This written submission is a soon-to-be-published Note that will appear in the Winter 2020 issue of the *Public Contract Law Journal*. Please do not circulate beyond the February 2020 joint meeting of the ABA Section of International Law (SIL) Anti-Corruption Committee and the ABA Public Contract Law Section (PCLS) Suspension and Debarment Committee.

The Kaspersky, ZTE, and Huawei Sagas: Why the United States Is in Desperate Need of a Standardized Method for Banning Foreign Federal Contractors

Grace Sullivan[*]
Mailing Address: 925 25th St. N.W. #507 Washington, D.C. 20037

[*] Grace Sullivan is a third-year student at The George Washington University Law School. She would like to thank Professor Sonia Tabriz for her guidance during the writing process. Grace can be contacted by email at gsullivan@law.gwu.edu.

Table of Contents

Abstract

The landscape of modern U.S. foreign policy towards Russia and China has been marred with accusations of election tampering, hacking, and spying. Russian and Chinese companies with close ties to their governments are at the heart of these accusations, and their actions have triggered concerns that they are a threat to U.S. national security. Since 2017, Congress has passed laws precluding three foreign cybersecurity and telecommunications companies—Kaspersky, ZTE, and Huawei—from entering into contracts with the federal government. These three corporations may not provide products or services to any agency or department of the federal government. While the federal government is well within its authority to enact these bans, the manner in which the bans were carried out was haphazard, confusing, and unnecessarily politicized.

This Note argues that in order to ease foreign policy tensions with Russia and China, exacerbated by federal contracting bans on companies with close ties to their governments, the U.S. should adopt a standardized method for enacting such bans. Once a determination has been made that a foreign company should be precluded from contracting with the federal government due to national security concerns, the company should be given an opportunity to defend itself in front of the Secretary of Homeland Security. If the company does not sufficiently assuage Homeland Security's concerns, the federal government should proceed to enact a contracting ban through the upcoming fiscal year's appropriations bill.

I. Introduction

Foreign federal government contractors "are susceptible to political whims."[1] Some go so far as to call such contractors "[g]eopolitical [p]awn[s]."[2] These statements have rung particularly true in the last few years. In the wake of increasing political and media attention on foreign government interference in U.S. affairs,[3] the federal government has taken steps to ban certain international companies from contracting with federal agencies.[4] The bans have targeted companies in Russia and China, countries long considered hostile to U.S. national security.[5] Indeed, contracting bans have become not only a means of protecting national security, but also a mirror of current political tensions.

The federal government is well within its rights to be vigilant of national security threats involving international contractors. Cybersecurity in particular is a pressing challenge, as experts expect cyberattacks against information technology (IT) systems to increase in number

---

[1] Alexander W. Major et al., *GSA Technology Acquisitions: How Cybersecurity Threats and Cloud Services Are Changing the Way the Government Buys Technology from Commercial Companies*, BRIEFING PAPERS, Aug. 2017, at 9 (alteration in original).

[2] *See* Paul Mozur & Kevin Granville, *What Is ZTE? A Chinese Geopolitical Pawn that Trump Wants to Rescue*, N.Y. TIMES (June 7, 2018), https://www.nytimes.com/2018/06/07/business/what-is-zte.html [https://perma.cc/7JEP-89CP].

[3] *See, e.g.*, Jane Mayer, *How Russia Helped Swing the Election for Trump*, NEW YORKER (Sept. 24, 2018), https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump [https://perma.cc/7UEZ-UZA2] (detailing allegations that Russia meddled in the 2016 presidential election).

[4] *See* National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1634(a), 131 Stat. 1283, 1739-40 (2017); *see also* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(a), (f)(3)(A), 132 Stat. 1636, 1917-18 (2018).

[5] *See* David Vergun, *China Is a Rising Threat to National Security, Say DOD Leaders*, U.S. DEP'T OF DEF. (Mar. 13, 2019), https://www.defense.gov/Newsroom/News/Article/Article/1784442/china-a-rising-threat-to-national-security-say-dod-leaders/ [https://perma.cc/X2CQ-MZUB]; *see also China and Russia Are Bigger Threats to the US than Terrorism, Claims Department of Defense*, SOUTH CHINA MORNING POST (Jan. 20, 2018), https://www.scmp.com/news/china/diplomacy-defence/article/2129774/china-and-russia-are-bigger-threats-us-terrorism-claims [https://perma.cc/E8BM-MJW6].

and severity in the coming years.[6] Consequences of weak cybersecurity include cybertheft, cyberespionage, denial-of-service (DoS) attacks, botnet malware, and attacks on industrial control systems.[7]

The federal government has a number of tools at its disposal to impose contracting bans on international contractors that threaten U.S. cybersecurity.[8] *That* is where the problem lies. Because the government has such a myriad of options, there is no uniform manner in which such bans are carried out.[9] The consequence of this lack of standardization, this Note argues, is that the bans take on a politically retaliatory flavor—even when based on genuine national security concerns—because each ban appears "tailored" to a specific political circumstance, a specific country, like Russia or China, or a specific world leader, like Vladimir Putin or Xi Jinping.[10]

---

[6] *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R43831, CYBERSECURITY ISSUES AND CHALLENGES: IN BRIEF 1 (Aug. 12, 2016).

[7] *See id.* at 2. A DoS attack occurs when a cybercriminal inundates a website with unexpected volumes of traffic, which "triggers a crash" and prevents anyone from accessing the site. *See What is a Denial of Service Attack (DoS)?: An Overview of DoS Attacks*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos [https://perma.cc/H48Y-SKW9] (last visited Sept. 16, 2019). A botnet, the amalgamation of the words "robot" and "network," is a virus that allows a cybercriminal to organize many computers "into a networks of 'bots' that the criminal can remotely manage." *What Is a Botnet?*, KASPERSKY LAB, https://usa.kaspersky.com/resource-center/threats/botnet-attacks [https://perma.cc/U2W7-U322] (last visited Oct. 12, 2019).

[8] *See, e.g.*, *Binding Operational Directive 17-01: Removal of Kaspersky-Branded Products*, U.S. DEP'T OF HOMELAND SECURITY (Sept. 13, 2017), https://cyber.dhs.gov/bod/17-01/ [https://perma.cc/PR2J-JNME] [hereinafter *BOD 17-01*] (discussing Binding Operational Directive procedures used to rid agency IT systems of Kaspersky products); John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 889(a), (f)(3)(A), 132 Stat. at 1917-18 (providing an example of a contracting ban enacted through a National Defense Authorization Act).

[9] *See infra* Part III-IV (providing examples and analysis of the differences between the federal contracting bans on Kaspersky, ZTE, and Huawei).

[10] *See generally Vladimir Putin: Russia's President in Power for 20 Years*, BBC NEWSROUND (Aug. 16, 2019), https://www.bbc.co.uk/newsround/44922487 [https://perma.cc/L3UK-XNPS] (noting that Putin is the president of Russia); Christopher Bodeen, *China's President Renews Commitment Not to Interfere in Hong Kong*, PBS NEWS HOUR (Sept. 30, 2019),

This Note argues that the current contracting ban procedures aggravate already-delicate foreign relations and confuse contractors and government agencies alike.[11] Nowhere is this phenomenon clearer than in the contracting bans on Chinese telecommunications (telecommunications or telecom) giants ZTE and Huawei and Russian cybersecurity firm Kaspersky Lab. Kaspersky was formally banned from contracting with the federal government in December 2017.[12] This was shortly after accusations swirled that the Russian government meddled in the 2016 presidential election.[13] ZTE and Huawei were formally banned from contracting with the federal government in August 2018.[14] Those bans came on the heels of a massive trade war the Trump administration began in early 2018.[15]

With these issues in mind, this Note proposes that the United States adopt a standardized method for enacting government contracting bans of indefinite length on foreign companies that pose national security threats. Part II of this Note lays the groundwork for the federal

---

https://www.pbs.org/newshour/world/chinas-president-renews-commitment-not-to-interfere-in-hong-kong [https://perma.cc/V9G9-5FMX] (noting that Xi Jinping is the president of China).

[11] *Cf.* Bill Bostock, *China Is Reportedly on the Brink of 'Major Retaliative Measures' Against the US as the Trade War Escalates Further*, BUS. INSIDER (May 31, 2019), https://www.businessinsider.com/us-huawei-ban-reaction-major-incoming-state-media-2019-5 [https://perma.cc/E2VX-77RZ] (describing China's retaliatory reaction after Huawei was restricted from selling products in the United States); *cf.* Derek B. Johnson, *For Contractors Late on Kaspersky Cleanup, DHS Considers Consequences*, FCW (May 8, 2018), https://fcw.com/Articles/2018/05/08/dhs-kaspersky-consequences.aspx?p=1 [https://perma.cc/48NT-8EBT] (stating that the preliminary method for banning Kaspersky from contracting, a Binding Operational Directive, did not state whether the ban applied to federal contractors, thereby leaving uncertainty as to the scope of the ban).

[12] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1634(a), 131 Stat. 1283, 1739-40 (2017).

[13] *See, e.g.*, Mayer, *supra* note 3.

[14] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(a), (f)(3)(A), 132 Stat. 1636, 1917-18 (2018).

[15] *See* Dorcas Wong & Alexander Chipman Koty, *The US-China Trade War: A Timeline*, CHINA BRIEFING (Sept. 11, 2019), http://www.china-briefing.com/news/the-us-china-trade-war-a-timeline/ [https://perma.cc/9HTE-5Y6K].

government's authority to enact these bans. Part III provides information on the ZTE, Huawei, and Kaspersky sagas and compares the methodology of each ban. Part IV discusses what was successful and what went wrong in each of the three case studies. Part IV then proposes a new way forward: a standardized procedure for the U.S. Government to follow in the event of a future need for a contracting ban on an international company. In brief, the proposed procedure borrows aspects from all three case studies but remains conscious of their many pitfalls. Once a federal agency or the executive branch believes that a foreign company should be precluded from contracting with the federal government, the company should be given an opportunity to be heard and to defend itself in front of the Secretary of Homeland Security. If, during this opportunity, the company does not sufficiently assuage Homeland Security's concerns, Congress should proceed to enact a contracting ban through the upcoming fiscal year's appropriations bill. If the national security concern is urgent and cannot wait until the passage of the next appropriations bill, the Department of Homeland Security (DHS) should immediately enact a binding operational directive. Part V concludes and looks to the future of foreign relations with Russia and China.

