July 21, 2025

The Honorable Brian Mast
Chairman, Committee on Foreign Affairs
U.S. House of Representatives
Washington, DC 20515

The Honorable Gregory Meeks
Ranking Member, Committee on Foreign Affairs
U.S. House of Representatives
Washington, DC 20515

Chairman Mast and Ranking Member Meeks:

The undersigned associations represent the most innovative technology companies in the United States, spanning across the technology ecosystem that drives the economy and America's global leadership in AI. We write on behalf of our members to express our serious concerns regarding the Chip Security Act (H.R. 3447) and respectfully urge the House Foreign Affairs Committee to consider alternative approaches before bringing it to a vote in the Committee.

While we greatly appreciate the Committee's efforts to address the issues raised, we remain concerned with a legislative approach that would require untested geolocation frameworks on the export of U.S. advanced compute chips and other technologies critical to AI data centers globally, and impose burdensome notification and reporting requirements on export license holders. The proposed new technology requirements are not validated at a global deployment scale, untested against adversarial environments, and untested for reliability and security. Before technology requirements are enacted into law, it is also necessary to understand the scope of the challenge, assess whether any such approach is appropriately targeted and effective to address the underlying challenge, determine whether other policy tools may be more effective or appropriate, and weigh the risks and unintended consequences.

We strongly oppose the illicit diversion and misuse of advanced American technologies and many of our companies have already deployed a range of effective "compliance-plus" tactics to counter this problem. We support the continued use of existing export enforcement resources to deter, detect, and disrupt illicit procurement of U.S.-origin advanced technology. As a first step, we believe Congress should prioritize adequately resourcing security and export control enforcement-related agencies and ensure that they work with our global partners to enforce the law. Enforcement agencies will require and have requested additional resources for intelligence and counterproliferation tools to identify malign end-users and diversion efforts and increase enforcement actions against bad actors.[1] Statutory technology requirements should be a tool of last resort.

The feasibility and effectiveness of any statutory technology solution should undergo rigorous technical standardization, be thoroughly tested in real-world environments, and prove to be a highly secure and scalable solution before enactment into law. Technology demonstrations conducted in closed, highly controlled settings do not reflect real-world complexities of large-scale deployment. Without first clearly defining the issues, studying the technical feasibility, developing technical standards and tested solutions, this proposed framework risks a fragmented, ineffective, insecure, and incompatible approach while imposing steep costs and regulatory

[1] Testimony of Under Secretary Kessler, Bureau of Industry and Security to HFAC Subcommittee on South and Central Asia (2025, June 12) https://docs.house.gov/meetings/FA/FA19/20250612/118369/HHRG-119-FA19-Wstate-KesslerJ-20250612-U1.pdf

burdens on U.S. industry and undermining trust in American technologies around the world. Rushing to enact unproven security features could also negatively impact performance and reliability of American technologies and, importantly, introduce security vulnerabilities.

The directives prescribed in the legislation also fail to consider the real-world feasibility and complexities of tracking tens of millions of chips and AI servers across the globe, including those already in circulation, and the ways in which bad actors can circumvent or manipulate the new security measures. For example, the legislation presumes all chips and data centers have reliable connectivity for location verification and remote attestation. In practice, many data centers operate in an "air-gapped" environment, with either intermittent or no internet connectivity blocking the ability to geolocate a chip or server. Unlawful access to technology may also occur remotely or via travel across borders to gain access to necessary compute power enabling the development of AI technologies or other advanced capabilities.[2] Failure to address these and other complex challenges would result in both a failure to achieve the goals of the legislation and place undue burden on American technology companies.

As an alternative to the technology directives in the bill, a more prudent approach would be for the National Institute of Standards and Technology (NIST) to lead a comprehensive technical feasibility and standardization review process. NIST has a proven record of conducting independent, science-based evaluations of security technologies—whether they be hardware, software, or firmware—ensuring that proposed mechanisms are technically sound and practically deployable. By placing NIST at the forefront, the review process would benefit from open collaboration with industry, academia, and government stakeholders. We strongly urge lawmakers to work with technical experts at NIST and in the semiconductor industry to jointly evaluate proposed technology security approaches before prescribing any new statutory requirements.

We respectfully request the Committee further consider these concerns and the approaches outlined above before moving forward with the Chip Security Act. Advancing legislation that authorizes untested technology requirements on industries key to America's global AI and technology leadership could come at too great a cost and without achieving its stated goals. We again commend the Committee's outreach to industry and look forward to continued engagement on this matter.

Sincerely,

Computer & Communications Industry Association (CCIA)
Consumer Technology Association (CTA)
CTIA
Cybersecurity Coalition
Semiconductor Industry Association (SIA)
TechNet
Technology Trade Regulation Alliance (TTRA)

[2] Reuters. (2024, August 23). *Factbox: List of Chinese entities who have turned to the cloud for access to restricted U.S. tech*. Reuters. https://www.reuters.com/technology/list-chinese-entities-who-have-turned-cloud-access-restricted-us-tech-2024-08-23/; Huang, R., & Lin, L. (2025, June 13). *Chinese AI companies dodge U.S. chip curbs by flying suitcases of hard drives abroad*. *The Wall Street Journal*. https://www.wsj.com/tech/china-ai-chip-curb-suitcases-7c47dab1