November 3, 2025

The Honorable Jamieson L. Greer
United States Trade Representative
Office of the United States Trade Representative
600 17th Street NW
Washington, DC 20508

Attn: Daniel Watson, Assistant USTR for the Western Hemisphere
Randall Oliver, Director for Canada (Randall.T.Oliver@ustr.eop.gov)
Braeden Young, Director for Mexico (Braeden.P.Young@ustr.eop.gov)

Comments on the Operation of the USMCA (Federal Register Notice: 2025-18010)

Dear Ambassador Greer:

The Business Software Alliance (BSA) appreciates the opportunity to submit comments on the ongoing operation of the United States-Mexico-Canada Agreement (USMCA).

The USMCA's Chapter 19 digital trade provisions remain a cornerstone of America's economic and national security strategy. These rules—prohibiting data localization mandates, protecting cross-border data flows, safeguarding encryption, and preventing forced transfers of source code—were negotiated and secured by the first Trump Administration and approved with overwhelming bipartisan support in both chambers of Congress. They embody the principles of the America First Trade Policy and related Administration policy memoranda that direct the US government to promote American technological leadership, defend US economic and national security interests, and secure the prosperity of American workers through open digital markets and innovation leadership.[1]

The America First Trade Policy, the AI Action Plan, and other policy documents explicitly recognize technology as the keystone of US economic strength. We urge USTR to carefully safeguard provisions on cross-border data access and data localization as essential to sustaining American leadership in AI, quantum computing, cybersecurity, and emerging technologies. Likewise, we encourage the Administration to explore opportunities for trilateral agreement in these areas and in trade & technology security controls. We elaborate below.

First, any effort to weaken these provisions would be a grave mistake. Proposals to dilute Chapter 19 mirror the failed digital trade retreat of the prior Administration – a policy that undermined the United States' longstanding support for pro-growth, pro-democracy, pro-science, and pro-security digital disciplines in international agreements.[2] By creating a strategic void for adversaries to fill, that Administration's action undermined US economic and national security, and provoked bipartisan criticism from nearly 100 Senators and House representatives.[3] This Administration should decline the invitation to weaken the existing USMCA provisions.[4]

Second, while BSA is strongly opposed to any weakening of the USMCA Chapter 19 provisions, there are several <u>new</u> areas in which the Agreement could be updated to strengthen US economic and national security. These areas include the AI supply chain, quantum computing, trade/technology security controls (e.g., export controls), and trusted vendor qualification mechanisms. We detail each of these areas in the Appendix to this submission.

We therefore urge the Administration to:

1. Firmly reject any proposal to reopen or dilute USMCA Chapter 19's digital trade commitments;

2. Affirm US leadership in defending cross-border data flows, encryption, source code protections, and digital nondiscrimination;

3. Signal continuity with the successful strategy of the first Trump Administration, which delivered these high-standard digital trade rules as part of a broader national security strategy;

4. If appropriate, explore new disciplines to strengthen US economic and national security – e.g., via new disciplines relating to the AI supply chain, cybersecurity certification mechanisms, quantum computing, trade/technology security controls (e.g., export controls), and trusted vendor qualification mechanisms.

5. Reassure Congress, allies, and US stakeholders that the US will continue to support the economic, security, and strategic potential of a robust cross-border data and digital trade agenda.

BSA appreciates your leadership and stands ready to support USTR in advancing an ambitious digital strategy in the USMCA and beyond to support US economic and national security.

Appendix

While BSA is strongly opposed to any weakening of the USMCA Chapter 19 provisions, there are several new areas in which the Agreement could be updated to strengthen US economic and national security. These areas include the AI supply chain, safeguards relating to cybersecurity certification, international standards for digital technologies and services, quantum computing, cross-border technology security controls (e.g., export controls), and trusted vendor qualification mechanisms. Below, we detail each of these areas, as well as existing USMCA provisions that must remain in place.

Prohibiting Foreign Digital Barriers

- **No Data Localization Requirements or Improper Restrictions on Data Transfers.** The USMCA must continue to prohibit infrastructure and data localization requirements, as well as unnecessary cross-border data restrictions, as negotiated by the first Trump Administration. The USMCA could also explore how to safeguard North American data transfers by building on mechanisms that our economies already support, such as the Global Cross-Border Privacy Rules Forum.

