Jan. 6, 2026

To Chairperson Curry, Chairperson Gere, and the distinguished members of the Committee on Housing and Economic Development—

My name is Joseph Lee, and I work for Cisco Systems.

Cisco Systems is a global technology company that develops, manufactures, and sells the networking hardware, software, and security solutions that power the internet. Our technology is primarily used in business-to-business and business-to-government contexts—from federal agencies to local school districts.

Cisco respectfully opposes LD 1908 due to the severe cybersecurity risks this bill would pose to critical infrastructure if passed as drafted. However, we believe these risks can be mitigated without undermining the bill's intent to help consumers.

While Cisco appreciates the arguments offered in favor of right to repair consumer devices, not all digital technology devices are equal. A router used in a home is fundamentally different from the infrastructure equipment used to manage a power grid or secure confidential state data.

To address this, we respectfully request two specific amendments on page 1 and 2 of the bill to clearly define the scope of covered devices. Specifically, we ask that the legislation be tailored to cover consumer technology devices only.

As currently written, the legislation inadvertently includes the networking and telecommunications equipment used by critical infrastructure owners and operators in government and enterprises. These industrial-grade devices are typically sold to the federal government—like the Pentagon and US Department of Homeland Security—as well as to state and local government customers like local Departments of Transportation and Public Safety. These devices take on massive workloads and carry sensitive information that our government customers rely on for their mission-critical operations.

The risks associated with forced disclosure of source code, encryption keys, schematics diagrams, and other sensitive or proprietary technical information are too high. Our nation's critical infrastructure has been under repeated attack by aggressive foreign nation-state actors, and providing unvetted access to this sensitive technical information creates a "blueprint" for cyberattacks against government and enterprise networks.

We also have concerns regarding the bill's definition of "independent repair provider" on page 6. Cisco maintains a rigorous vetting process for our partners and authorized resellers to ensure the delivery of high-quality, secure products and services for our customers, as well as safety and environmental responsibility. Detailed technical knowledge and training are required to repair or refurbish products, and Cisco carefully vets, trains, and authorizes professionals to carry out the crucial tasks of repairing, recouping, decommissioning, and refurbishing devices.

The standards outlined in the proposed draft could be detrimental to the technology marketplace by requiring disclosure of sensitive security information to any entity claiming to have a need to repair a Cisco device. This broad mandate could force manufacturers to hand over security bypass tools to unverified actors—potentially including those with malicious intent—under the guise of repair.

We understand the argument that this bill addresses major concerns by protecting trade secrets and scoping out the requirement to disclose security-sensitive information. However, in practice, these exceptions are insufficient to protect national security assets.

The bill prioritizes the rights of a single equipment owner over the collective security of the entire network. While such a balance might be appropriate for consumer IoT devices, it presents disproportionate risks when applied to commercial and enterprise ICT technologies that support critical infrastructure, national security, and emergency preparedness.

Thank you for allowing me to testify on this important issue. I respectfully ask that this bill receive additional consideration because of the cybersecurity implications and the credible threats that are likely if this legislation were to pass in its current form.