Testimony of Robert Mayer

Senior Vice President
Cybersecurity and Innovation
USTelecom – The Broadband Association

U.S. House of Representatives Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

Hearing on

Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking

May 1, 2024

Chairman Andrew Garbarino, Ranking Member Eric Swalwell, Members of the Subcommittee, thank you for convening this hearing on implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), perhaps the most important of the foundational cybersecurity-related statutes Congress has passed. My name is Robert Mayer, and I am the Senior Vice President, Cybersecurity and Innovation at USTelecom and serve as the Chair of the Communications Sector Coordinating Council and Co-Chair of the DHS ICT Supply Chain Risk Management Task Force.

It is absolutely crucial to our national security that CISA, critical infrastructure entities, and other government agencies work collaboratively to implement Congress's vision for this law – to deepen and operationalize the partnership between government and industry that is indispensable to our defense against cyber threats.

As this Subcommittee is well aware, the United States' adversaries – China, Russia, Iran, North Korea – are increasingly becoming an aggressive military alliance, and those governments and their criminal proxies have extremely sophisticated cyber capabilities. We need close and well-coordinated teamwork between government and industry to ensure our defense.

CIRCIA can be a profoundly powerful tool in deepening this collaboration and teamwork, and I implore the Subcommittee to push this principle relentlessly in the years to come.

Unfortunately, parts of our government risk undermining this principle, as we increasingly see a rigid regulatory mindset focused on prescriptive compliance rather than dynamic teamwork. This manifested last week in the FCC's misguided order that will impose 20th century utility-based prescriptive regulations on Internet Service Providers — including even in the realm of cybersecurity — which are investing billions of dollars to innovate for the 21st century.

As the most dynamic and innovative nation in history, we need to recognize that our defense against these threats requires us to deepen our collaboration. We need to double down on, not undermine, the government-industry partnership. At this very moment, and literally every moment, experts in government and private industry are working shoulder to shoulder to outwit and outpace highly

organized efforts to infiltrate our nation's critical infrastructure. That is the only approach that will work.

Thankfully, the launch of CIRCIA can help get this right, because CIRCIA – if properly implemented – is fundamentally about collaboration and holistic situational awareness. Now, it is incumbent on government and industry partners to roll up our sleeves and collectively begin the work of translating Congress's directions into operational reality.

To be clear, CIRCIA implementation is an enormous task – CISA estimates that 300,000 entities will be covered by its requirements – and it will take years and multiple iterative exchanges between government and critical infrastructure entities to fully mature. Here again, the more collaboration and partnership we practice, the more we can develop mutual understanding and expectations of what is needed and how to achieve it.

There are several areas in particular that we believe need our collective attention.

For one, we need clarity on the terms and definitions in the rule. Without sufficient specificity, this is difficult to accomplish. The proposed scope of "covered entities" and "covered cyber incident" are expansive and currently lack key guidance that cybersecurity practitioners will need, as they seek to provide CISA with information that is responsive to the agency's mission.

Moreover, it is imperative for our government partners to recognize the substantial cyber resources that will be allocated to assess whether an event meets the reporting criteria. The industry requires more precise definitions and clear reporting thresholds. Without these, there is a real risk that, in an effort to comply with the law, the industry will report numerous events that could easily overwhelm CISA's capacity to act on the information. Such overreporting could unnecessarily burden government resources and undermine the effectiveness of CIRCIA. It is crucial to establish definitions that are not excessively broad, as overly inclusive terms could divert essential resources away from cyber defense and towards regulatory compliance for its own sake.

Critically, we believe that covered cyber incidents should only be those pertaining directly to the mission of CISA and avoid unproductive and disproportionate focus on routine events.

It is also important to underscore that partnership implies reciprocity. To fulfill CIRCIA's purpose, CISA needs to establish mechanisms of rapidly disseminating valuable defensive advisories to critical infrastructure entities while also supporting victims as they respond to highly debilitating attacks.

The estimated cost to industry of these new requirements is $1.4 billion over eleven years, and it is estimated the federal government will incur costs of $1.2 billion over the same timeframe. Collectively, our nation needs a return on this investment and for the law to achieve its aims. We will work with CISA to ensure that meaningful incident reports lead to broader situational awareness and to increased operational preparedness and response capabilities.

It is also vital that we achieve harmonization and efficiency in reporting. Our members, from the smallest to the largest, have expressed concern about the substantial resources they will need to dedicate to complying with a rapidly growing patchwork of incident reporting requirements. Our ask from federal government partners is this: Providers need to be able to submit reports to a single agency. It will be essential to streamline the contents of reports as much as possible – by developing a common format – while allowing a variety of flexible reporting mechanisms that could ideally be tailored to the unique needs of organizations.

Finally, we call on CISA to establish ex parte communications for the CIRCIA rulemaking. This is a critical step toward ensuring a robust regulatory framework that reflects the intricate realities of cybersecurity in critical infrastructure sectors. As CISA now possesses enhanced regulatory powers, it is imperative that the agency adopts a transparent and open process akin to that employed by other regulatory bodies. This approach will facilitate continuous and meaningful input from industry stakeholders, whose expertise and firsthand experience are invaluable for crafting regulations that are not only effective but also practical. Such a process would not only enhance the quality and applicability of the regulatory outcomes but also bolster the credibility and trustworthiness of CISA as a regulatory authority in the eyes of the industries it regulates.

Deep and persistent collaboration is the key to achieving Congress's intent in implementing CIRCIA, and USTelecom and its members will continue to work closely with CISA, our sector risk management agency, through the Communications Sector Coordinating Council and other fora, and by actively participating in the CIRCIA rulemaking process. For decades, we have engaged consistently with CISA, its predecessors, and other government agencies to provide information about cyber threats and to advance law enforcement investigations, and we will continue to deepen and evolve that practice.

We seek the government's continuing partnership in making that a reality. I look forward to your questions.