



Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
Direct: 408 526 4000  
www.cisco.com

January 23, 2024

The Honorable Jacquelyn Baginski  
House Innovation, Internet and Technology Committee, Chair

Cisco's Position on H 7095: Support with Amendments

Dear Chair Baginski,

Cisco Systems—a global technology company that develops, manufactures, and sells networking hardware, telecommunications equipment, and cybersecurity and technology services—can support H 7095 with amendments that keep the bill focused on consumer products by exempting business-to-business (B2B) and business-to-government (B2G) product lines, and that introduce adequate protections to ensure the security of networking infrastructure.

As written, H 7095 will have the unintended consequence of overreaching into enterprise products, which is particularly concerning for products in network infrastructure. Allowing unauthorized, third-party entities unfettered access to trade secrets and private information could compromise cybersecurity for enterprises and governments as well as potentially expose their data or sensitive account information. To address this, we recommend limiting the scope to specific products—such as laptops, smartphones, and tablets—and to exempt products sold for use by enterprises and governments.

At Cisco, our enterprise resellers are contractually bound to meet Cisco's strict security standards, and they undergo a rigorous program where they are trained and certified to sell, provide customer service, and troubleshoot problems. We are also rethinking how our business operates and how we can provide products and services more sustainably. We want to reuse more equipment, and when we work with a business, we are considering the entire lifecycle of the service we provide. When 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 new sections—definition of "critical infrastructure" under *Subsection 13. 6-60-3. Definitions*, and a new exemption in *Subsection 6-60-5 Limitations*:

*Definition. 13. "Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."*

*6-60-5 Limitations. (f) Nothing in this chapter shall apply to: A. any product sold under a specific business-to-government or business-to-business contract, which is not typically offered for sale directly by a retail seller; B. information technology equipment that is intended for use in critical infrastructure as defined."*

Sincerely,

Jeff Campbell  
SVP & Chief Government Strategy Officer  
Cisco