USTELECOM | THE BROADBAND ASSOCIATION

**Testimony of Robert Mayer**

**Senior Vice President Cybersecurity & Innovation, USTelecom – The Broadband Association**

**Before the**

**U.S. House of Representatives Committee on Homeland Security,**

**Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation**

**Hearing on:**

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

**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 firsthand 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

[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.

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. And 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.

We have also seen the benefit of this engagement in the DHS ICT Supply Chain Risk Management Task Force over the past two 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

[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.

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

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

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 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 ongoing 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). Policymakers 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.