American University National Security Law Brief

Volume 11 | Issue 1 Article 4

2021

The Case for Presumptions of Evil: How the E.O. 13873 'Trump' Card Could Secure American Networks from Third-Party Code Threats

Caroline Elyse Burks

The Case for Presumptions of Evil: How the E.O. 13873 'Trump' Card Could Secure American Networks from Third-Party Code Threats

Caroline Elyse Burks[*]

[*] Caroline Burks is a law student at the University of Texas School of Law. She is a Brumley Next Generation Graduate Fellow in Cybersecurity, Robert Strauss Center for International Security and Law. The author would like to thank Professor Ronald Sievert for overseeing this project, for providing guidance, for giving research advice, and for producing helpful comments.

American University National Security Law Brief, vol. 11, issue 1 (Spring 2021), pp. 95–119.

I. THE THIRD-PARTY CODE THREAT IS HERE – UNNOTICED AND UNMANAGED – AND MUST BE DEALT WITH NOW.

Over two-thirds of all website code is created by third parties; this code is often referred to as third-party code (3PC) or open source code.[1] This allows developers to focus on the key portions of their application, while leaving supporting capabilities to open source code libraries, allowing for quicker entry to market.[2] As development teams are pushed to develop more advanced applications faster, "creating every single line of code from the ground up is often not a sustainable practice."[3] Three-fifths of developers underestimate the magnitude of code which comes from third-party developers while 10% openly admit that they don't know the percentage of their site run by third-party code.[4]

Open source codes are often not written with security in mind.[5] Only 11% of website decision-makers, those charged with managing the site, believe they have complete knowledge of the third-party code running on their sites, three-fifths admit third-party code running on the client side poses risks.[6] Only 27% of website decision-makers trust their third-party code sources fully.[7] Nearly three-fourths of these applications contain an Open Web Application Security Project (OWASP) Top 10 vulnerability when first assessed;[8] this is 9% lower than internally-

[1] OSTERMAN RESEARCH, THIRD-PARTY CODE: THE HIDDEN RISK OF YOUR WEBSITE 2 (2019); Sakthivel Rajendran, *Safeguarding Mobile Applications with Secure Development Life Cycle Approach*, 3 ISACA J. 1, 4 (2017).
[2] Rajendran, *supra* note 1, at 4.
[3] Pedro Fortuna, *Supply Chain Attacks: When Things Go Wrong*, INFOSECURITY MAG. (Apr. 26, 2019), https://www.infosecurity-magazine.com/opinions/supply-chain-attacks-wrong-1-1/.
[4] OSTERMAN RESEARCH, *supra* note 1, at 3.
[5] MARK SHERMAN, S5: NEW THREATS TO CYBER-SECURITY 10 (2014).
[6] OSTERMAN RESEARCH, *supra* note 1, at 4.
[7] *Id*. at 8.
[8] Lumena Mukherjee, *What is OWASP? What are the OWASP Top 10 Vulnerabilities?*, INFOSEC INSIGHTS (Oct. 10, 2019), https://sectigostore.com/blog/what-is-owasp-what-are-the-owasp-top-10-vulnerabilities/ (listing top ten critical web application security risks for 2019, as identified by OWASP participants, experts which often include industry imbedded security experts).

developed applications.[9] This is especially alarming considering that 47% of developers do not perform security reviews for third-party code.[10] Even if the developer does perform an initial security scan of the code, 36.1% of applications are only scanned for vulnerabilities once a year and 32.9% are only scanned every 2-6 months.[11] To add another layer to the problem, many developers don't have an inventory of the third-party code built into their application, so it is difficult to search for publicly announced vulnerabilities.[12] Further, there is no standard process to update code found to be vulnerable.[13] Once a vulnerability is found, open sourced or third-party code takes approximately a month longer to repair than insourced code.[14]

Attacking a third-party or open source code as opposed to internally produced code is known as a supply chain attack.[15] The use of third-party code is attractive to hackers.[16] Hackers no longer have to find vulnerabilities in a code used by a singular application – they can find vulnerabilities in the third-party code script being used by multiple applications and exploit that vulnerability to target many applications at once.[17] To analogize, applications using open source, or publicly available, third-party code is like everyone in the neighborhood using the same key because it's easy – when a thief gets a copy of one key, he can unlock any door he wants.[18] Although the third-party code is not built with security in the forefront, the code is given the

[9] VERACODE, STATE OF SOFTWARE SECURITY, VOLUME 6: FOCUS ON INDUSTRY VERTICALS 3 (2015) [hereinafter STATE OF SOFTWARE SECURITY].
[10] Sherman, *supra* note 5, at 11–12.
[11] STATE OF SOFTWARE SECURITY, *supra* note 9, at 15.
[12] Rajendran, *supra* note 1, at 8.
[13] Sherman, *supra* note 5, at 11–12.
[14] STATE OF SOFTWARE SECURITY, *supra* note 9, at 33.
[15] Fortuna, *supra* note 3 ("A supply chain attack is characterized as 'an intentional malicious action (e.g., insertion, substitution or modification) taken to create and ultimately exploit a vulnerability in information and communication technology (hardware, software, firmware) at any point within the supply chain with the primary goal of disrupting or surveilling a mission using cyber resources.'").
[16] Steve Mansfield-Devine, *Nation-state hacking – a threat to everyone*, 2018 COMPUT. FRAUD & SEC. 17, 17 (2018).
[17] *Id*. at 18.
[18] *See generally id*.

"same permissions as the code that companies develop in-house."[19] With 75% of organizations relying on open source code as the foundation for applications, it's important to recognize that supply chain security is increasingly ignored.[20] As such, "[a]ttackers have clearly identified this [as the] weakest line in the software supply chain – being able to breach high-profile companies without ever having to go near their servers or code."[21]

II. IMPACT OF EXECUTIVE ORDER 13873 ON INFORMATION AND COMMUNICATION TECHNOLOGY TRANSACTIONS:

Executive Order 13873 [hereinafter E.O. or E.O. 13873] instructed the U.S. Department of Commerce to develop regulations to protect America's telecommunications networks from supply chain threats posed by foreign adversaries..[22] Issued on May 15, 2019, E.O. 13873 in essence forces U.S.-based companies to take control of the code used in telecommunications, including internet communications.[23] The E.O. is often referred to as the 'Huawei Order' because many believed that the E.O., "which prohibits technology transactions that pose a risk to national security or the digital economy," is meant to target physical technology only.[24] That is far from true; the order is written incredibly broad, encompassing "services designed, developed, manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."[25] The largest impact could be the prohibition of using third-party code (3PC) from foreign adversaries, which currently accounts for most of the code

