have some sense of what happened. Again——

Mr. CLYDE. Right.

Mr. MAYER [continuing]. Going back to what constitutes confirmation, you are going to know it. You have got a serious cascading impact on critical infrastructure. You may not know attribution, you may not know all the elements, all the systems that have

been impacted. You will know you are dealing with a significant incident. So I think you accomplish that balance.

The other thing I would add—and, again, I am looking for it here, in the Executive Order 14028 that the White House issued on improving the Nation's cybersecurity with respect to what Federal agencies are required to do and their contractors, they established, subject to check, I believe 3 days as the time line for providing information.

So I am sure a lot of thought went into that, discussion with other agencies. As it was pointed out, I think there are general standards around that time. So it is a reasonable amount of time. I think if you tried to make it 7 days, I think a good case could be made that things would be, you know, at that point, too far down the road in terms of potential damage. So——

Mr. CLYDE. OK.

Mr. MAYER [continuing]. We wouldn't—I don't think anybody on the industry is going to—you are going to find anybody arguing for that—that amount of time——

Mr. CLYDE. Well, all right. Thank you. Maybe we should tighten up the Federal Government's requirement then.

Last, Ms. Denbow, do you concur with that? I saw you shaking your head yes.

Ms. DENBOW. Thank you very much, Congressman.

There is not really a good answer to exactly what the right number should be. Should it be 72? Should it be 70? Should it be 68? It is more of—the key is that they are allowed to confirm first that they have an incident rather than just speculating that they have an incident.

By giving it the 72 hours, now you are allowing the operator more time to gather valuable, useful information rather than just spitting information to CISA, where CISA is going to come back and ask more questions anyway.

So it just allows that little comfort zone and space to be able to do the investigation that is needed to be able to provide preliminary information.

Mr. CLYDE. Well, thank you very much.

Madam Chair, I see my time has expired, but I appreciate the witnesses' information here.

You know, it is my intent that we have good industry input in the rule-making process to establish this bill, because I think that is very, very important. So thank you, and I yield back.

Ms. CLARKE. Thank you, Mr. Clyde.

The Chair now recognizes for 5 minutes the gentlewoman from Texas, Ms. Jackson Lee.

Ms. Lee, are you muted? I think you may need to unmute.

Ms. JACKSON LEE. Can you hear me?

Ms. CLARKE. We can hear you now.

Ms. JACKSON LEE. Thank you so very much.

Thank you very much, Madam Chair, for your leadership on this very crucial issue. I just have two questions that I would like to pose for those who would answer it and give their insight.

We know that a key consideration on the value of reporting is sharing information on the cyber attack, how a system was

breached or compromised so that effective defenses can be developed.

I would like to raise the point of whether or not is it important for Pfizer—CISA to share this type of data with critical infrastructure owners and operators knowing that, even to date, there are at least 85 percent or more of the critical infrastructures in the private sector?

The second question would be how this legislation would have impacted Colonial Pipeline and the trajectory that they utilized, which was not open, which was not—they did not come forward quickly, and they did not provide information quickly.

So I pose those two questions, and I do those to the particular witnesses who choose to answer them. Or either I will call on each of you.

Mr. BUSHAR. Yes, ma'am. I will take a shot at the first question.

It is absolutely important and critical, and as we testified today, that the bidirectional information sharing is absolutely important for any information-sharing regimen to be considered. So those indicators, those technical pieces of information around the specific vulnerabilities that were exploited and the way in which they were exploited are exactly the sorts of data points that CISA should be collecting and then, you know, turning around to covered entities or to specific sectors as appropriate.

As we know, in much of our infrastructure today, it is fairly common technology sets, so that, in many cases, those sorts of information and indicators will apply broadly. But there may be very, very specific vulnerabilities that only apply to certain pieces of technology that are only relevant in certain industries, and, therefore, CISA will be—you know, they will have to tailor that information sharing in a way that is, again, relevant to the defense—defensibility of those particular pieces of technology in those sectors.

Ms. JACKSON LEE. Can you hear me?

Mr. BUSHAR. Yes, ma'am.

Ms. JACKSON LEE. Good. Can I have other witnesses answer the question, please?

Ms. DENBOW. I will gladly answer. This is Kimberly with the American Gas Association.

Ms. JACKSON LEE. Thank you.

Ms. DENBOW. Yes, ma'am.

So, repeating what Ron said, yes, the bidirectional is extremely important.