II. The Federal Government Possesses the Authority to Enact Permanent Federal Contracting Bans on International Companies.

Discussion of ZTE, Huawei, and Kaspersky first necessitates an overview of the source of the federal government's authority to ban an international company from contracting with the government. This Note defines a "ban" as an indefinite, complete preclusion of a company from contracting with any federal agency or department of the United States.[16] An important source

[16] Please note that this definition is of the author's own making but is based on language found in the relevant National Defense Authorization Acts. *See* National Defense Authorization Act for Fiscal Year 2018 § 1634(a), 131 Stat. at 1739-40; *see also* John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 889(a), (f)(3)(A), 132 Stat. at 1917-18.

of authority is the Federal Information Security Management Act of 2002 (FISMA), which established IT security standards for the federal government.[17] FISMA was later amended in 2014 to provide the DHS with broad authority to safeguard the federal government's IT systems.[18]

A. The Federal Information Security Management Act of 2002

1. The Original FISMA

Generally, the federal government finds the authority to suspend or debar contractors within the Federal Acquisition Regulation (FAR).[19] In the cases of Kaspersky, Huawei, and ZTE, however, the government relied on its authority grounded in federal statute.[20] FISMA is a foundational statute in terms of providing the government with the power to ensure federal cybersecurity.[21] FISMA "mark[ed] the culmination of two decades during which Congress addressed . . . information security problems piecemeal through a scattered mosaic of legislation."[22] The statute combined key portions of its predecessors: "the Government Information Security Reform Act, the Computer Security Act of 1987, the Clinger-Cohen Act, and the Paperwork Reduction Act of 1980."[23] The statute also "established standard IT security requirements for federal systems."[24] In addition, it mandated the creation of the Federal Risk

---

[17] *See* Federal Information Security Management Act of 2002, Pub. L. No. 107-347, § 3541, 116 Stat. 2899, 2946 (2002).
[18] *See* Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 3553(b), 128 Stat. 3073, 3075-76 (2014).
[19] *See* FAR 9.4.
[20] *See* National Defense Authorization Act for Fiscal Year 2018 § 1634(a), 131 Stat. at 1739-40; *see also* John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 889(a), (f)(3)(A), 132 Stat. at 1917-18.
[21] *Cf.* Federal Information Security Management Act of 2002 § 3543(a), 116 Stat. at 2947-48.
[22] Robert Silvers, Note, *Rethinking FISMA and Federal Information Security Policy*, 81 N.Y.U. L. REV. 1844, 1847 (2006) (alteration in original).
[23] *Id.*
[24] Major et al., *supra* note 1, at 7.

and Authorization Management Program, which ensured that "contractors providing cloud services to the [g]overnment were compliant with FISMA requirements."[25]

The early years under the FISMA regime were relatively unsuccessful: from 2002 to 2006, despite federal agencies spending around $4.2 billion on safeguards for IT systems, "none of the [twenty-four] major agencies . . . fully implemented agency wide information security programs as required by FISMA."[26] One of FISMA's most glaring problems was its treatment of IT systems whose installation or maintenance was contracted out to private companies.[27] The statutory language was unclear as to whether a federal agency bore the responsibility of safeguarding data that was stored on a private contractor's IT system.[28] Moreover, enforceability and oversight were weak because it was uncertain what an agency's responsibility was in general.[29] Lastly, FISMA allocated no new appropriations to agencies; thus, agencies were mandated to strengthen IT systems within "the constraints of their [meager] preexisting budgets."[30]

2. FISMA's 2014 Amendments

In recognition of the gaps in the original statute, Congress amended FISMA in 2014.[31] The amendments provided a much more comprehensive framework for the federal government's

[25] *Id.* (alteration in original).
[26] *No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards Before the H. Comm. on Government Reform*, 109th Cong. 32 (2006) (alteration in original); *see also* Silvers, *supra* note 22, at 1849.
[27] *See* Silvers, *supra* note 22, at 1853.
[28] *See id.*
[29] *See id.* at 1847.
[30] *Id.* at 1859 (alteration in original).
[31] *See* Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3073 (2014).

cybersecurity practices.[32] For example, in response to the lack of clear enforcement authority under the 2002 statute, the 2014 amendments delegate to the DHS the power to "administer the implementation of [agency] information security policies" for non-national security agencies.[33] Under the updated law, the authority to "oversee the federal information security scheme" is delegated to the Director of the Office of Management and Budget (OMB), and the Director, in turn, is tasked with "work[ing] in conjunction with" the DHS Secretary.[34] In essence, "OMB provides oversight and policy direction, while DHS has operational responsibility for civilian agency information security."[35] The amended FISMA also gives DHS heightened authority to implement security policies in emergency situations.[36]

For the purposes of this Note, the most important amendment was one that conferred authority upon the Director of OMB and the DHS Secretary to issue binding operational directives (BOD).[37] Pursuant to their BOD authority, the Director and the Secretary may give a federal agency a "compulsory direction" to take steps to safeguard their IT system "from a known or reasonably suspected" security threat.[38] A threat or "incident" is an occurrence that

---

[32] *See* Hannah Vail, *Cybersecurity Reform in the Wake of the OPM Breach*, 50 SUFFOLK U. L. REV. 221, 224 (2017); *see also Federal Information Security Modernization Act*, U.S. DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/fisma [https://perma.cc/8MPC-YG3V] (last visited Nov. 15, 2018) [hereinafter *DHS Overview of FISMA*] (noting that the amendments "codify [DHS] authority to administer the implementation of information security policies for non-national security federal [e]xecutive [b]ranch systems" and provide clarity on OMB's oversight authority).

[33] *Id.* (alteration in original); *see also* Federal Information Security Modernization Act of 2014 § 3553(b), 128 Stat. at 3075.

[34] Vail, *supra* note 32 (alteration in original); *see also* Federal Information Security Modernization Act of 2014 § 3553(a)(1), (b)(1), 128 Stat. at 3075-76.

[35] Mike Vernick & Mike Scheimer, *Cybersecurity Developments in 2015*, 58 GOV'T CONTRACTOR ¶ 34, Feb. 3, 2016, at 2.

[36] *See* FISCHER, *supra* note 6, at 7.

[37] *See* Federal Information Security Modernization Act of 2014 § 3553(b)(2), 128 Stat. at 3076.

[38] *Id.* §§ 3552(b)(1).

"actually or imminently jeopardizes . . . the integrity, confidentiality, or availability" of an agency's IT system.[39] FISMA provides:

> The [DHS] Secretary, in consultation with the Director [of OMB], shall administer the implementation of agency information security policies and practices for information systems . . . including . . . developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director . . . including . . . requirements for reporting security incidents . . . requirements for the mitigation of exigent risks to information systems . . . monitoring agency implementation of information security policies and practices . . . convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices . . . [and] other actions as the Director or the Secretary, in consultation with the Director, may determine necessary to carry out this subsection.[40]

Thus, as the law stands now, the DHS and OMB wield fairly broad authority to issue BODs and ensure the security of federal IT systems. There are only minor limits to this discretion. First, when implementing a BOD, the DHS Secretary must consider any guidelines instituted by the National Institute of Standards and Technology (NIST) and issued by the Secretary of Commerce.[41] Second, the DHS Secretary and the Director of OMB generally do not oversee IT safety for non-civilian national security systems—the responsibility for safeguarding those systems falls instead to the Secretary of Defense or the Director of National Intelligence.[42]

Despite this robust statutory framework, federal government cybersecurity continues to be lacking.[43] For example, in 2015, the U.S. Office of Personnel Management "discovered that the background investigation records of current, former, and prospective [f]ederal employees and

---

[39] *Id.* § 3552(b)(2)(A).
[40] *Id.* § 3553(b).
[41] *Id.* § 3553(f)(1).
[42] *Id.* § 3553(b), (d)-(e).
[43] *Cf. Cybersecurity Resource Center Cybersecurity Incidents: What Happened,* U.S. OFF. OF PERSONNEL MGMT., https://www.opm.gov/cybersecurity/cybersecurity-incidents/ [https://perma.cc/3VKR-ZJAH] (last visited Jan. 25, 2019) (providing two examples of recent cyber attacks that the federal government failed to prevent).

contractors had been stolen."[44] The attack, reportedly carried out by Chinese hackers, exposed the social security numbers of 21.5 million federal employees.[45] Therefore, the current cybersecurity statutory framework is far from foolproof and may fail to function in certain situations.[46]

B. Congress's Legislative Power and the National Defense Authorization Acts

Congress, too, has a role to play in protecting federal agencies from cybersecurity threats. Congress, of course, always retains the power to legislate and may therefore pass a law, such as a National Defense Authorization Act (NDAA), banning certain international contractors.[47] Congress typically passes an NDAA each fiscal year, pursuant to its constitutional mandate to provide for the common defense and its constitutional power of the purse.[48] An NDAA "is a law that authorizes appropriations and sets policies for Department of Defense programs and activities."[49] NDAAs not only authorize "the policies under which funding will be set by the appropriations committees," but, in the Trump years, have also acted as "a [c]ongressional expression of concern . . . on the president's policies toward Russia, China and the Koreas."[50]

---

[44] *Id.* (alteration in original).
[45] *See* Vail, *supra* note 32, at 221.
[46] *See id.* at 222-23 (arguing that existing information security laws are a "hodgepodge" and focus too much on "responding to cyber attacks rather than preventing them").
[47] *See* U.S. CONST. art. I, § 1.
[48] *See* U.S. CONST. pmbl.; U.S. CONST. art. I, § 9, cl. 7 (the Appropriations Clause); *see also* JIM INHOFE & JACK REED, FY 2020 NATIONAL DEFENSE AUTHORIZATION ACT: EXECUTIVE SUMMARY 2 (2019).
[49] Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 311 F. Supp. 3d 187, 202 (D.D.C. 2018).
[50] Nick Schifrin, *What's in the Defense Authorization Act?*, PBS NEWS HOUR (Aug. 13, 2018) (alteration in original) https://www.pbs.org/newshour/nation/whats-in-the-defense-authorization-act https://perma.cc/JZY9-5AD9].