[19] Fortuna, *supra* note 3.
[20] Sherman, *supra* note 5, at 9.
[21] Fortuna, *supra* note 3.
[22] Securing the Information and Communications Technology and Services Supply Chain, Exec. Order No. 13,873, 84 Fed. Reg. 22689, 22689 (2019) [hereinafter Exec. Order No. 13873].
[23] *New Executive Order Applies to Foreign Third-Party Code*, THE MEDIA TRUST (Sept. 22, 2019), https://mediatrust.com/blog/new-executive-order-applies-foreign-third-party-code.
[24] *Id*.
[25] Exec. Order No. 13873, *supra* note 22, at 22,689.

executing today's mobile apps and websites.[26] However large the economic impact of such a regulation, it is difficult to dispute its necessity since the majority of eCommerce and social media site code is created by third parties.[27] Third party code is how the majority of malicious malware from foreign threat actors, including ransomware and botnets, is spread today.[28] The order spells out five criteria for the prohibition of the "acquisition, importation, transfer, installation, dealing in, or use of…" an information or communication technology by a government or private entity within the United States due to national security concerns.[29]

A. "A transaction…

Using common English definitions or Black's Law Dictionary, courts have broadly defined the term "transaction" as "the carrying on or completion of business…."[30] Although the order is "clearly intended to target transactions where U.S. persons might purchase products or

[26] *New Executive Order Applies to Foreign Third-Party Code*, *supra* note 23 ("80-95% of the code running on top media and eCommerce domains originates from [third-party coders]…[and] 3PC drives the majority of malware spread today from state actors and organized crime including ransomware, identity theft, keystroke logging, disinformation, botnets, malvertising, and data/IP theft.").
[27] *Id*.
[28] Hugh Taylor, *Insights into the Impact of Executive Order (EO) 13873,* J. OF CYBER POL'Y (Oct. 11, 2019), https://journalofcyberpolicy.com/2019/10/11/insights-impact-executive-order-eo-13873/ ("A small percentage of malicious 3PC drives the majority of malware spread today from state actors and organized crime including ransomware, identity theft, keystroke logging, disinformation, botnets, malvertising, and data/IP theft.").
[29] Matthew Moore*, Future Supply-Chain Rules to Be Implemented Under Executive Order 13873, and Under Sections 889(a)(1)(B) and 889(b) of the 2019 NDAA*, REDSTONE GOV'T CONSULTING (Sept. 26, 2019), http://info.redstonegci.com/blog/non-tariff-supply-chain-restrictions-on-it/telecom-products-and-services-part-3-of-3.
[30] *See, e.g.,* Datascape, Inc. v. Kyocera Wireless Corp., No. 1:05-CV-1651-CC, 2008 WL 11342941, at *111-12 (N.D. Ga. May 7, 2008), *report and recommendation adopted,* No. 1:05-CV-1651-CC, 2009 WL 10675007 (N.D. Ga. Mar. 31, 2009) ("The term "transaction" is a common English language word, which one source defines as…the carrying on or completion of business etc.,… That which his or has been transacted, esp. a piece of business, a deal… A physical operation, action, or process… as "an instance of buying or selling something, a business deal *in an ordinary commercial transaction*…." (quoting NEW OXFORD AMERICAN DICTIONARY 1787 (2d ed. 2005); SHORT OXFORD ENGLISH DICTIONARY 3324 (5th ed. 2002)); United States v. Radley, 632 F.3d 177, 183 (5th Cir. 2011) ("Black's Law Dictionary defines a transaction as '[t]he act or an instance of conducting business or other dealings; esp., the formation, performance, or discharge of a contract.'" (quoting BLACK'S LAW DICTIONARY 1535 (8th ed. 2004)).

services from 'foreign adversaries' for projects being performed in the U.S.",[31] the order is written broadly enough to encompass transactions that primarily take place outside of the United States. The E.O. explicitly exempts any transaction that was initiated, pending or completed prior to May 15, 2019.[32]

B. …that involves information and communications technology or services…

E.O. 13873 explicitly defines information and communications technology or services as "any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communications by electronic means, including transmission, storage and display…."[33] This is an expansive definition as everything "from watches to cars now includes information and data processing technologies. Just about the only things not potentially covered by [E.O. 13873] are raw materials and other commodities."[34] The order leaves a significant portion of the definition up for interpretation as it doesn't state "how such technology or services will be identified…."[35] The inclusion of services in addition to products, "likely reflects concerns that have developed in recent years within U.S. national security agencies about risks that may be introduced through service providers…."[36] It

[31] Damiya Park, Grant Leach & Courtney Morgan, *President Trump Declares National Emergency over Technology Threats*, BYTE BACK (May 30, 2019), https://www.bytebacklaw.com/2019/05/president-trump-declares-national-emergency-over-technology-threats/#more-2382.
[32] Exec. Order No. 13873, *supra* note 22, at 22,690; John B. Reynolds, Jeanine P. McGuinness & Will Schisa, *U.S. Government Takes Aim at China with Entity List Additions and New Executive Order*, FINREG (May 22, 2019), https://www.finregreform.com/single-post/2019/05/22/u-s-government-takes-aim-at-china-with-entity-list-additions-and-new-executive-order/.
[33] Exec. Order No. 13873, *supra* note 22, at 22,691.
[34] Rod Hunter, *President Trump Issues Supply Chain Executive Order*, BAKER MCKENZIE (May 29, 2019), https://www.bakermckenzie.com/en/insight/publications/2019/05/president-trump-issues-executive-order.
[35] *National Security Update: President Trump Signs Executive Order on Information and Communication Technology Supply Chain; Commerce Department Adds Huawei to Entity List*, COVINGTON 3 (May 16, 2019), https://www.cov.com/-/media/files/corporate/publications/2019/05/national_security_update_president_trump_signs_executive_order_on_information_and_communications_technology_supply_chain_commerce_department_adds_huawei_to_entity_list.pdf.
[36] *Id.*

would be unreasonable to assume third-party code does not fall under the definition of information and communication technology.[37] However, even if third-party code is not swept up in the definition of products, it is likely that it could be prohibited under the definition of services.[38]

C. … designed, developed, manufactured, or supplied by…

Notably, design through supply encompasses nearly every stage of the supply chain in some form, except retail possibly.[39] As the order is purposefully broad, it is unlikely that this will be a major point of contention in determining when a transaction will be declined by the Commerce Department.[40]

D. … persons owned by, controlled by, or subject to the jurisdiction or discretion of a foreign adversary…

Executive Order 13873 rests the prohibition power partially in the hands of the Secretary of Commerce, who will have the power to define which countries are 'foreign adversaries,' thereby allowing for the prohibition of technology transactions originating from these

