Congressional Research Service
Informing the legislative debate since 1914

Huawei and U.S. Law

February 23, 2021

Congressional Research Service
https://crsreports.congress.gov
R46693

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46693

February 23, 2021

Stephen P. Mulligan
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Huawei and U.S. Law

Huawei Technologies Co., Ltd. (Huawei) has grown to be the world's largest telecommunications equipment manufacturer since its founding in 1987 by a former engineer in China's People's Liberation Army. The Shenzhen, China-based company has become the focus of a host of legal actions that seek to protect the United States' national security and economy. In 2012, the House Permanent Select Committee on Intelligence (HPSCI) released a report describing the potential counterintelligence and security threats posed by Huawei's access to U.S. telecommunications systems. Senior officials in the Trump Administration asserted that Huawei's products present an inherent security threat because the Chinese government can force Huawei to share confidential information or create "backdoors" by which the Chinese government could access Huawei systems. Huawei denies that its products create a security threat, and third-party analysts have not reached uniform conclusions about the security of Huawei systems.

Given the security debate, Congress and the executive branch have initiated a variety of legal efforts to limit Huawei's access to international supply chains, telecommunications systems, and markets. These legal actions have evolved from narrow restrictions on federal spending to an effort to remove Huawei equipment from domestic and international telecommunications networks.

After HPSCI's 2012 report, the United States enacted several laws that restrict federal procurement of, and grant and loan spending on, Huawei systems. In 2019 and 2020, Congress and the President expanded their efforts and imposed Huawei-related restrictions on a broad set of public- and private-sector transactions. In May 2019, the Trump Administration added Huawei and its affiliates to the Entity List, thereby limiting U.S. companies' ability to export products and services to Huawei. On the same day, President Trump issued Executive Order 13873, declaring a national emergency due to the threat of foreign adversaries exploiting vulnerabilities in U.S. information and communications technology and services (ICTS).

The Federal Communications Commission (FCC) has also taken steps to restrict Huawei's access to U.S. communications infrastructure. In November 2019, the FCC prohibited telecommunications carriers from using Universal Service Fund (USF) subsidies to purchase Huawei products and services. This restriction particularly affects rural telecommunications carriers, many of which depend on the Universal Service Fund and already use Huawei equipment in their networks. In addition, in March 2020, the United States passed the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act), which similarly prohibits companies from using FCC-administered subsidies like the USF for certain communications equipment and services from Huawei and other entities that pose a national security risk. The law also directs the FCC to set up a program to reimburse carriers for removing and replacing such equipment in their networks. Following the Secure Networks Act, the FCC issued an additional order establishing the reimbursement program contemplated by the law. The order goes beyond the Secure Networks Act by requiring carriers receiving USF support to remove and replace existing Huawei equipment in their networks, regardless of whether they choose to participate in the reimbursement program.

In other legal actions over the past two years, the United States has pursued criminal charges against Huawei and its Chief Financial Officer (CFO), issued visa restrictions for Huawei employees, and banned trade in Huawei securities. Most recently, the 116th Congress passed the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA) over President Trump's veto. The FY2021 NDAA embarks on a new endeavor of using federal programs to support private competitors to Huawei that can offer secure, alternative communications networks domestically and abroad.

Some observers view the suite of legal actions involving Huawei as part of a broader effort to "decouple" the United States' economy from problematic aspects of China's economy. Others see it as a microcosm of the increasing complexity of challenges caused by China's rise on the global stage. Some stakeholders argue that these legal actions may have unintended consequences, such as denying low-cost technology to American consumers, lost profits for American companies barred from selling to Huawei, and the risk that technology companies might move operations overseas to avoid U.S. trade restrictions. Efforts to account for these considerations are ongoing and may continue in the 117th Congress and the Biden Administration.

This report outlines recent Huawei-related legal activities and examines the statutory authorities underlying each action.

Contents

Contacts

Huawei Technologies Co., Ltd. (Huawei)—the world's largest telecommunications equipment manufacturer[1]—is at the center of a host of legal activities that seek to protect the United States' national security and economy. In 2012, the House Permanent Select Committee on Intelligence (HPSCI) released a report describing the counterintelligence and security threat posed by Huawei's access to U.S. telecommunications systems and supply chains.[2] Senior executive branch officials in the Trump Administration, including the Vice President and Secretary of State, stated that Huawei's products present an inherent security threat because the Chinese government may be able to access confidential information via secret "backdoors" by forcing Huawei to share such information or provide access to its networks.[3] Huawei denies that it purposefully creates "back doors" for the Chinese government,[4] and third-party analysts have not reached uniform conclusions about the security of Huawei's products.[5]

Given the security debate, Congress and the executive branch have initiated a variety of legal efforts to limit Huawei's access to international supply chains, telecommunications systems, and markets. These legal actions have evolved from narrow restrictions on federal spending to an international effort to remove Huawei equipment from telecommunications networks domestically and abroad.

After HPSCI's 2012 report, the United States enacted several laws that restrict federal procurement of, and grant and loan spending on, Huawei systems.[6] These efforts soon expanded beyond federal spending limitations to include restrictions on a broad set of Huawei-related

[1] Press Release, U.S. Dep't of Justice, Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud (Jan 28, 2019), https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial [hereinafter January 2019 DOJ Press Release].

[2] *See* CHAIRMAN MIKE ROGERS AND RANKING MEMBER C.A. DUTCH RUPPERSBERGER, PERMANENT SELECT COMMITTEE ON INTELLIGENCE, U.S. HOUSE OF REPRESENTATIVES, INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE (Oct. 8, 2012), https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf [hereinafter HPSCI REPORT].

[3] *See, e.g.*, Remarks by Vice President and Prime Minister Trudeau of Canada in Joint Press Statements | Ottawa, Canada (May 30, 2019), https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-prime-minister-trudeau-canada-joint-press-statements-ottawa-canada/ (statement of Vice President Pence) ("The simple fact is that the legal framework within China gives the Chinese government access to information and data that is collected by Chinese companies like Huawei."); Interview with U.S. Sec'y of State Michael R. Pompeo by Maria Bartiromo, (May 28, 2019), https://www.state.gov/interview-with-maria-bartiromo-of-mornings-with-maria-on-fox-business-network-5/ ("Huawei is an instrument of the Chinese Government. . . . [If] the Chinese Communist Party wanted to get information from technology that was in the possession of Huawei, it is almost certainly the case that Huawei would provide that to them."); Remarks by Dr. Christopher Ashley Ford, Assistant Sec., Bureau of Int'l Sec. and Nonproliferation, U.S. Dep't of State, Multilateral Action on Sensitive Technologies (MAST) Conference, Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications (Sep. 11, 2019), https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/ [hereinafter MAST Conference Remarks] ("Firms such as Huawei . . . have no meaningful ability to tell the Chinese Communist Party 'no' if officials decide to ask for their assistance . . . .").

[4] *See, e.g.*, *Media Statement Regarding WSJ "Backdoor" Story*, HUAWEI.COM, https://www.huawei.com/en/facts/voices-of-huawei/media-statement-regarding-wsj (last visited Dec. 16, 2020); *5G Security. Huawei: Facts, Not Myths*, HUAWEI.COM, https://www.huawei.com/en/facts/voices-of-huawei/5g-security (last visited Dec. 16, 2020) [hereinafter *Huawei: Facts, Not Myths*].

[5] *See, e.g.*, ROBERT D. WILLIAMS, EXEC. DIR. PAUL TSAI CHINA CTR., YALE L. SCHOOL, BEYOND HUAWEI AND TIKTOK: UNTANGLING U.S. CONCERNS OVER CHINESE TECH COMPANIES AND DIGITAL SECURITY 25-26 (Oct. 30, 2020); Timothy R. Heath, *Public Evidence of Huawei as a Cyber Threat May be Elusive, but Restrictions Could Still be Warranted*, RAND (Mar. 7, 2019), https://www.rand.org/blog/2019/03/public-evidence-of-huawei-as-a-cyber-threat-may-be.html.

[6] *See infra* § Federal Spending Restrictions.

public and private sector transactions.[7] In 2019 and 2020, Congress and the executive branch crafted laws and policies designed to eliminate Huawei's presence in U.S. telecommunications networks—even if existing Huawei equipment must be "ripped and replaced."[8] The United States took other forceful legal actions during this time, pursing criminal charges against Huawei and its Chief Financial Officer (CFO),[9] issuing visa restrictions for Huawei employees,[10] banning trade in Huawei securities,[11] and engaging in international efforts to convince foreign countries to ban Huawei from their networks.[12] Most recently, in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA; Pub. L. No. 116-283),[13] passed over President's Trump's veto, the 116th Congress embarked on a new endeavor of using federal funds to support private competitors to Huawei that can offer secure and affordable communications networks domestically and internationally.[14]

Some observers view this suite of legal actions involving Huawei as part of a broader effort to "decouple" the United States' economy from problematic aspects of China's economy.[15] Some contend, however, that these efforts may have unwanted side effects, such as denying low-cost technology to American consumers, loss of profitability for American companies that can no longer sell to Huawei, and the risk that technology companies may move operations overseas to avoid U.S. trade restrictions.[16] Efforts to account for these considerations are ongoing and may continue in the 117th Congress and in the Biden Administration.[17] This report outlines recent Huawei-related legal activities by the U.S. government and examines the statutory authorities underlying each action.[18]

[7] *See infra* §§ Export Restrictions; Executive Orders Under the International Emergency Economic Powers Act (IEEPA); Federal Communications Commission's Actions.

[8] *See infra* § Federal Communications Commission's Actions.

[9] *See infra* § United States' Criminal Prosecutions.

[10] *See infra* § Visa Restrictions.

[11] *See infra* § Executive Order 13959: Securities Ban.

[12] *See infra* § Diplomacy and Foreign Aid.

[13] Pub. L. No. 116-283 (2021) [hereinafter FY2021 NDAA]; 166 CONG. REC. D1148 (daily ed. Jan. 1, 2021) (passing FY2021 NDAA over the President's veto).

[14] *See infra* § National Defense Authorization Act for Fiscal Year 2021.

[15] *See, e.g.*, Ian Bremmer and Cliff Kupchan, *Risk 2: The Great Decoupling*, EURASIA GROUP (Jan. 6, 2020), https://www.eurasiagroup.net/live-post/risk-2-great-decoupling; Jamie Gorelick, Stephen Preston, and Matthew Ferraro, *Decoupling from China: Part 2—Security Requirements*, LAW360 (Oct. 29, 2020), https://www.law360.com/articles/1323848/decoupling-from-china-part-2-security-requirements; Yuan Yang, *US Tech Backlash Forces China to Be More Self-Sufficient*, FIN. TIMES (Jan. 15, 2020), https://www.ft.com/content/c6993200-1ff3-11ea-b8a1-584213ee7b2b. For more discussion of the potential decoupling between the U.S. and Chinese economies, see CRS In Focus IF10119, *U.S.-China Relations*, by Susan V. Lawrence, Michael F. Martin, and Andres B. Schwarzenberg.

[16] *See infra* § Addition of Huawei to the Entity List.

[17] *See, e.g.*, Jacky Wong, *The U.S.-China Tech War Won't End Under Biden*, WALL ST. J. (Dec. 14, 2020), https://www.wsj.com/articles/the-u-s-china-tech-war-wont-end-under-biden-11607939916; Jeanne Whalen, *Biden Likely to Remain Tough on Chinese Tech Like Huawei, but with More Help from Allies*, WASH POST. (Nov. 16, 2020), https://www.washingtonpost.com/technology/2020/11/16/biden-huawei-trump-china/.

[18] While this report provides background on Huawei and discusses the impetus for recent U.S. legal activity, it does not evaluate whether Huawei products actually present security risks or whether the Chinese government could require Huawei to provide access to data on Huawei systems and equipment.

