hackerone

November 3, 2025

Office of the United States Trade Representative
600 17th St NW
Washington, DC 20508

VIA ELECTRONIC SUBMISSION

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,

HackerOne 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).[1] We appreciate the opportunity to contribute to this important review process and commend the governments for their continued commitment to advancing digital trade, cross-border cybersecurity collaboration, and intellectual property protections under the framework of the USMCA.

By way of background, HackerOne is a global leader in offensive security solutions. Our HackerOne Platforms combines AI with the ingenuity of the largest community of security researchers to find and fix security, privacy and AI vulnerabilities across the software development lifecycle. The platform offers bug bounty, vulnerability disclosure, pentesting, AI red teaming, and code security. We are trusted by industry leaders like Amazon, Anthropic, Crypto.com, General Motors, GitHub, Goldman Sachs, Uber, and the U.S. Department of Defense.

In these comments, HackerOne focuses on the need for all three USMCA parties to adopt and promote national policies supporting Coordinated Vulnerability Disclosure (CVD). As digital trade and cross-border data flows increase under the USMCA, so too does the need for consistent and effective cybersecurity protections. CVD offers a structured and effective framework for receiving, identifying, and triaging vulnerability reports. Often referred to as the internet's "see something, say something" policy, CVD encourages individuals to report security risks they encounter, allowing organizations to address these issues promptly before they can be exploited.[2] They help organizations reduce blind spots, respond to real-world threats faster, and continuously harden systems against emerging risks.

---

[1] Office of the United States Trade Representative (USTR), *Request for Comment on the Joint Review of USMCA,* 90 Fed. Reg. 44869 (September 17, 2025), https://www.govinfo.gov/content/pkg/FR-2025-09-17/pdf/2025-18010.pdf.

[2] HackerOne VDP Report, https://www.hackerone.com/sites/default/files/2021-03/vulnerability-disclosure-policy-what-is-it-why-you-need-one-how-to-get-started.pdf

Despite its demonstrated benefits, the adoption of CVD across USMCA countries remains uneven. While the United States has made notable progress to institutionalize CVD at the federal level, the other two countries have not followed suit. The United States has taken concrete action, including the passage of the Internet of Things Cybersecurity Improvement Act of 2020, which requires civilian federal agencies to establish Vulnerability Disclosure Programs (VDPs) that operationalize CVD by providing clear reporting processes, legal protections for researchers, and defined scopes for testing.[3] This mandate was reinforced by subsequent directives from the Office of Management and Budget[4] and the Department of Homeland Security[5], which require federal agencies to implement VDPs as a baseline cybersecurity practice. Additionally, NIST guidance encourages organizations to establish formal mechanisms to receive and respond to vulnerability reports from external sources.[6] Currently, Congress is considering the Federal Contractor Cybersecurity Vulnerability Reduction Act, which would extend VDP requirements to all U.S. government contractors.[7] Collectively, these measures enhance federal cybersecurity posture and set a leading example for integrating CVD into broader national security strategies.

Recognizing that cybersecurity vulnerabilities transcend borders and that effective CVD benefits all stakeholders, the United States should leverage its leadership in this area to promote adoption of CVD policies in digital trade negotiations. Incorporating vulnerability disclosure provisions into modernized trade agreements would encourage governments to establish clear and consistent frameworks that enhance cybersecurity cooperation.

Additionally, it is important to view vulnerability disclosure not only as a cybersecurity best practice but also as a critical enabler of international trade. Businesses rely on secure products and services to operate globally, and consistent CVD processes build trust among consumers, partners, and regulators. Aligning vulnerability disclosure norms with international standards helps reduce trade barriers by providing regulatory clarity and preventing conflicting requirements that can hinder cross-border commerce.

In light of these considerations, we urge the U.S. Trade Representative to advocate for the formal inclusion of coordinated vulnerability disclosure provisions in the USMCA and other trade agreements. Encouraging the development and adoption of national CVD policies across all member countries would strengthen regional cybersecurity, facilitate trust in digital trade, and contribute to a more secure and open digital economy.

* * *

HackerOne commends the ongoing efforts of the USMCA partners to advance cybersecurity collaboration and resilience. We encourage the governments of the United States,

---

[3] Public Law No: 116-207, https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf.
[4] Office of Management and Budget, OMB Memorandum 20-32,
https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf
[5] Department of Homeland Security, DHS BOD 20-01,
https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy
[6] National Institute of Standards and Technology (NIST), Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, Sept. 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.
[7] S.1899, Federal Cybersecurity Vulnerability Reduction Act, 119th Cong.,
https://www.congress.gov/bill/119th-congress/senate-bill/1899.

Mexico, and Canada to align on clear, practical vulnerability disclosure policies that promote timely remediation while ensuring organizations have the necessary guidance and flexibility to address risks responsibly.

Respectfully Submitted,

Ilona Cohen
Chief Legal and Policy Officer
HackerOne