[37] *New Executive Order Applies to Foreign Third-Party Code*, *supra* note 23; s*ee also Detail for CIP Code 11.0103,* NAT'L CTR FOR EDUC. STAT., https://nces.ed.gov/ipeds/cipcode/cipdetail.aspx?y=55&cipid=87244 (last visited Sept. 12, 2020) (the education department taxonomic coding for educational programs lists information technology degrees to include the "principles of computer hardware and software components, algorithms, databases, telecommunications, user tactics, application testing, and human interface design.").
[38] Hunter, *supra* note 34 ("He could also prohibit U.S. businesses from buying inputs from foreign firms from allied countries that employ, say, programmers or technicians the Secretary thinks are subject to the direction of a foreign adversary. Arguably, he could even effectively prohibit U.S. companies from employing in the United States foreign individuals the Secretary believes are subject to the direction of a foreign adversary").
[39] *See, e.g.,* Maj. Michael B. Siegl, *Understanding the Supply Chain Operations Reference Model,* 40 ARMY LOGISTICIAN 1, 3 (2008); John Rauser, *Building a model of the software supply chain,* INFOWORLD (Jan. 8, 2018), https://www.infoworld.com/article/3245800/building-a-model-of-the-software-supply-chain.html; *How to Start Digitizing Your Supply Chain Management*, SLIDE MODEL (August 15, 2019), https://slidemodel.com/how-to-start-digitizing-your-supply-chain-management.
[40] *See generally* Exec. Order No. 13873, *supra* note 22.

countries.[41] Additionally, foreign adversaries don't necessarily need to be nation-states as the definition provided by E.O. 13873 defines a foreign adversary as "any foreign government or *foreign non-government person* engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of United States persons."[42] However, it is likely that enforcement of this order will center on trade with China, as FBI Director Christopher Wray has stated that "[n]o country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China."[43] China has also announced an expanded role of the Chinese government within the economy through the "Made in China 2025" plan.[44]

A comparison to the current CFIUS regime shows how broadly 'controlled by' can be interpreted. Control, in the context of CFIUS, does not apply only to majority interests but can appear in minority interests of 10 percent or fewer shares where the party still has the ability to influence important matters.[45] Important matters can include "the sale, transfer, or encumbrance of principal assets; merger and dissolution; the closing of facilities; major expenditures; the selection of business lines; the entry into or nonfulfillment of contracts; proprietary information policy; the appointment of senior managers or employees with access to sensitive information; and the amendment of the business's governing document."[46] Essentially, only a completely passive investment of 10% or less, through which the party doesn't even have the option to engage in broader controlling activities, would be considered not having control.[47] As an

[41] *Id*. at 22, 689.
[42] *Id*. at 22,691(emphasis added).
[43] Wayne M. Morrison, *U.S.-China Trade Issues*, CONG. RES. SERV. (June 23, 2019), https://fas.org/sgp/crs/row/IF10030.pdf.
[44] *Id*.
[45] *Overview of the CFIUS Process*, LATHAM & WATKINS LLP (2017), https://www.lw.com/thoughtLeadership/overview-CFIUS-process.
[46] *Id*.
[47] *See generally id*.

example, a company headquartered in Hong Kong was considered controlled by China, a foreign adversary under CFIUS, because Hong Kong is controlled by China which is naturally a red flag in CFIUS proceedings.[48]

E. … which poses an undue risk."

The transaction must, at the determination of the Secretary of Commerce in conjunction with other relevant agencies, pose an "undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;… pose[] an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or…otherwise pose[] an unacceptable risk to the national security of the United States or the security and safety of United States persons.".[49] Again, a comparison to CFIUS may be useful in determining which risks will attract the attention of the Commerce Department. It is likely that the responsible Commerce Department officials will have access to classified information and may place great emphasis on remote risks not known to the public, making it difficult for the relevant transaction parties to predict the risk level.[50] Notably, the risk may even be external to the parties' control and relate to geographical proximity: In 2012, Ralls Corp., a Chinese-owned company, was forced to divest from an Oregon-based wind farm project because it was geographically close to a sensitive naval institution.[51]

[48] In re Glob. Crossing Ltd., 295 B.R. 726, 732 (Bankr. S.D.N.Y. 2003).
[49] Exec. Order No. 13873, *supra* note 22, at 22,690.
[50] *Overview of the CFIUS Process*, *supra* note 45.
[51] *See, e.g.,* Ralls Corp. v. Comm. on Foreign Inv., 758 F.3d 296, 324 (D.C. Cir. 2014); *see also Overview of the CFIUS Process*, *supra* note 45.

III. THE COMMERCE DEPARTMENT'S PROPOSED GUIDELINES DO NOT PROVIDE CLARITY, BUT HINT AT ULTERIOR MOTIVE.

On November 27th, 2019, the Commerce Department proposed regulations that highlight an identical set of considerations as E.O. 13873. [52] But the guidelines only provide minor insight on the process by which transactions will be denied by the Commerce Department.[53] The process will be similar to CFIUS, where the Secretary of Commerce has the veto power over any transaction involving a foreign entity. Notably, unlike CFIUS, there is no way to gain advance approval and no red-flag nations have been explicitly named.[54] While many entities likely hoped the Commerce Department policy would bring greater clarity, the proposed case-by-case, fact-specific analysis will offer very little clarity and insert uncertainty into many Information and Communications Technology (ICT) transactions.[55]

A. The definition of a foreign adversary remains vague but statements from reviewing U.S. government officials may prove informative about potential "red-flag" actors.

The Commerce Department has invited comments regarding the policy but has explicitly said that "the determination of "foreign adversaries" for the purpose of the Executive Order is solely within the Secretary's discretion."[56] It is not apparent whether the Commerce Department will publish a list or provide notice to companies and nations prior to designating them as foreign

[52] This is based upon the draft published to the Federal Register on November 27th, 2019, the most recent announcement. *See* Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65,316 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7).
[53] *Id*.
[54] *Id*.
[55] *USCIB Opposes Proposed Rule on ICT-Related Transactions*, U.S. COUNCIL FOR INT'L BUS., https://www.uscib.org/uscib-opposes-proposed-rule-on-ict-related-transactions/ (last visited Sept. 12, 2020).
[56] *U.S. Department of Commerce Proposes Rule for Securing the Nation's Information and Communications Technology and Services Supply Chain*, U.S. DEP'T OF COM. (Nov. 26, 2019), https://www.commerce.gov/news/press-releases/2019/11/us-department-commerce-proposes-rule-securing-nations-information-and.

adversaries—instead reserving the decision until a transaction is reviewed. It appears that the Department of Homeland Security and the Office of the Director of National Intelligence, along with other relevant cabinet-level secretaries, will have a part in evaluating what constitutes a 'foreign adversary.'[57] Therefore, statements provided by these agencies have offered some suggestions of 'red flag' actors who will be declared foreign adversaries. Christopher Krebs, Director of DHS-CISA, proposed that "foreign adversaries… include Russia, China, North Korea, and Iran."[58] Additionally, "the U.S.'s National Counterintelligence and Security Center [states that], '[w]e anticipate that China, Russia, and Iran will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace.'"[59] Another potential source of information is the current Export Administration Regulations Entity List.[60] As E.O. 13873 was issued concurrently with the announcement that sixty-eight Huawei affiliates would be added to the Entity List, it appears that the Entity List may be closely aligned with the interests of the E.O..[61]

B. The administration may be using this as political whack-a-mole, rather than targeting specific and harmful threats, which could create a devastating precedent.