Together, FISMA and the Congress's legislative power provide a foundation for a contracting ban on an international company.[51]

III. Background: The Three Companies

This Note now turns to *how* the U.S. Government has exercised its authority to ban companies posing cybersecurity threats from contracting with the federal government. The Note focuses on three foreign contractors: ZTE, Huawei, and Kaspersky. Part III will provide a basic background on the series of political and economic events that led to these companies' eventual contracting bans.[52]

A. Zhongxing Telecommunications Equipment Corporation

Zhongxing Telecommunications Equipment Corporation (ZTE) is a telecommunications company based in Shenzhen, China.[53] It is one of two major Chinese companies currently banned from contracting with any U.S. federal agencies.[54] While best known for selling inexpensive smartphones in developing markets,[55] the company has also made a name for itself in the production of cloud-computing products and 5G network technology.[56] 5G networks are expected to be immensely important for the development of "smart devices such as self-driving

---

[51] *See supra* Part II(A)-(B).
[52] This Note contains updated information through October 15, 2019. Please be aware that the events involving these companies are constantly evolving, and thus new information may be available after this Note's publication.
[53] *See U.S. Suspends Export Control Deal with China's ZTE*, XINHUA (Apr. 17, 2018), http://www.xinhuanet.com/english/2018-04/17/c_137116923.htm [https://perma.cc/32CP-SVPF].
[54] *See* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(a), (f)(3)(A), 132 Stat. 1636, 1917-18 (2018).
[55] *See* Mozur & Granville, *supra* note 2.
[56] *See* Rachel Layne, *3 Things to Know About ZTE and Huawei*, CBS NEWS (June 7, 2018), https://www.cbsnews.com/news/3-things-to-know-about-zte-and-huawei/ [https://perma.cc/4XLP-RVKG].

cars, home appliances, . . . automated and semi-automated manufacturing, . . . and utilities, like water and sewage systems" and are already a major point of competition between U.S. and Chinese tech companies.[57] ZTE's smartphones are also sold by American telecom heavyweights such as AT&T, Verizon, and T-Mobile.[58]

While ZTE has long been on the radar of U.S. companies because of patent infringement accusations,[59] U.S. national security concerns over ZTE began when federal agents discovered that it had sold almost "$40 million worth of U.S.-origin goods" to Iran and North Korea, "in knowing violation of" U.S. sanctions laws.[60] The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 imposes a ban on U.S. Government procurement for any person that exports sensitive technology, such as telecommunications equipment, to Iran.[61] The United States enforces a similar sanction regime on North Korea, which includes an import and export ban to or from North Korea on (among other items) technology, in part to hamper North Korea's development of nuclear weapons.[62] The danger of ZTE's sanctions violations is that "[t]ech supply chains are so intertwined these days that just about every product that ZTE makes has some American components or software in it . . . [s]o if ZTE sells a smartphone to

---

[57] *Id.*
[58] *See id.*
[59] *See* David Kline, *What President Trump Doesn't Know About ZTE*, TECHCRUNCH (May 26, 2019), https://techcrunch.com/2018/05/26/what-president-trump-doesnt-know-about-zte/ [https://perma.cc/P783-7LLH] (stating that ZTE has been sued for patent infringement 126 times in the past five years).
[60] *See* William F. McGovern et al., *Chinese Companies with U.S. Ambitions Give Rise to New Enforcement Priorities*, 31 WESTLAW J. GOV'T CONT. 3, 3-4 (2017).
[61] U.S. GOV'T ACCOUNTABILITY OFF., GAO-11-706R, THE U.S. GOVERNMENT IS ESTABLISHING PROCEDURES FOR A PROCUREMENT BAN AGAINST FIRMS THAT SELL IRAN TECHNOLOGY TO DISRUPT COMMUNICATIONS BUT HAS NOT IDENTIFIED ANY FIRMS 3 (2011).
[62] *See* Eleanor Albert, *What to Know About Sanctions on North Korea*, COUNCIL ON FOREIGN REL. (July 16, 2019), https://www.cfr.org/backgrounder/what-know-about-sanctions-north-korea [https://perma.cc/BM89-7T6E].

North Korea [or Iran], it might also be selling a [United States brand] Qualcomm chip inside that phone."[63] ZTE's illegal export plot was accomplished by utilizing third-party "isolation companies" to feed the products through China before their sale to Iran and North Korea and by employing a "team of internal information technology employees who deleted references to Iran in the company's internal database."[64] ZTE senior managers also misled counsel from 2014 through 2016 about the company's involvement in the scheme, which caused "counsel to unknowingly give false information to investigators."[65]

In March 2016, following investigations by agents from the DHS, the Department of Justice (DoJ), the Office of Foreign Assets Control, the Treasury Department, the Federal Bureau of Investigation (FBI), and the Commerce Department, the Commerce Department placed ZTE on the Entity List.[66] The Entity List designates companies that pose national security or foreign policy threats to the United States and imposes strict licensing requirements on those companies; placement on the Entity List essentially meant that ZTE could not buy U.S.-made technology that is critical to its business.[67] On March 7, 2017, ZTE reached a settlement agreement with the Commerce Department in relation to its sanctions violations.[68] It agreed to pay an $892 million fine (which had the potential to expand to $1.19 billion if ZTE violated the settlement terms).[69] ZTE also agreed to abide by audit and compliance requirements.[70]

---

[63] Mozur & Granville, *supra* note 2 (alteration in original).
[64] *See* McGovern et al., *supra* note 60, at 3-4.
[65] *Id.* at 4.
[66] *See* Additions to the Entity List, 81 Fed. Reg. 12,004 (Mar. 8, 2016) (to be codified at 15 C.F.R. pt. 744); *see also* McGovern et al., *supra* note 60, at 4.
[67] *See* Additions to the Entity List, 81 Fed. Reg. at 12,004; *see also* McGovern et al., *supra* note 60, at 4.
[68] *See* McGovern et al., *supra* note 60, at 3.
[69] *Id.*
[70] Press Release, U.S. Commerce Dep't, Sec'y of Commerce Wilbur L. Ross, Jr. Announces $1.19 Billion Penalty for Chinese Co.'s Export Violations to Iran and N. Korea (Mar. 7, 2017)

In April 2018, U.S. officials took further action after discovering that ZTE had failed to comply with the terms of the original settlement agreement.[71] Officials implemented additional penalties, which were two-fold—additional monetary fines were coupled with a ban on ZTE importing United States-origin goods for at least seven years.[72] The import ban "threatened to cripple ZTE's global telecommunications business" and deprived ZTE of necessary U.S.-brand components used to manufacture its mobile phones, such as a chip produced by San Diego's QualComm.[73] ZTE's manufacturing plants even temporarily suspended all major operations in May of that year.[74]

Around this time, concerns about ZTE as a serious national security threat began to gain traction.[75] At an April 2018 hearing at which the Federal Communications Commission (FCC) voted "in favor of banning federal funds from being spent with companies determined to be a risk to U.S. national security," FCC Chairman Ajit Pai stated:

> For years, U.S. [G]overnment officials have expressed concern about the national security threats posed by certain foreign communications equipment providers in the communications supply chain . . . Hidden "backdoors" to our networks in routers, switches, and other network equipment can allow hostile foreign powers to

(on file at https://www.commerce.gov/news/press-releases/2017/03/secretary-commerce-wilbur-l-ross-jr-announces-119-billion-penalty [https://perma.cc/NZ4S-TJMP]).

[71] *See* Press Release, U.S. Commerce Dep't, Sec'y Ross Announces $1.4 Billion ZTE Settlement; ZTE Bd., Mgmt. Changes and Strictest BIS Compliance Requirements Ever (June 7, 2018) (on file at https://www.commerce.gov/news/press-releases/2018/06/secretary-ross-announces-14-billion-zte-settlement-zte-board-management [https://perma.cc/Q5GJ-UAN6]).

[72] *See id.* (detailing the new monetary penalties); *see also* Ana Swanson & Kenneth P. Vogel, *Faced with Crippling Sanctions, ZTE Loaded Up on Lobbyists*, N.Y. TIMES (Aug. 1, 2018), https://www.nytimes.com/2018/08/01/us/politics/zte-sanctions-lobbying.html [https://perma.cc/6HNV-XTNK] (discussing the seven-year ban).

[73] Swanson & Vogel, *supra* note 72.

[74] *See China's ZTE Ceases Major Operations After U.S. Trade Ban*, BLOOMBERG NEWS (May 9, 2018), https://www.bloomberg.com/news/articles/2018-05-10/china-s-zte-ceases-major-operations-after-u-s-trade-ban [https://perma.cc/QT35-2NMZ].

[75] *See* Todd Shields, *Huawei and ZTE Targeted While Security Ban Advances at U.S. FCC*, BLOOMBERG TECH. (Apr. 17, 2018), https://www.bloomberg.com/news/articles/2018-04-17/huawei-zte-targeted-as-security-ban-advances-at-u-s-fcc [https://perma.cc/77HN-LTGN].