Background on Huawei

Ren Zhengfei, a former member of the engineer corps of China's People's Liberation Army (PLA), founded Huawei in Shenzhen, China in 1987.[19] The company started as an importer of telecommunications switches—a basic networking technology—but began to develop its own products in the early 1990s.[20] Early on, Huawei promoted its products to rural communities in China.[21] By the late 1990s, it had won large contracts to provide communications infrastructure for the PLA and major Chinese cities like Beijing.[22] Since then, Huawei has expanded its operations internationally and grown to be the world's largest manufacturer of telecommunications equipment.[23] Some observers attribute Huawei's success to financial and other state support from the Chinese government,[24] but the extent to which Huawei's growth stems from government support is the subject of debate.[25]

Early Legal Actions and Congressional Interest

Huawei first attracted congressional attention in the early 2000s, when observers accused it of violating U.N. sanctions by providing fiber optic technology to the Saddam Hussein regime in Iraq.[26] The company again became the subject of congressional scrutiny in 2007 as part of a

[19] *See* NATHANIEL AHRENS, CENT. FOR STRATEGIC & INT'L STUDIES, CHINA'S COMPETITIVENESS: MYTH, REALITY, AND LESSONS FOR THE UNITED STATES AND JAPAN, CASE STUDY: HUAWEI 2 (2013); Bruce Gilley, *Huawei's Fixed Line to Beijing*, 94 FAR EASTERN ECON. R., Dec. 28, 2000, at 94; *Milestones*, HUAWEI.COM (last visited Mar. 3, 2020), https://www.huawei.com/us/about-huawei/corporate-information/milestone. For additional background on the PLA, see CRS Report R41007, *Understanding China's Political System*, by Susan V. Lawrence and Michael F. Martin, at 25. Some accounts place Huawei's founding in 1988. *See, e.g.*, Briefing Proliferation Issues, Hearings before the U.S.-China Security Review Comm'n, 107th Cong (2001), *in* Compilation of Hearings Held Before the U.S.-China Sec. Rev. Comm'n, 107th Cong. 579 (2001-2002) (Prepared Statement of Gary Milhollin, Director, Wisconsin Project on Nuclear Arms Control) [Milhollin Proliferation Statement]; *The Huawei Way*, NEWSWEEK (Jan. 15, 2006), https://www.newsweek.com/huawei-way-108201.

[20] AHRENS, *supra* note 19, at 3; Keith Johnson, Elias Groll, *The Improbable Rise of Huawei*, FOREIGN POLICY (April 3, 2019), https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/.

[21] *See* AHRENS, *supra* note 19, at 3.

[22] *Id.*; Karishma Vaswani, *Huawei: The Story of a Controversial Company*, BBC (Mar. 6, 2019), https://www.bbc.co.uk/news/resources/idt-sh/Huawei.

[23] *See* January 2019 DOJ Press Release, *supra* note 1.

[24] *See, e.g.*, Global Public Affairs, U.S. Dep't of State, *Huawei: Myth vs. Fact*, (Dec. 9, 2019), https://translations.state.gov/2019/12/09/huawei-myth-vs-fact/ ("Beijing's state-backed banks provide tens of billions of dollars in subsidized financing to Huawei so the [People's Republic of China] can gain access to foreign markets and achieve strategic global dominance."); Melanie Hart and Jordan Link, *There is a Solution to the Huawei Challenge*, CTR. FOR AM. PROGRESS (Oct. 14, 2020), https://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge/ ("Beijing deploys powerful industrial policies to make Huawei equipment cheaper to deploy").

[25] *Compare, e.g.*, sources cited *supra* note 24 (describing state support for Huawei); *with Huawei: Facts, Not Myths*, *supra* note 4 ("Like many other companies in the telecom industry, we [Huawei] take advantage of government funding when it's available, but the sums involved are comparatively small. . . . We don't get special support from the Chinese government."); *and* AHRENS, *supra* note 19, at 6-10 (analyzing China's state support for Huawei as part of a broader national effort to develop a more independent and self-sustaining domestic telecommunications industrial base); *and* Milhollin Proliferation Statement, *supra* note 19 (attributing Huawei's success during the 1990s to technology transfers from U.S. companies).

[26] *See, e.g., U.S. Policy Toward Iraq: Hearing Before the Subcomm. on the Middle East and S. Asia of the H. Comm. on Int'l Relations*, 107th Cong. 34, 41 (2001) (discussing Huawei's transactions in Iraq); 148 CONG. REC. S8337 (daily ed. Sep. 9, 2002) (statement of Senator Kyl) ("Media reports indicate that the Chinese firm Huawei Technologies—an important player for many U.S. firms who want to reach the Chinese telecom and data communications market—

review by the Committee on Foreign Investment in the United States (CFIUS).[27] CFIUS is an interagency committee that advises the President on whether to block or suspend mergers, acquisitions, and takeovers of U.S. companies because of national security risks.[28] In 2007, Huawei partnered with American private investment firm Bain Capital LP in an effort to acquire an ownership interest in 3Com Corporation (3Com)—an American digital electronics firm.[29] The deal raised national security concerns because 3Com provided cybersecurity systems to the U.S. military.[30] Some executive branch officials and Members of Congress argued that the acquisition would compromise cybersecurity protections at the Department of Defense (DOD).[31] Several Members of the 110th Congress urged CFIUS to analyze the transaction and identify national security concerns, [32] which CFIUS ultimately did.[33] Bain Capital abandoned the deal after CFIUS stated that it intended to recommend that the President stop the acquisition.[34]

By 2010, Huawei faced greater U.S. government scrutiny as it tried to expand operations in the United States. At the urging of executive branch officials and some Members of Congress, Sprint Nextel Corp. (Sprint) excluded Huawei and ZTE Corporation (ZTE)—China's second largest telecommunications equipment manufacturer—from a multi-billion contract to supply telecommunications equipment in the United States.[35] Later that year, a group of Senators wrote

assisted Iraq with fiber-optics to improve its air-defense system. This was not only a violation of U.N. sanctions, it also greatly increased the danger to U.S. and British pilots patrolling the no-fly zones."). Some observers criticized U.S. export control policy at the time because it allowed U.S. companies to transfer technology to Huawei despite reports that Huawei used American technology in systems sold to U.S. adversaries. *See, e.g.*, Milhollin Proliferation Statement, *supra* note 19, at 579-80; Kelly Motz and Jordan Richie, *Techno Two-Timing*, WALL ST. J. (Mar. 19, 2001), https://www.wsj.com/articles/SB984950042398710644.

[27] *See, e.g., National Industry Security Program: Addressing the Implications of Globalization and Foreign Ownership for the Defense Industrial Base: Hearing Before the H. Comm. on Armed Servs.*, 110th Cong. 17 (2008) (statement of Rep. Hunter); 153 CONG. REC. 26339 (2007) (statement of Rep. McCotter).

[28] See 50 U.S.C. § 4565. For background on CFIUS, see CRS Report RL33388, The Committee on Foreign Investment in the United States (CFIUS), by James K. Jackson.

[29] *See, e.g., Congress to Probe 3Com-Huawei Deal*, WASH. TIMES (Feb. 2, 2008), https://www.washingtontimes.com/news/2008/feb/2/congress-to-probe-3com-huawei-deal/.

[30] *See id*; U.S.-CHINA ECON. AND SEC. REVIEW COMM'N., THE NATIONAL SECURITY IMPLICATIONS OF INVESTMENTS AND PRODUCTS FROM THE PEOPLE'S REPUBLIC OF CHINA 28-30 (Jan 2011), https://www.uscc.gov/sites/default/files/Research/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf [hereinafter U.S.-CHINA 2011 REPORT]; Steven R. Weisman, *Sale of 3Com to Huawei is Derailed by US Security Concerns*, N.Y. TIMES (Feb. 21, 2008), https://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html.

[31] *See, e.g.*, Weisman, *supra* note 30; 153 CONG. REC. 26339 (2007) (statement of Rep. McCotter) ("Communist China's Huawei Technologies' stake in the 3Com Corporation will gravely compromise our free Republic's national security.").

[32] *See, e.g., National Industry Security Program: Addressing the Implications of Globalization and Foreign Ownership for the Defense Industrial Base: Hearing Before the H. Comm. on Armed Servs.*, 110th Cong. 17 (2008) (statement of Rep. Hunter); 153 CONG. REC. 26339 (2007) (statement of Rep. McCotter); *see also* H.Res. 730, 110th Cong. (2007) (expressing concern that Huawei's planned acquisition of an interest in 3Com triggers CFIUS review and that the preponderance of evidence suggests the proposed acquisition threatens U.S. national security).

[33] *See, e.g.*, U.S.-CHINA 2011 REPORT, *supra* note 30, at 28-29.

[34] *See, e.g., id*.; *Bain Capital Drops Its Bid for 3Com*, WALL ST. J. (Mar. 21, 2008), https://www.wsj.com/articles/SB120603627253952409.

[35] *See* Joann S. Luplin and Shayndi Rice, *Security Fears Kill Chinese Bid in U.S.*, WALL ST. J. (Nov. 5, 2010), https://www.wsj.com/articles/SB10001424052748704353504575596611547810220; Letter from Senator Kyl et al. to Honorable Timothy Geithner, U.S. Sec'y of Treasury, et al. (Aug. 18, 2010), graphics8.nytimes.com/packages/pdf/business/20100823-telecom.pdf.

to the Federal Communications Commission (FCC) Chairman expressing concerns about using Huawei or ZTE technology in U.S. telecommunications systems.[36]

In 2011, Huawei divested itself of assets purchased from an American company that specialized in server technology, 3Leaf Systems, after CFIUS raised national security concerns.[37] Later that year, Huawei published an "open letter" to the U.S. government denying the security concerns and inviting a formal investigation to relieve the U.S. government's apprehensions.[38] HPSCI responded to the invitation by investigating potential counterintelligence and security threats posed by Huawei and ZTE.[39] In its 2012 report, HPSCI recommended, among other things, that the United States view Chinese telecommunications companies' efforts to penetrate U.S. markets "with suspicion."[40] HPSCI also recommended that Congress consider legislation to "better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build infrastructure."[41]

Federal Spending Restrictions

Beginning in 2013, the year after HPSCI's report, Congress began to enact legislation limiting Huawei and other Chinese telecommunication companies' access to U.S. markets and supply chains.[42] These legislative efforts began with limitations on specific agencies' ability to procure Huawei products and services, but later expanded into broader spending restrictions that apply to all executive branch agencies.

Appropriations Restrictions

Beginning with the Consolidated and Further Appropriations Act, 2013 (2013 Appropriations Act), the federal government has enacted a series of appropriations laws that prohibit some executive branch agencies from using appropriated funds to acquire information technology systems from entities connected with the Chinese government.[43] The provision, which Congress has placed in an amended format in later appropriations laws,[44] applies to the Department of Commerce (Commerce), Department of Justice (DOJ), National Aeronautics and Space Administration (NASA), and the National Science Foundation.[45] It restricts these agencies from

[36] *See* Letter from Senator Jon Kyl et al. to Hon. Julius Genachowski, Chairman, FCC (Oct. 19, 2010), https://www.hsgac.senate.gov/media/minority-media/congressional-leaders-cite-telecommunications-concerns-with-firms-that-have-ties-with-chinese-government [hereinafter Kyl-FCC Letter] ("We are very concerned that [Huawei and ZTE] are being financed by the Chinese government and are potentially subject to significant influence by the Chinese military which may create an opportunity for manipulation of switches, routers, or software embedded in American telecommunications network[s] so that communications can be disrupted, intercepted, tampered with, or purposely misrouted. This would pose a real threat to our national security.").

[37] *See, e.g. Huawei Drops a Controversial US Takeover Bid for 3Leaf*, BBC (Feb. 21, 2011), https://www.bbc.com/news/business-12520640.

[38] *See* Ken Hu, Deputy Chairman of Huawei Technologies, Chairman of Huawei USA, Huawei Open Letter, http://online.wsj.com/public/resources/documents/Huawei20110205.pdf (accessed Mar. 4, 2020).

