

Comments On Negotiating Objectives For A US-EU Trade Agreement (Docket No. USTR-2018-0035)

December 10, 2018

Before the United States Trade Representative

Rapid7 submits these comments in response to the United States Trade Representative's (USTR) request for public comment on negotiating objectives for a US-European Union (EU) Trade Agreement.¹ Thank you for the opportunity to provide input and support efforts to grow the US digital economy.

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cybersecurity. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks. Rapid7 is a member of the USTR Industry Trade Advisory Committee on Digital Economy.

Rapid7 urges USTR to consider the following negotiation objectives related to cybersecurity and the digital economy:

1. Include cybersecurity in a digital trade chapter.
2. Encourage interoperable cyber risk management frameworks.
3. Build capabilities of national cybersecurity entities.
4. Strengthen existing cybersecurity collaboration mechanisms.
5. Identify regulatory restrictions to defensive cybersecurity activity.
6. Encourage transparency of consumer IoT security.
7. Prohibit requirements to weaken encryption.
8. Prohibit requirements to store data locally or use local computing facilities.

¹ United States Trade Representative, Request for Comments on Negotiating Objectives for a U.S.-European Union Trade Agreement, 83 Fed. Reg. 57526, Nov. 15, 2018, <https://www.federalregister.gov/documents/2018/11/15/2018-24979/request-for-comments-on-negotiating-objectives-for-a-us-european-union-trade-agreement>.

1. Include cybersecurity in a digital trade chapter.

Rapid7 urges USTR to engage the EU on cybersecurity issues in digital trade negotiations, as a reflection of the importance of digital trade and cybersecurity to the economies of both the US and EU.

Cybersecurity threats undermine confidence in digital trade, as noted in the US-Mexico-Canada Agreement (USMCA) text.² Many US business sectors – such as manufacturing, agriculture, and healthcare – depend on secure computers for daily operations and international trade. 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. Security lapses in especially sensitive systems, such as critical infrastructure, can lead to major economic damage and harm to individuals. Effective computer security domestically and abroad is crucial to strengthening the system of international trade and enabling US businesses of all types to operate.

In addition, cybersecurity itself is a large and growing industry in the US.³ 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.⁴

2. Encourage interoperable cyber risk management frameworks

Rapid7 recommends USTR seek a commitment requiring the Parties to develop, employ, and promote the implementation of interoperable cybersecurity risk management approaches within and across both the public and private sectors. The risk management approach should rely on consensus-based international standards and risk management best practices to identify and protect against cybersecurity risks, and to detect, respond to, and recover from cybersecurity events. In addition, the Parties should seek

² USMCA Art. 19.15(1).

³ 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 Bipartisan Congressional Trade Priorities and Accountability Act of 2015, Pub. L. No. 114-26, Jun. 29, 2015, Sec. 102(a)(4).

interoperability of their cybersecurity risk management approaches so that their general practices are comparable across jurisdictions.

This recommendation is similar to language agreed to in USMCA, with additional emphasis on interoperability.⁵ As with USMCA, the trade agreement text need not dictate the content of the approach beyond basic principles, but should instead encourage the development, alignment, and use of cybersecurity risk management approaches.

The National Institute of Standards and Technology's (NIST) Cybersecurity Framework for Critical Infrastructure ("the Cybersecurity Framework") is an example of a US cyber risk management framework with strong adoption among critical infrastructure and non-critical infrastructure organizations, companies, and government agencies.⁶ The NIST Cybersecurity Framework is standards-based and organized around the principles of identifying and protecting against cybersecurity risks, and detecting, responding to, and recovering from cybersecurity incidents.

International interoperability and alignment of cybersecurity principles would benefit US companies by enabling them to better assess global risks, make more informed decisions about security, hold international partners and service providers to a consistent security standard, and ultimately better protect global customers and constituents. If risk management frameworks were aligned across international markets, cybersecurity companies and customers would be better able to consistently communicate how specific products and services fit within the frameworks' overarching protection plan, streamlining trade.

3. Build capabilities of national cybersecurity entities.

Rapid7 recommends USTR seek a commitment requiring the Parties to build the capabilities of their national entities responsible for cybersecurity incident response and coordinated vulnerability disclosure. This should include national entities that facilitate coordinated disclosure of vulnerabilities between private sector organizations, as well as national entities that facilitate disclosure of nonpublic security vulnerabilities from the government to private sector organizations.

⁵ USMCA Art. 19.15(2).

⁶ 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>.