> inject viruses and other malware, steal Americans' private data, [and] spy on U.S. businesses.[76]

Despite the devastating nature of the second round of sanctions, the ZTE ordeal was far from over. Throughout May and June 2018, as steam picked up in Congress and among defense officials to institute a permanent ban on ZTE purchasing American products, President Trump appeared to temporarily mend his tumultuous relationship with President Xi Jinping.[77] After a personal plea from Xi, Trump announced that he would rescind the penalties on ZTE, effectively saving the telecom giant from closing.[78] He confirmed this change in policy via the popular platform, Twitter: "President Xi of China, and I, are working together to give massive Chinese phone company, ZTE, a way to get back into business, fast. Too many jobs in China lost. Commerce Department has been instructed to get it done!"[79] The decision induced bipartisan backlash.[80]

The ZTE saga culminated in August 2018, when Congress passed the 2019 John S. McCain National Defense Authorization Act (2019 NDAA).[81] Section 889 of the bill included a provision banning ZTE from contracting with the U.S. Government.[82] However, the final bill's language removed some of the harsher sanction language that was apparently present in earlier

---

[76] *Id.* (alteration ins original).
[77] *See* Ana Swanson, *Trump Strikes Deal to Save China's ZTE as North Korea Meeting Looms*, N.Y. TIMES (June 7, 2018), https://www.nytimes.com/2018/06/07/business/us-china-zte-deal.html [https://perma.cc/X775-EGPF].
[78] *See id.*
[79] Donald J. Trump (@realDonaldTrump), TWITTER (May 13, 2018, 8:01 AM), https://twitter.com/realdonaldtrump/status/995680316458262533?lang=en [https://perma.cc/ZAD6-7EPF].
[80] *See* Swanson & Vogel, *supra* note 72.
[81] *See* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018).
[82] *See id.* § 889(a), (f)(3)(A).

drafts.[83] This was allegedly due to an aggressive lobbying campaign helmed by the law firm Hogan Lovells.[84] Since the ban, ZTE has kept a relatively low profile in the United States; it has instead focused on its global and China-based market and remains a viable player in emerging 5G technology.[85]

B. Huawei Technologies Co. Ltd.

Huawei Technologies Co. Ltd. (Huawei), also headquartered in Shenzhen, China, is China's largest telecommunications manufacturer and the world's second-largest manufacturer of smartphones, with over $90 billion in revenue in 2017 alone.[86] It is one of two major Chinese companies currently banned from entering into contracts with any U.S. federal agency.[87]

Suspicion surrounding the telecom giant dates back to 2012, when the House Intelligence Committee issued a report that concluded that both ZTE and Huawei were national security threats because of a sketchy record of respecting U.S. intellectual property laws and their ability

---

[83] *See* Swanson & Vogel, *supra* note 72.
[84] *See id.*
[85] *See* Juan Pedro Tomás, *ZTE Reaches 25 5G Contracts, Ships Over 50,000 Base Stations: Executive*, RCR WIRELESS NEWS (June 26, 2019), https://www.rcrwireless.com/20190626/5g/zte-reaches-25-5g-contracts-ships-over-50000-base-stations-executive https://perma.cc/MB5L-4S5A].
[86] *See* Frank Chen, *Inside Huawei's Huge HQ Campus in Shenzhen*, ASIA TIMES (June 28, 2019), https://www.asiatimes.com/2019/06/article/inside-huaweis-huge-hq-campus-in-shenzhen/ [https://perma.cc/NB6F-RHKT]; Samuel Gibbs, *Huawei Beats Apple to Become Second-Largest Smartphone Maker*, GUARDIAN (Aug. 1, 2018), https://www.theguardian.com/technology/2018/aug/01/huawei-beats-apple-smartphone-manufacturer-samsung-iphone [https://perma.cc/DB4X-FT2J]; Daisuke Wakabayashi & Alan Rappeport, *Huawei C.F.O. Is Arrested in Canada for Extradition to the U.S.*, N.Y. TIMES (Dec. 5, 2018), https://www.nytimes.com/2018/12/05/business/huawei-cfo-arrest-canada-extradition.html[https://perma.cc/4HZ7-XDZL].
[87] *See* John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 889(a), (f)(3)(A), 132 Stat. at 1917-18.

to tamper with U.S. telecom through "malicious hardware or software implants."[88] The Committee also warned of the corporations' loyalty to the Chinese government and pointed out that both receive subsidies from Beijing.[89] Notably, despite its harsh criticism of the companies, the Committee did not go so far as to call for a boycott of their products.[90]

Six years later, however, national security leaders changed their tune. During a Senate Intelligence Committee hearing in February 2018, FBI Director Christopher Wray voiced concerns that the Chinese government could easily harness Huawei to collect intelligence on the United States.[91] When asked whether he would recommend that U.S. citizens use Huawei or ZTE products or services, Director Wray—among other heads of federal agencies present at the hearing, including Mike Pompeo, then of the Central Intelligence Agency (CIA) and Michael Rogers of the National Security Agency (NSA)—indicated he would not.[92] Shortly thereafter, news emerged that the DoJ was investigating Huawei for allegedly selling U.S.-origin equipment to Iran and other countries, in violation of sanctions laws.[93] In August 2018, Congress passed the 2019 NDAA.[94] Section 889 of the 2019 NDAA codified the Huawei ban.[95] Huawei has

[88] *See* MIKE ROGERS & DUTCH RUPPERSBERGER, INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE 3, 31, 42, 44 (2012).
[89] *See id.* at 21, 37.
[90] *See generally id.* (lacking mention of a boycott in the recommendations section of the report).
[91] *See Open Hearing on Worldwide Threats: Hearing Before the S. Comm. on Intelligence*, 115th Cong. 64-65 (2018) (statement of Christopher Wray, Dir., Fed. Bureau of Investigation).
[92] *See id.* at 65.
[93] *See* Karen Freifeld & Eric Auchard, *U.S. Probing Huawei for Possible Iran Sanctions Violations: Sources*, REUTERS (Apr. 25, 2018), https://www.reuters.com/article/us-usa-huawei-doj/u-s-probing-huawei-for-possible-iran-sanctions-violations-sources-idUSKBN1HW1YG [https://perma.cc/U73U-T8QM].
[94] *See generally* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018).
[95] *Id.* § 889(a), (f)(3)(A).

since filed suit against the U.S. Government, asking a Texas district court to find the 2019 NDAA unconstitutional.[96]

The turmoil between Huawei and U.S. authorities raged on into early December 2018, when the company's Chief Financial Officer (and daughter of the founder), Meng Wanzhou, was arrested in Canada.[97] The arrest was carried out at the request of U.S. officials.[98] U.S. officials also requested her extradition, though at the time, no reason for the request was provided to the public.[99] The arrest took place on the same day that President Trump and President Xi agreed to a ninety-day cease-fire in the ongoing trade war, which had been a positive sign of ameliorating tensions between the United States and China.[100] As of late September 2019, Meng remains on house arrest in Vancouver, pending further extradition hearings in Canadian court.[101]

Chinese retaliation against Canada was swift and unyielding.[102] In an arguably purely political move, a Chinese court re-tried and re-sentenced a Canadian man to death for a drug trafficking conviction—the original sentence, decided prior to Meng's arrest, was fifteen years in prison.[103] In a separate incident, China detained two Canadians on charges of endangering

---

[96] *See generally* Huawei Techs. USA, Inc. v. United States, No. 4:19-cv-00159-ALM (E.D. Tex. filed Mar. 6, 2019). The author is not aware of any further developments in the case.
[97] *See* Wakabayashi & Rappeport, *supra* note 86.
[98] *Id.*
[99] *See id.*
[100] *See id.*
[101] *See* Jason Proctor, *Meng Wanzhou Back in the Spotlight as Lawyers Set to Argue for Disputed Arrest Documents*, CBC NEWS (Sept. 22, 2019), https://www.cbc.ca/news/canada/british-columbia/meng-wanzhou-september-hearing-1.5289143 [https://perma.cc/EDH8-9SEK].
[102] *Cf.* Gerry Shih, *Canadian Convicted on Drug Charges in China Will Appeal Death Sentence*, WASH. POST (Jan. 15, 2019), https://www.washingtonpost.com/world/asia_pacific/canadian-convicted-on-drug-charges-in-china-will-appeal-death-sentence/2019/01/15/c196ecbe-18b7-11e9-a804-c35766b9f234_story.html?utm_term=.e1a94926ca73 [https://perma.cc/7ZXT-F8FD] (detailing an example of an allegedly retaliatory measure by Beijing against Canada in the wake of the Meng arrest).
[103] *Id.*

national security.[104] In a show of how the arrest also created a strain between Canada and the United States, Canada's ambassador to China claimed that it would be "great" if the United States rescinded Meng's extradition request.[105] Canadian Prime Minister Justin Trudeau promptly fired the ambassador.[106]

On January 28, 2019, the DoJ unsealed a thirteen-count indictment against Huawei, its affiliates, and Meng.[107] The charges "outlin[ed] a decade-long attempt by the company to steal trade secrets, obstruct a criminal investigation and evade economic sanctions on Iran"[108] and included charges of bank fraud, wire fraud, violations of the International Emergency Economic Powers Act, conspiracy to commit money laundering, and conspiracy to obstruct justice.[109] These criminal charges, coupled with FBI Director Wray's statement during the unveiling of the charges—that Huawei is both an economic threat and a national security threat[110]—certainly didn't help mend the strain between the United States and China. Beijing's Foreign Ministry responded by calling the charges an "unreasonable suppression of Chinese companies."[111] It

---

[104] *Id.*
[105] *See McCallum Says It Would Be "Great for Canada" If Meng Not Extradited: Report*, GLOBAL NEWS CAN. (Jan. 25, 2019), https://globalnews.ca/news/4891212/john-mccallum-meng-wanzhou-huawei-extradition/ [https://perma.cc/4QNM-SC4U].
[106] *See Trudeau Fires Canada's Ambassador to China Amid Huawei Controversy*, BBC NEWS (Jan. 27, 2019), https://www.bbc.com/news/world-us-canada-47015700 [https://perma.cc/5LHH-JPD9].
[107] *See* Press Release, U.S. Dep't of Justice Off. of Pub. Affairs, Chinese Telecomm. Conglomerate Huawei & Huawei CFO Wanzhou Meng Charged with Fin. Fraud (Jan. 28, 2019) (on file at https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial [https://perma.cc/YG57-YR7W]) [hereinafter Huawei Indictment Press Release].
[108] David E. Sanger et al., *Huawei and Top Executive Face Criminal Charges in the U.S.*, N.Y. TIMES (Jan. 28, 2019) (alteration in original), https://www.nytimes.com/2019/01/28/us/politics/meng-wanzhou-huawei-iran.html [https://perma.cc/D4U8-2A47].
[109] Huawei Indictment Press Release, *supra* note 107.
[110] *See id.*
[111] Sanger et al., *supra* note 108.

