August 9, 2017

The Honorable Robert Lighthizer
United States Trade Representative
600 17th Street, NW
Washington, DC 20508

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]

---

[1] Office of the United States Trade Representatives, Summary of Objectives for the NAFTA Renegotiation, Jul. 17, 2017, https://ustr.gov/sites/default/files/files/Press/Releases/NAFTAObjectives.pdf.
[2] *Id.*, pg. 3.
[3] Estimates vary. *See* Steve Morgan, Worldwide Cybersecurity Spending Increasing To $170 Billion By 2020, Forbes, Mar. 9, 2016, https://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#587a7b8d6832. *See also* Cyber Security Market Share & Trends, 2015 – 2021: Global Industry to Reach $181.77 Bn by 2021, Zion Market Research, Jun. 23, 2017, https://globenewswire.com/news-release/2017/06/23/1028447/0/en/Cyber-Security-Market-Share-Trends-2015-2021-Global-Industry-to-Reach-181-77-Bn-by-2021.html.
[4] Cyber Security Market Share & Trends, 2015 – 2021, Zion Market Research, Jul. 23, 2017, https://globenewswire.com/news-release/2017/06/23/1028447/0/en/Cyber-Security-Market-Share-Trends-2015-2021-Global-Industry-to-Reach-181-77-Bn-by-2021.html.
[5] Steve Morgan, Cybersecurity job market to suffer severe workforce shortage, CSO, Jun. 22, 2017, http://www.csoonline.com/article/3201974/it-careers/cybersecurity-job-market-statistics.html.
[6] Exec. Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017, Sec. 3(d)(i).

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,

---

[7] Bipartisan Congressional Trade Priorities and Accountability Act of 2015, Pub. L. No. 114-26, Jun. 29, 2015, Sec. 102(a)(4).

[8] The manufacturing sector, for example, was the top target of phishing attacks in 2016. *See* 2017 Data Breach Investigations Report, Verizon, Apr. 2017, pgs. 9-12, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017.

[9] Consider the impact of recent examples. Since May 2017, two economically-motivated ransomware attacks, "WannaCry" and "Petya", together damaged hundreds of thousands of computers in a wide variety of business sectors – including healthcare, pharmaceutical, energy, financial, transportation, legal, and shipping firms – in more than one hundred countries, including the U.S. *See* United States Computer Emergency Readiness Team, Petya Ransomware, Jul. 7, 2017, https://www.us-cert.gov/ncas/alerts/TA17-181A. *See also* United States Computer Emergency Readiness Team, Indicators Associated With WannaCry Ransomware, May 19, 2017, https://www.us-cert.gov/ncas/alerts/TA17-132A. *See also* New ransomware, Old Techniques: Petya Adds Worm Capabilities, Microsoft, Jun. 27, 2017, https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities.

[10] North America, particularly the U.S., is a top target for such attacks. *See* North America Cyber Security Market: Analysis and Forecast (2016 to 2022), BIS Research, Jul. 2016, https://bisresearch.com/industry-report/north-america-cyber-security-market-report-forecast.html. *See also* 2016 Cost Of Cyber Crime Study & The Risk Of Business Innovation, Ponemon Institute, Oct. 2016, pgs. 4-7, http://www.ponemon.org/library/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation.

cryptographic design specification, or other restrictive technology requirements.[11] 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.[12]

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.[13] 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.[14]

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.[15] The NIST Cybersecurity Framework compiles essential cybersecurity risk management processes and provides references to standards and guidance to aid implementation.

---

[11] *See, e.g.*, Office of the U.S. Trade Representative, Key Barriers To Digital Trade, Mar. 2017, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade.

[12] *See* Nigel Corey, Border Data Flows: Where Are the Barriers, and What Do They Cost?, Information Technology and Innovation Foundation, May 2017, pgs. 6-12, http://www2.itif.org/2017-cross-border-data-flows.pdf.

[13] Office of the United States Trade Representatives, Summary of Objectives for the NAFTA Renegotiation, Jul. 17, 2017, pgs. 8-9, https://ustr.gov/sites/default/files/files/Press/Releases/NAFTAObjectives.pdf.

[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".

[15] National Institute of Standards and Technology, Cybersecurity Framework for Critical Infrastructure, Feb. 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. This adoption has extended to Canada and Mexico in some limited ways. For example, Cyber Security Standards for the North American Electric Reliability Corporation are largely aligned with the Cybersecurity Framework. See US Government Accountability Office, GAO-12-92, Critical Infrastructure Protection, Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use, pgs. 35-39, Dec. 2011, http://www.gao.gov/assets/590/587529.pdf. We believe NAFTA should encourage and extend such domestic and international alignment of cybersecurity practices.

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