Going on to the Colonial Pipeline matter. I will say that for nearly a dozen years, if not more so, the oil and natural gas sector, as well as the pipeline sector coordinating councils, have been asking Government for a more streamlined reporting approach. Regardless of whether it was mandated or voluntary, we said: Is there a one-stop shop where we can report a cyber incident? And there is constant, well, yes; well, no, not really.

So until that can be worked out, I believe the industry operators are reporting to whom they feel they need to report to, one, under certain given requirements, but then, also, I know that, at least with AGA-member utilities, we tell them to connect with the FBI.

So, given the absence of that further information, that is kind-of what we are working under, as well as to report to the TSOC, the Transportation Security Operations Center.

Ms. JACKSON LEE. So legislation—thank you. Legislation that would give a framework for this would be helpful, and also the sharing of information would be helpful as well?

Ms. DENBOW. That bilateral part is so important. We feel like—we feel like when we share with the Government, it becomes a landfill of information with nothing valuable coming back out to us in a timely fashion. That is not to criticize the individuals that are working with the process on the Government side. Much like having a valuable by-product out of landfills, such as renewable natural gas, it would be valuable if we could have a valuable by-product out of this data landfill being bidirectional information sharing in a timely fashion of actionable information.

Ms. JACKSON LEE. Thank you.

Any other witnesses——

Mr. MILLER. Congresswoman Jackson Lee, could I also jump in on this briefly?

Ms. JACKSON LEE. I would be very pleased if you would, Mr. Miller. Thank you.

Mr. MILLER. Thank you very much.

You know, just to add on to this—the bidirectional point. It is absolutely critical, and, you know, again, as I was suggesting earlier, you know, it is not only bidirectional information sharing. I mean, what is really key is what is the—what is the goal, and what is the—and what is this bill, for instance, trying to do with—this incident notification bill?

I think that the bill does a good job of articulating some of the different operational, you know, goals that the bill has for CISA. You know, greater situational awareness is certainly part of it. We can all agree that that would be useful, not only for the Government, but for the critical infrastructure community.

But then, also, at least based on our conversations with, you know, the relatively new team at CISA, you know, I think they are really interested in driving deeper operational collaboration between CISA, other Government partners, critical infrastructure owners and operators. I mean, that is really key, right, to—you know, we always hear cybersecurity is a team sport. Maybe it is a cliché because it is true, right?

I mean, CISA—we shouldn't think of it as, you know, does CISA have the information it needs to protect the world from cyber threats, because that is—they are never going to have enough resources to do that. So they have to work with the private sector, and that is why private sector also needs this information.

Ms. JACKSON LEE. This is a new world. We even expect ransomware from now on, and I think we do need this cooperative, collegiate, and important dialog and discourse every moment, if we can, in order to fight against those who intend to really break our infrastructure.

Madam Chair, I am sorry, I am not seeing the time, but do I have any more time?

Ms. CLARKE. Ms. Jackson Lee, your time has expired. We are entering into a second round of questioning. If your time permits and

you have further questions, please keep your camera on and we will acknowledge you.

Having said that, I want to acknowledge——

Ms. JACKSON LEE. That is it. Thank you so very much. I appreciate your patience.

Ms. CLARKE. Absolutely. Absolutely.

I am going to acknowledge myself for 5 more minutes. There are a few more questions that I have for our panelists, and I know that our Ranking Member will be joining me in questioning.

Mr. Bushar, how can CISA use data on cyber incidents to empower security researchers outside of CISA to improve security systemically across sectors? Can CISA do this in a way that protects confidentiality and anonymity of covered entities?

Mr. BUSHAR. Thank you for that question, Madam. Yes, absolutely. There is valuable use cases for information that CISA can share with either universities, public sector, other public-sector entities or private-sector research firms to do deeper-dive analysis, more complex, you know, analytics on information. Things that were mentioned earlier by, I believe, one of the other Members related to more complex sorts of calculations related to machine learning algorithms or other sorts of artificial intelligence-based capabilities that are—today reside largely either in the private sector and academia.

I think there is a huge amount of value in that collaboration and information sharing to allow a broader research community to fully understand and analyze not only individual attacks, but, again, the totality of what we are seeing in cyber space, and hone in on what are some key areas of either resiliency or defensibility, you know, to better protect our sectors or our infrastructure overall.

To your other question related to how that information can be shared or can it be shared anonymously or in a protected way for covered entities, absolutely. We do this all the time as part of our cooperation, not only with Government entities but with research partners, et cetera, where we are able to take collective data in a way that removes any sort of attribution to the source of that information or to the identity of the victim.