- **No Customs Requirements on Electronic Transmissions.** The USMCA must prohibit the imposition of customs requirements on software or data transmitted electronically, as negotiated by the first Trump Administration.

- **No Forced Technology Transfer.** The USMCA must continue to prohibit requirements for companies to transfer or disclose their technology—such as source code, algorithms, or other trade secrets—as a condition for market access, as negotiated by the first Trump Administration.

- **No Digital Technical Barriers to Trade.** The USMCA should support voluntary, internationally recognized standards, and refrain from imposing conflicting national standards on market participants.

- **No Nationality-Based Discrimination Among Technologies**. The USMCA must continue to prohibit nationality-based discrimination among technologies – i.e., measures that systematically disfavor technologies developed in the United States from being marketed in Canada or Mexico – as negotiated by the first Trump Administration.

Strengthening National Security Through Robust Cyber and Data Security Policies

- **Strong Cyber- and Supply-Chain Security.** The USMCA should promote North American readiness to mitigate cyber- and supply-chain security threats, including through risk management and vulnerability disclosure processes that are based on internationally recognized standards.

- **Ensuring that "Cybersecurity" Measures Actually Advance Cybersecurity:** The USMCA should also contain a shared commitment to combat disguised trade restrictions that are advanced in the name of "cybersecurity" but that, in fact, weaken cybersecurity. Examples of such problematic measures include France's "SecNumCloud" cybersecurity "certification" certifications measure that does not align with international standards; that contains data localization requirements; that mandates immunity from foreign legal jurisdiction; and that imposes nationality-based restrictions on ownership, management role, and other disguised restrictions.

- **Strong Data Security.** The USMCA should allow for robust legal frameworks to protect personal information without allowing for either improper restrictions on data transfers or data localization mandates.

- **Strong Encryption-Based Information Security.** The USMCA should support strong encryption and bilateral commitments to cooperate on upgrading systems to post-quantum cryptography.

- **Strong Export Control, Sanctions, and Other National Security Tools.** To protect sensitive technologies from improper dissemination, the USMCA should contain provisions to promote close

North American collaboration on export controls, sanctions, and ICTS and investment review mechanisms. The North American economies could seek to better align substantive and procedural aspects of their technology control regimes; improve information sharing; and develop advance warning mechanisms.

- **Strong Protections for Due Process in Digital Law Enforcement.** The USMCA should contain strong provisions to protect due process in connection with law enforcement requests to access digital content. The USMCA should also leverage mechanisms to resolve differing legal requirements between jurisdictions, such as via CLOUD Act Agreements.

- **Strong National Security Protections:** The USMCA should maintain existing provisions negotiated by the first Trump Administration reaffirming each Party's freedom to apply measures that it considers necessary for the protection of its own essential security interests. The USMCA should also maintain the robust public policy exception negotiated by the first Trump Administration.

Advancing North American Leadership in Emerging Technologies

- **Leadership in Artificial Intelligence:** The USMCA should counter trade barriers and other impediments to shared AI leadership and innovation, while fostering the development of AI to support cybersecurity, innovation, economic growth, and national defense.

- **Promoting a North American AI Supply Chain:** BSA strongly supports the Administration's stated policy "to sustain and enhance" America's global AI leadership in order to promote human flourishing, economic competitiveness, and national security". BSA also supports the goal of strengthening US and closely allied technological capacity and resilience in relation to advanced robotics, semiconductors, electrical components, and other Essential AI Inputs. To achieve this goal, BSA urges USTR negotiate provisions that will secure preference US access to Essential AI Inputs from across the North American supply chain.

- **Cooperation in Quantum Information Science:** The USMCA could also promote trade in quantum hardware and software (e.g., quantum algorithms, quantum-resistant cryptography, quantum simulations), as well as collaborative research programs and shared principles.

- **Fostering Industrial Data Exchange:** The USMCA could also better support frameworks for secure industrial data sharing, with an emphasis on: (1) industry-recognized data protection standards; (2) technical protocols for interoperability; and (3) agreements for trusted and secure industrial data exchange.