The Commerce Department states that being a 'foreign adversary' means having "engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security

---

[57] *Id*.
[58] *Supply Chain Security, Global Competitiveness, and 5G: Hearing before the United States Senate Committee on Homeland Security and Government Reform*, 116th Cong. 3 (2019) (Testimony of the Hon. Christopher C. Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Dept. of Homeland Security).
[59] *Id.* (quoting U.S. NAT'L COUNTERINTELLIGENCE AND SEC. CTR., FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE 5 (2018)).
[60] The list is published and maintained by the Bureau of Industry and Security at the U.S. Department of Commerce. *See Entity List*, BUREAU OF INDUS. AND SEC. (Nov. 13, 2019), https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file.
[61] *Legal Alert: US Government Targets Tech Giant Huawei in China Trade War*, EVERSHEDS SUTHERLAND (May 31, 2019), https://us.eversheds-sutherland.com/mobile/NewsCommentary/Legal-Alerts/221222/Legal-Alert-US-government-targets-tech-giant-Huawei-in-China-trade-war.

of the United States or security and safety of United States persons."[62] Nevertheless, the inevitable inclusion of Huawei creates a precedent of punitive response for common backdoors without the requirement of hard evidence of adverse conduct.[63] Notably, Samsung's similar vulnerabilities allowed CIA's WeepingAngel malware to listen to conversations, but Samsung has yet to be added to the Entity List.[64] To lower the bar to such an indiscriminate standard would provide justification for other countries to take similar precautions.[65] Such actions could also set off a spiraling and very damaging, trade war.[66] Additionally, the use of such a low standard will lead to criticisms that the administration is using the ban as a form of political whack-a-mole to further trade negotiations rather than to protect legitimate national security concerns.[67]

---

[62] Exec. Order No. 13873, *supra* note 22, at 22,689.
[63] Andrew Huang, *Open Source Could Be a Casualty of the Trade War*, BUNNIE STUDIOS (June 21, 2019), https://www.bunniestudios.com/blog/?cat=5.
[64] *Id*.
[65] Some countries are already following the lead of the U.S. and banning Huawei products. Raymond Zhong, *Australia Bars China's Huawei From Building 5G Wireless Network*, N.Y. TIMES (Aug. 23, 2018), https://www.nytimes.com/2018/08/23/technology/huawei-banned-australia-5g.html; Raymond Zhong, *Is Huawei a Security Threat? Vietnam Isn't Taking Any Chances*, N.Y. TIMES (July 18, 2019), https://www.nytimes.com/2019/07/18/technology/huawei-ban-vietnam.html (citing Vietnam as evidence countries are already following the lead of the U.S. and banning Huawei products).
[66] Shutting Huawei could cause $11B in economic loses for partners. This is more damaging, economically, than the largest oil refinery explosion in recent history, causing $1.8B in damages. Even more alarming, a supply chain 'war' could have unintended consequences long past the target company itself, extending to suppliers that the U.S. government has no legitimate security interests in. MARSH & MCLENNAN COMPANIES, THE 100 LARGEST LOSSES 1974-2013: LARGE PROPERTY DAMAGE LOSSES IN THE HYDROCARBON INDUSTRY 5 (23d ed. 2014); Huang, *Open Source Could Be a Casualty of the Trade War*, *supra* note 63; Sherisse Pham, *Losing Huawei as a Customer Could Cost US tech Companies $11 Billion*, CNN (May 17, 2019), https://www.cnn.com/2019/05/17/tech/huawei-us-ban-suppliers/index.html.
[67] *See* Aaron Boyd, *Commerce Secretary Proposes "Case-by-Case' Enforcement of Telecom Ban*, NEXTGOV (Nov. 26, 2019), https://www.nextgov.com/cybersecurity/2019/11/commerce-secretary-proposes-case-case-enforcement-telecom-ban/161562/; *see also* Philip Heijmans & Haslinda Amin, *Ross Optimistic on China Deal Trump Wants it Signed in U.S.*, BLOOMBERG (Nov. 3, 2019), https://www.bloomberg.com/news/articles/2019-11-03/ross-optimistic-on-china-trade-deal-says-huawei-licenses-coming (detailing that Wilbur Ross has connected the pending trade deal with China to the issuance of licenses to work with Huawei on multiple occasions, the most recent being in early November 2019); Bryce Baschuk & Brendan Murray, *How Blacklisting Companies Became a Trade War Weapon*, BLOOMBERG (Oct. 10, 2019), https://www.bloomberg.com/news/articles/2019-10-11/how-blacklisting-companies-became-a-trade-war-weapon-quicktake (detailing the Trump Administrations use of blacklists, such as the Entity List, as a policy tool in trade negotiations rather than to preserve national security).

C. The evaluation process will create uncertainty, and the ability to challenge the findings will not present a meaningful check on Executive power.

i. The Commerce Department may initiate a review on its own prerogative or based on information submitted by private parties.

The proposed rule states that the Commerce Department may initiate a review on its own initiative, at the request of another head of certain federal agencies, or in response to information submitted by private parties that the Commerce Department finds credible.[68] There are at least three ways this new policy and order could disrupt the industry without advancing legitimate national security interests: (1) competitors tattling on each other to the Commerce Department to interrupt business and lower competition;[69] (2) the Executive Branch playing trade deal whack-a-mole in an effort to effect their economic policies;[70] and (3) foreign nation states providing anonymous tips about U.S. companies that aggressively compete with their domestic alternatives in order to slow innovation.[71] The policy allows government agencies, such as Department of Defense (DoD) and Department of Homeland Security (DHS), to closely monitor projects of