[39] HPSCI REPORT, *supra* note 2.

[40] *Id.* at 43.

[41] *Id.* at 46.

[42] *See infra* § Appropriations Restrictions.

[43] Pub. L. No. 113-6, § 516, 127 Stat. 198, 273 (2013).

[44] *See, e.g.*, Consolidated Appropriations Act, 2020, Pub. L. No. 116-93, § 514, 133 Stat. 2317, 2427 (2019).

[45] *See* Pub. L. No. 113-6, § 516(a).

using appropriated funds to acquire an information technology system made or assembled by an entity owned, directed, or subsidized by the Chinese government.[46] Although the provision does not name Huawei, some observers and Members of Congress described it as designed to address risks posed by Huawei and ZTE.[47]

2018 NDAA

In the National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA; Pub. L. No. 115-91), the United States placed Huawei-related restrictions into federal law beyond the appropriations context.[48] The 2018 NDAA prohibits DOD from procuring certain telecommunications equipment or services from Huawei and others as part of DOD's missions related to nuclear deterrence and homeland defense.[49] Unlike earlier appropriations provisions, the 2018 NDAA names Huawei in the legislation.[50] The 2018 NDAA prohibits DOD from procuring, obtaining, extending, or renewing contracts that include telecommunications equipment or services provided by Huawei, ZTE, or any entity that the Secretary of Defense reasonably believes is owned, controlled by, or "otherwise connected to" the Chinese or Russian governments.[51] To fall within the 2018 NDAA, the telecommunications equipment or services must be a *substantial or essential component*[52] or *critical technology*[53] of the system provided to DOD for its nuclear deterrence or homeland defense missions.[54]

2019 NDAA

While the appropriations restrictions and 2018 NDAA were limited to specific federal agencies, section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA; Pub. L. No. 115-232) provides a broader set of Huawei-related restrictions that apply across the executive branch.[55] Section 889(a)(1)(A) bars *all* executive branch agencies from procurement or contracting that includes telecommunications equipment or services from Huawei, ZTE, and certain other Chinese corporations[56] as a substantial or essential component or

[46] *Id.* The prohibitions contain an exception if the head of the procuring agency, in consultation with the Federal Bureau of Investigation (FBI) or other "appropriate" federal entity, provides a written determination that the acquisition is in the national interests of the United States. *Id.* § 516(b).

[47] *See*, *e.g.*, Adam Mazmanian, *China Sourcing Rules Reappear in Appropriations*, FCW (July 11, 2013), https://fcw.com/articles/2013/07/11/wolf-china-technology.aspx.

[48] Pub. L. No. 115-91, § 1656, 131 Stat. 1283, 1761 (2017) (codified in 10 U.S.C. § 491 note) [hereinafter 2018 NDAA].

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] DOD procurement regulations define a substantial or essential component as any component "necessary for the proper function or performance of a piece of equipment, system, or service." *See* Covered Defense Telecommunications Equipment or Services, 84 Fed. Reg. 72231, 72238 (Dec. 31, 2019) [Dec. 31, 2019 NDAA Rule] (codified at 48 C.F.R. § 252.204-7018).

[53] Critical technology is defined in DOD procurement regulations at 48 C.F.R. § 252.204-7018. The definition is derived from the Foreign Investment Risk Review Modernization Act, Pub. L. No. 115-232, § 1703(6) (codified at 50 U.S.C. § 4565(6)). Critical technologies include defense articles and defense services on the U.S. Munitions List; certain dual-use items on the Commerce Control List; certain nuclear equipment, materials, software, and facilities; select agents and toxins; and emerging foundational technologies. 48 C.F.R. § 252.204-7018.

[54] 2018 NDAA, *supra* note 48, § 1656(b).

[55] *See* Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917 (2018) [hereinafter 2019 NDAA].

[56] Section 889 of the 2019 NDAA applies to Huawei, ZTE, Hytera Communications Corporation, Hangzhou Hikvision

critical technology.[57] Section 889(a)(1)(B) of the 2019 NDAA bars executive agencies from transacting with a company that uses Huawei or other covered entities' telecommunications equipment or services as a substantial or essential component or critical technology.[58] Whereas the first prohibition (Part A) restricts executive agencies from procuring systems that contain Huawei equipment or services, the second provision (Part B) prohibits executive agencies from contracting with companies that use Huawei equipment or services in the *companies' own systems*—even if those systems are not sold to the government.[59] Section 889 also prohibits the use of federal grant or loan funds to obtain anything prohibited in Parts A and B, unless an exception applies.[60]

If a company that would be barred from transacting with an executive branch agency requests a waiver of section 889, the head of the executive agency can issue a one-time waiver for up to two years, provided the request meets certain conditions.[61] The Director of National Intelligence (DNI) possesses broader waiver authority when the DNI determines that a waiver is in the U.S. national security interest.[62]

Huawei's Legal Challenge to Section 889 of the 2019 NDAA

Section 889 of the 2019 NDAA names Huawei as an entity that is barred from covered transactions.[63] Huawei has argued, however, that the Constitution's Bill of Attainder Clause[64] prohibits Congress from singling out and excluding a specific company in this fashion.[65] The Bill of Attainder Clause forbids the United States from inflicting a "punishment" on a person or entity by legislative act without a judicial trial.[66] Huawei filed a lawsuit in the United States District

---

Digital Technology Company, Dahua Technology Company, any subsidiary or affiliate of such entities, and any entity that the Secretary of Defense, in consultation with the Director National Intelligence (DNI) and the FBI Director, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of China. *Id.* § 889(f).

[57] *Id.* § 889(a)(1)(A). The definitions of "substantial or essential component" and "critical technology" are identical in DOD regulations implementing the 2018 and 2019 NDAAs. *Compare* 48 C.F.R. § 252.204-7018 (required contract clauses implementing 2018 NDAA) *with* 48 C.F.R. § 4.2101 (regulations implementing 2019 NDAA).

[58] 2019 NDAA, *supra* note 55, § 889(a)(1)(B).

[59] Some observers and Members of Congress debate whether Part B of Section 889 is overbroad and should be narrowed legislatively or through implementing regulations. *See, e.g.*, Justin Doubleday, *Senate Proposal to Delay Huawei Ban Faces Stiff Opposition from China Hawks*, INSIDE CYBERSECURITY (Dec. 14, 2020), https://insidedefense.com/daily-news/senate-proposal-delay-huawei-ban-faces-stiff-opposition-china-hawks.

[60] *Id.* § 889(b)(1). Section 889 includes certain exceptions to its grant and loan fund restrictions, including (1) entities that provide a service that connects the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements, and (2) "telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles." *Id.* § 889(b)(3). For additional discussion on the grant and loan fund restrictions, see OFFICE MGMT. BUDGET, PROHIBITION ON COVERED TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT, https://www.performance.gov/CAP/Sec.%20889%20of%202019%20NDAA_FAQ_20201124.pdf.

[61] 2019 NDAA, *supra* note 55, § 889(d). The entity seeking a waiver must provide a "compelling justification" for additional time to implement the law, and the head of the executive agency must submit to Congress a "full and complete laydown of the presences of covered telecommunications or video surveillance equipment or services in the entity's supply chain and a phase-out plan to eliminate" such equipment or services. *Id.* § 889(d)(1).

[62] *Id.* § 889(d)(2).

[63] 2018 NDAA, *supra* note 55, § 889. For a list of other entities identified in the 2019 NDAA, see *supra* note 56.

[64] *See* U.S. CONST. art. I, § 9 ("No Bill of Attainder or ex post factor Law shall be passed.").

[65] *See generally* Complaint, Huawei Technologies USA, Inc. v. United States, No. 4:19-cv-00159 (E.D. Tex. Mar. 6, 2019) [hereinafter Huawei Complaint].

[66] *See* Cummings v. Missouri, 71 U.S. 277, 323 (1866) ("A bill of attainder is a legislative act which inflicts

Court for the Eastern District of Texas alleging, among other things, that the 2019 NDAA violates this prohibition.[67] Relying on the Supreme Court's interpretation of the Bill of Attainder Clause[68] and recent federal appellate court decisions rejecting claims based on it,[69] the district court rejected Huawei's constitutional challenge and dismissed the suit in February 2020.[70]

Export Restrictions

While annual appropriations provisions and the 2018 and 2019 NDAAs marked the opening salvo in what has become a broader legal confrontation between Huawei and the U.S. government, those restrictions generally were limited to transactions involving federal spending in the form of procurement and grant and loan funds.[71] Entities that did not participate in federal procurement or receive grant and loan funds could continue to transact business with Huawei without violating the restrictions.[72] In May 2019, the Trump Administration expanded the scope of Huawei-related prohibitions outside the federal spending context by exercising its authority under the Export Controls Act of 2018 (ECA).[73]

The ECA provides the President with powers to control the export of, among other things, certain U.S. dual-use goods and technology.[74] A *dual-use* item can serve both civilian purposes and military, terrorism, weapons of mass destruction, or law enforcement purposes.[75] The ECA requires the Secretary of Commerce to establish and maintain a list, known as the *Entity List*, of foreign entities that are subject to export license requirements because they are threats to U.S. national security and foreign policy.[76] The ECA authorizes the executive branch to control

punishment without a judicial trial.").

[67] *See* Huawei Complaint, *supra* note 65.

[68] *See, e.g.*, Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 468-84 (1977) (describing three avenues for determining whether a law inflicts a punishment within the meaning of the Bill of Attainder Clause: (1) a historical analysis, (2) a functional text; and (3) an analysis of Congress's motivation for the law in question).

[69] *See, e.g.*, SBC Commc'ns, Inc. v. FCC, 154 F.3d 226, 247 (5th Cir. 1998) (concluding that the Telecommunications Act of 1996's restrictions on 20 specific former subsidiaries of AT&T was not a Bill of Attainder); ACORN v. United States, 618 F.3d 125, 136–42 (2d Cir. 2010) (rejecting Bill of Attainder challenge to provision of the 2010 Consolidated Appropriations Act that excluded the non-profit organization ACORN and "affiliates, subsidiaries, and alli[es]" from federal funding); Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec., 909 F.3d 446, 453-64 (D.C. Cir. 2018) (holding that a provision in the National Defense Authorization Act for Fiscal Year 2017 prohibiting federal procurement of "hardware, software or services" developed by Russian cybersecurity company Kaspersky Lab did not violate the Bill of Attainder Clause).

[70] *See* Memorandum Opinion and Order, Huawei Technologies USA, Inc. v. United States, No. 4:19-cv-00159 (E.D. Tex. Feb. 18, 2020). For additional discussion of Huawei's suit and the Bill of Attainder Clause, see CRS Legal Sidebar LSB10274, *Huawei v. United States: The Bill of Attainder Clause and Huawei's Lawsuit Against the United States*, coordinated by Joanna R. Lampe.

[71] *See supra* § Federal Spending Restrictions.

[72] While the NDAAs limited the federal government's ability to procure Huawei systems, they did not prevent state governments from doing so. *See* Frank Konkel, *Report Warns of Tech Threats from 'Other' Chinese Companies*, NEXTGOV (Feb. 24, 2020) ("While the federal government has cracked down on the use of Chinese-owned companies at the federal level in recent years over espionage and data safety concerns, at least 43 states hold important IT contracts with other Chinese-owned companies and could be at risk . . . .").

[73] 50 U.S.C. §§ 4801-4826.

[74] *Id.* § 4812. For background on the ECA and its authority, see CRS Report R41916, *The U.S. Export Control System and the Export Control Reform Initiative*, by Ian F. Fergusson and Paul K. Kerr and CRS In Focus IF11627, *U.S. Export Control Reforms and China: Issues for Congress*, by Ian F. Fergusson and Karen M. Sutter.

[75] 50 U.S.C. § 4801(2).

