Testimony of Robert Mayer
SVP, Cybersecurity
USTelecom – The Broadband Association

Before the House Homeland Security Committee's Subcommittee on Cybersecurity and Infrastructure Protection

Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime

March 11, 2025

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee,

Thank you for the opportunity to testify today on the critical issues of cybersecurity incident reporting and regulatory harmonization. We are committed to strengthening the public-private partnership to bolster our national security and stay ahead of our adversaries. This Committee has an extraordinary opportunity to reset our national cybersecurity policy in ways that directly impact security outcomes.

Our nation is under constant cyberattack, with estimates of up to $23 trillion in annual damages by 2027, increasing at a rate of more than 20% per year.[1] We must take immediate action to eliminate redundant or conflicting cyber regulations, which can consume up to 70% of cybersecurity resources.[2] By streamlining these requirements, we can free up critical resources for threat mitigation and incident response—at virtually no cost.

Let me reaffirm our view that it is essential we fix how the Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) needs to be implemented. While well-intentioned, it is essential that we refine its execution to ensure consistency with the law's original intent. Specifically, key terms such as "covered incident," "covered entity," and "reasonable belief" must be clearly defined. The liability protections designed to safeguard cyberattack victims and promote candid reporting must be strengthened. As of today, none of these fundamental issues have been meaningfully addressed in a manner visible to industry, nor has our sector been substantively engaged in addressing these concerns.

We urgently need an ex parte process—which is to say a formal, transparent, and common process that encourages CISA to hear and consider industry perspectives. In fact, USTelecom spearheaded a letter by 21 organizations that formally requested that CISA establish such as process; a request that was rejected.

Had this request been granted immediately, we would have already been working together to resolve these challenges. If we do not act quickly, we will end up with a rule that does more harm than good.

---

[1] *See* The Economist, "Unexpectedly, the cost of big cyber-attacks is falling" (May 17, 2024).
[2] Chamber of Commerce, Briefing with Majority and Minority Staff of Senate Homeland Security and Government Affairs Committee (May 29, 2024).

We must also recognize that this law does not exist in isolation. The patchwork of federal, state, and sector-specific cyber incident reporting requirements presents an ever-growing burden on organizations attempting to comply with multiple, often conflicting, mandates. Fortunately, there is a strong lawmaker interest to harmonize cyber regulations, including incident reporting requirements.

We believe the Office of the National Cyber Director (ONCD) should play a leading role in rationalizing cybersecurity regulations and incident reporting regimes. Solving the problem of fragmented state laws will require clear federal preemption, complemented by robust safe harbor provisions. This work must be prioritized, as it is directly tied to our national security.

We believe it is important that Congress acts now. We do not have time for further studies, requests for information, commissions, or pilot programs. Every moment spent delaying reform provides adversaries with additional opportunities to undermine our collective security. We must move swiftly and decisively to enhance our cybersecurity posture.

Major recent cybersecurity incidents have highlighted the importance of a stronger and more coordinated information sharing and incident response partnership between the federal government and the private sector. Congress advanced that project with the Cybersecurity Information Sharing Act of 2015, which is set to sunset in September 2025. We ask that Congress extend the Act, and establish additional policies to improve the public-private partnership.

Key pillars for improve this partnership include:

- ***There Should Be a Single Responsible Federal Agency for Major Cybersecurity Incidents.*** In the midst of a major incident, an operator's cybersecurity team is tightly focused on understanding and mitigating the challenge, and may be coordinating with other affected entities and/or with one or more law enforcement or national security agencies. It is practically difficult and often inadvisable to pull away from those operational imperatives to engage in briefings or other general information sharing and analysis activities (which takes substantial time and effort) with multiple government stakeholders absent concrete benefits to doing so.
    - Accordingly, Congress should ensure a unified, whole-of-government approach to major cybersecurity incidents: In the wake of a major incident with national security implications, a single "Responsible Agency" should have formal responsibility for (i) coordinating with the private sector and (ii) overseeing government information-sharing during a cybersecurity event.

- ***Power to Suspend Reporting Obligations***. Congress should grant the Responsible Agency the power to suspend all federal, state, and contractual reporting obligations upon a finding that doing so is in the national interest. Otherwise, the existing patchwork of reporting regimes (e.g., FCC, SEC, CIRCIA, government contracts, private contracts) could cause highly sensitive information to be promulgated in a haphazard manner.

- **Expanded Government Sharing of Actionable Cybersecurity Information.** Whether sharing information about a specific incident or a potential or known threat, the government should focus on getting detailed, actionable tactical information in the hands of the private sector personnel responsible for protecting communications networks.
    - ***Security Clearances for Private Sector Leaders.*** Private sector CISOs and other key cybersecurity professionals should be granted security clearances (subject to appropriate vetting). Security clearances should not be tied to whether an individual is involved in a particular government project or program.
    - ***Secure transfer mechanisms.*** Congress should fund a streamlined method for government agencies and the private sector to securely transmit and receive sensitive information.

- ***Promote Meaningful Private Sector Sharing of Sensitive Information.*** Policies for promoting information sharing need to promote voluntary private sector information sharing:
    - ***Confidentiality of information shared by industry.*** Enact legislation that would create major penalties for individuals within the government that breach confidentiality or share information without authorization during a national security cyberattack investigation. The private sector will not share highly sensitive information with the government if there is a risk government employees receiving the information will leak it.
    - ***Immunity for information shared by industry.*** Establish a strong "Reverse Miranda" regime where information shared by a private actor cannot be used against it in any future action or proceeding.
    - ***Limited number of recipients.*** Private actor needs assurances that sensitive information it shares will only be available to a small number of government officials and companies. Operators will not meaningfully share information if the pool of recipients is too large or includes potentially untrusted persons/entities.

We must also be willing to reconsider policies that have failed to produce meaningful security benefits. One such example is the Securities and Exchange Commission's (SEC) cyber disclosure requirements, which, rather than enhancing security, have inadvertently provided malicious actors with a roadmap to exploit vulnerabilities. These mandates must be reassessed to prevent them from serving as a tool for cybercriminals.

In conclusion, success in cybersecurity requires close collaboration between industry and government, including Congress and the Office of the National Cyber Director. We must act now to ensure that our cybersecurity policies are well-reasoned, well-informed, and designed to maximize efficiency and effectiveness. By fixing CIRCIA's implementation, harmonizing cyber regulations, and eliminating unnecessary burdens, we can strengthen our nation's cyber defenses and uphold our commitment to protecting national security.

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