WRITTEN COMMENTS OF THE NEW ENGLAND CONNECTIVITY & TELECOMMUNICATIONS ASSOCIATION REGARDING SENATE BILL No. 2487

March 3, 2026

Dear Chair LaMountain and Members of the Senate Judiciary Committee,

On behalf of the New England Connectivity and Telecommunications Association (NECTA), I appreciate the opportunity to submit testimony in opposition to Senate Bill No. 2487, establishing a Digital Electronics Right to Repair Act. Overall, this legislation would impact cable broadband operators' ability to conduct routine maintenance and deploy upgrades to their services and also poses significant security and privacy risks to our company's various electronic products, networks, and customers.

First, because many cable and broadband customers lease equipment from their providers, the definitions of SB.2487 are overly broad and unnecessary. Most customers elect to lease for a variety of reasons, including the convenience of swapping out a device if it is not working properly. In these instances, the consumer has no obligation to repair the device, which completely defeats the purpose of the bill by requiring companies to offer more consumer choice in the repair process.

Further, modern cable broadband networks routinely conduct maintenance and service upgrades remotely on electronic devices in customers' homes. These upgrades add functionality, proactively make repairs, and address emerging performance issues. With millions of devices connected to the network, these upgrades are carefully choreographed, complex exercises that are designed to ensure customers can use their newly upgraded or repaired equipment without any interruption. Even well-intended repairs made by an independent repair provider could impede the deployment of updates, upgrades, and customer service measures or make these necessary updates and upgrades ineffective. Changes made to devices by independent providers could thereby result in degraded functionality and customer dissatisfaction.

In addition to its impact on routine maintenance and service upgrades, SB.2487 would also pose extreme security risks to cable operators' services. Cable operators deliver video content over their cable systems, subject to extensive contractual obligations with program suppliers. These include requirements that content will be delivered securely using robust content protection methods both in the network and in the set-top boxes and other leased equipment used by customers, as well as substantial contractual penalties if these security measures are breached. SB.2487 would create significant risks that could be exploited by pirates using unauthorized parts to hack into cable set-top boxes and the cable network and steal content. The end result could be billions of dollars in potential liability to cable

operators, to say nothing of lost revenues from the proliferation of pirate video services. Section 629(b) of the federal Communications Act makes clear that neither the Federal Communications Commission nor the states can "prescribe regulations [that] would jeopardize the security of multichannel video programming and other services offered over multichannel video programming systems or impede the legal rights of a provider of such services to prevent theft of service." Yet, SB.2487 would do precisely that.

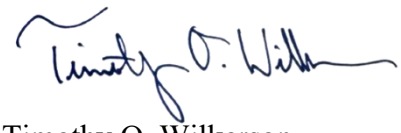
Finally, SB.2487 would expose broadband networks to security threats that could negatively impact customer security and privacy by allowing any individual who owns a repair company, or claims to be qualified to repair or offer maintenance services, access to virtually any electronic device's security protocols, including the device's firmware. This includes the right to unlock and disable a device's security features. Access to these features creates an unacceptable level of risk to the customer and the provider. It is entirely reasonable to foresee that malicious actors will use these provisions to gain access to individuals' and businesses' most closely held secrets. For example, access to a home security device could allow changes to the system to allow unauthorized use or exploitation. Such uses might include unauthorized unlocking of door locks, thus allowing access to homes and business premises. Other acts could include unauthorized access to a customer's video cameras or other in-home devices to allow remote viewing or monitoring. Likewise, access to providers' modems and Wi-Fi devices by malicious actors could expose broadband cable customers to substantial security risks. Bad actors could implant additional software (malware) on provider's modems and Wi-Fi devices to steal sensitive customer information or monitor a customer's activity.

In order to ensure the security of our cable and broadband customers, NECTA respectfully requests that the committee amend the bill to include the following provision:

(f) Nothing in this chapter shall apply to any entity or their affiliates regulated by the Federal Communication Commission or the Rhode Island Public Utilities Commission.

Without the inclusion of this important clarifying language, NECTA must oppose the legislation. Thank you for your attention to this matter. Please do not hesitate to reach out with any questions.

Sincerely,



Timothy O. Wilkerson
President

About NECTA

NECTA is a five-state regional trade association representing substantially all private cable broadband providers in Rhode Island, Connecticut, Massachusetts, New Hampshire, and Vermont. In Rhode Island, NECTA represents Cox Communications. Cox produces an estimated $850 million annually in economic activity in the state and employs over 600 Rhode Island residents generating over $57 million in wage and salary payments.