[76] *Id.* § 4813(a)(2). The Entity List is available at 15 U.S.C. pt. 744, supp. 4. The ECA requires the Secretary of

exports, re-exports,[77] and "in-country transfers" (i.e., transfers within a foreign country[78]) to companies on the Entity List.[79] The Bureau of Industry and Science (BIS) in the Department of Commerce maintains the Entity List.[80]

Addition of Huawei to the Entity List

In several final rules, issued over the course of 2019 and 2020, BIS added Huawei and more than 150 non-U.S. affiliates of Huawei to the Entity List.[81] An interagency committee[82] determined that there is reasonable cause to believe that Huawei has been involved in activities that are contrary to the national security or foreign policy interests of the United States.[83] The interagency committee cited Huawei and its affiliates' alleged violation of U.S. sanctions on Iran (which are also the subject of a criminal prosecution, discussed below[84]) as an illustration of the risks Huawei poses to U.S. national security and foreign policy.[85]

Because Huawei and other Chinese telecommunications companies depend on certain U.S. products, such as microchips, for their equipment, the prohibition of exports from the United States can potentially damage their business.[86] For example, in 2018, U.S. export restrictions on ZTE reportedly forced ZTE to suspend business operations temporarily when it could not access the U.S. semiconductors needed for its supply chain.[87] At the same time, there may be compelling

Commerce to consult with the Secretaries of State, Defense, and Energy and "the heads of other Federal agencies as appropriate" in establishing the Entity List. 50 U.S.C. § 4813(a).

[77] The term "re-export" refers to the shipment of an item subject to export controls from one foreign country to another foreign country. 15 C.F.R. § 734.14.

[78] *See id.* § 734.16 ("[A] Transfer (in-country) is a change in end use or end user of an item within the same foreign country. Transfer (in-country) is synonymous with In-country transfer.").

[79] *See* 50 U.S.C. § 4812(a)(1).

[80] Bureau of Indus. and Sci., Dep't of Commerce, *FAQs – Entity List FAQs*, https://www.bis.doc.gov/index.php/cbc-faqs/cat/36-entity-list-faqs-2#faq_281 (last visited Feb. 26, 2021)

[81] Addition of Entities to the Entity List, 84 Fed. Reg. 22961 (May 21, 2019) (codified at 15 C.F.R. pt. 744) [hereinafter May 21, 2019 Rule]; Addition of Entities to the Entity List and Revision of Entries on the Entity List, 84 Fed. Reg. 43493 (Aug. 21, 2019) (codified at 15 C.F.R. pt. 744) [hereinafter August 21, 2019 Final Rule]; Addition of Huawei Non-U.S. Affiliates to the Entity List, 85 Fed. Reg. 51596 (Aug. 20, 2020) (codified at 15 C.F.R. pts. 736, 744, 762) [hereinafter August 20, 2020 Final Rule].

[82] The End-User Review Committee is composed of representatives of the Departments of Commerce, State, Defense, Energy and, "where appropriate," the Treasury. 15 C.F.R. pt. 744, supp. 5 appx.

[83] May 21, 2019 Rule, *supra* note 81, at 22961. *See also* August 20, 2020 Final Rule, *supra* note 81, at 51596 (addressing the "continuing threat to U.S. national security and U.S. foreign policy interests posed by Huawei and its non-U.S.-affiliates").

[84] *See infra* § United States' Criminal Prosecutions.

[85] May 21, 2019 Rule, *supra* note 81, at 22961-962.

[86] *See, e.g.*, Janne Suokas, *Huawei Lists 33 US Companies Among Core Suppliers*, GLOBAL TIMES (Nov. 30, 2018), https://gbtimes.com/huawei-lists-33-us-companies-among-core-suppliers ("In November 2018, Huawei released a list of core suppliers, and 33 of 92 suppliers were U.S. companies.");Yuan Yang and Lucy Hornby, *China Raises Alarm Over Its Dependency on Foreign Chips*, FIN. TIMES (July 18, 2018), https://www.ft.com/content/410306d8-8ae0-11e8-bf9e-8771d5404543 ("China relies on imported semiconductors to build the hardware — including phones, telecoms gear and computers — that account for almost one-third of its exports . . . ."). *But see* Asa Fitch and Dan Strumpf, *Huawei Manages to Make Smartphones Without American Chips*, WALL ST. J. (Dec. 1, 2019), https://www.wsj.com/articles/huawei-manages-to-make-smartphones-without-american-chips-11575196201 ("Huawei has made significant strides in shedding its dependence on parts from U.S. companies.").

[87] *See, e.g.*, Sijia Jiang, *China's ZTE Says Main Business Operations Cease Due to U.S. Ban*, REUTERS (May 9, 2018), https://www.reuters.com/article/us-zte-ban/chinas-zte-corp-says-main-business-operations-cease-due-to-u-s-ban-idUSKBN1IA1XF?il=0.

reasons to avoid causing serious commercial harm to Huawei and other Chinese telecommunications firms. For example, some rural areas of the United States depend on Huawei for their telecommunications infrastructure, and an export ban can hinder telecommunications in rural America.[88] Denial of exports may also affect the revenue and profitability of U.S. businesses that cannot sell their products to companies on the Entity List.[89] Moreover, not all exports to Huawei present the same level of national security concerns, according to Commerce.[90] And addition of Huawei and its affiliates to the Entity List could prevent American companies from participating in international organizations that develop standards for 5G systems and other technology.[91]

To account for these competing considerations, BIS has sought to calibrate its export restrictions—contained in the Export Administration Regulations (EAR)[92]—by authorizing certain limited types of exports to Huawei. Shortly after adding Huawei to the Entity List, BIS temporarily authorized exports to Huawei and its affiliates, provided the exports were: (1) necessary to maintain and support existing telecommunications networks and equipment; (2) necessary to provide service and support to existing Huawei handsets; (3) made to provide information related to cybersecurity vulnerabilities in Huawei networks or products or research related to cybersecurity; and (4) part of engagement with Huawei and its affiliates necessary for developing 5G standards at a recognized international standards body.[93]

This temporary authorization—which BIS called a *temporary general license*—expired on August 13, 2020.[94] But BIS amended its regulations to exclude permanently variations of the

[88] *See*, *e.g.*, Reply Comments of the Rural Wireless Ass'n, Inc. at 15, In the Matter of Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain Through FCC Programs, 33 F.C.C. Rcd. 4058 (2018) (estimating that 25% of members of the Rural Wireless Association would be impacted by the proposal to limit use of certain federal funds to purchase equipment or services from Huawei and ZTE). *See* August 20, 2020 Final Rule, *supra* note 81, at 51599 ("Companies detailed would be required for their organization or industry to cease using Huawei equipment. Time and money were common themes, emphasizing that continued short-term reliance on Huawei for maintaining existing systems in the U.S. will be required."); Ceilia Kang, *Huawei Ban Threatens Wireless Service in Rural Areas*, N.Y. TIMES (May 25, 2019), https://www.nytimes.com/2019/05/25/technology/huawei-rural-wireless-service.html ("Huawei is essential for many wireless carriers that serve sprawling, sparsely populated regions because its gear for transmitting cell signals often costs far less than other options.").

[89] *See*, *e.g.*, Asa Fitch, *Broadcom to Take $2 Billion Hit from Huawei Ban*, WALL ST. J. (June 13, 2019), https://www.wsj.com/articles/broadcom-lowers-revenue-outlook-amid-trade-tensions-11560459528; Jeanne Whalen et al., *Huawei Supply Ban Roils Stocks as U.S. Companies Begin to Cut Off China Tech Giant*, WASH. POST (May 20, 2019), https://www.washingtonpost.com/technology/2019/05/20/google-cuts-off-huawei-after-trump-administration-crackdown/.

[90] *See* August 20, 2020 Final Rule, *supra* note 81, at 51598 (explaining that, in BIS's view, certain limited sets of exports to Huawei and its affiliates may be "consistent with U.S. national security and foreign policy interests"); Alexandra Alper and Karen Freifeld, *U.S. to Approve Sales It Deems Safe to Blacklisted Huawei*, REUTERS (July 9, 2019), https://www.reuters.com/article/us-usa-china-huawei-tech/us-to-approve-sales-it-deems-safe-to-blacklisted-huawei-idUSKCN1U41GP (reporting that the Secretary of Commerce stated during a conference that the Department of Commerce will issue export licenses to Huwaei "where there is no threat to U.S. national security").

[91] *See* Release of "Technology" to Certain Entities on the Entity List in the Context of Standards Organizations, 85 Fed. Reg. 36719 (June 18, 2020) (codified at 15 C.F.R. pts. 744 and 772) [hereinafter Standards Organizations Rule]. *See also* Ari Schwartz, *Standards Bodies are Under Friendly Fire in the War on Huawei*, LAWFARE (May 5, 2020), https://www.lawfareblog.com/standards-bodies-are-under-friendly-fire-war-huawei.

[92] The EAR is located in 15 C.F.R. pts. 730-774.

[93] Temporary General License, 84 Fed. Reg. 23468, 23468-69 (May 22, 2019).

[94] August 20, 2020 Final Rule, *supra* note 81, at 51600.

third[95] and fourth[96] categories from export restrictions. Some commentators and stakeholders called for BIS to extend or adopt permanently all facets of the temporary general license, but BIS determined that the United States national security and foreign policy interests did not support maintaining the first and second categories of transactions.[97]

BIS also issues other licenses, known as *specific licenses*, that authorize individual U.S. companies to export to Huawei and its affiliates under defined conditions.[98] While the temporary general license automatically applied to all exporters that met its requirements, BIS only grants specific licenses to companies that apply for them.[99] For example, Microsoft Corp. (Microsoft) reportedly applied for and received a specific license to export certain "mass-market" software to Huawei and its affiliates.[100] Media outlets report that Commerce officials have told members of the semiconductor industry that it will grant licenses if companies can demonstrate their technology does not support 5G systems.[101]

Foreign Direct Product Rule and *De Minimis* Rules

While U.S. export restrictions in the EAR apply to all U.S. origin items, wherever located,[102] they can also apply to certain foreign-made items. Under the foreign direct product rule, the EAR applies to certain foreign-made goods that are created as a "direct product" of U.S.-origin items.[103] And under the *de minimis* rules, the EAR applies to items that contain more than certain specified percentages of U.S. content.[104] After Huawei was added to the Entity List in 2019, reports emerged that many U.S.-owned companies were able to use foreign subsidiaries and affiliates to continue exporting to Huawei under these rules.[105] In particular, Commerce found that

[95] BIS regulations permit disclosure to Huawei and affiliates of "information regarding security vulnerabilities in items owned, possessed, or controlled by Huawei or any of its non-U.S. affiliates when related to the process of providing ongoing security research critical to maintaining the integrity and reliability of existing and currently 'fully operational network' and equipment." *Id*. at 51629 (codified at 15 C.F.R. pt. 736 n.2).

[96] BIS regulations authorize release of certain technology to "members of standards organization without a license, including Huawei, if released for the purpose of contributing to the revision or development of a standard." *See* Standards Organizations Rule, *supra* note 90, at 36719.

[97] August 20, 2020 Final Rule, *supra* note 81, at 51598-600.

[98] *See, e.g.*, *U.S. Begins Issuing Some Licenses for Companies to Supply Goods to Huwaei*, REUTERS (Nov. 20, 2019), https://www.reuters.com/article/usa-china-huawei-tech/u-s-begins-issuing-some-licenses-for-companies-to-supply-goods-to-huawei-idUSL2N2800JU ("The U.S. Commerce Department confirmed Wednesday it has begun issuing licenses for some U.S companies to supply non-sensitive goods to China's Huawei Technologies Co. Ltd.").

[99] For additional analysis of U.S. export licensing policy, see CRS Report R41916, *supra* note 74, at 3.