National entities responsible for cybersecurity incident response are helpful for building trust in digital products and services by coordinating private and public sector organizations to respond to cybersecurity incidents, such as attacks that can cause economic harm. The USMCA includes a commitment that the Parties shall endeavor to build the capabilities of such entities, and USTR should seek the same commitment in a US-EU Trade Agreement.⁷

In addition, USTR should seek a commitment that the Parties will also build the capabilities of their national entities responsible for coordinated vulnerability disclosure. Coordinated vulnerability disclosure (CVD) is a voluntary process of gathering information about security vulnerabilities (such as flaws passed on by external discoverers), and coordinating the sharing and disclosure of that information to relevant stakeholders (such as software companies and the public) to boost the likelihood of a positive cybersecurity outcome (such as mitigating the vulnerability).⁸ Coordinated vulnerability disclosure is increasingly recognized as a key cybersecurity practice.⁹ National entities controlled or funded by the Parties' governments (such as, but not limited to, the US CERT Coordination Center and the Netherlands NCSC-NL) facilitating CVD aid private companies in assessing, disclosing, and communicating technical information about security vulnerabilities, strengthening trust and reliability of digital products and services.¹⁰

The commitment to build the capabilities of national entities responsible for CVD should incorporate not just entities that facilitate disclosure between private organizations, but also national entities that facilitate disclosure of vulnerabilities from government to private organizations that are not publicly known ("zero-day" vulnerabilities). Governments often have unique knowledge of cybersecurity vulnerabilities, and responsible disclosure of these vulnerabilities to software vendors help secure the

⁷ USMCA Art. 19.15(1)(a).

⁸ See Householder et. al., *The CERT Guide to Coordinated Vulnerability Disclosure*, Carnegie Mellon University, Aug. 2017, pgs. 1-4. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.

⁹ See NIST Cybersecurity Framework for Critical Infrastructure, RS.AN-5. See also U.S. House of Representatives Energy and Commerce Committee, Majority Staff white paper, *The Criticality of Coordinated Disclosure In Modern Cybersecurity*, Oct. 23, 2018, <https://energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf>. See also Department of Homeland Security, *Strategic Principles for Securing the Internet of Things*, Nov. 16, 2016, pg. 7, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.

¹⁰ See National Cyber Security Centre, Ministry of Security and Justice, *Coordinated Vulnerability Disclosure*, Oct. 11, 2018, <https://www.ncsc.nl/english/Incident+Response/responsible-disclosure.html>.

systems upon which the digital economy relies, and help maintain trust that digital products and services are less susceptible to attack.¹¹ In the US, this may include the "vulnerabilities equities process" (VEP).

A commitment in the US-EU Trade Agreement need not stipulate details of the process for considering whether or how to disclose vulnerabilities, which may include consideration of national security issues. Instead, like the USMCA language on incident response, the commitment should focus on building the capabilities of the entities responsible for the process.

4. Strengthen existing cybersecurity collaboration mechanisms

Rapid7 recommends USTR seek a commitment to strengthen existing collaboration mechanisms, including public-private partnerships, for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks and use those mechanisms to swiftly address cybersecurity incidents, as well as the sharing of information for awareness and best practices.

The USMCA includes this language,¹² and we urge USTR to carry it forward to a US-EU Trade Agreement. The processing and sharing of cyber threat information is a necessary component of a comprehensive security program.¹³ Collaborating with other industry stakeholders and Information Sharing and Analysis Organizations to identify and respond to cyber threats helps companies protect their business critical systems, safeguard sensitive data, and maintain trust in digital products and services.

5. Identify regulatory restrictions to defensive cybersecurity activity.

Rapid7 recommends USTR seek a commitment that the Parties shall endeavor to review and identify regulations and policies that inappropriately restrict legitimate defensive cybersecurity activity, products, and services.

¹¹ Charlet et. al., It's Time for the International Community to Get Serious About Vulnerability Equities, Carnegie Endowment for International Peace, Nov. 15, 2017, <http://carnegieendowment.org/2017/11/15/it-s-time-for-international-community-to-get-serious-about-vulnerability-equities-pub-74750>.

¹² USMCA Art. 19.15(1)(b).

¹³ See, for example, ID.RA-2 and RS.CO-5 on information sharing in the NIST Cybersecurity Framework.

Effective cybersecurity solutions require regulatory policies that enable data sharing and threat analysis. Regulations that broadly restrict the processing and sharing of data can disrupt cybersecurity activity that builds trust in digital goods, and also hinder trade in cybersecurity products and services.¹⁴ This may include, though is not limited to, export and privacy restrictions that limit private sector processing and sharing of cyber threat information and security vulnerabilities for the purpose of protecting data security and privacy.

