TESTIMONY OF THE NEW ENGLAND CONNECTIVITY & TELECOMMUNICATIONS ASSOCIATION, INC. REGARDING HB 1728

February 10, 2025

Chairman Vose, Vice Chairman Thomas, and distinguished Members of the House Committee on Science, Technology and Energy,

On behalf of the New England Connectivity and Telecommunications Association (NECTA), we appreciate the opportunity to submit testimony detailing our industry's concerns with HB 1728, ***An Act requiring sufficient cybersecurity protections for critical infrastructure and technology projects.*** Throughout New England, NECTA members provide state-of-the-art Internet, video, voice, and wireless offerings as well as cutting-edge products, services, and emerging technologies. NECTA members operating in New Hampshire include Breezeline, Charter Communications, and Comcast. Together, our members service approximately 485,000 customers and offer their services to more than 695,000 locations in 185 New Hampshire communities.

In an era of rapidly evolving cyber threats, NECTA members are committed to protecting their networks and customer data. Connecting computers, phones, tablets, game systems, security systems and smart home devices wouldn't be possible without secure network protocols, that enable devices to exchange information safely and reliably. Successful cybersecurity strategies are integral to the company culture of NECTA members who participate in national and global industry initiatives with both the private and public sectors. In partnership with federal and state agencies, NECTA members and the larger communications industry are constantly assessing and improving our preparedness and response to potential and realized threats to our critical infrastructure. Our member companies take very seriously our obligation to ensure that our nation's communications infrastructure is secure and safe from threats.

HB 1728 contemplates requiring a standard of care for operators of critical infrastructure, including communications systems, to secure such systems from cyber-attacks. If enacted, this bill would contravene established Federal policy, codified in the Cybersecurity Enhancement Act of 2014, favoring reliance upon voluntary mechanisms forged through public-private processes and industry-driven initiatives to combat cybersecurity threats. The 2014 Act expressly

established "voluntary, consensus-based, industry-led" measures as the preeminent Federal policy mechanism for strengthening the cyber defenses of American companies. The ever-evolving nature of cybersecurity threats requires partnership, trust and cohesion between government and business. To impose a new state legal standard (one that has not been adopted in any other state or by the federal government) to cybersecurity protection would have a chilling effect on coordinated preventative response measures.

Our industry works tirelessly to ensure the safety and security of our customers. Not only do we actively participate in emergency preparations with federal and state agencies, but we also work to ensure the functionality of 911/988 systems, broadband infrastructure, and cybersecurity. Our members detect, deter and defeat billions of attempted cyber intrusions against our network and our customers annually.[1] In addition to investing heavily in cybersecurity measures to protect our networks, NECTA members also participate or follow federal law and guidelines. Below are some examples of how our members work with government to prepare and address cybersecurity attacks.

National Institute of Standards and Technology (NIST) Cybersecurity Framework

The NIST Cybersecurity Framework established a voluntary, risk-based approach to strengthen security for network operators. It focuses on six core functions (govern, identify, protect, detect, respond, recover) to manage risks, secure supply chains, and protect infrastructure. Following the NIST standards is also a mandatory and essential requirement for compliance with the Broadband Equity Access and Deployment (BEAD) program under which New Hampshire is set to receive just under $200 million.

Cybersecurity and Infrastructure Security Agency (CISA) National Emergency Communications Plan

CISA has written guidelines to protect against events such as natural disasters, network and grid failures, terrorism, lightning, and electromagnetic pulse events. The plan includes addressing interoperability challenges, increased information sharing, ensuring the most critical information gets to the right people in time to effectively act, building resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 also imposed obligations on operators of critical infrastructure to report cyber incidents to CISA within specified timeframes.

Federal Communications Commission (FCC) Mandatory Disaster Response

Our industry participates in exercises testing emergency plans for all levels of disasters including ones that would completely cripple our communications and cybersecurity infrastructure. The

[1] file:///C:/Users/ALucey/Downloads/2025_Comcast_Business_Cybersecurity_Threat_Report.pdf; https://policy.charter.com/protecting-our-networks

FCC provides significant guidance on how to prepare.[2] The guidance includes preparations for communications and continuity of operations, redundant/back-up communication systems, diversity of communication systems, emergency notifications, security, power, equipment testing, mutual aid agreements, emergency response process, and recovery procedures.[3] The FCC's Enforcement Bureau also investigates data breaches in the telecommunications sector.

Finally, the duty of care standard proposed in HB 1728 would do little to prevent cybersecurity attacks. The harsh reality of network security and the activity of nation-state actors is that even well-defended systems, both public and private, get breached. Given the national security implications involved with a breach, it is important that operators of critical infrastructure are open about attacks to assess whether other businesses face a similar threat and improve security measures. Fear of liability, like HB 1728 would create, would undermine such necessary transparency among operators.

As there is already a strong federal framework for cybersecurity prevention and incident reporting that HB 1728 would disrupt, we respectfully urge the Committee to vote HB 1728 inexpedient to legislate. We thank you for your attention to this testimony. Please do not hesitate to reach out with any questions.

Sincerely,

Timothy O. Wilkerson, President
NECTA
twilkerson@connectingne.com
781.843.3418

Maura M. Weston
MM Weston & Associates, PLLC
maurаweston@comcast.net
603.491.2853

[2] *See* https://www.fcc.gov/research-reports/guides/emergency-planning-public-safety-answering-points
[3] *Id.*