[100] Stephen Nellis and Alexandra Alper, *Microsoft Granted License to Export "Mass-Market" Software to Huawei*, REUTERS (Nov. 21, 2019), https://www.reuters.com/article/us-microsoft-huawei/microsoft-granted-license-to-export-mass-market-software-to-huawei-idUSKBN1XV2LE. *See also* Josh Horwitz, *Intel gets U.S. Licenses to Supply Some Products to Huawei*, REUTERS (Sep. 22, 2020), https://www.reuters.com/article/intel-huawei-idUSKCN26D0I3.

[101] Kathrin Hille, Edward White, Kana Inagaki, *US Allows Sales of Chips to Huawei's non-5G Businesses*, FIN. TIMES (Oct. 28, 2020), https://www.ft.com/content/508b0828-bcd5-46a6-84f8-d05cb2887e0a.

[102] 15 C.F.R. § 743.4(a)(2).

[103] *Id.* §§ 734.4(a)(4), 736.2(b)(3).

[104] *Id.* § 734.4. For additional discussion of the de minimis rule and its components, see Bureau of Indus. and Sci., Dep't of Commerce, De Minimis Rules and Guidelines (Nov. 5, 2019), https://www.bis.doc.gov/index.php/documents/pdfs/1382-de-minimis-guidance/file.

[105] *See, e.g.*, Ian King and Jenny Leonard, *U.S. Companies Find Legal Ways Around Trump's Huawei Blacklist*, BLOOMBERG (June 25, 2019), https://www.bloomberg.com/news/articles/2019-06-26/u-s-companies-are-finding-a-legal-way-around-huawei-blacklist; Dan Strumpf et al., *American Tech Companies Find Ways Around Huawei Ban*, WALL ST. J. (June 25, 2019), https://www.wsj.com/articles/american-tech-companies-find-ways-around-huawei-ban-

Huawei "continued to use U.S. software and technology to design semiconductors, undermining the national security and foreign policy purposes of the Entity List by commissioning their production in overseas foundries using U.S. equipment."[106]

To counteract this trend, BIS amended the foreign direct product rule twice in 2020 so that it has broader application to Huawei and its affiliates on the Entity List.[107] The amended rule makes technical changes to the EAR designed to prevent Huawei from acquiring microchips made outside the United States that are developed or produced with tools sourced from the United States.[108] Although the rule changes are technical, some commentators view them as likely to cause a major disruption to Huawei's manufacturing capability.[109] Other observers assert that the rule change will adversely affect the U.S. semiconductor industry and other American technology companies that sell products used in Huawei's supply chains.[110] Commerce and Department of State officials contend the change is necessary to prevent Huawei and its affiliates from circumventing U.S. export restrictions.[111]

Media outlets reported in 2020 that the Trump Administration also was considering modifying the *de minimis* rules in an attempt to limit transactions further with Huawei involving U.S.-sourced items.[112] The *de minimis* rules permits companies that make and export products to Huawei from outside the United States to incorporate U.S. components, technology, and software if the U.S. content does not exceed 25% of the product's value.[113] News outlets reported that the Trump

11561517591.

[106] U.S. Dep't of Commerce, Office of Pub. Affairs, *Commerce Addresses Huawei's Efforts to Undermine Entity list, Restricts Products Designed and Produced with U.S. Technologies* (May 15, 2020), https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts.

[107] *See* Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, 85 Fed. Reg. 97 (May 19, 2020) (codified as amended at 15 C.F.R. pt. 744 n.1); August 20, 2020 Final Rule, *supra* note 81, at 51629 (codified at 15 C.F.R. pt. 744 n.1).

[108] The changes to the foreign direct product rule for Huawei and its affiliates on the Entity List are codified at footnote 1 to 15 C.F.R. pg. 744. *See also* U.S. Dep't of Commerce, Office of Pub. Affairs, *Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List*, (Aug. 17, 2020), https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and ("This amendment further restricts Huawei from obtaining foreign made chips developed or produced from U.S. software or technology to the same degree as comparable U.S. chips.").

[109] *See*, *e.g.*, *Life is Getting Much Harder for Huawei*, BLOOMBERG (Aug. 20, 2020), https://www.bloomberg.com/news/newsletters/2020-08-21/life-is-getting-much-harder-for-huawei.

[110] *See*, *e.g.*, Semiconductor Indus. Ass'n, *SIA Statement on Export Control Rule Changes*, (Aug. 17, 2020), https://www.semiconductors.org/sia-statement-on-export-control-rule-changes-2/; Richard Altieri and Benjamin Della Rocca, *U.S. Further Tightens Huawei Blacklist, Putting a "Blanket Ban" on the Company*, LAWFARE (Aug. 28, 2020).

[111] *See Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List*, *supra* note 108; Michael R. Pompeo, U.S. Sec'y of State, Press Statement, *The United States Further Restricts Huawei Access to U.S. Technology*, (Aug. 17, 2020), https://www.state.gov/the-united-states-further-restricts-huawei-access-to-u-s-technology/. ("[The amended] Foreign Direct Product Rule . . . will prevent Huawei from circumventing U.S. law through alternative chip production and provision of off-the-shelf (OTS) chips produced with tools acquired from the United States.").

[112] *See*, *e.g.*, Alexandra Alper et al., *Trump Administration Moves Toward Blocking More Sales to Huawei: Sources*, REUTERS (Jan 14, 2020), https://www.reuters.com/article/us-usa-huawei/trump-administration-moves-toward-blocking-more-sales-to-huawei-sources-idUSKBN1ZD2VD; Bob Davis and Katy Stech Ferek, *Tech Tensions Simmer in Washington as U.S., China Near Trade Truce*, WALL ST. J. (Jan. 14, 2020), https://www.wsj.com/articles/tech-tensions-simmer-in-washington-as-u-s-china-near-trade-truce-11579041159.

[113] 15 C.F.R. § 734.4(d).

Administration considered reducing the *de minimis* threshold to 10% for Huawei transactions,[114] and the 116th Congress introduced at least one bill that would require Commerce to reduce the threshold,[115] but thus far no change has been made.

Conditions on Huawei's Removal from the Entity List

Normally, an interagency committee[116] in the executive branch chaired by Commerce is responsible for "all decisions to make additions to, removals from or changes to the Entity List."[117] In Huawei's case, however, Congress placed conditions on Commerce's ability to remove Huawei from the list.[118] The National Defense Authorization Act for Fiscal Year 2020 (2020 NDAA; Pub. L. No. 116-92) provides that the Secretary of Commerce may not remove Huawei from the Entity List unless the Secretary certifies[119] that four conditions exist:

1. Huawei has resolved the charges that were the basis for its addition to the Entity List;
2. Huawei has resolved any other charges that it violated U.S. sanctions;
3. "[R]egulations have been implemented that sufficiently restrict exporting to, and importing from, the United States items that would pose a national security threat" to U.S. telecommunications systems;
4. Commerce has mitigated, to the maximum extent possible, other threats to U.S. national security posed by Huawei.[120]

The 2020 NDAA also requires Commerce to provide an annual report describing licenses issued for exports to Huawei.[121]

Executive Orders Under the International Emergency Economic Powers Act (IEEPA)

Although U.S. export restrictions have significant legal and economic consequences, they do not affect all transactions involving Huawei and U.S. companies. In particular, the addition of Huawei to the Entity List does not, on its own accord, prevent *importing* Huawei products into the United States.[122] Under the International Emergency Economic Powers Act (IEEPA), the

[114] *See supra* note 112.

[115] S. 3316, 116th Cong. (2020).

[116] *See supra* note 82.

[117] 15 C.F.R. pt. 744, supp. 5.

[118] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1260I (2019).

[119] Commerce must provide its certification to the Senate Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence of the Senate, the House Committee on Foreign Affairs, and the House Permanent Select Committee on Intelligence. *Id.* § 1260I(c)(1).

[120] *Id.* § 1260I(a)(1-4).

[121] *Id.* § 1260I(b).

[122] *Accord* Bureau of Indus. and Sci., U.S. Dep't of Commerce, Huawei Entity List and Temporary General License Frequently Asked Questions (FAQs) at 2, (Sep. 18, 2019), https://www.bis.doc.gov/index.php/documents/pdfs/2447-huawei-entity-listing-faqs/file ("Imports of Huawei goods into the United States are not impacted by the addition of Huawei and its affiliates to the Entity List.").

President possesses much broader authority to influence Huawei imports and other Huawei-related transactions and property interests.[123]

IEEPA grants the President power to regulate diverse economic transactions when the President declares that a national emergency exists.[124] Upon an emergency declaration, the President may (subject to certain exceptions[125]) investigate, regulate, or prohibit foreign exchange transactions, transfers of credit involving foreign nationals or foreign countries, and imports or exports of currency and securities involving any persons or property subject to U.S. jurisdiction.[126] IEEPA also allows the President to block or "freeze"[127] foreign-owned property and assets.[128]

Executive Order 13873: Information and Communications Technology and Services

On May 15, 2019 (the same day Commerce announced the addition of Huawei to the Entity List), President Trump issued Executive Order 13873.[129] In that executive order, President Trump declared that a national emergency exists because of the threat of foreign adversaries creating and exploiting vulnerabilities in information and communications technology and services (ICTS).[130] In response to this threat, Executive Order 13873 prohibits various transactions[131] involving foreign-owned[132] ICTS when Commerce, in consultation with other executive branch agencies,[133] makes two determinations.[134]

First, Commerce must determine that the transaction involves ICTS designed, developed, manufactured, or supplied by persons or entities owned by, controlled by, or subject to the jurisdiction or direction of a *foreign adversary.*[135] The executive order defines foreign adversary

[123] Pub. L. No. 95-223, 91 Stat. 1626 (1977) (codified as amended at 50 U.S.C. §§ 1701-1708).

[124] For detailed analysis of IEEPA, see CRS Report R45618, *The International Emergency Economic Powers Act: Origins, Evolution, and Use*, coordinated by Christopher A. Casey.

[125] Exceptions to IEEPA authority are defined in 50 U.S.C. § 1702(b).

[126] 50 U.S.C. § 1702(a)(1)(A).

[127] "Blocking" and "freezing" generally are synonymous terms that refer to an "across-the-board prohibition against transfers or dealings of any kind with regard to the property." *See* U.S. Dep't of the Treasury, *OFAC FAQs: General Questions* (last updated Feb. 6, 2019), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx.

[128] 50 U.S.C. § 1702(a)(1)(B).

[129] Exec. Order No. 13873 of May 15, 2019, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (published May 17, 2019).

[130] *Id.*

[131] The term "transaction" in Executive Order 13873 includes any "acquisition, importation, transfer, installation, dealing in, or use . . . ." *Id.* § 1.

[132] *Id.* More specifically, the transaction must involve property in which a foreign country or foreign national has any interest, including through an interest in a contract for the provision of the technology or service. *Id.*

[133] Executive Order 13873 directs the Secretary of Commerce to consult 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 (agencies)…." *Id.*

[134] In addition to the requisite determinations by Commerce, in order to fall under Executive Order 13873, the transaction must post-date the executive order and be made by an individual or entity subject to U.S. jurisdiction or involve property subject to U.S. jurisdiction. *Id.* § 1(a).

[135] *Id.* § 1(a)(i).

as those "engaged in a long-term pattern or serious instances of conduct significantly adverse" to U.S. security or the safety of U.S. persons.[136] In its regulations implementing the order, discussed below,[137] Commerce identified China (including Hong Kong), Cuba, Iran, North Korea, Russia, and the Nicolás Maduro regime[138] in Venezuela as foreign adversaries.[139]

Second, to fall within the scope of Executive Order 13873, Commerce must determine that the transaction presents:

1. An undue risk of sabotage or subversion to ICTS in the United States;
2. An undue risk of catastrophic effects on the security or resiliency of critical infrastructure or the digital economy in the United States; or
3. Unacceptable risk to U.S. national security or the security and safety of U.S. persons.[140]

Executive Order 13873 authorizes the Secretary of Commerce to develop rules and regulations to implement the order and to employ all powers granted to the President by IEEPA.[141] Some observers interpreted the order as designed to, among other things, address the risks posed by Huawei and other Chinese communications equipment manufacturers.[142]

ICTS Review Process

In January 2021, Commerce issued an interim final rule (ICTS Rule) which implements Executive Order 13873 in a way that differs from many prior IEEPA-based national emergencies.[143] Many executive orders that invoke IEEPA lead to the compilation of a list of individuals[144] or entities[145] with whom transactions are restricted.[146] Other IEEPA-based executive orders prohibit transactions involving specific items.[147] In the ICTS Rule, however, Commerce

[136] *Id.* § 3(b).

