



October 19, 2025

Cisco's Position on HB 301: Support with Amendments

To Dear Chair Claggett, Vice Chair Workman, Ranking Member Mohamed, and the Honorable Members of the Technology and Innovation Committee,

Cisco Systems, a global technology company that develops, manufactures, and sells networking hardware, telecommunications equipment, and technology services, supports HB 301 with amendments.

While Cisco understands the legislative argument on Right to Repair, the proposed regulations found in HB 301 can pose a risk to existing repair operations performed by original electronic manufacturers, because of two main reasons: 1. Cisco cannot determine who "an independent repair provider" is; and 2. The security risk of sensitive information within the equipment.

On pages 3-4, HB 301 does not properly review or closely examine who qualifies to be an "independent repair provider" whereas Cisco maintains a rigorous vetting process with its partners that focuses on the delivering high quality products for our customers. There is no substitute for the technical skills needed to repair or refurbish products, and the standards outlined in HB 301 could be detrimental to the technology marketplace.

The risk increases for products where sensitive data may be put at risk during the repair process. There will be unintended consequences where Cisco's proprietary information could be compromised by handing it over to an unvetted third party, which could expose more vulnerabilities with customer's data or sensitive account information.

There are also the issues of sustainability and the environment. For companies like Cisco, this means that we are re-thinking the way our business operates and the way we provide products and services to our customers. We want to reuse more of our equipment. We also want to re-manufacture and refurbish more of the products we make, so we can give them new life with more customers.

This means that when we work with a business, we are considering the entire lifecycle of the service we provide. The hardware that enables that service might be leased or used as-a-service rather than purchased directly. When the hardware is no longer needed, it is easily returned to Cisco. That equipment can then be remanufactured or refurbished to have new life somewhere else — all while maintaining the security for which Cisco is known.

To remedy Cisco's concerns, I suggest the insertion of two of the following amendments:

- (k). digital electronic equipment sold in a transaction involving only business or governmental entities.*
- (l). information technology equipment that is intended for use in critical infrastructure as defined by 42 U.S.C. Section 5195c(e)*

Under Section (2) "Digital electronic equipment" does not include any of the following, on page 2.

Regards,
Joseph Lee