[68] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65,316, 65,321 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7).
[69] Steven F. Hill, Stacy J. Ettinger, Jeffrey Orenstein & Erica L. Bakies, *Commerce Proposes Process to Evaluate Transactions Involving Information and Communications Technology and Services for National Security Concerns,* K&L GATES (Dec. 3, 2019), https://www.klgates.com/Commerce-Proposes-Process-to-Evaluate-Transactions-Involving-Information-and-Communications-Technology-and-Services-for-National-Security-Concerns-12-03-2019.
[70] They could essentially impose a trade ban by banning all contracts for a particular service with a country, similar to how trade negotiations with China went under the Trump administration. Jenny Leonard et al., *Trump Blacklisted Huawei After China Trade War Negotiations Stalled*, FORTUNE (May 21, 2019), https://fortune.com/2019/05/21/trump-huawei-ban-china-trade-war/.
[71] *See* Adam Jourdan, *China's new breed of whistleblowers takes on big business*, REUTERS (Apr. 17, 2014), https://www.reuters.com/article/us-china-corruption-whistleblower/chinas-new-breed-of-whistleblowers-takes-on-big-business-idUSBREA3G29X20140417 ("Whistleblowers are quite normal in China… The [shepherd] lawyers guide potential whistleblowers to collect the information needed to report to the SEC, which leads U.S. investigations against corruption and corporate malpractice.").

their interests. [72] Reporting could be especially harmful where a transaction is already completed as the Commerce Department could effectively order an undoing of the arrangement.[73] The determination of what information the Commerce Department will find credible is further muddied by the concerns of a low evidentiary standard, even at the ordering of a ban.[74]

ii. The Commerce Department and other agencies will be able to request trade secrets and confidential business information, further straining public-private partnerships.

The technology transaction in question will then be assessed by a variety of federal parties to see if it meets the five criteria highlighted within the Executive Order for a ban.[75] The parties will be notified once a review has been commenced.[76] In conducting an evaluation, the Secretary can request confidential business and trade secret information, along with relevant publicly

[72] *See* Cybersecurity & Infrastructure Security Agency, *EO 13873 Response: Methodology for Assessing the Most Critical ICT and Services,* CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (2020) https://www.cisa.gov/publication/ict-eo-13873-response (CISA identifies 5G operations as those they will be monitoring for national security risks).
[73] *See* Paul Marquardt & Nathaniel Kurcab*, Proposed Regulations Create National Security Review of U.S. IT and Telecom Transactions Linked to "Foreign Adversaries"*, CLEARY GOTTLIEB (Nov. 27, 2019), https://www.clearygottlieb.com/-/media/files/alert-memos-2019/proposed-regulations-create-national-security-v2-pdf.pdf ("Commerce can impose draconian penalties for violations of these regulations or any material mitigation measures… the Proposed Regulations appear to contemplate that persons within U.S. jurisdiction will be subject to reviews requiring them to discard, reverse, or install safeguards around goods and services already acquired."); David McLaughlin, Saleh Mohsin & Jacob Rung, *All About CFIUS, Trump's Watchdog on China Dealmaking: QuickTake*, THE WASHINGTON POST (Feb. 13, 2020) https://www.washingtonpost.com/business/energy/all-about-cfius-trumps-watchdog-on-china-dealmaking-quicktake/2020/02/13/76510e36-4e1e-11ea-967b-e074d302c7d4_story.html.
[74] *See* Lawyer Monthly, *Can We Legally Ban TikTok?*, LAWYER MONTHLY (Sept. 14, 2020), https://www.lawyer-monthly.com/2020/09/can-we-legally-ban-tiktok/ (the low evidentiary standard used in the ban of TikTok through CFIUS was thought to set a dangerous precedent for U.S. tech companies).
[75] *See* Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316, 65321 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7) ("…in consultation with the Secretary of the Treasury, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and, as appropriate, the heads of other executive departments and agencies…").
[76] *Id*.

available and classified information from U.S. and foreign sources.[77] Trade secrets and confidential business information will not be released to the public, except where legally required.[78]

The ability of the government to request trade secret information relating to emerging technology transactions will further strain the public-private information security partnerships.[79] The Cybersecurity Information Sharing Act aimed to establish further public-private cooperation but has attracted less than a dozen nonfederal entities despite lawmakers assuming thousands would sign up to share data.[80] Perhaps now that private sector entities will otherwise have to disclose information to the government, the federal agencies will see further public-private engagement.[81] However, "[the] private sector takes the time to differentiate between threats and risks, while the public sector doesn't do that…[the public sector] can't afford to ignore any kind of risk."[82] This leads to a fear in the private sector that the government will create overreaching regulations that become burdensome to creativity.[83] With Christopher Krebs stating that "[n]o company out there, no state out there is going to overcome this challenge by themselves. We

[77] *Id*.
[78] *Id*.
[79] *See generally id*.
[80] *See* Derek Hawkins, *The Cybersecurity 202: 'We have to work together.' Government Struggling with Sharing Cyberthreat Information, Officials Say*, WASH. POST (July 23, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/07/23/the-cybersecurity-202-we-have-to-work-together-government-struggling-with-sharing-cyberthreat-information-officials-say/5b5496c31b326b1e646954bf/; *see also* Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE ((Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ (explaining the voluntary nature of the program and key provisions).
[81] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. at 65321.
[82] John P. Mello Jr., *Info-sharing between the feds and private sector needs work, says NSS*, CSO ONLINE (May 31, 2013), https://www.csoonline.com/article/2133549/info-sharing-between-the-feds-and-private-sector-needs-work--says-nss.html.
[83] *Id*.

have to work together,"[84] it is unlikely that forcing tech companies to release trade secrets will improve public-private relationship.

iii. The review and determination may be arbitrary, and there is little meaningful ability to challenge such a determination.

The reviewing parties will work to determine if the transaction meets the five criteria for a ban. Under the proposed rule,the Commerce Department "will consider a number of factors, including, but not limited to, the laws and practices of the foreign adversary; equity interest, access rights, seats on a board of directors or other governing body, contractual arrangements, voting rights, and control over design plans, operations, hiring decisions, or business plan development."[85] If a transaction meets the five criteria, the parties to the transaction will receive written notice of a preliminary determination with an explanation for the basis of the determination and an explanation that the parties can submit an opposition to the determination or suggestions for mitigation.[86]

The proposed regulation specifically states that an explanation will only be provided if it is consistent with national security (does not reveal classified information).[87] Accordingly, parties may not receive an explanation if it would endanger national security. This could be a loophole by which the Commerce Department could ban transactions in order to advance political rather than national security concerns.[88] This is further compounded by the limitations of review that are present when classified information is used;[89] the 3rd Circuit Court of Appeals has recognized

[84] Hawkins, *supra* note 80.
[85] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. at 65,321.
[86] *Id*.
[87] *Id*.
[88] *See generally id*.
[89] Classified information is defined under the Classified Information Procedures Act and is, essentially, the exact information that the Commerce Department would need to use to decide. *See* Judy Wang, *Ralls Corp. v. CFIUS: A New Lok at Foreign Direct Investments to the US,* 54 COLUM. J. TRANSNAT'L L. BULLETIN 30, 50–51 (2016)