[137] *See infra* § ICTS Review Process.

[138] For background on the Maduro regime the competing claims to recognition as Venezuela's government, see CRS Report R44841, *Venezuela: Background and U.S. Relations*, coordinated by Clare Ribando Seelke.

[139] Securing the Information and Technology and Services Supply Chain, Interim Final Rule; Request for Comments, 86 Fed. Reg. 4909 (2021) (codified at 15 C.F.R. pt. 7) [hereinafter ICTS Rule]. The Secretary of Commerce has discretion to revise the list of foreign adversaries "as necessary." 15. C.F.R. § 7.4.

[140] Exec. Order No. 13873, *supra* note 129, § 1(a)(ii).

[141] *Id.* § 2.

[142] *See, e.g.*, *President Trump Issues Executive Order Seemingly Aimed at China and Huawei*, TIME (May 15, 2019), http://time.com/5589947/executive-order-huawei-products/; Dan Strumpf, Toko Kubota, and Wenxin Fan, *Silicon Valley Will Feel Sting of Export Restrictions Against Huawei*, WALL ST. J. (May 16, 2019), https://www.wsj.com/articles/silicon-valley-will-feel-sting-of-export-restrictions-against-huawei-11558021918 ("The Commerce Department action was paired with a White House executive order seen as a precursor to a ban on selling Huawei-made products in the U.S.").

[143] See ICTS Rule, 86 Fed. Reg. at 4909. For additional information on the ICTS Rule, see CRS In Focus IF11760, *The Information and Communications Technology and Services (ICTS) Rule and Review Process*, by Stephen P. Mulligan.

[144] *See, e.g.*, Exec. Order No. 13818, Annex A, Blocking the Property of Persons Involved in Serious Human Rights Abuse or Corruption, 82 Fed. Reg. 60839 (issued Dec. 20, 2017).

[145] *See, e.g.*, Exec. Order. 13942, Addressing the Threat Posed by TikTok, and Taking Additional Steps to Address the National Emergency with Respect to Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 48637 (issued Aug. 6, 2020); Exec. Order No. 13581, Annex A, Blocking Property of Transnational Criminal Organizations, 76 Fed. Reg. 44757 (issued July 24, 2011).

[146] *See* CRS Report R45618, *supra* note 124, at 19 (surveying IEEPA executive orders).

[147] *See, e.g.*, Exec. Order. No. 12735, Chemical and Biological Weapons Proliferation, 55 Fed. Reg. 48587 (issued

has established a new review process through which the Secretary of Commerce will evaluate individual transactions on a "case-by-case basis, based upon the particular facts and circumstances" to determine whether they raise the risks described in Executive Order 13873.[148] Because the rule regulates individual *ICTS transactions*—broadly defined as "any acquisition, importation, transfer, installation, dealing in, or use of any [ICTS]"[149]—it could subject a wide range of commercial interactions to a new review process.[150]

The ICTS Rule provides three ways to initiate review of a transaction: (1) Commerce can unilaterally begin review at the Secretary of Commerce's discretion; (2) other federal agencies can request that Commerce review a transaction; or (3) Commerce can begin review upon receipt of public or other types of information.[151] Commerce also plans to create a licensing process through which companies can seek pre-approval for a proposed or pending ICTS transaction.[152] If, after an initial review, Commerce concludes that an ICTS transaction may pose an undue or unacceptable risk, Commerce must engage in an interagency consultation.[153] After the consultation, Commerce will make an initial determination on whether to permit a transaction, prohibit it, or propose measures to mitigate risks.[154] Unless it permits the transaction in full, Commerce must provide a written determination to the parties.[155] Next, the parties have 30 days to respond to the initial determination and propose their own remedial measures.[156] If the parties respond,[157] Commerce must engage in a second interagency consultation.[158] After that consultation, Commerce may issue a final, written determination on whether the transaction is prohibited, not prohibited, or permitted subject to an agreement on risk-mitigation measures.[159] The total process must be completed within 180 days, unless Commerce determines in writing that additional time is necessary.[160] Violation of Commerce's final determination can result in civil and criminal penalties.[161]

To be subject to the ICTS review process, a transaction must meet several criteria. An individual or entity owned, controlled by, or subject to the jurisdiction of a foreign adversary must conduct

---

Nov. 16, 1990).

[148] ICTS Rule, 86 Fed. Reg. at 4909.

[149] 15 C.F.R. § 7.2.

[150] *See* ICTS Rule, 86 Fed. Reg. at 4911 ("The Department [of Commerce] acknowledges that the term[] "transaction," . . . [is] broad, and retain[s] [its] commonly-accepted meaning[] in the rule."); Alan Enslen and Julius Brodie, *Commerce Rules May Heighten Network Security Enforcement*, LAW360 (Jan. 3, 2020), https://www.law360.com/articles/1230258/commerce-rules-may-heighten-network-security-enforcement ("The proposed regulations are far reaching and stand to impact a wide range of industries, as the ICTS sector is integrated into just about every significant U.S. industry imaginable . . . .").

[151] 15 C.F.R. § 7.103.

[152] ICTS Rule, 86 Fed. Reg. at 4913. The ICTS Rule states that Commerce intends to publish procedures governing the licensing process by March 15, 2020. *Id.*

[153] 15 C.F.R. § 7.104.

[154] *Id.* § 7.105.

[155] *Id.* § 7.105(b). The initial determination may be served on the parties or published in the Federal Register. *Id.* § 7.105(b)(2).

[156] *Id.* § 7.107.

[157] If the parties do not respond to the initial determination within 30 days, Commerce may issue a final determination without undertaking a second interagency consultation. *Id.* § 7.107(f).

[158] *Id.* § 7.108.

[159] *Id.* § 7.109.

[160] *Id.* § 7.109(b).

[161] *Id.* § 7.200.

the transaction.[162] The transaction must have a nexus to the United States by involving property subject to U.S. jurisdiction or being conducted by an individual or entity subject to U.S. jurisdiction.[163] The transaction also must involve property in which a foreign country or foreign national has an interest, and the process only applies to transactions initiated, pending, or completed after January 19, 2021.[164] Finally, the transaction must involve one of the following types of technology:

1. ICTS that will be used by a party to a transaction in a critical infrastructure sector, as designated in Presidential Policy Directive 21 (PPD 21);[165]
2. Software, hardware, or any other product or service integral to wireless local area networks, mobile networks, satellite payloads, satellite operations and control, cable access points, wireline access points, core networking systems, or long- and short-haul systems;
3. Software, hardware, or products or services integral to data hosting or computing services that process or are expected to process sensitive personal data on more than one million U.S. persons;
4. Certain ICTS products—including webcams, routers, modems, and drones—when more than one million units have been sold to U.S. persons;
5. Software designed primarily for connecting with and communicating on the Internet that is in use by more than one million U.S. persons; or
6. ICTS that is integral to artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics.[166]

The ICTS Rule excludes from review a U.S. person's acquisition of ICTS items as part of a U.S. government-industrial security program because those acquisitions are subject to other forms of

[162] *Id.* §§ 7.2-7.3. When determining whether the foreign adversary requirement is met, Commerce may consider:

> (1) whether the party [to the transaction] or its component suppliers have headquarters, research, development, manufacturing, test, distribution, or service facilities or other operations in a foreign country, including one controlled by a foreign adversary; (2) personal and professional ties between the party—including its officers, directors or similar officials, employees, consultants, or contractors—and any foreign adversary; (3) laws and regulations of the foreign adversary in which the party is headquartered or conducts operations, including research and development, manufacturing, packaging, and distribution; and (4) any other criteria that the Secretary deems appropriate.

Id. § 7.100(c).

[163] *Id.* § 7.3(a).

[164] *Id.*

[165] PPD 21 designates the following critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; nuclear reactors, materials and waste; transportation systems; and waste and wastewater systems. Presidential Policy Directive – Critical Infrastructure Security and Resilience, (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[166] 15 C.F.R. § 7.3(a)(4).

U.S. government oversight. [167] It also excludes any transaction that CFIUS, discussed above, [168] is actively reviewing or has reviewed.[169]

Executive Order 13959: Securities Ban

In November 2020, President Trump issued his second Huawei-related executive order using IEEPA authority, Executive Order 13959, *Addressing the Threat from Securities Investments that Finance Chinese Military Companies*.[170] The executive order prohibits U.S. persons from engaging in any transaction in publicly traded securities of any *Communist Chinese Military Company* (CCMC), effective January 11, 2021.[171] It also prohibits any transaction in securities that are derivative of, or designed to provide investment exposure to such publicly traded securities.[172] Companies that purchased such securities before the order's effective date must divest them by November 11, 2021.[173] The definition of CCMC is derived from the National Defense Authorization Act for Fiscal Year 1999, as amended (1999 NDAA; Pub. L. No. 105-261), which defines CCMC as an entity that is (i) owned or controlled by, or affiliated with, the People's Liberation Army or a ministry of the Chinese government, or that is owned or controlled by an entity affiliated with the Chinese government's defense industrial base; and (ii) is engaged in commercial services, manufacturing, producing, or exporting.[174] Huawei is included in the list of CCMCs, which the Secretary of Defense prepares.[175]

Other Supply Chain Protection Initiatives

Other executive branch agencies have started efforts to protect U.S. communications networks from alleged security threats potentially caused by Huawei and other entities. For example, in November 2018, the Department of Homeland Security convened the Information and Communications Technology Supply Chain Risk Management Task Force—a public-private partnership formed to provide recommendations on how to identify and manage risk to the global information and telecommunications supply chain.[176] The Department of State engaged in the Multilateral Action on Sensitive Technologies (MAST) process, a group of 15 nations that meet to

[167] *Id.* § 7.3(b)(1). *See also* ICTS Rule, 86 Fed. Reg. at 4913.

[168] *See supra* § Early Legal Actions and Congressional Interest.

[169] 15 C.F.R. § 7.3(b)(2).

[170] Exec. Order No. 13959 of Nov. 12, 2020, *Addressing the Threat from Securities Investments that Finance Chinese Military Companies*, 85 Fed. Reg. 73185 (published Nov. 17, 2020) [hereinafter Exec. Order 13959].

[171] *Id.* § 1(a).

[172] *Id.*

[173] *Id.* § 1(b).

[174] *See* Pub. L. No. 105-261, § 1237, as amended by Pub. L. No. 106-398, § 1233 and Pub. L. No. 108-375, § 1222 (codified at 50 U.S.C. § 1701 note).