remains to be seen whether the DoJ will *actually* pursue the charges: then-Acting Attorney General Matthew Whitaker declined to say "whether the White House would interfere in the criminal case against" Meng.[112] President Trump, however, said that he would consider "using her case for leverage in . . . trade negotiations, which fueled speculation that the United States may be more interested in . . . Meng's value in winning trade concessions than in obtaining a conviction."[113] Secretary of State Mike Pompeo later contradicted the president by implying that Meng would not be used as a "bargaining chip" in the ongoing trade war.[114]

Overlapping with the ongoing Meng controversy, in mid-May 2019, President Trump issued an executive order effectively banning Huawei from being involved with U.S. carrier networks—a huge blow to the Chinese telecom giant.[115] That same month, the "Commerce Department put Huawei on a trade blacklist [called the Entity List] that [for all intents and purposes] bans [U.S.] companies from doing business with the Chinese firm," unless the U.S

[112] *Id.*
[113] *Id.* (alteration in original).
[114] *See Huawei's Meng Wanzhou Not a Bargaining Chip, Says Pompeo*, BBC NEWS (Aug. 22, 2019), https://www.bbc.com/news/world-us-canada-49365079 [https://perma.cc/4CJK-TSKG].
[115] *See* Exec. Order No. 13,873, 84 Fed. Reg. 22,689 (May 17, 2019); Corinne Reichert & Sean Keane, *Huawei Says Trump's Ban Will Hurt US 5G Deployment*, CNET (May 16, 2019) (stating that Huawei effectively will be banned by Executive Order No. 13,873), https://www.cnet.com/news/trump-effectively-bans-huawei-with-national-security-order/ [https://perma.cc/3YNZ-6TE4].

company has a special license.[116] In response, Huawei ordered employees to cancel meetings with U.S. contacts and sent away some U.S. citizens working at its Shenzhen headquarters.[117]

These restrictions were far from absolute, however: almost immediately, the Commerce Department temporarily "scaled back its restrictions on Huawei's access to American components and software that go into its devices."[118] Creating even more confusion for both American companies and Huawei itself, the Commerce Department extended its original grace period (which allowed companies with special licenses to do business with Huawei even after the announcement of the blacklist) for another ninety days, meaning the grace period now would not end until mid-November 2019.[119] While the future of foreign relations with China remains volatile and unclear, it appears likely the fate of Huawei will play an important part in that relationship for years to come.

---

[116] Sijia Jiang, *Huawei Challenges U.S. Defense Bill as Sanctions Fight Ramps Up*, REUTERS (May 28, 2019) (alteration in original), https://www.reuters.com/article/us-huawei-tech-usa-filing/huawei-challenges-u-s-defense-bill-as-sanctions-fight-ramps-up-idUSKCN1SZ08C [https://perma.cc/Z2ZB-3W59]; *see also* Press Release, U.S. Commerce Dep't, Dep't of Commerce Announces the Addition of Huawei Techs. Co. Ltd. to the Entity List (May 15, 2019) (on file at https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd [https://perma.cc/9GA4-XEGF]).

[117] Sean Keane, *Huawei Reportedly Orders Employees to Cancel US Meetings*, CNET (May 31, 2019), https://www.cnet.com/news/huawei-reportedly-orders-employees-to-cancel-us-meetings/ [https://perma.cc/9QKD-NXAJ].

[118] Abrar Al-Heeti & Sean Keane, *Huawei Gets Slight Reprieve on US Trade Ban*, CNET (May 21, 2019), https://www.cnet.com/news/huawei-already-seeing-a-reprieve-on-us-trade-ban-report-says/ [https://perma.cc/WZU9-5KJK].

[119] *See* Press Release, U.S. Commerce Dep't, Dep't of Commerce Adds Dozens of New Huawei Affiliates to the Entity List & Maintains Narrow Exemptions through the Temporary Gen. License (Aug. 19, 2019) (on file at https://www.commerce.gov/news/press-releases/2019/08/department-commerce-adds-dozens-new-huawei-affiliates-entity-list-and [https://perma.cc/UG8A-UQY8]).

C. Kaspersky Lab

Kaspersky Lab (Kaspersky) is a Russian cybersecurity firm that sells antivirus and cybersecurity software.[120] It is currently banned from contracting with all federal agencies.[121] Before the ban, about fifteen percent of federal agencies had Kaspersky software in their computer systems.[122] In most cases, the agencies did not directly purchase Kaspersky software; rather, the products were "obtained . . . as part of a larger package of digital protection services."[123]

In recent years, particularly since the 2016 election, concerns have grown that the Russian government may be using Kaspersky products to collect information from the U.S. Government.[124] While no specific non-classified evidence of interference has been revealed to the U.S. public, the concern generally centers around founder and CEO Eugene Kaspersky's ties to the Kremlin.[125] Before founding Kaspersky, he was a graduate of the KGB's cryptology institute and "a software engineer for Soviet military intelligence."[126] Another concern is that, under Russian law, the company is required to assist the Federal Security Service (FSB) in its operations; that is, telecommunications service providers are required to install software or

---

[120] *See* Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 311 F. Supp. 3d 187, 193 (D.D.C. 2018); *see also About Us*, KASPERSKY, https://usa.kaspersky.com/about [https://perma.cc/T2AM-HMK7] (last visited Nov. 18, 2018).
[121] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1634(a), 121 Stat. 1283, 1739-40 (2017).
[122] Joseph Marks, *Kaspersky Software Found at 15% of Federal Agencies*, NEXTGOV (Nov. 14, 2017), https://www.nextgov.com/cybersecurity/2017/11/kaspersky-software-found-15-federal-agencies/142533/[https://perma.cc/5TFH-7KX6].
[123] *Id.* (alteration in original).
[124] *See* Jeanne Shaheen, *The Russian Company That Is a Danger to Our Security*, N.Y. TIMES (Sept. 4, 2017), https://www.nytimes.com/2017/09/04/opinion/kapersky-russia-cybersecurity.html [https://perma.cc/U9WH-ZACM] (an op-ed by Democratic Senator Jeanne Shaheen).
[125] *See id.*
[126] *Id.*

hardware "needed by the FSB to engage in 'operational/technical measures,'" and the FSB has the power to intercept all Russian telecommunications.[127] Kaspersky, of course, denies the accusations that it is a national security threat—and in its defense, it *has*, in the past, demonstrated good faith efforts to protect U.S. security: in 2016, for example, it reported to the NSA that it received messages from a former NSA contractor asking to speak to Eugene Kaspersky.[128] That contractor was later arrested and charged with stealing fifty terabytes of data from the NSA "that included highly sensitive hacking tools."[129]

Despite this, U.S. officials remain skeptical of Kaspersky; in September 2017, the DHS issued BOD 17-01, which directed executive departments and agencies to identify Kaspersky products in their information systems and to develop a plan to remove and discontinue use of those products.[130] The agencies were given ninety days to implement the plans.[131] Kaspersky had a chance to respond to the accusations before the DHS made a final decision on whether to officially implement the BOD.[132] On the same day that the BOD was issued, then-DHS Secretary Elaine Duke sent a letter to Eugene Kaspersky informing him of the BOD and providing him "an opportunity to provide [DHS] with any information that [he thought was] relevant to [DHS's] ongoing deliberations concerning [Kaspersky] products and services."[133]

---

[127] Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 311 F. Supp. 3d 187, 199 (D.D.C. 2018).
[128] *See* Ellen Nakashima, *Russian Firm That Was Barred from U.S. Networks as a Spy Threat Helped NSA Nab Suspect in Massive Breach*, WASH. POST (Jan. 9, 2019), https://www.washingtonpost.com/world/national-security/russian-firm-barred-from-us-networks-as-a-spy-threat-helped-the-nsa-nab-suspect-in-massive-breach/2019/01/09/4cbae45e-141b-11e9-b6ad-9cfd62dbb0a8_story.html [https://perma.cc/Y6BG-YSEK].
[129] *Id.*
[130] *See BOD 17-01*, *supra* note 8.
[131] *See id.*
[132] *Kaspersky*, 311 F. Supp. 3d at 200.
[133] *Id.* (alteration in original).

The letter also informed Mr. Kaspersky that he could "initiate a review by DHS by providing the [d]epartment with a written response to the BOD and supporting evidence."[134] Kaspersky was given forty-five days to respond.[135] Despite Eugene Kaspersky's response, and his efforts to convince DHS officials that the company's products were safe, Acting Secretary Duke issued a final decision confirming BOD 17-01.[136] On December 12, 2017, Congress enacted the National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA).[137] Section 1634 prohibited all federal agencies, departments, and organizations from using Kaspersky products.[138] The 2018 NDAA "effectively superseded" the BOD.[139]

Over the course of 2018, Kaspersky Lab, Inc. (Kaspersky's American entity) and Kaspersky Lab, Ltd. (Kaspersky's U.K.-based holding company) filed two lawsuits against the United States, alleging, in relevant part to this discussion, (1) that the 2018 NDAA was a bill of attainder[140] and (2) that BOD 17-01 violated the Due Process Clause of the Fifth Amendment.[141] The District Court for the District of Columbia found that the 2018 NDAA was *not* a bill of attainder because while punishment was indeed inflicted specifically on Kaspersky, the company is not "a flesh and blood individual" and thus cannot be the target of such a bill.[142] Moreover,

---

[134] *Id.* (alteration in original).
[135] *Id.*
[136] *See id.* at 201.
[137] *See generally* National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283 (2017).
[138] *Id.* § 1634(a).
[139] *Kaspersky*, 311 F. Supp. 3d at 202 (implying that an act of Congress would necessarily overrule a mere directive from an executive agency).
[140] A bill of attainder is an action "of legislatures . . . that single out a specific individual (or entity), declare that person or entity to be guilty, and impose punishment – all without a court trial." Lyle Denniston, *Rediscovering the Ancient "Bill of Attainder,"* CONST. DAILY (May 24, 2019), https://constitutioncenter.org/blog/rediscovering-the-ancient-bill-of-attainder [https://perma.cc/VE2W-SY7J]. Bills of attainder are unconstitutional. *See id.*
[141] *See Kaspersky*, 311 F. Supp. 3d at 193, 195.
[142] *Id.* at 207-08, 223.