It is how we produce a number of our own strategic reports, you know, in—for our customers and for the wider community, and we believe that there is concrete ways for that to be done in a way that protects the identity and confidentiality of the sources of that information but benefits all parties from a research and development effort perspective.

Ms. CLARKE. From your perspective, having worked with CISA and critical infrastructure clients to respond to incidents, what role do you see incident response firms like Mandiant playing in this new reporting regime? Are you concerned that forcing security vendors to report on their customers will undermine trust and discourage owners and operators from working with the companies that have expertise and tools to make them more secure?

Mr. BUSHAR. Thank you for that question, Madam. Yes. On the point of the role that private security firms play in protection and response to cyber threats, it is certainly a capacity issue, as was stated earlier. We believe that there is roles specifically for the

Government to assist directly with victims as well as private-sector partners like us and other firms.

In order to do that in either model, frankly, there has to be a trust relationship. These are often some of the worst days that organizations are facing. There is very, very sensitive information that is being analyzed within the—during the breach and within the organization. You are in a situation of high trust with your clients, whether you are Government support, whether you are FBI, whether you are Mandiant responding to a breach.

The challenge with a mandated model where you are asking a trusted partner of a victim to then report independently of that victim's authorization to the Government of the fact of a breach puts us in a real challenging position—any individual—any organization in a challenging position of betraying one trust in order to provide information to another partner. We don't believe that that encourages a real cooperation or collaboration or effective way of sharing information.

It also can potentially create challenges with contracts and language around legal requirements that we put in place whenever we are working with clients in a trusted manner.

So I do think that the model that has been put forth in this bill, where it is the covered entity themselves, it is the organization that is the victim that is required to and responsible for ultimately reporting is the right model. I think organizations like ourselves are in a good place to advise and support that compliance for the victim, but that organization's security vendor should not be compelled to do that independently of the client that they are working on behalf of.

Ms. CLARKE. Very well. One of the goals in drafting this legislation was to provide CISA with enough information to analyze and understand threats, but do—but to do so without inundating CISA with false positives or inaccurate helpful—unhelpful reports. I think that was raised in the conversation with Mr. Clyde. Toward that end, we have directed CISA to consider a number of factors when defining covered cyber incidents.

This is to the panel. What are the risks of improperly scoping the definition of covered cyber incidents, and how would that frustrate the goals of cyber incident reporting?

Yes.

Mr. MAYER. So I might start here. So what you want to look for is the Goldilocks solution here. It can be too narrow or it could be too broad, and you really have to find that right balance in terms of, you know, laser on that kind of consideration. So the fact that there is a process of engagement, that there is going to be a continuous dialog, I believe, there will be opportunities to say, we didn't do enough, we did too much, or it was too narrow, too broad, and to refine that. But I think there are risks on both sides of that equation.

Ms. CLARKE. Thank you, Mr. Mayer.

Ms. Hogsett, I think I saw your hand.

Ms. HOGSETT. Yes, ma'am. Thank you.

I agree with Robert. I think the thing—the point that we would caution here is, for a number of our financial institutions, they will potentially see thousands of pings against their systems. So if you

leave the definition and the scope too broad, you would literally have, from a single firm, potentially hundreds if not thousands of reports going in, which just is a massive amount, and it is not really the things that are going to, I think, cause the level of concern that you are looking to focus on.

So, again, we do believe that, you know, the opportunity for public comment and dialog with sectors through the rule-making process will help us get to a good place, but we also do need to be respectful that this is going to be a new—new work capability for CISA to build, and we don't want to send too much information to them, because that would be too much noise in the system and you would miss potentially really big things.

Also, for a firm who is then having to report, what that means is you are taking your front-line cyber defenders away from focusing on defending the firm and continuing to keep up with this dynamic threat environment that we have, and instead they are focusing on making sure that they are submitting Government reports so that they are not, you know, missing that perspective.

So I think that is a really critical component to get right, and we appreciate at least that the structure you have put in place would allow for that dialog to get to the Goldilocks moment that Robert mentioned.

Ms. CLARKE. Thank you.

My time has expired. I thank my Ranking Member for his indulgence, and I now yield to him for any additional questions that he may have.

Mr. GARBARINO. Of course, Madam Chairman. That is actually an important question to get out, so I appreciated and enjoyed the witnesses'—their answers.