For example, companies have expressed concern that the draft EU ePrivacy Regulation lacks clear protections for cybersecurity service providers to process and report cyber threat data on behalf of clients.¹⁵ Companies must process and share cyber threat information that may also fall under common definitions of "personal information," and therefore be subject to privacy restrictions. To detect and avoid a suspected phishing email attack, cybersecurity service providers may process the email address, purported identity, and IP address of the email sender. This information may be processed on behalf of a third party client and shared with other organizations to help them avoid the attack. While numerous privacy regulations acknowledge the need for processing and sharing information for cybersecurity and fraud prevention, including GDPR,¹⁶ this recognition is not always embedded from the start.

Another example: The Wassenaar Arrangement – of which the US and many EU nations are members – established export controls for "intrusion software" in 2013. Though well-intentioned, the controls encompassed legitimate defensive cybersecurity activities, such as incident response and vulnerability disclosure, posing difficulties to the development and use of cybersecurity products and services.¹⁷ Both the US and EU struggled to implement the 2013 Wassenaar Arrangement controls in a way that did not negatively impact the legitimate cybersecurity industry and its customers.¹⁸ The Wassenaar Arrangement

¹⁴ See Cybersecurity Coalition, Comments to the National Telecommunications and Information Administration on "Developing the Administration's Approach to Consumer Privacy," Nov. 9, 2018, pg. 2, <https://www.cybersecuritycoalition.org/request-for-comment-on-developing-t>.

¹⁵ See Business Software Alliance, The Unintended Impact of the Draft EU ePrivacy Regulation on Cybersecurity, Dec. 4, 2017, https://www.bsa.org/~/_media/Files/Policy/Data/12042017BSAEUePrivacyexamplescybersecurity.pdf.

¹⁶ See, for example, Recitals 47 and 49 of the EU General Data Protection Regulation.

¹⁷ Testimony of Ian Mulholland before the US House of Representatives Committee on Oversight and Government Reform, Subcommittee on Information Technology, Wassenaar: Cybersecurity and Export Control, Jan. 12, 2016, pg. 2, <https://oversight.house.gov/wp-content/uploads/2016/01/Mulholland-VMware-Statement-1-12-Wassenaar.pdf>.

¹⁸ Testimony of Cheri McGuire before the US House of Representatives Committee on Oversight and Government Reform, Subcommittee on Information Technology, Wassenaar: Cybersecurity and Export Control, Jan. 12, 2016, pg. 10, <https://oversight.house.gov/wp-content/uploads/2016/01/McGuire-Symantec-Statement-1-12-Wassenaar.pdf>.

was modified in 2017 to provide flexibility for cyber incident response and vulnerability disclosure, though it is up to each country to individually implement the controls.¹⁹

Many regulations were enacted before defensive cybersecurity became a widely understood priority. The Parties should identify whether legitimate cybersecurity activity is hindered by other regulations, which may then prompt consideration of how to enable such activity without undermining their regulatory goals. This commitment need not require the Parties to revise regulations, but instead focus on a regulatory review to identify potential areas of improvement.

6. Encourage transparency of consumer IoT security.

Rapid7 recommends USTR seek a commitment that the Parties shall endeavor to facilitate the development of voluntary, consensus-based processes that enhance the transparency of critical security features of consumer Internet of Things (IoT) devices. The goal of this process should be to enable consumers to make informed purchasing decisions regarding data protection features of such devices.

Security of IoT devices is increasingly important to the security and safety of consumers, businesses, and others. As IoT continues to enter mainstream use in areas such as healthcare, automotive, home appliances, and smart cities, IoT users will need to routinely evaluate device security as part of purchasing. Yet consumers often have little insight into the presence of security features in an IoT device prior to purchase, hindering informed buying decisions.

The concept of an IoT security rating or "nutrition label" is routinely floated in reports, legislation, and private sector efforts to help address this lack of transparency.²⁰ Recently, the Departments of Commerce and Homeland Security released their "Botnet Roadmap" – a series of actions to be undertaken by both

¹⁹ Wassenaar Arrangement, Summary of Changes, List of Dual-Use Goods & Technologies and Munitions List, Dec. 7, 2017, pg. 2, <https://www.wassenaar.org/app/uploads/2015/06/Summary-of-Changes-to-2017-Lists-Website.pdf>.