the court held that only a fraction of Kaspersky's U.S. sales were to the federal government, so the harm was not sufficiently severe to amount to a bill of attainder.[143] The court also stated that Congress is well within its rights to pass a "law of general applicability" when a perceived national security risk calls for "real-time need to take action."[144] It further noted: "[t]hese defensive actions may very well have adverse consequences for some third-parties. But that does not make them unconstitutional."[145] On the due process claim, the court held that Kaspersky lacked standing because there was no redressability—because the 2018 NDAA was already in effect, there was no evidence that Kaspersky's alleged injury would be cured if the BOD was repealed.[146]

In implementing the 2018 NDAA, in June 2018, the Department of Defense (DoD), NASA, and the General Services Administration (GSA) issued an interim rule imposing the ban on federal contractors and agencies.[147] The final rule (implemented without change) was published in the Federal Register in early September 2019.[148] With the ban extending to even the minute aspects of IT systems, such as payroll systems for federal contractors, the rule was a "clear message from the U.S. [G]overnment[:] . . . just get [Kaspersky] out of your systems."[149]

---

[143] *Id.* at 208-09.
[144] *Id.* at 213.
[145] *Id.* at 193 (alteration in original).
[146] *See id.* at 218-19, 223.
[147] *See* Use of Products and Services of Kaspersky Lab, 83 Fed. Reg. 28,141, 28,141 (June 15, 2018) (to be codified at 48 C.F.R. pts. 1, 4, 13, 39, & 52).
[148] *See* Use of Products and Services of Kaspersky Lab, 84 Fed. Reg. 47,861, 47,861 (Sept. 10, 2019) (to be codified at 48 C.F.R. pts. 1, 4, 13, 39, & 52); *see also* Aaron Boyd, *U.S. Finalizes Rule Banning Kaspersky Products from Government Contracts*, NEXTGOV (Sept. 9, 2019), https://www.nextgov.com/cybersecurity/2019/09/us-finalizes-rule-banning-kaspersky-products-government-contracts/159742/ [https://perma.cc/K97S-W3JU].
[149] Boyd, *supra* note 148 (quoting Alan Chvotkin, executive vice president and counsel at the Professional Services Council) (alteration in original).

IV. Analysis: The United States Should Implement a Standardized Method for Enacting Contracting Bans on Foreign Companies.

While the Kaspersky, Huawei, and ZTE bans were all carried out in different manners, they do share some core similarities. Part IV will identify these similarities and differences and analyze which aspects of the bans were successful and which were problematic.

A. The Commonalities Between the Bans: All Three Bans Were Codified in Appropriations Bills and Were Accompanied by Calls for Increased Cybersecurity.

First, all three contracting bans were finalized in appropriations bills: the 2018 NDAA (Kaspersky) and the 2019 NDAA (ZTE and Huawei).[150] The language of the 2018 NDAA stated that "[n]o department, agency, organization, or other element of the [f]ederal [g]overnment may use . . . any hardware, software, or services developed or provided, in whole or in part, by . . . Kaspersky Lab."[151] Likewise, the 2019 NDAA included language that singled out ZTE and Huawei, instituting a prohibition on heads of agencies from entering into contracts for the purchase of "covered telecommunications equipment or services" and a bar on entering into or extending or renewing a contract with a covered entity.[152] Those covered entities included Huawei and ZTE, among other smaller Chinese tech companies.[153] The prohibition applied as long as "a substantial or essential component" of the system contained a covered entity's equipment or service.[154]

---

[150] *See* National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1634(a), 131 Stat. 1283, 1739-40 (2017); John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(a), (f)(3)(A), 132 Stat. 1636, 1917-18 (2018).
[151] National Defense Authorization Act for Fiscal Year 2018 § 1634(a), 131 Stat. at 1739-40 (alteration in original).
[152] John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 889(a), (f)(3)(A), 132 Stat. at 1917-18.
[153] *Id.* § 889(f)(3)(A)-(B).
[154] *Id.* § 889(a)(A).

Second, the NDAAs called for heightened cybersecurity within the federal government.[155] The 2018 NDAA stressed the importance of cybersecurity efforts, particularly efforts related to the protection of U.S. election systems.[156] For example, the law called for the Secretary of Defense and the DHS Secretary to carry out "[c]yber [g]uard [e]xercise[s]" relating to election cybersecurity.[157] It also directed the DoD to set up a "[s]trategic [c]ybersecurity [p]rogram" to bolster U.S. "[o]ffensive cyber systems" and "[n]uclear deterrent systems."[158] Similarly, the 2019 NDAA included calls to reinforce cybersecurity and represented "a more aggressive posture on U.S. cybersecurity policy."[159] The statutory language also covered foreign cyber-attacks which "significantly disrupt the normal functioning of [U.S.] democratic society or government (including attacks against critical infrastructure that could damage systems used to provide key services to the public or government)."[160] In addition, the 2019 NDAA directed the Secretary of Defense to "create a list of countries that pose a risk to the cybersecurity" of the U.S. "national security systems and infrastructure."[161]

---

[155] *See* National Defense Authorization Act for Fiscal Year 2018 § 1638, 131 Stat. at 1744; John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 1636(a), 132 Stat. at 2126.
[156] *See* National Defense Authorization Act for Fiscal Year 2018 § 1638, 131 Stat. at 1744.
[157] *See id.* § 1638(a).
[158] *Id.* § 1640(a), (c) (alteration in original).
[159] *See* Meghan L. Brown et al., *Important Cyber Provisions Now Law Under the 2019 NDAA*, WILEY REIN LLP (Aug. 13, 2018), https://www.wileyrein.com/newsroom-articles-Important-Cyber-Provisions-Now-Law-Under-the-2019-NDAA.html [https://perma.cc/VX2S-G6FX]. This aggressive stance is demonstrated in the stated cyber warfare policy: "the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests . . . ." John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 1636(a), 132 Stat. at 2126.
[160] John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 1636(a)(2), 132 Stat. at 2126 (alteration in original).
[161] *Id.* § 1654(a).

B. The Differences Amongst the Bans: Not All Companies Were Provided an Opportunity to Defend Themselves, and Differences in Enactment Created Confusion and Hardship for All Parties Involved.

First—and most importantly—there is a difference in the foreign contractors' opportunity to "plead their case" with the federal government before the contracting bans were actually put into place.[162] After BOD 17-01 was announced, the DHS gave CEO Eugene Kaspersky an opportunity to respond to the agency's allegation that his company's products posed a cybersecurity threat.[163] He, accompanied by counsel, met with DHS officials in November 2017 and discussed the ban and its potential effects on Kaspersky's business, the company's corporate structure, and potential mitigation proposals.[164] It was only *after* Mr. Kaspersky had an opportunity to defend his products that the final BOD was officially enacted.[165]

In contrast, Chinese officers from ZTE and Huawei were not given the same opportunity to provide evidence of their companies' "innocence," for lack of a better term.[166] A tenuous argument *could* be made that ZTE actually did have an opportunity to rebut claims that it was a

---

[162] *Compare* Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 311 F. Supp. 3d 187, 200 (D.D.C. 2018) (describing Kaspersky's opportunity to provide DHS with information before BOD 17-01 was formally enacted) *with* Swanson, *supra* note 77 (describing an informal conversation between President Trump and President Xi regarding ZTE's sanctions, but lacking any discussion of a formal hearing of any sort) *and* Iris Deng, *Trump's Blacklisting of Huawei Is Unfair and Un-American, Microsoft President Says*, SOUTH CHINA MORNING POST (Sept. 9, 2019), https://www.scmp.com/tech/gear/article/3026376/trumps-blacklisting-huawei-unfair-and-un-american-microsoft-president [https://perma.cc/J4JM-Q84D] (discussing comments made by a Microsoft executive who believes that the Huawei ban was not grounded in logic, due process, or the rule of law because the basis of the ban is not clear, thereby implying that the company did not have a true opportunity to plead its case).

[163] *See Kaspersky*, 311 F. Supp. 3d at 200.

[164] *Id.* at 201.

[165] *See id.*

[166] *Cf.* Swanson, *supra* note 77 (detailing an informal phone call between President Xi and President Trump which led to the temporary lifting of sanctions regarding, but lacking any discussion of a formal hearing); Deng, *supra* note 162 (discussing comments by a Microsoft executive who believes that the Huawei ban lacked due process).

threat to national security when President Trump temporarily lifted the ban in June 2018 after a phone conversation with President Xi.[167] Regardless, this Note argues that no *truly formal* opportunity to be heard by DHS officials was granted to ZTE or Huawei. This fact may have influenced China's over-the-top reaction to the Huawei ban—China's foreign minister Wang Yi called the United States' punitive treatment of Huawei "not only unfair but also immoral."[168]

Second, one significant issue with the Kaspersky ban was that originally, it was not clear to government contractors or agencies if contractors were prohibited from using Kaspersky products and services.[169] The 2019 NDAA is clearer in that regard because it specifically states that contractors are restricted from purchasing and using Huawei and ZTE products.[170]

Third, the 2018 NDAA required agencies to remove any Kaspersky products or services from existing systems.[171] The 2019 NDAA did not contain such a requirement (though reports do indicate that agencies are working to remove Chinese tech from their systems).[172] From a cybersecurity perspective, "rooting out [these products] from federal computers and

