We the undersigned companies write to respectfully urge the United States Trade Representative (USTR) to incorporate cybersecurity trade issues in the upcoming modernization of the North American Free Trade Agreement (NAFTA). USTR recently released negotiating objectives for NAFTA, and despite the welcome inclusion of new digital goods and services priorities, trade issues related directly to the U.S. cybersecurity industry are absent.¹

A modernized NAFTA that seeks to ensure "the highest standards covering the broadest possible range of goods and services" should include promotion of cybersecurity goods and services.² Cybersecurity itself is a large and growing industry in the U.S. Many U.S. business sectors – such as manufacturing, agriculture, and healthcare – depend on secure computers for daily operations and international trade. Overbroad international cybersecurity regulations can put U.S. companies at a disadvantage. To help address these issues, we respectfully urge USTR to promote alignment of voluntary cybersecurity risk management frameworks in NAFTA and other trade agreements going forward.

The U.S. cybersecurity industry is large and growing

Cybersecurity was not a central focus when NAFTA was originally negotiated, but today it is a major global economic force. Global spending on cybersecurity is estimated to reach more than $100 billion by 2018, and more than $170 billion by 2020.³ North America is the largest cybersecurity market, with a wide range of industry offerings, of which the United States accounts for the biggest portion.⁴ The U.S. cybersecurity industry is also an important source of well-paying jobs,⁵ and addressing the domestic cybersecurity workforce shortage is a national goal.⁶

² Id., pg. 3.
An industry of this size, vibrancy, and degree of priority should be a part of U.S. trade agreements and strategy. Facilitating and streamlining international trade in cybersecurity products and services will foster continued industry growth, promote employment in the field of cybersecurity, and strengthen U.S. competitiveness and leadership in the cybersecurity marketplace.\(^7\)

**U.S. businesses depend on cybersecurity for trade**

Cybersecurity is an enabler of economic activity. Manufacturing, agriculture, healthcare, and virtually all other industries are going digital, making computer security crucial for their daily operations and future success.\(^8\)

Because digital networks are linked globally and cyberattacks are not constrained by national borders, security lapses abroad can result in harm to U.S. business activity in disparate sectors.\(^9\) When computers are damaged, disabled, or compromised due to exploitation of security vulnerabilities, international trade can be inhibited, intellectual property can be stolen, and companies can incur substantial costs.\(^10\) Attacks on especially sensitive systems, such as critical infrastructure, can lead to substantial economic damage and harm to individuals.

Cyberattacks continue to grow in seriousness, sophistication, and frequency. Effective computer security domestically and abroad will be key to strengthening the system of international trade and enabling U.S. businesses of all types to operate. By helping to raise the baseline cybersecurity level of trading partners, NAFTA and other trade agreements can provide greater security to U.S. businesses.

**Interoperable cybersecurity norms can help address trade barriers**

Numerous countries are currently considering or implementing regulations related to cybersecurity that create trade barriers, such as data localization, transfer of source code, and other controls.

---


cryptographic design specification, or other restrictive technology requirements. Such overbroad regulations put U.S. businesses in multiple sectors at a competitive disadvantage, create risks to intellectual property and security, and dampen U.S. economic growth.

Directly addressing these digital trade barriers in trade agreements – as USTR proposes to do with data localization and source code disclosure in NAFTA – is critical. However, promoting standards-based cybersecurity norms would also be helpful to providing clear alternatives to detrimental practices ostensibly undertaken for cybersecurity, steering the discussion to interoperable principles and processes.

Recommendation: Align approaches to cyber risk management

One way to address these issues is to promote development and alignment of voluntary cyber risk management frameworks among the parties to NAFTA.

The maturity of the cybersecurity markets, as well as the strength and sophistication of cybersecurity protection, varies between North American countries. Broad alignment on a comprehensive framework of cybersecurity principles would help the parties aim at the same cybersecurity goals, make informed decisions about investments in security products and services, hold service providers to a consistent standard, and foster the overall maturity of the North American cybersecurity marketplace. If similar risk management frameworks were common across international markets, cybersecurity companies and customers would be better able to consistently communicate how products and services fit within an overarching protection plan, streamlining trade.

The National Institute of Standards and Technology's (NIST) Cybersecurity Framework for Critical Infrastructure (“the Cybersecurity Framework”) is an example of a U.S. cyber risk management framework with strong adoption among critical infrastructure and non-critical infrastructure organizations, companies, and government agencies. The NIST Cybersecurity Framework compiles essential cybersecurity risk management processes and provides references to standards and guidance to aid implementation.

---

14 Bipartisan Congressional Trade Priorities and Accountability Act of 2015, Pub. L. No. 114-26, Jun. 29, 2015, Sec. 102(b)(7)(D), "to seek greater openness, transparency, and convergence of standards development processes, and enhance cooperation on standards issues globally”.
To keep pace with innovation and evolving threats, prevent standards from reducing market access, and incorporate the input of private sector experts, the risk management framework should be voluntary, flexible, and developed in an industry-led and transparent process. For example, the NIST Cybersecurity Framework is voluntary and was developed through a transparent multistakeholder process.

The final trade agreement text need not dictate the framework content beyond basic principles, but should instead encourage the development, alignment, and use of cybersecurity frameworks. We respectfully urge USTR to consider adopting the following two negotiating objectives:

- Commit the parties to develop a voluntary, comprehensive cybersecurity risk management framework through transparent and open processes.
- Ensure the parties recognize the importance of international alignment of cybersecurity frameworks, standards, and processes.

Thank you for your consideration. We look forward to working with you to modernize NAFTA to expand economic opportunities. Please contact us with any questions or for more information.

Sincerely,

Rapid7
Arbor Networks
Bugcrowd
CA Technologies
Cybereason
Forescout
McAfee
Mimecast
Symantec
Tenable

Cc. Secretary Wilbur Ross, U.S. Department of Commerce