"a significant caveat to the due process protections by not 'requiring disclosure of classified information supporting official action.'"[90] The concerns are furthered by the "government itself [having]the final authority to classify documents that it reviews… What is to stop the government from altering the classification of documents to avoid disclosing information?"[91] This arbitrary classification is exactly what the Administrative Procedures Act is meant to safeguard against.[92] However, the Federal Government settled the only Administrative Procedures Act challenge to CFIUS, the most analogous current regulation, so arbitrary review hidden by classification has avoided review by the courts.[93]

While CFIUS offers no opportunities to oppose a decision,[94] the proposed rules allow for a party to submit an opposition or explanation of mitigations that will occur, which will be reviewed within 30 days of receipt and before a final determination is issued.[95] However, a company's ability to challenge the findings in court does not guarantee success. In issuing a final determination, the Commerce Department "need not address every comment, but . . . must

---

("Interestingly, the definition of 'classification categories' itself lines up conveniently with the fairly vague parameters of 'national security' in the CFIUS statute. Specifically, the Classified National Security Information Act includes in 'classification' information pertaining to (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security; (f) United States Government programs for safeguarding nuclear materials or facilities; or (g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security… Therefore, definitionally speaking, it seems that a CFIUS determination necessarily requires consideration of documents that are classified; they are almost one and the same.").

[90] *Id*. (quoting Ralls Corp. v. Comm. on Foreign Inv., 758 F.3d 296, 319 (D.C. Cir. 2014)).

[91] *Id*. at 51.

[92] *Department of Commerce Issues Proposed Rule Establishing National Security Review for Acquisitions of Information and Communications Technology and Services*, CLIFFORD CHANCE (Dec. 6, 2019), https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2019/12/Department-of-Commerce-Issues-Proposed-Rule-Establishing-National-Security-Review-for-Acquisitions-of-Information-and-Communications-Technology-and-Services.pdf.

[93] Wang, *supra* note 89, at 53.

[94] As shown in *Ralls Corp.,* one could sue the Federal Government, but this is rarely done and, due to the previously raised classified information due process restrictions, judicial review is unlikely to provide a meaningful review of the process. *See supra* notes 89-91; *see generally Ralls Corp.*, 758 F.3d at 314, 319-20.

[95] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316, 65321 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7).

respond in a reasoned manner to those that raise significant problems."[96] Even if a court considers a company's opposition materials and proposed mitigations as "significant comments," the Department's obligation to respond is "not particularly demanding.".[97] Furthermore, as the parties of the transaction are not privy to the national security information that will be the basis of the preliminary determination, any mitigations proposed will be unlikely to fully address the national security concerns known to the Commerce Department.[98]

iv. By creating categories where a threat is presumed, the Commerce Department could reduce uncertainty and shift the mitigation burden to the companies.

Currently, the Commerce Department has specifically stated that it has "declined to identify classes of transactions that are subject to prohibition or are excluded from prohibition."[99] However, a list of telecommunications and IT equipment and services covered by the rules, including internet service providers, internet application operators/developers, and software providers, has been published.[100] By offering a presumption against certain types of technology, the Commerce Department could provide more notice to companies that a transaction is likely to be banned. Specifically, technology types that have posed threats repeatedly and are intimately connected to foreign adversaries should come with a presumption of a ban, thus forcing the burden on companies from the start to prove they can adequately mitigate threats or face steep penalties.[101]

---

[96] City of Waukesha v. EPA, 320 F.3d 228, 257 (D.C. Cir. 2003) (citation omitted).
[97] Ass'n of Private Sector Colleges and Universities v. Duncan, 681 F.3d 427, 441 (D.C. Cir. 2012) (citation omitted).
[98] E. Maddy Berg, *A Tale of Two Statutes: Using IEEPA's Accountability Safeguards to Inspire CFIUS Reform*, 118 COLUM. L. REV. 1763, 1773 n. 64 (2018).
[99] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. at 65,320.
[100] *Id.* at 65,318–19.
[101] *See id.* at 65,322 ("Any person who, after [effective date of final rule], violates a material provision of a mitigation measure or a material condition imposed by the United States under § 7.103 or § 7.104 may be liable to

IV. THIRD-PARTY CODE CREATED BY FOREIGN ADVERSARIES SHOULD COME WITH A PRESUMPTION OF THREAT.

Third-party code created by private threat groups and nation states[102] has presented a continuous risk for U.S. citizens affecting 25 million cellular devices in the summer of 2019 alone.[103] U.S. companies have become far too trusting or lazy[104] in reviewing the code provided by third parties considering that, in 2018, nearly 60% of companies suffered a data breach caused by third-party code.[105] Yet still companies have a greater reliance on third-party code than ever before.[106] This is exactly the form of threat that E.O. 13873 and the proposed Commerce Department rules should be attempting to combat. Due to the immediate, widespread and well-known threat that third-party code poses, the Commerce Department should declare it a presumed threat, or at the very least pay close attention to third-party code transactions.

A. Third-party code has been a consistent method for hackers to attack US citizens online.

On June 27th, Ticketmaster announced that malicious software was identified in their third-party supplier's application.[107] Ticketmaster has since released details of a long-running

---

the United States for a civil penalty under 50 U.S.C. 1705, not to exceed $302,584, as adjusted annually for inflation under 15 CFR 6.5, per violation or the value of the transaction. Any penalty assessed under this paragraph (b) shall be based on the nature of the violation and shall be separate and apart from any damages sought pursuant to a mitigation measure or any action taken under § 7.103.").

[102] Any third-party code, regardless of vendor, should be reviewed as a potential threat to ICT. Foreign adversaries are not above exploiting the fourth-party vendor loophole, where they provide the code to a 3PC vendor in a trusted nation, who then passes it on to US vendors. However, such an extreme review process would be unlikely to succeed due to the significant personnel needed by such an undertaking. Mathew J. Schwartz, *Developers Skip Third Party Code Checks*, DARK READING (May 5, 2011), https://www.darkreading.com/risk-management/developers-skip-third-party-code-checks/d/d-id/1097650

[103] Taylor, *supra* note 28.

[104] Jose Pagliery, *Why was Your Credit Card Number Stolen? Retailers are Lazy*, CNN BUSINESS (March 11, 2015), https://money.cnn.com/2015/03/11/technology/security/credit-card-hack/index.html.

[105] PONEMON INSTITUTE, DATA RISK IN THE THIRD-PARTY ECOSYSTEM 5-6 (2017).

[106] Kelly Sheridan, *Who's the Weakest Link in Your Supply Chain?*, DARK READING (Nov. 27, 2018), https://www.darkreading.com/threat-intelligence/whos-the-weakest-link-in-your-supply-chain/d/d-id/1333349.