I want to do a little follow-up. Ms. Hogsett, maybe you could—since most of your Members already deal with reporting requirements, both nationally and for a lot of States, what can we do—is there anything we can do in this legislation to help, you know, harmonize, you know, what you—what your Members have to—have to do so that they are not sending—they are not reporting on several different hacks, you know, one for one agency, one for another, you know, based on different standards? You know, how—what can we do so it is easier for your Members to comply with this law?

I will extend that to some of the other witnesses as well after she answers, because I am sure you all have great opinions.

Ms. HOGSETT. Well, thank you for the question. That is a really critical thing for us.

Attached to my testimony, we did include sort-of a compendium or a summary of the variety of requirements that we already have. This is why there is a provision in the bill currently that requires CISA to coordinate and harmonize requirements for those sectors that already have them in place.

So, for us, this would mean, you know, we would really strongly encourage CISA to work not only with our sector risk management agency, which is Treasury in our case, but also Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation. I mean, we have a multitude. Hopefully, we have done a lot of that work to help funnel that to

a good place where we can help align for them with what we already do, but that is really such a critical point for us, that this gives us an opportunity, hopefully, to have a streamlined requirement with a common set so firms can provide information to one place, and then CISA should be in a position to help work across the Government, including independent regulatory agencies, to share that information out.

Based on the conversations we have been having with our regulators, we do think that everyone is really trying to align and do the right thing to help everybody, you know, protect their institutions, their organizations, and also the broader sector and our Nation. So this is a unique opportunity to do that, and your help and support by ensuring in the implementation that that coordination—that required coordination occurs would be really helpful for us.

Mr. GARBARINO. Great. Thank you.

Anybody else want to add on to that?

Ms.—Mr. Miller?

Mr. MILLER. Sure. Thank you, Ranking Member Garbarino.

Yes. You know, as I mentioned in my—I mentioned it briefly in my oral testimony, and it is certainly in my written testimony as well. I mean, this is really a major issue, and, frankly, even extends beyond the cyber incident reporting context, right? I mean, we have often talked about the need for regulatory streamlining, because we not only—we have a lot of different sector-specific regulators. You know, I don't need to say anything more about that since Heather just took care of that.

But, you know, the reality is there are a number of different security incident notification requirements out there already, right, on companies, you know, not only in the regulated sectors, but, you know, Federal contractors. We have the new Executive Order provision that was mentioned earlier.

One of the things that we recommend is really, you know, leveraging these—the various existing channels that are already set up and having CISA do that to really make sure that, you know, that, frankly, the information is also being shared amongst the regulators, the Federal agency, right? We are talking about bidirectional information sharing but, in this context, it is almost tridirectional.

We also need CISA talking to FBI and the financial regulators and anyone else who really has information or is receiving these reports. One of our recommendations is that perhaps, you know, the Office of Management and Budget could issue guidance to Federal regulators and law enforcement requiring this sort-of sharing of information to make sure that we are actually having a—you know, an impact on the regulatory overload, you know. I appreciate the bill for taking the first step in acknowledging the need, so thank you.

Mr. GARBARINO. Yes. Ms. Denbow, I know you are—I think one of the next things we have to do is maybe do a little Federal preemption, all these different State rules that you all have to deal with. We won't get into it now, but I know—I am sure I could guess how you all feel, but——

Mr. MILLER. Right. It is beyond your scope perhaps, but there are also international rules that we need to deal with, so——

Mr. GARBARINO. Oh, yes. One thing at a time.

Ms. DENBOW. So I believe that the biggest challenge really is—and I speak from experience at the American Gas Association. We worked effortlessly to try to pull together a harmonization of all the different cyber assessments out there, from all the different agencies: Department of Energy, Department of Homeland Security, TSA. We were able to do something like that. But then when you take it back to those different offices, they believe that their system is the one system that works best.

So I believe that is where—the challenge is actually going to be on Congress to convince the different agencies that there is one system as opposed to all the different systems, or how the—all the different systems that are out there are not going to be overly burdensome to the operator.

Mr. GARBARINO. I appreciate those answers. Thank you so much. We will definitely take that into consideration.

Madam Chairwoman, I yield back, but thank you again for having this great hearing today.

Ms. CLARKE. I thank you very much, Mr. Ranking Member.

I want to thank our witnesses for their valuable testimony, and the Members of the subcommittee for their questions.

The Members of the subcommittee may have additional questions for our witnesses, and we ask that you respond expeditiously in writing to those questions.

The Chair reminds Members that the subcommittee will—record will remain open for 10 days—10 business days.

Without objection, the subcommittee now stands adjourned. Thank you for joining us today.

[Whereupon, at 1:47 p.m., the subcommittee was adjourned.]

○