---

[167] *Cf.* Swanson, *supra* note 77.
[168] *See* William Zheng, *Huawei's Treatment by Foreign Countries 'Unfair and Immoral', China's Foreign Minister Says*, SOUTH CHINA MORNING POST (Jan. 26, 2019), https://www.scmp.com/news/china/diplomacy/article/2183751/huaweis-treatment-foreign-countries-unfair-and-immoral-chinas [https://perma.cc/HYN5-56Z5]. Minister Wang also said that U.S. treatment of Huawei was rife with "obvious political tensions and manipulation." *Id.*
[169] *See* Johnson, *supra* note 11.
[170] *See* Jack Corrigan, *OMB Chief: Contractors Need More Time to Cut Ties with Huawei, ZTE*, NEXTGOV (June 10, 2019), https://www.nextgov.com/cybersecurity/2019/06/omb-chief-contractors-need-more-time-cut-ties-huawei-zte/157611/ [https://perma.cc/A2V5-W7TV].
[171] *See* National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1634(c)(A)-(B), 131 Stat. 1283, 1740-41 (2017).
[172] *See* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917-18 (2018); Thomas Brewster, *Exclusive: Kaspersky Software Lingers on Sensitive Government Systems 2 Years After U.S. Ban*, FORBES (Aug. 8, 2019), https://www.forbes.com/sites/thomasbrewster/2019/08/08/exclusive-kaspersky-software-lingers-on-sensitive-government-systems-2-years-after-us-ban/#4c0fbec4381c [https://perma.cc/V6VG-CSQY].

networks . . . [is] absolutely vital to national security."[173] Yet, despite the federal government's best intentions, the actual Kaspersky removal was a logistical nightmare: the effort to completely remove Kaspersky from federal agency systems has been largely ineffective.[174] Former DHS Secretary Kirstjen Nielsen admitted before the Senate Appropriations Committee's Homeland Security panel in May 2018 that the removal process was still incomplete because many federal contractors were unaware that the company's anti-virus software was even running on their products.[175] This problem likely stems from the fact that Kaspersky products were often not purchased directly from the company but rather bought in IT packages containing many brands.[176]

Lastly, while the Kaspersky ban was largely enacted by the 2018 NDAA, it was not carried out solely in that single appropriations bill.[177] In September 2017, well before the 2018 NDAA was signed into law, DHS issued BOD 17-01, which, as previously discussed, directed agencies to develop a plan to remove Kaspersky from their IT systems.[178] Besides the BOD, amendments to the FAR via the Federal Register were also a key component of the federal government's effort to implement the Kaspersky ban and to extend the ban to contractors, not just agencies.[179] In July 2018, the DoD, GSA, and NASA published an interim rule in the

---

[173] *Id.* (quoting U.S. Senator Jeanne Shaheen) (alteration in original).
[174] *See id.* (discussing the fact that two years post-ban, Kaspersky software remains even in sensitive military computer networks).
[175] Joseph Marks, *Kaspersky Is Off All Federal Networks but Remains on Contractor Systems*, NEXTGOV (May 8, 2018), https://www.nextgov.com/cybersecurity/2018/05/kaspersky-all-federal-networks-remains-contractor-systems/148056/ [https://perma.cc/SQ7V-EN4K].
[176] *See* Marks, *supra* note 122.
[177] *See supra* Part III(C) (detailing the Kaspersky ban, which included mechanisms such as BOD 17-01, the 2018 NDAA, and additions to the Federal Register).
[178] *See BOD 17-01*, *supra* note 8.
[179] *See* Boyd, *supra* note 148 (discussing the final rule published in the Federal Register banning Kaspersky from government and contractor systems).

Federal Register requiring contracts to include FAR Clause 52.204-23 ("Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab or Other Covered Entities").[180] The final rule was issued just over a year later.[181] In contrast, the Huawei and ZTE bans were conducted in one fell swoop: the 2019 NDAA.[182]

C. A New Method for the Future: The United States Should Implement a Standardized Procedure for Banning International Contractors.

Given the tumult caused by the Kaspersky, ZTE, and Huawei bans, along with the failures and uncertainties of the current cybersecurity statutory framework, a standardized method for implementing a contracting ban on foreign companies is long past due. And considering that these contracting bans often target companies that have ties to countries with which the United States has unstable foreign relations, this Note argues that a go-to standard is even *more* crucial.[183] A standardized procedure would hopefully ensure that these countries do not believe there are being singled out or treated differently because of external political or economic situations.

---

[180] *See* Use of Products and Services of Kaspersky Lab, 83 Fed. Reg. 28,141, 28,141 (June 15, 2018) (to be codified at 48 C.F.R. pts. 1, 4, 13, 39, & 52). *See also* FAR 52.204-23 (the official FAR clause).

[181] *See* Use of Products and Services of Kaspersky Lab, 84 Fed. Reg. 47,861, 47,861 (Sept. 10, 2019) (to be codified at 48 C.F.R. pts. 1, 4, 13, 39, & 52).

[182] *Cf.* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(a), (f)(3)(A), 132 Stat. 1636, 1917-18 (2018).

[183] *Cf.* Bob Davis et al., *Trump Allows U.S. Sales to Huawei as Trade Talks Resume*, WALL STREET J. (June 29, 2019), https://www.wsj.com/articles/trump-says-he-is-set-to-discuss-huawei-with-xi-11561769726 [https://perma.cc/3BCZ-9FJC] (describing the United States and China as having a "slowly deteriorating relationship" in the midst of the trade war and ongoing Huawei drama); *US-Russia Relationship*, AM. SECURITY PROJECT, https://www.americansecurityproject.org/us-russia-relationship/ [https://perma.cc/8TQF-H5BB] (last visited Sept. 30, 2019) (noting that U.S.-Russia relations have long been fraught with conflict).

This Note proposes that the standardized procedure draw from the successful parts of the Huawei, ZTE, and Kaspersky bans. It should also recognize the faults of those bans and seek to avoid them. The standardized banning procedure should have two key components: (1) an opportunity to be heard for the company; and (2) when, practicable, a single enactment mechanism.

The procedure should begin with a "pre-ban" process, which should follow the steps taken by the DHS prior to enactment of BOD 17-01 against Kaspersky.[184] Once a federal agency determines that a foreign contractor is a threat to U.S. national security, the head of that agency should notify the Secretary of Homeland Security, and a DHS official (Secretary or otherwise) should be charged with moving forward with the pre-ban mechanisms. Appointing a DHS employee as the officiator of the pre-ban process mirrors the responsibilities relegated to the DHS under FISMA (i.e., to ensure cybersecurity within federal agencies).[185] This mirroring of responsibilities would streamline and simplify the entire process because the DHS should already (theoretically, at least) be adept at understanding cybersecurity issues concerning federal agencies. The DHS should then immediately contact the foreign contractors' officers to provide notice and explanation of the *potential* of a ban. Next, the DHS should offer the company's officials an opportunity to provide evidence of "innocence" at an oral hearing. The company

---

[184] *See generally* Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 311 F. Supp. 3d 187, 200-01 (D.D.C. 2018) (noting that the CEO of Kaspersky had an opportunity to defend Kaspersky in front of DHS officials before a contracting ban was officially put in place).

[185] *See* Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 3553(b), 128 Stat. 3073, 3075 (2014) (stating that the DHS Secretary is tasked with implementing "information security policies" for government IT systems); *DHS Overview of FISMA*, *supra* note 32.

should be given roughly forty-five days—a reflection of the time afforded to Kaspersky to respond to the DHS BOD letter—to decide if it would like to participate in such a hearing.[186]

At this point, this Note assumes that the DHS will have compelling evidence that the company's products or practices are a cybersecurity risk; thus, the hearing need not be a full oral evidentiary hearing akin to a trial. Rather, the DHS could base the hearing on debarment procedures found in FAR 9.4. FAR 9.4 requires that before a contractor is debarred, the debarring agency affords the contractor "an opportunity to submit, in person, in writing, or through a representative, information and [an] argument in opposition to the proposed debarment."[187] Because the foreign contracting bans are quite similar to a debarment,[188] this Note argues that drawing on existing debarment procedures is a logical maneuver.

The "opportunity to be heard" is so crucial because it will provide a semblance of "rights" to the companies, just as, under the FAR, contractors are afforded a right to oppose their debarment.[189] Typically, a company may not be debarred from contracting with the U.S. Government *unless* and *until* the government provides it with (1) notice and (2) an opportunity to respond in some way to allegations that it is an unfit contractor or that it has committed errors in performance.[190] While this Note does not advocate that the government follow FAR debarment procedures "to a T," the procedures do provide a helpful guideline for the proposed pre-ban

[186] *See Kaspersky*, 311 F. Supp. 3d at 200.
[187] FAR 9.406-3(b)(1) (alteration in original).
[188] A "[d]ebarment removes a contractor from eligibility for future contracts with the government for a fixed period of time." KATE M. MANUEL, RL34754, DEBARMENT AND SUSPENSION OF GOVERNMENT CONTRACTORS: AN OVERVIEW OF THE LAW INCLUDING RECENTLY ENACTED AND PROPOSED AMENDMENTS 1 (Nov. 19, 2008) (alteration in original).
[189] *See* FAR 9.406-3(b).
[190] *See* TLT Constr. Corp. v. United States, 50 Fed. Cl. 212, 215 (2001).

process because they emphasize fairness. Finally, the goal of the hearing should be for the DHS to ensure that it has no reason to doubt that the company in question poses a cybersecurity risk.

If, in this opportunity, the company does not sufficiently assuage the DHS's national security concerns, the Secretary should notify Congress of its decision that the company should be indefinitely precluded from federal contracting. When coming to a final decision, the DHS should consult with the heads of agencies that would be affected by a ban. A collaborative decision would be in the spirit of FISMA's mandate that DHS consult with OMB, NIST, and the Commerce Department.[191] Ultimately, however, the authority to make a final call should rest with the DHS.

As for the ban itself, it should be enacted in a single law if at all possible. This Note recommends that Congress do so through the upcoming fiscal year's appropriations bill.[192] This is consistent with the Huawei method, where Congress included a clear contracting ban on Huawei, ZTE, and other Chinese companies in the 2019 NDAA.[193] This Note argues that the Huawei method is preferable to the Kaspersky method because the original Kaspersky banning mechanism (BOD 17-01) contributed to the uncertainty of the scope of the ban, i.e., whether, for example, contractors were also precluded from contracting with Kaspersky.[194] The Huawei method is also preferable to the ZTE method because, in the case of ZTE, President Trump took measures into his own hands and temporarily lifted the ZTE ban before the 2019 NDAA was

[191] *Cf.* Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 3553(b), (f)(1), 128 Stat. 3075, 3077 (2014).
[192] For example, the 2020 NDAA passed the House in July 2019. *See* H.R. 2500, 116th Cong. (2019). A future ban on an international company could be added to a similar bill.
[193] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(a), (f)(3)(A), 132 Stat. 1636, 1917-18 (2018).
[194] *See* Johnson, *supra* note 11.

actually codified.[195] This tinged the entire ZTE saga with political favoritism,[196] and, in this Note's view, made the eventual 2019 NDAA ban appear like a part of a larger political game. The ban should be indefinite in length until the DHS makes a finding that it is no longer necessary.