[107] *Information About Data Security Incident by Third-Party Supplier*, TICKETMASTER (June 27, 2018), https://security.ticketmaster.co.uk/.

skimming operation on their site: from September 2017 to June 23, 2018, for any purchase over Ticketmaster International, Ticketmaster UK, GETMEIN! and TicketWeb, the customer's name, email, address, phone number, payment details and login details were sent to Magecart, a cyber threat group known for web-based card skimming.[108] Simply put, Ticketmaster embeds a special JavaScript module written by Inbeta Technology, a third-party code supplier, into their website in order to process payments.[109] The code caused any information on the screen to be transmitted to a new server run by Magecart, who would then either use the stolen cards themselves for theft or sell the information to other criminals.[110] Both Ticketmaster and its customer service chatbot provider have been attributing the breach to each other– who was supposed to monitor the code for malware and who should be responsible for the potential fines and class-action damages?[111]

On September 6th, 2018, British Airways announced that over 380,000 customers were effected by a data breach.[112] Payment through the main website and mobile app were skimmed for customer personal and financial information, exclusive of travel details, over the period of August 21st to September 5th.[113] Magecart did so by tampering with the code British Airways had pulled from the MIT open source code library.[114] These are not isolated instances: Magecart has infiltrated an estimated 800 e-commerce sites with similar digital card-skimming code through

[108] Yonathan Klijnsma & Jordan Herman, *Inside and Beyond Ticketmaster: The Many Breaches of Magecart*, RISKIQ (July 9, 2018), https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/.
[109] *Id.*
[110] *Id.*
[111] Richard Smirke, *Law Firm Launches $6.5 Million Action Against Ticketmaster Over Data Breach*, BILLBOARD (Apr. 4, 2019), https://www.billboard.com/articles/business/touring/8505737/law-firm-launches-65-million-action-against-ticketmaster-over-data.
[112] *British Airways Admits That Over 380,000 Customers Had Their Data Stolen*, THE ECONOMIST (Sept. 9, 2018), https://www.economist.com/gulliver/2018/09/09/british-airways-admits-that-over-380000-customers-had-their-data-stolen.
[113] Lily Hay Newman, *How Hackers Slipped by British Airways' Defenses*, WIRED (Sept. 11, 2018), https://www.wired.com/story/british-airways-hack-details/.
[114] Yonathan Klijnsma, *Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims*, RISKIQ (Sept. 11, 2018), https://www.riskiq.com/blog/labs/magecart-british-airways-breach/.

the use of third-party applications as of July 2018.[115] By infiltrating third-party code suppliers, Magecart is able to affect more sites through one action because many e-commerce sites use the same providers for credit card processing.[116]

B. Nation-states are in an ideal position to exploit third-party code vulnerabilities.

Nation-states are well positioned to exploit third-party code because it takes an immense amount of resources, especially technically skilled human resources. [117] They have recognized the opportunity of attacking a single "very small company or developer… [to] breach thousands of major enterprises."[118] In addition, supply chain attacks are generally harder to detect, allowing for more covert surveillance, as the code which is altered is trusted by the system by default.[119] Thus, the attack can occur "without arousing the suspicion of network defenders."[120] With much of today's third-party code already originating from foreign sources, third-party code is "the ideal backdoor for bad actors of every stripe to attack U.S. infrastructure and abuse U.S. citizens."[121] Between August and October of 2019 alone, 25 million Android devices were hacked by 3PC malware originating in Russia and China; this illustrates just two out of thousands of instances of foreign infiltration in the summer of 2019.[122]

[115] Klijnsma & Herman, *supra* note 107.
[116] *Id.*
[117] Mansfield-Devine, *supra* note 16, at 17-18, 20.
[118] Fortuna, *supra* note 3.
[119] *Id.*
[120] *Id.*
[121] *New Executive Order Applies to Foreign Third-Party Code*, *supra* note 23.
[122] Taylor, *supra* note 28.

C. The effects of presumptively banning third-party code could be far-reaching.

i. Open Source Code platforms could die off.

As Huawei is closely linked to the type of 'foreign adversary' the Commerce Department intends to ban transactions with, concerns have been raised about the livelihood of the Linux Foundation, an open source Linux code bank for which Huawei is a platinum sponsor and a top contributor.[123] Many companies use code supplied by the Linux Kernel project or other open source platforms.[124] Open source code can save a company 20-55% on development costs, while reducing bloatware, lock-in contracts, and training time.[125] It would not be easy to identify and remove the portions of the code inserted by Huawei, let alone other contributors who may find themselves being deemed a 'foreign adversary' due to nationality.[126] Additionally, open source code developers worry that they may inadvertently be labeled as engaging in 'transactions' with foreign adversaries by posting their code and making it available non-discriminatorily.[127] One possible solution would be to have a trusted U.S. company double-check all the code supplied by

[123] JONATHAN CORBET & GREG KROAH-HARTMAN, THE LINUX FOUNDATION, 2017 LINUX KERNEL DEVELOPMENT REPORT 14 (2017).
[124] Steven J. Vaughan-Nichols, *It's an Open-Source World: 78 Percent of Companies Run Open-Source Software*, ZDNET (Apr. 16, 2015), https://www.zdnet.com/article/its-an-open-source-world-78-percent-of-companies-run-open-source-software/.
[125] Bill Weinberg, *6 Reasons Why Open Source Software Lowers Development Costs*, LINUX (Feb. 28, 2017), https://www.linux.com/news/6-reasons-why-open-source-software-lowers-development-costs/.
[126] Klint Finley, *The WIRED Guide to Open Source Software*, WIRED (Apr. 24, 2019), https://www.wired.com/story/wired-guide-open-source-software/; Maria Korolov, *Open Source Software Security Challenges Persist*, CSO ONLINE (Apr. 2, 2018), https://www.csoonline.com/article/3157377/open-source-software-security-challenges-persist.html.
[127] Andrew Huang, *Open Source Could Be a Causality of the Trade War*, BUNNIE STUDIOS (June 21, 2019), https://www.bunniestudios.com/blog/?p=5590 ("There's nothing in Github (or any other source-sharing platform) that prevents your code from being accessed by a foreign adversary and incorporated into their technological base, so there is an argument that open source developers are aiding and abetting an enemy by effectively sharing technology with them.").

Huawei and other foreign adversaries, but the costs of this would largely defeat the purpose of open source code libraries.[128]

ii. There would be a substantial financial effect on digital companies.