- **Good Regulatory Practices on Digital Policy:** The USMCA should foster legal certainty and a predictable business climate by promoting democratic norms of transparency and accountability in connection with measures impacting digital and technology issues arising under the Agreement.

- **Voluntary, Industry-Driven Standards for Emerging Technologies:** The USMCA should promote adherence to voluntary, industry-driven standards relating to AI, quantum, and other technologies.

- **A Shared ICT Procurement Marketplace for Trusted and Verified North American Vendors:** The USMCA should promote better alignment between the US Federal Risk and Authorization Management Program (**FedRAMP**) and Canadian and Mexican procurement standards to promote procurement security. This could also include processes for evaluation of hardware and software suppliers as part of a robust and comprehensive "trusted vendor" approach to network security.

- **Joint Digital and Economic Security Council:** The USMCA should establish a council to cooperate on trade and emerging technology priorities under the Agreement and via coordinated positions in other international organizations.

[1] BSA, Safeguarding US Technology Leadership via Digital and Economic Security Agreements (2025), at https://www.bsa.org/policy-filings/us-safeguarding-us-technology-leadership-via-digital-and-economic-security-agreements
[2] See generally, Global Data Alliance, Myths v. Facts - Cross-Border Data and Access to Information (2025), at https://globaldataalliance.org/wp-content/uploads/2024/03/10212025gdamythsvsfacts.pdf
[3] See generally, Global Data Alliance, Congressional Statements on USTR's Digital Policy Reversal (2023), at https://globaldataalliance.org/wp-content/uploads/2023/11/11212023gdaustrcomp.pdf
[4] Those who have asked the Trump Administration to weaken Chapter 19 cross-border data provisions have asserted - inaccurately - that the USMCA cross-border data and digital trade provisions would conflict with US laws and regulations that restrict bulk data sales or transactions involving China, North Korea, Venezuela, Iran, or Cuba. This assertion is incorrect for many reasons, including because: (1) the USMCA provisions apply to Canada and Mexico - not the listed countries of concern; and (2) the USMCA allows for derogations from any USMCA commitment on national security grounds (i.e., a self-judging exception).

The US Department of Justice has specifically refuted these assertions. The US Department of Justice has stated:

> The proposed rule's prohibitions and restrictions on access to U.S. sensitive personal data and government-related data by countries of concern are consistent with access restrictions on sensitive personal data that have long been imposed in other national security contexts, including for some transactions reviewed by CFIUS and the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector ("Team Telecom").... Those access restrictions, in turn, are consistent with or otherwise permissible under trade and other international agreements.
>
> For example, the World Trade Organization's ("WTO") General Agreement on Trade in Services ("GATS"), like other trade agreements to which the United States is a party, includes an essential security interests exception that states that nothing in the agreement shall be construed to prevent a party to such an agreement from taking any action that it considers necessary for the protection of its essential security interests. As a result, rather than prohibiting such access restrictions, GATS and other relevant international agreements to which the United States is a party explicitly authorize national security-based restrictions on data access and data flows through the longstanding essential security exception. The proposed rule, like conditions restricting access in CFIUS or Team Telecom mitigation agreements to address identified national security risks, is necessary to protect the essential security interests of the United States and is thus consistent with such international agreements to which the United States is a party.[17]
>
> Notably, consistent with the United States Government's long-standing support of cross-border data flows, the proposed rule does not require data localization or wholly restrict data flows to any specific country. Rather, the proposed rule only limits data transfers in narrow, specifically defined circumstances necessary to safeguard security interests, and it is being developed through a process that enables stakeholder consultation and input. The proposed rule is also consistent with the United States' longstanding support for Data Free Flows Trust ("DFFT"). The categories of prohibited and restricted transactions in the proposed rule identify circumstances that present an unacceptable national security risk of enabling countries of concern to access and exploit Americans' sensitive personal data—circumstances that lack the trust required for free data flows.

See US Department of Justice, Notice of Proposed Rulemaking for DOJ Data Security Program (2024), at: https://www.federalregister.gov/documents/2024/10/29/2024-24582/provisions-pertaining-to-preventing-access-to-us-sensitive-personal-data-and-government-related-data#page-86136