[175] Exec. Order 13959, *supra* note 170, at Annex. The executive order labels "Huawei" as a CCMC, and it does not identify any specific Huawei corporate entity or entities. *Id.*

[176] Dep't of Homeland Sec., Press Release, *DHS Announces ICT Supply Chain Risk Management Task Force Members* (Nov. 15, 2018), https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members. *See also* DEP'T OF HOMELAND SEC., INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE: INTERIM REPORT (Sep. 2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

share information about technology transfer threats.[177] And the SECURE Technology Act,[178] which became law in December 2018, established an interagency Federal Acquisition Security Council (FASC).[179] The FASC is responsible for, among other things, developing a government-wide strategy that addresses information and telecommunications supply chain risks and facilitates information-sharing within the government and with the private sector.[180]

Federal Communications Commission's Actions

The FCC and the U.S. Congress have taken steps to restrict Huawei's access to U.S. telecommunications infrastructure. These actions primarily affect smaller telecommunications carriers who rely on the Universal Service Fund (USF). The USF subsidizes, among other things, voice and broadband internet service in rural and high-cost areas.[181] Federal law requires long-distance telecommunications carriers (such as AT&T and Verizon) to contribute a percentage of their revenue to maintain the USF,[182] and the FCC uses the fund to support eligible telecommunications carriers (ETCs) that serve high-cost areas.[183]

In November 2019, the FCC issued an order (2019 Order) prohibiting ETCs from using USF funds to purchase Huawei or ZTE equipment or services.[184] At the same time, it issued a Further Notice of Proposed Rulemaking (2019 FNPRM) that proposed requiring ETCs to remove and replace existing Huawei and ZTE equipment from their networks (often called "rip-and-replace"[185]) and proposed establishing a reimbursement program to cover the cost of the removal and replacement.[186]

Following the FCC's adoption of its order and proposed rule, Congress passed the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act), which the President signed into law in March 2020.[187] Like the 2019 Order, the Secure Networks law prohibits companies from using FCC administered subsidies to obtain or maintain "covered communications equipment or services" that pose national security risks to U.S. communications networks, including certain Huawei or ZTE equipment.[188] The Secure Networks Act also directs the Commission to establish a rip-and-replace reimbursement program, similar to the one

[177] *See* Remarks by Dr. Christopher Ashley Ford, Assistant Sec., Bureau of Int'l Sec. and Nonproliferation, Conference on Great Power Competition, Bureaucracy and Counterstrategy: Meeting the China Challenge (Sep. 11, 2019), https://www.state.gov/bureaucracy-and-counterstrategy-meeting-the-china-challenge/. [hereinafter Ford Remarks].

[178] Pub. L. No. 115-390, 132 Stat. 5173.

[179] The Federal Acquisition Security Council includes representatives from the Office of Management and Budget (which also chairs the Council), GSA, DHS, ODNI, DOJ, DOD, and Commerce. *See* 41 U.S.C. § 1321.

[180] *Id.* § 1323.

[181] *In re* Universal Serv. Fund Telephone Billing Practices Litig., 300 F. Supp. 2d 1107, 1114 (D. Kan. 2003); *Universal Service*, FCC, https://www.fcc.gov/general/universal-service (last visited Feb. 1, 2021).

[182] 47 U.S.C. § 254(d).

[183] *Id.* §§ 214(e), 254(e).

[184] In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd. 11423 (2019) [hereinafter 2019 Order and FNPRM].

[185] *See, e.g.*, Ajit Pai, *Protecting National Security and Public Safety*, FCC (Oct. 28, 2019), https://www.fcc.gov/news-events/blog/2019/10/28/protecting-national-security-and-public-safety.

[186] 2019 Order and FNPRM, 34 FCC Rcd. at 11470, para. 122.

[187] 47 U.S.C. §§ 1601–1609 (2020).

[188] *Id.* §§ 1601–1602.

contemplated in the 2019 FNPRM, and requires ETCs to remove covered equipment if they participate in that program.[189]

The FCC has taken steps to implement the Secure Networks Act, most notably by adopting another final order in December 2020.[190] This order establishes the reimbursement program required by the Secure Networks Act.[191] The order also goes beyond the Secure Networks Act by requiring carriers receiving USF support to remove and replace existing covered equipment in their networks, regardless of whether they choose to participate in the reimbursement program.[192] Shortly after this final order was adopted, Congress passed the Consolidated Appropriations Act, 2021 (Pub. L. No. 116-260), which provides funding for the reimbursement program and makes several changes to the program's scope.

These actions have significant implications for rural carriers and their customers and are discussed further below.

Rural Telecommunications Carriers and Huawei

While larger carriers such as AT&T and Verizon have indicated they do not use Huawei equipment in their U.S. networks,[193] many rural carriers use Huawei's technology in their networks for cost reasons.[194] For instance, the Rural Wireless Association (RWA), a trade association representing providers of wireless phone and broadband service, estimated in 2018 that 25% of its members had deployed Huawei or ZTE equipment in their networks.[195] Because rural carriers rely on the USF to operate, these limitations on USF recipients' use of Huawei equipment have significant implications for Huawei's presence in the nation's communications network.[196]

[189] *Id.* § 1603.

[190] In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Second Report and Order, 35 FCC Rcd. 14284 (Dec. 11, 2020).

[191] *Id.* at 14285, para. 1.

[192] *Id.* at 14290–14309, paras. 17–50.

[193] *See, e.g.*, Jessica Bursztynsk, *Verizon CEO: We're Doing Just Fine Without Using Any Equipment from Chinese Tech Giant Huawei*, CNBC (July 11, 2019), https://www.cnbc.com/2019/07/11/ceo-hans-vestberg-says-verizon-does-not-use-any-huawei-equipment.html; David Shepardson, *AT&T CEO Says China's Huawei Hinders Carriers from Shifting Suppliers for 5G*, REUTERS (March 20, 2019), https://www.reuters.com/article/us-att-ceo-huawei-tech/att-ceo-says-chinas-huawei-hinders-carriers-from-shifting-suppliers-for-5g-idUSKCN1R12TX; Todd Shields, *T-Mobile CEO to Congress: We Won't Use Huawei Equipment After Spring Acquisition*, FORTUNE (Feb. 12, 2019), https://fortune.com/2019/02/12/t-mobile-congress-testimony-huawei-equipment-sprint-acquisition/; Dianne Zatz, Liana B. Baker, Greg Roumeliotis, *Exclusive: T-Mobile, Sprint see Huawei Shun Clinching U.S. Deal – Sources*, REUTERS (Dec. 14, 2018), https://www.reuters.com/article/us-sprint-corp-m-a-tmobile-huawei-exclu/exclusive-t-mobile-sprint-see-huawei-shun-clinching-u-s-deal-sources-idUSKBN1OD2HO.

[194] Rural Wireless Association, Reply Comments, In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89, at i (July 2, 2018) [hereinafter RWA NPRM Reply Comments] ("[M]any RWA members and other rural wireless carriers have lowered costs by utilizing less costly Chinese-manufactured network infrastructure equipment to provide wireless broadband service to rural America.").

[195] Rural Wireless Association, Reply Comments, In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89, at 15 (Dec. 7, 2018) [hereinafter RWA NDAA Reply Comments] (estimating that "at least 25% of its carrier members would be impacted" by a requirement to "rip-and-replace" Huawei or ZTE equipment.).

[196] RWA NPRM Reply Comments, *supra* note 194, at 10–11 (Explaining that its members rely on USF funds because, due to "[l]ow population density, high poverty rates, difficult terrain, and challenging weather conditions in many rural

2019 Order

In November 2019, the FCC adopted the 2019 Order, prohibiting ETCs from using USF funds to purchase, upgrade, maintain, or otherwise support any services or equipment provided by Huawei and ZTE.[197] To support its action, the FCC explained that Congress and the executive branch had repeatedly raised concerns over the threat of foreign actors exploiting U.S. communications networks.[198] The Commission cited, in particular, congressional and executive actions such as the 2019 NDAA and Executive Order 13873.[199] The 2019 Order also states that the Commission found it "very significant" that the DOJ supported its conclusion that USF funds should "be used to deploy infrastructure and provide services that do not undermine our national security."[200]

The FCC further reasoned that the record supported specifically designating Huawei and ZTE as the initial entities covered by the USF fund prohibition.[201] The 2019 Order states that both companies have "ties to the Chinese government and military apparatus," and it cites the 2012 HPSCI report for the proposition that Chinese state security laws obligate these companies "to cooperate with any request by the Chinese government to use or access their systems."[202] The FCC rejected Huawei's arguments that its U.S. affiliates are not subject to these state security laws, reasoning that affiliates remain subject to Chinese law "[i]rrespective of their physical location."[203] While the 2019 Order's designation of Huawei and ZTE as covered entities only served as an "initial designation," the 2019 Order gives the FCC's Public Safety and Homeland Security Bureau (PSHSB) authority to make a final designation after a period of public comments.[204] It further directs the PSHSB to make future determinations about whether to designate additional companies or to reverse earlier determinations.[205] On June 30, 2020, following the comment period, the PSHB issued its final designation decision on Huawei and ZTE, naming them as covered entities (Designation Orders).[206] Huawei sought review of the designation, but, on Dec. 11, 2020, the Commission rejected its challenges and upheld the PSHB's designation.[207]

parts of the country . . . there is simply not a business case for rural wireless broadband service providers to provide service absent USF support.").

[197] 2019 Order and FNPRM, 34 FCC Rcd. at 11423.

[198] *Id.* at 11425–28, paras. 6–17.

[199] *Id.* at 11427–29, paras. 13, 17. *See* §§ 2019 NDAA and Executive Order 13873, *infra*, for a further discussion of these actions.

[200] 2019 Order and FNPRM, 34 FCC Rcd. at 11433, ¶ 28.

[201] *Id.* at 11439–41, paras. 43–46.

[202] *Id.* at 11442, para. 48.

[203] *Id.* at 11442, para. 49. Among other things, the Order refers to the fact that the "Chinese government maintains an internal Communist Party Committee within Huawei that can exert additional influence on the company's operations and decisions." *Id.* at 11443, para. 50.

[204] *Id.* at 11449, para. 65.

[205] 2019 Order and FNPRM, 34 FCC Rcd. at 11449, para. 64.

[206] In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation, Order, 35 FCC Rcd. 6604 (June 30, 2020); In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation, Order, 35 FCC Rcd. 6633 (June 30, 2020).

[207] In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation, Memorandum Opinion and Order, 35 FCC Rcd. 14435 (Dec. 11, 2020).

As a legal basis for the 2019 Order's prohibition, the FCC reasoned that its "authority to place reasonable public interest conditions on the use of USF funds" is "well established."[208] The FCC explained that Section 254 of the Communications Act allows the Commission to consider the extent to which USF-supported telecommunications services are "consistent with the public interest, convenience, and necessity."[209] More generally, section 201(b) of the Communications Act allows the Commission to promulgate rules and regulations "as may be necessary in the public interest to carry out the provisions of [the] Act."[210] The FCC wrote that it is "well established" that "promotion of national security is consistent with the public interest" because Section 1 of the Communications Act states that the FCC was created for, among other things, "the purpose of national defense [and] for the purpose of promoting safety of life and property."[211] The 2019 Order also states that it is implementing or otherwise furthering the goals of other federal laws, including Section 889 of the 2019 NDAA[212] and federal law that prohibits unauthorized surveillance in telecommunication carriers' networks.[213]

Huawei has petitioned for review of the 2019 Order in the U.S. Court of Appeals for the Fifth Circuit.[214] While this case remains ongoing, one key issue is the extent to which the Communications Act allows the FCC to consider national security as part of its public-interest analysis. In its briefing, Huawei argues that the Act does not allow the Commission to make national security determinations—both in the universal service context and generally—because, among other things: (1) national security does not further any of the statutorily enumerated goals of the universal service program;[215] (2) whenever the Act confers power to make national security judgments, it gives it to the President, rather than the Commission;[216] and (3) the Act's public-interest standard must be interpreted based on the broader context of the Act and "cannot be interpreted to give national security authority to the FCC, when that authority is statutorily and constitutionally committed to the President."[217]Along with the arguments based on the Communications Act, Huawei's briefing makes several other statutory and constitutional arguments. For instance, Huawei argues that the 2019 Order is "arbitrary and capricious" in violation of the Administrative Procedure Act because, among other thing, it ignores evidence that the rule would undermine the purposes of the USF provision.[218] Huawei further argues that the Order's initial designation of Huawei violated the Constitution's Due Process Clause by

[208] 2019 Order and FNPRM, 34 FCC Rcd. at 11434, para. 29.

[209] *Id.* at 11434–35, paras. 31–33.

