Cybersecurity Coalition

November 3, 2025

Via electronic submission
Jamieson Greer
U.S. Trade Ambassador
600 17th St NW
Washington, DC 20508

Re: Request for Comments on the Operation of the Agreement between the United States of America, the United Mexican States, and Canada - Docket No: USTR-2025-0004

Dear Ambassador Greer,

The Cybersecurity Coalition (the Coalition) submits these comments in response to the Office of the United States Trade Representative's request for comments on the Operation of the Agreement between the United States of America, the United Mexican States, and Canada (USMCA or Agreement).[1]

The Coalition is composed of leading companies with a specialty in cybersecurity products and services, who are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace and effective policy environment that will encourage companies of all sizes to take steps to improve cybersecurity risk management.

Building upon the Coalition's prior submissions to USTR during the 2017 NAFTA modernization process[2] and the 2019 U.S.-UK trade discussions,[3] this submission reflects the Coalition's continued commitment to advancing strong cybersecurity provisions in trade agreements. In our earlier comments, we emphasized the importance of enabling secure cross-border data flows and promoting cooperation on cybersecurity information sharing – principles that we are pleased to see reflected in the current USMCA text.

[1] Office of the United States Trade Representative (USTR), "USTR Seeks Public Comment on the Review of USMCA," Sept. 16, 2025, ustr.gov/about/policy-offices/press-office/press-releases/2025/september/ustr-seeks-public-comment-joint-review-usmca.
[2] Cybersecurity Coalition, Comments re NAFTA Renegotiation, Jun. 2017, https://www.regulations.gov/document/USTR-2017-0006-1273.
[3] Cybersecurity Coalition, Request for Comments Response to the United States Trade Representative on Negotiating Objectives for a U.S.-United Kingdom Trade Agreement, Jan. 2019, www.cybersecuritycoalition.org/filings/request-for-comments-response-to-the-united-states-trade-representative-on-negotiating-objectives-for-a-u-s-united-kingdom-trade-agreement.

We commend the inclusion of these foundational provisions and urge the Parties to reinforce and expand upon them to reflect the central role that data flows and information sharing play in today's cybersecurity environment. The ability to transfer data securely across borders is essential for identifying, mitigating, and responding to cyber threats in real time. Likewise, clear commitment to cross-jurisdictional information sharing among government and private sector partners are critical to collective defense and to ensuring that digital trade remains secure and resilient.

Building on this strong foundation, our recommendations address areas not yet covered in the USMCA, such as coordinated vulnerability disclosure and mutual recognition of cyber labelling schemes and propose enhancements to existing provisions to ensure the agreement remains adaptable to emerging technologies and the evolving cyber threat landscape.

Coordinated Vulnerability Disclosure

The Coalition recommends that the updated USMCA include language ensuring that all Parties develop and strengthen the capabilities of national entities responsible for the coordinated disclosure of cybersecurity vulnerabilities. Coordinated vulnerability disclosure (CVD), the process by which security researchers or organizations responsibly share information about discovered vulnerabilities with affected vendors or operators, is essential to maintaining trust, security, and stability in the digital economy.

Including provisions that promote CVD capacity building would directly support digital trade by reducing the risk of cyber incidents that disrupt supply chains, compromise data integrity, or erode confidence in cross-border digital services. Such language would help ensure that vulnerabilities are disclosed and mitigated in a consistent and predictable manner across jurisdictions, thereby enhancing resilience and interoperability among trading partners. The Coalition recommends that this effort account for both entities that facilitate disclosure between private sector organizations and those that manage the disclosure of nonpublic vulnerabilities from government to private sector entities.

Mutual Recognition of Cybersecurity Labels & Assessments

As connected technologies and digital products become increasingly embedded in everyday life, a growing number of national cybersecurity labeling and certification schemes have emerged. While these efforts aim to enhance transparency and trust, their divergence across jurisdictions creates significant compliance challenges for manufacturers operating in multiple markets. Even when cybersecurity labels are recognized across borders, differing conformity assessment requirements can introduce costly redundancies, delay product deployment, and fragment supply chains.

To address these challenges, the Coalition recommends that the updated USMCA include a provision encouraging broad mutual recognition of cybersecurity labelling and conformity assessment frameworks. This commitment should apply broadly across categories of digital

products, however, mutual recognition of baseline security standards for internet of things (IoT) labeling could serve as an early and practical step toward broader regulatory interoperability. By adopting a mutual acceptance of certification outcomes, the USMCA Parties could ensure that conformity assessments conducted in one jurisdiction are accepted by others. Such an approach would enhance interoperability, strengthen supply chain efficiency, support innovation, and promote trust in connected technologies across North America.

Interoperable Cybersecurity Risk Management

A risk-based cybersecurity framework is essential for helping governments and enterprises prioritize resources, manage evolving threats, and strengthen resilience across the digital ecosystem. The Coalition is encouraged that the existing USMCA text recognizes this by promoting the use of voluntary, risk-based, and consensus-driven cybersecurity approaches.[4] However, this language can be strengthened to emphasize the need for greater interoperability and alignment among the Parties' respective risk management frameworks.

The Coalition recognizes that while the parties may tailor its risk management approach to its unique national context and priorities, interoperability should remain a guiding principle. The adoption of compatible, interoperable frameworks would enable governments and enterprises to collaborate more effectively across borders, reducing friction in responding to global cyber threats. Such alignment would also yield important trade benefits, minimizing duplicative compliance requirements for cybersecurity product manufacturers, ensuring companies are not forced to design to country-specific standards, and providing all industries with a more secure and predictable digital infrastructure to conduct cross-border trade.

Encryption

Encryption is essential to protecting sensitive information and maintaining trust in the digital economy. Governments, businesses, and consumers depend on strong encryption to secure the data they store, use, and exchange. The Coalition believes that encryption capabilities in widely available commercial products should not be restricted or regulated, as mandating or favoring specific encryption technologies would raise costs and reduce, not enhance, security in the face of evolving cyber threats.

The Coalition is pleased that the current USMCA text prohibits Parties from requiring manufacturers or suppliers of commercial ICT products to transfer proprietary cryptographic information, use or integrate a particular algorithm or cipher, or partner with local entities as a condition of market access.[5] This language rightly affirms the Parties' commitment to refrain from requiring private companies to weaken encryption protocols or disclose sensitive cryptographic details.

[4] United States-Mexico-Canada Agreement (USMCA), Chapter 19, Article 19.15.2, July 2020, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement
[5] Ibid, Article 12.C.2

However, USMCA could go further by expressly prohibiting any requirement for private companies to implement technical designs that enable government “backdoor” access to encrypted data. While some governments have pursued such mandates for law enforcement purposes, these measures undermine encryption, introduce new vulnerabilities, and create technical barriers to trade. Backdoor requirements would be difficult for companies to implement while maintaining robust privacy protections and would expose consumers and enterprises to greater risk.

* * *

The Coalition appreciates the opportunity to comment on this important engagement and looks forward to continued collaboration with USTR as they conduct this review process. As cyber threats evolve and digital trade continues to expand, ongoing cooperation between government and industry will be essential. The Coalition is committed to working with USTR and all USMCA Parties to strengthen cybersecurity provisions that enhance the collective security of our region.

Respectfully Submitted,

The Cybersecurity Coalition

CC: Ari Schwartz, Venable LLP