²⁰ See Commission on Enhancing the National Cybersecurity, Report on Securing and Growing the Digital Economy, Action Item 3.1.1, White House, Dec. 1, 2016, pg. 30, <https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf>. See also Department of Homeland Security, Strategic Principles for Securing the Internet of Things, Nov. 16, 2016, pg. 11, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf. See also Cyber Shield Act of 2017, S. 2020, 115th Cong., Oct. 26, 2017, <https://blog.rapid7.com/2017/06/26/legislation-to-strengthen-iot-marketplace-transparency>.

government and private sector stakeholders to reduce the volume and impact of automated attacks. The Botnet Roadmap includes several tasks related to labeling and assessment programs, for both consumer and industrial IoT, as part of a workstream to develop robust markets for trustworthy IoT devices.²¹

The Parties should endeavor to facilitate this transparency on a voluntary basis through an open and consensus-based process. Recently, the National Telecommunications and Information Administration facilitated such a process with regard to IoT security update capability.²² Providing consumers with clear information about critical security features in IoT devices will foster market competition based on security, promote innovation in security, and build trust in the security of IoT products.

7. Prohibit requirements to weaken encryption

Rapid7 recommends USTR seek a commitment that the Parties will not require, as a condition of market access, manufacturers or suppliers of products using cryptography to weaken the cryptography, transfer proprietary information related to the cryptography, provide a private key or other "back door," or include local design details.

Encryption is a fundamental means of protecting data from unauthorized access or use. Critical infrastructure, commerce, government, and individual internet users depend on strong security for communications, and this reliance on encryption will only continue to grow as more of the world is digitized. However, strong encryption can also pose challenges to government access to data, prompting some calls for regulations that would forbid the use of strong encryption without providing a means of access to data, such as an encryption "backdoor."

Market access rules requiring weakened encryption would create technical barriers to trade and put products with weakened encryption at a competitive disadvantage with uncompromised products. Requirements to weaken encryption would impose significant security risks on US companies by creating

²¹ Dept. of Commerce, A Road Map Toward Resilience Against Botnets, Nov. 29, 2018, pgs. 5-8,

https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf.

²² National Telecommunications and Information Administration, Communicating IoT Device Security Update Capability to Improve Transparency for Consumers, Jul. 18, 2017,

https://www.ntia.doc.gov/files/ntia/publications/communicating_iot_security_update_capability_for_consumers_-_jul_2017.pdf.

diverse new attack surfaces for bad actors, including cybercriminals and unfriendly international governments.²³ The environment resulting from regulations to weaken encryption would most likely be highly complex, vulnerable to misuse, and burdensome to businesses and innovators – ultimately undermining the security of the end-users, businesses, and governments.²⁴

Article 12.C.2 of the USMCA includes a general prohibition on requirements to weaken encrypted goods as a condition of market access. However, USMCA Article 12.C.2 includes several exceptions that we urge USTR to narrow in a US-EU Trade Agreement, to the extent possible. For example, the Article excludes regulation of financial instruments from the scope of the encryption protection, but this is a broad category and could instead focus on the particular concerns driving this exception.

8. Prohibit data localization requirements.

Rapid7 urges USTR to seek a commitment that the Parties will not require local storage of data or use of computing facilities in the Parties' territory as a condition of market access.

US companies seeking to provide global access to digital services are impeded by data localization – laws or norms compelling companies that do business within a country to store data associated with that country's citizens locally, rather than in data centers located elsewhere. Data localization erodes the analytic capabilities, standardization, and cost savings that cloud computing can provide. Segregating data collected from particular countries, maintaining servers locally in those countries, and navigating complex geography-based laws are all activities that require significant resources, increasing overhead costs without boosting product development or innovation. These costs can price smaller companies out of a country market entirely, which reduces the commercial choices for the citizens in the localizing country. The resulting fragmentation also undermines the fundamental concept of a unified and open global internet.²⁵

²³ Abelson et al., Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory, Jul. 6, 2015, pg. 15, <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>.

²⁴ Center for Democracy, CALEA II: Risks of Wiretap Modifications to End points, May 17, 2013, <https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf>.

²⁵ See First Report of the Digital Economy Board of Advisors, US Dept. of Commerce, Dec. 2016, pgs. 35-39, https://www.ntia.doc.gov/files/ntia/publications/deba_first_year_report_dec_2016.pdf.

The USMCA includes language prohibiting the Parties from requiring use of local computing facilities, as well as language generally prohibiting restrictions on cross-border flow of information for business purposes.²⁶ We urge USTR to include this language in a US-EU Trade Agreement.

*

*

*

We appreciate the opportunity to share our views. If there are additional questions or if Rapid7 can provide any further assistance, please contact Harley Geiger, Director of Public Policy, at HGeiger@rapid7.com. Thank you.

²⁶ USMCA Arts. 19.11 - 19.12.