One of the primary attractions of third-party code is the ability to outsource functionality, saving development time and easing a regulatory burden.[129] However, the suggestion here is not to ban third-party code altogether, but to require companies to prove they can mitigate the posed threat or avoid purchasing code from vendors associated with foreign adversaries. There are costs associated with mitigation that will need to be weighed against the costs of insourcing for companies who use third-party code. One of the largest imaginable effects of a third-party code presumptive ban would be the loss of interactive customer service chatbots on websites.[130] Surely it would be more expensive to fully develop a customer service chatbot, much less hire fulltime customer service agents, when those capabilities could be procured through third-party code and service providers in foreign nations.[131] However, the U.S. has a continuing interest in providing jobs for U.S. citizens.

---

[128] *See* Huawei Cyber Sec. Evaluation Ctr., Huawei Cyber Security Evaluation Centre (HSCEC) Oversight Board Annual Report 2019: A report to the National Security Adviser of the United Kingdom 1-3 (2019); Korolov, supra note 125. *Contra* Lily Hay Newman, *Huawei's Problem Isn't Chinese Backdoors. It's Buggy Software*, WIRED (Mar. 20, 2019), https://www.wired.com/story/huawei-threat-isnt-backdoors-its-bugs/.

[129] Smith, *The Cyber Threats of Third-Party Features*, BUSINESS NEWS LINE (Jan. 1, 2020), https://www.businessnewsline.com/the-cyber-threats-of-third-party-features/.

[130] Mai-Hanh Nguyen, *The Latest Market Research, Trends, and Landscape in the Growing AI Chatbot Industry*, BUSINESS INSIDER (Jan. 23, 2020), https://www.businessinsider.com/chatbot-market-stats-trends.

[131] *See* Trips Reddy, *How Chatbots Can Help Reduce Customer Service Costs by 30%*, IBM (Oct. 17, 2017), https://www.ibm.com/blogs/watson/2017/10/how-chatbots-reduce-customer-service-costs-by-30-percent/ ("265 billion customer support requests are made every year, and it costs businesses a whopping $1.3 trillion to service them. Chatbots can reduce these costs significantly when companies upgrade from antiquated, inefficient IVR technology to AI, chatbots, virtual assistants, messaging and other new technologies that are already helping transform call centers across the world… businesses can reduce customer service costs by up to 30% by implementing conversational solutions like virtual agents and chatbots. Freeing up human agents at contact centers to address complex inquiries allows representatives to take their time and provide better service. It also reduces the number of agents required on the call center floor as well as employee attrition due to the repetitive nature of routine calls. All of these lead to significant cost savings.").

Chatbots will save U.S. businesses $8 billion per year in customer service costs by 2022; this will mean that $8 billion in customer service personnel salaries will be replaced by automation.[132] To outsource a chatbot, which would mean providing the third-party code supplier an ability to modify internally produced code and see back-end customer information, a company would only need to invest $50/month[133] or $15,000 to $30,000 to buy outright.[134] The cost of in-house production is roughly $10,000 to $20,000.[135] Alternatively, purchasers could prove their ability to mitigate third-party code risks by implementing a thorough code review every time a change is made. This is, admittedly, the bane of many programmers' existence.[136] However, thorough code review can mitigate most breaches and maintain data security.[137] By forcing companies to produce code in-house or employee technically skilled code reviewers, the U.S. would secure an increased need for technically skilled employees.

D. Companies with third-party code should be, but are not, prepared to remove it quickly.

[132] *See* Karen Gilchrist, *Chatbots Expected to Cut Business Costs by $8 Billion by 2022*, CNBC (May 9, 2017), https://www.cnbc.com/2017/05/09/chatbots-expected-to-cut-business-costs-by-8-billion-by-2022.html ("Chatbots could help trim business costs by more than $8 billion per year by 2022, according to new research which is anticipating a surge in automated customer service programs as companies move to embrace artificial intelligence (AI)… As artificial intelligence advances, reducing reliance on human representatives undoubtedly spells job losses…").
[133] *See, e.g., Botsify Pricing*, BOTSIFY, https://botsify.com/pricing (last visited Sept. 6, 2020) (exemplifying outsourced chatbot provider pricing. This may not be the lowest price but is representative of average industry pricing).
[134] *See, e.g., How Much Does it Cost to Build a Chatbot in 2020?*, AZATI (Sept. 17, 2020), https://azati.ai/how-much-does-it-cost-to-build-a-chatbot/ (detailing that the final cost for a custom chatbot is typically priced between $15,000 and $30,000).
[135] *See Id. Compare* Andrew DePietro, *How Much Computer Programmers Earn in Each State*, FORBES (Feb. 18, 2019), https://www.forbes.com/sites/andrewdepietro/2019/02/18/computer-programmers-salary-state/#14e4b60c36b0 (demonstrating the high programming cost in the U.S., where the average salary of a computer programmer is $87,530) *with* (listing the average salary of a computer programmer in various countries - Ukraine ($11,600), Russia ($22,100), China ($23,100), and Saudi Arabia ($26,600)).
[136] Michaela Greiler, *How to Avoid Code Review Pitfalls that Slow Your Productivity Down*, DOCTOR MCKAYLA, https://www.michaelagreiler.com/code-review-pitfalls-slow-down/ (last visited Sept. 6, 2020).
[137] Gary Glover, *Code Reviews: A Method to Reveal Costly Mistakes*, SECURITYMETRICS (Mar. 23, 2016), https://www.securitymetrics.com/blog/code-reviews-method-reveal-costly-mistakes.

Many companies do not actively track which portions of code come from which vendors, yet they could be forced, under the proposed rules, to undo third-party code involved in a transaction after May 15, 2019 with very little notice.[138] Most cyber insurance policies, under current common boilerplate contract language, will not cover losses sustained by companies who suddenly find themselves without code to run their applications due to regulatory enforcement.[139] So not only will companies find themselves removing code, but they will be forced to scramble to replace such code or risk substantial losses in revenue. If they cannot even identify which code comes from a third-party, they will either need to take down any site which may have third-party code or risk the penalties of non-compliance.

V. CONCLUSION

Despite the downsides of a threat presumption against third-party code, it is indisputable that third-party code has presented a continuous threat to information and communication technology in the U.S. and citizens personal and financial information. As the technology features that are often associated with third-party code continue to expand in popularity and are moving further into the healthcare and financial sector, the new regulations pose a novel opportunity to combat the threat posed by third party code. The Commerce Department should seize the opportunity to protect U.S. security interests with little need to explain specific rationale and create a presumption of threat against third-party code.

[138] Rajendran, *supra* note 1, at 8; Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65,316, 65,322 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7).
[139] Daniel B. Garrie, *Executive Order 13873 Could Expand the Reach of War Exclusions in Cyber Policies*, FORBES (July 16, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/07/16/executive-order-13873-could-expand-the-reach-of-war-exclusions-in-cyber-policies/#4074e95a75b3.