The language of a future ban within the NDAA should largely mirror the language of the Russian and Chinese bans.[197] It should preclude agencies and contractors from purchasing or possessing products in whole or in part manufactured by the foreign company in question, as the previously discussed bans do.[198] The language of the ban should also direct agencies to develop an action plan within a specified amount of time to remove existing products. Admittedly, that specified amount of time may not be sufficient to entirely rid federal agencies of a specific product, but it is important to set firm deadlines nonetheless. OMB, in conjunction with the DHS, should oversee the removal process because OMB already holds similar responsibilities under FISMA.[199]

The proposed method can be enacted under existing legislation. FISMA provides the DHS with fairly broad authority to protect federal agencies' cybersecurity.[200] Moreover, because the proposed method is largely a combination of the ZTE, Huawei, and Kaspersky bans, along

---

[195] *See* Swanson, *supra* note 77.
[196] *Cf. id.*
[197] *See generally* National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1634(a), 131 Stat. 1283, 1739-40 (2017); John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 889(a), (f)(3)(A), 132 Stat. at 1917-18.
[198] *See* National Defense Authorization Act for Fiscal Year 2018 § 1634(a), 131 Stat. at 1739-40; John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 889(a), (f)(3)(A), 132 Stat. at 1917-18.
[199] *See* Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 3553(a)-(b), 128 Stat. 3073, 3075 (2014) (granting OMB and DHS broad authority to implement and oversee agency cybersecurity policy).
[200] *See id.* § 3553(b).

with existing debarment procedures, it is well established that the federal government has the authority to carry out this Note's proposal. Nevertheless, it would be beneficial for both agencies and contractors for the DHS to promulgate a press release or memorandum when it adopts this new method that details the procedural steps.

D. Benefits of the Proposed Method

A standardized banning mechanism would be beneficial for a number of reasons. First, it would provide direction for U.S. contractors that provide IT services to federal agencies. As stated earlier in the Note, when the government first banned Kaspersky products, U.S.-based government contractors experienced confusion as to whether they were required to adhere to the ban or whether they were still free to purchase Kaspersky products.[201] The proposed method would provide essential clarity to U.S. contractors on when they can and cannot use products from banned companies in their maintenance of agencies' IT networks.

Second, a standardized banning method would be useful to the agencies themselves. The effort to completely remove Kaspersky products from agency IT systems can be fairly characterized as a disaster, given that many contractors were not even aware that their systems contained Kaspersky[202] and that evidence suggests Kaspersky software still lingers on both military and civilian agency systems.[203] The proposed method would help solve this issue by providing clear directions to agencies about banned products.

Lastly, the proposed method would help to make bans appear less politically retaliatory. This Note argues that lack of standardization among the ZTE, Kaspersky, and Huawei bans means that the bans appear specially "tailored" to a specific country, like Russia or China. China

[201] *See* Johnson, *supra* note 11.
[202] *See* Marks, *supra* note 175.
[203] *See* Brewster, *supra* note 172.

in particular has interpreted the Huawei ban as a personal affront.[204] While the proposed method wouldn't by itself *mend* strains in foreign relations between the United States and China and Russia, it would not *exacerbate* tensions further. Foreign relations considerations are especially important when the banned company has a substantial effect on its country's economy (e.g., Huawei is one of the largest companies in all of China) or when the company enjoys close ties to its government.[205]

It is important to map out the current challenges of United States-China relations in order to understand what consequences another haphazard contracting ban could have. ZTE and Huawei already have a history of patent infringement litigation against U.S. technology companies.[206] The trade war continues, despite a brief respite in late 2018.[207] U.S. tariffs on Chinese goods reached $250 billion in 2018, and Vice President Pence has indicated that he would have no problem counseling President Trump to double that amount in the future.[208]

United States-Russian relations are equally fraught. While President Putin and President Trump appear to be on good personal terms,[209] ongoing accusations by U.S. officials that the

---

[204] *See* Zheng, *supra* note 168 (discussing a Chinese official's comments that the treatment of Huawei is "not only unfair but also immoral").
[205] *See* Wakabayashi & Rappeport, *supra* note 86 (stating that Huawei is China's largest telecom company and generates substantial annual revenue).
[206] *See* Infogation Corp. v. ZTE Corp., No. 16-cv-01901-H-JLB, 2016 U.S. Dist. LEXIS 195203, at *2-3 (S.D. Cal. Dec. 21, 2016) (describing a case where a U.S. company sued both ZTE and Huawei for patent infringement of its mobile navigation system technology); Kline, *supra* note 59 (stating that ZTE has been sued in the United States for patent infringement a whopping 126 times in the past five years).
[207] *See* Wakabayashi & Rappeport, *supra* note 86 (reporting that in December 2018, President Trump and President Xi agreed to a 90-day pause in the trade war).
[208] *See* Josh Rogin, *Pence: It's Up to China to Avoid a Cold War*, WASH. POST (Nov. 13, 2018), https://www.washingtonpost.com/news/josh-rogin/wp/2018/11/13/pence-its-up-to-china-to-avoid-a-cold-war/?utm_term=.7ef9470a7ec6 [https://perma.cc/9S76-N79P].
[209] *Cf.* Robert E. Hamilton, *The Reset That Wasn't: The Permanent Crisis of U.S.-Russia Relations*, FOREIGN POL'Y RES. INST. (Dec. 14, 2018), https://www.fpri.org/article/2018/12/the-reset-that-wasnt-the-permanent-crisis-of-u-s-russia-relations/ [https://perma.cc/P5WR-HMKX].

Russian government meddled in the 2016 presidential elections have strained relations.[210] In one recent incident, among many others, Russian diplomats were expelled from the United States after Russian nationals conducted a nerve agent attack in the United Kingdom.[211]

When contracting bans are lifted by the U.S. president at the request of a foreign leader, or when contracting bans are enacted in multiple acts staggered over periods of time that may correspond with political turmoil between the United States and that company's country (with increasingly dire results for the company), this Note believes the bans appear more like reactions to certain political or economic events. A standardized method helps control that unwanted consequence.

E. Potential Issues with the Proposed Method

Admittedly, this Note's proposed method may not *completely* avoid the pitfalls of the previous Russian and Chinese bans. Given that these companies are very much tied to their respective governments,[212] a standardized method can never completely take away the political nature of such a ban. As an example, the Chinese central government backs Chinese companies like ZTE and Huawei and has directed state-controlled banks to provide financial assistance in times of loss.[213] Thus, any ban on a Huawei or a ZTE may necessarily be viewed by a leader like Xi Jinping as an attack on the government itself.

---

[210] *See* Mayer, *supra* note 3.
[211] *See* Hamilton, *supra* note 209.
[212] *See* Rogers & Ruppersberger, *supra* note 88, at 21, 37 (stating that Huawei and ZTE receive financial support from the central government); Shaheen, *supra* note 124 (noting that the CEO of Kaspersky previously worked for Russian intelligence).
[213] *See* Raymond Zhong, *China's ZTE, Saved by U.S., Has a Checkered Past and Shaky Future*, N.Y. TIMES (June 8, 2018), https://www.nytimes.com/2018/06/08/technology/zte-china-corruption.html [https://perma.cc/LU7R-YEJ9] (explaining Beijing's financial support of ZTE).

A second problem not initially addressed by the proposed method is what to do in the event of a national security crisis necessitating an immediate ban. Because appropriations bills are passed once each federal fiscal year, in some circumstances it could be upwards of several months before an appropriations bill could respond to an imminent national security crisis.[214] If, for example, a foreign cybersecurity or telecommunications company was found to be interfering in an election occurring in the very near future, it would not be sensible for the DHS to wait until the passage of the upcoming NDAA to enact a ban. In an absolute emergency like this, this Note recommends that the DHS be allowed to bypass the proposed method and enact a BOD, which empowers the DHS to take "swift action . . . to address constantly evolving cyber-threats."[215] The temporary BOD could then be superseded by a permanent ban in the following fiscal year's NDAA.

V. Conclusion

Political and economic conflict between the United States and Russia and China show little sign of resolution. The battle to be the leader of 5G technology is just ramping up,[216] which likely means relations between the United States and China will actually worsen. On the Russian side of things, President Trump's abrupt withdrawal of U.S. troops from Syria has given Russian troops an opportunity to advance, assist Bashar Al-Assad in re-gaining territory, and further cement its place "as a rising power broker in the Middle East" at the expense of the United

---

[214] *See A Brief Guide to the Federal Budget and Appropriations Process*, AM. COUNCIL ON EDUC., https://www.acenet.edu/news-room/Pages/A-Brief-Guide-to-the-Federal-Budget-and-Appropriations-Process.aspx [https://perma.cc/ZD4P-XXNA] (last visited Mar. 3, 2019).
[215] Kaspersky Lab, Inc. v. U.S. Dep't of Homeland Sec., 311 F. Supp. 3d 187, 197 (D.D.C. 2018) (alteration in original).
[216] *See* Susan Crawford, *China Will Likely Corner the 5G Market – And the US Has No Plan*, WIRED (Feb. 20, 2019), https://www.wired.com/story/china-will-likely-corner-5g-market-us-no-plan/ [https://perma.cc/C5B6-UD47].

States.[217] Because of these political realities, it is vitally important that the United States take every step possible, however small, to de-politicize bans involving international contractors with strong ties to their governments. The proposed standardized method will help to achieve de-politicization while ensuring U.S. national security interests are protected.

[217] Ben Hubbard et al., *In Syria, Russia Pleased to Fill an American Void*, N.Y. TIMES (Oct. 15, 2019), https://www.nytimes.com/2019/10/15/world/middleeast/kurds-syria-turkey.html [https://perma.cc/6ULX-PXYR].