[210] *Id.* at 11436, para. 34.

[211] *Id.* at 11435–36, paras. 33–34.

[212] *See supra* § 2019 NDAA.

[213] *See* Communications Assistance in Law Enforcement Act, 47 U.S.C. § 1004 (requiring telecommunications carriers to ensure "any interception of communications or access to call-identifying information effected within its switching premises" is done only pursuant to "lawful authorization" and with "affirmative intervention of an individual officer or employee of the carrier acting in accordance with [FCC regulations]").

[214] Petition for Review, Huawei Technologies USA, Inc. v. FCC, No. 19-60896 (5th Cir. Dec. 4, 2019) [hereinafter Huawei Petition].

[215] Petitioners Brief, Huawei Technologies USA, Inc. v. FCC, No. 19-60896, at 27–30 (5th Cir. Mar. 26, 2020) [hereinafter Huawei Brief]. Section 254(b) enumerates several "principles" on which the Commission "shall base policies for the preservation and advancement of universal service," including providing "access to advanced telecommunications and information services" in "all regions of the Nation" and providing consumers "in rural, insular, and high cost areas" with "access to telecommunications and information services." 47 U.S.C. § 254(b).

[216] Huawei Brief, *supra* note 215, at 28–29.

[217] *Id.* at 33–35.

[218] *Id*. at 44–51.

depriving it of its "constitutionally protected reputational interests" without affording an adequate pre-deprivation hearing.[219]

2019 FNPRM

Along with the Order, the FCC issued the 2019 FNPRM.[220] In the 2019 FNPRM, the Commission proposed to condition any future USF support on recipients agreeing not to use equipment or services from "covered companies" for a period of time.[221] The proposed covered companies would be the same companies designated national security threats under the 2019 Order (*i.e.*, Huawei and ZTE).[222] The FCC also proposed requiring ETCs receiving USF funds to remove and replace existing equipment and services provided by covered companies from their network operations.[223] To mitigate the cost of this replacement, the FCC proposed to establish a "reimbursement program" that would offset "reasonable transition costs."[224] The FCC proposed seeking an "appropriation or authorization of funds from Congress" to fund this reimbursement program.[225] It also sought comment on the appropriate funding needed to cover replacement costs, noting that the estimated costs of removing and replacing the covered equipment varied, with one commentator estimating it at "approximately $150 million plus installation" and another estimating costs of "$800 million to $1 billion."[226]

Secure Networks Act

Overview

With the Secure Networks Act (Pub. L. No. 116-124), signed into law in March 2020, Congress acted to provide additional statutory grounds and direction for the FCC's current efforts to limit Huawei's presence in the U.S. communications network.[227]

Much like the 2019 Order, the Secure Networks Act prohibits companies from using FCC administered subsidies to obtain or maintain communications equipment or services that pose national security risks to U.S. communications networks.[228] The Act directs the FCC to publish a list of the equipment and services subject to this limitation (the Covered List).[229] Equipment or services must meet two conditions for it to be added to the Covered List. First, either (1) certain agencies have made a "specific determination" that the particular equipment or services are a national security risk[230] or (2) the equipment or services are covered by section 889(f)(3) of the

[219] *Id.* at 57–63. The federal district court presiding over Huawei's challenge to Section 889 of the 2019 NDAA rejected a similar due process challenge. *See* Memorandum Opinion and Order at 51-53, Huawei Technologies USA, Inc. v. United States, No. 4:19-cv-00159 (E.D. Tex. Feb. 18, 2020).

[220] 2019 Order and FNPRM, 34 FCC Rcd. at 11470, para. 122.

[221] *Id.*

[222] *Id.* at 11472, para. 127.

[223] *Id.* at 11470, para. 122.

[224] *Id.*

[225] *Id.* at 11476–77, para. 143.

[226] *Id.* at 11477, paras. 144–145.

[227] Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. §§ 1601–1609 (2020).

[228] *Id.* §§ 1601–1602.

[229] *Id.* § 1601(a).

[230] The determination must have been made by an "appropriate national security agency," an "executive interagency

2019 NDAA (*i.e.*, be equipment or services provided by Huawei and ZTE).[231] Second, the equipment or services must be "capable of" (1) "routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles," (2) "causing the network of a provider of advanced communications service to be disrupted remotely," or (3) "otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons."[232]

Furthermore, similar to the 2019 FNPRM, the law directs the FCC to implement a so-called "rip-and-replace" reimbursement program.[233] Under this program, small[234] communications providers would be reimbursed for the cost of removing and replacing equipment on the Covered List.[235] To participate in the program, applicants would have to provide an "initial reimbursement cost estimate" and supporting materials.[236] While participation in the program is voluntary, providers who chose to participate in the program must complete the "permanent removal, replacement, and disposal" of covered equipment or services within one year of receiving the funds, unless the FCC grants an extension.[237] While the law does not expressly appropriate any funds for the program, it appears to assume an initial reimbursement budget of $1 billion, as it directs the FCC to notify Congress if it determines during implementation of the reimbursement program that $1 billion "will not be sufficient to fully fund all approved applications for reimbursements" under the program.[238] The law requires the FCC to begin rulemaking within 90 days after its enactment to implement the reimbursement program.[239]

Lastly, the Act includes a reporting requirement, directing "each provider of an advanced communications service" to submit an annual report to the Commission detailing whether they have "purchased, rented, leased or otherwise obtained any covered communications equipment."[240] Providers must further include a "detailed justification" for their use of the equipment and state whether they have removed or replaced the equipment or plan to do so.[241]

FCC Implementation and the Consolidated Appropriations Act, 2021

The FCC has taken several steps to integrate the Secure Networks Act into its ongoing actions. On July 17, 2020, the FCC released a declaratory ruling finding that, by adopting the 2019 USF Order, it had already "substantially implemented" the Secure Networks Act's subsidy

body with appropriate national security expertise," or the Department of Commerce pursuant to Executive Order No. 13873. *Id.* § 1601(c)(1)–(2), (4).

[231] *Id.* § 1601(c)(3).

[232] *Id.* § 1601(b)(2).

[233] *Id.* § 1603.

[234] The Secure Networks Act, as originally enacted, provided that carriers could receive funding assistance if they have "2,000,000 or fewer customers." Pub. L. No. 116-124, § 4(b)(1), 133 Stat. 158 (2020). However, the Consolidated Appropriations Act, 2021, amended this provision by increasing the limit to 10,000,000 million or fewer customers. Pub. L. No. 116-260, Div. N, Tit. IX, § 901 (2020).

[235] 47 U.S.C. § 1603(a).

[236] *Id.* § 1603(d)(2).

[237] *Id.* § 1603(d)(6).

[238] *Id.* § 1603(d)(5)(B).

[239] *Id.* § 1603(g).

[240] *Id.* § 1604(a).

[241] *Id.* § 1604(c).

limitations.[242] Furthermore, on December 11, 2020, the FCC issued a final order (2020 Order) implementing the Act's remaining provisions.[243] Namely, the 2020 Order implements the Secure Networks Act by (1) establishing the reimbursement program to subsidize small communications providers that rip-and-replace equipment on the Covered List; (2) establishing procedures and criteria for creating and maintaining the Covered List; and (3) adopting reporting requirements for carriers to inform the FCC about the ongoing presence of equipment on the Covered List in communications networks.[244] The 2020 Order also goes beyond the Secure Networks Act by requiring any ETCs receiving USF funds, as well as participants in the reimbursement program, to rip-and-replace covered equipment from their networks.[245]

While the 2020 Order made ETC's rip-and-replace obligation contingent on a "Congressional appropriation to fund the Reimbursement Program,"[246] the Consolidated Appropriations Act, 2021, appropriates $1.9 billion to "carry out" the Secure Networks Act, with $1.895 billion of that amount going towards the reimbursement program.[247] The Appropriations Act also includes several amendments to the Secure Networks Act's provisions on the reimbursement program. For instance, it broadens the entities eligible for funding, allows reimbursement for the removal of equipment covered by the 2019 Order and Designation Orders (which cover *any* Huawei and ZTE equipment, rather than simply Huawei and ZTE equipment on the Covered List), and establishes a prioritization paradigm that favors small providers and non-commercial educational institutions in the allocation of reimbursement funds.[248] On February 17, 2021, the Commission adopted a notice of proposed rulemaking that seeks comment on proposals to implement these changes.[249]

United States' Criminal Prosecutions

The United States has brought several criminal charges involving Huawei.[250] In the United States District Court for the Western District of Washington, a grand jury indicted two Huawei affiliates[251] on charges arising from the alleged theft of trade secrets from T-Mobile USA (T-Mobile) and obstruction of justice when T-Mobile threatened to file a lawsuit.[252] In the United States District Court for the Eastern District of New York, the United States is pursuing a criminal

[242] Declaratory Ruling and Second Further Notice of Proposed Rulemaking, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, 35 FCC Rcd. 7821, 7828, para. 22 (July 17, 2020).

[243] Second Report and Order, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, 35 FCC Rcd. 14284 (Dec. 11, 2020).

[244] *Id.* at 14285, para. 1.

[245] *Id.* at 14290–14309, paras. 17–50.

[246] *Id.* at 14290, para. 18.

[247] Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, Div. N, Tit. IX, § 906(2) (2020).

[248] *Id.* § 901.

[249] Third Further Notice of Proposed Rulemaking, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89 (Feb. 17, 2021).

[250] Huawei is involved in a range of civil litigation with private entities that is outside the scope of this report. *See, e.g.*, Mike LaSusa, *Huawei Hits Verizon With a One-Two Punch of Tech IP Suits*, LAW360 (Feb. 6, 2020), https://www.law360.com/articles/1241400/huawei-hits-verizon-with-a-one-two-punch-of-tech-ip-suits; Takashi Kawakami, *Samsung and Huawei Drop Lawsuits in Latest Smartphone Truce*, NIKKEI ASIAN REV. (May 15, 2019), https://asia.nikkei.com/Business/Companies/Samsung-and-Huawei-drop-lawsuits-in-latest-smartphone-truce.

[251] The defendants in the Western District of Washington are Huawei Device Co., LTD and Huawei Device USA, Inc.

[252] Indictment, United States v. Huawei Device Co., LTD and Huawei Device USA, Inc., No. CR19-010 (RSM) (W.D. Wash., Jan. 16, 2019).

indictment against Huawei, two corporate affiliates,[253] and Meng Wanzhou—Huawei's CFO and the daughter of Huawei founder Ren Zhengfei.[254] The New York prosecution arises out of alleged misappropriation of intellectual property and an alleged scheme to avoid U.S. sanctions on Iran and North Korea.[255]

Huawei denies the charges in both prosecutions.[256] Huawei also has filed a Freedom of Information Act (FOIA) suit against the United States in the U.S. District Court for the District of Columbia seeking documents relating to the investigation and prosecution of Huawei and Meng, U.S.-China trade relations, and 5G competition. [257]

In December 2018, Canadian authorities arrested Meng pursuant to a U.S. extradition request arising out of the New York prosecution.[258] Later that month, Chinese authorities arrested two Canadian citizens in China on espionage charges, in what some observers interpret as retaliation for Meng's arrest.[259] Meng is challenging the extradition request in the Canadian legal system.[260] The two Canadian citizens remain in Chinese custody.[261] Some Members of the 116th Congress introduced measures that would have commended Canada for apprehending Meng and expressed concern over China's detention of Canadian citizens.[262]

[253] The corporate affiliates in the Eastern District of New York case are Huawei Device USA Inc. and Skycom Tech Co. Ltd.

[254] Third Superseding Indictment, United States v. Huawei Technologies, Ltd. et al., No. 18-457(S-2) (AMD) (E.D. N.Y., Feb. 13, 2020).

[255] *See id*.

[256] *See, e.g.* Stewart Bishop, *Huawei Denies RICO, Trade Secret Theft Charges in NY Case*, LAW360 (Mar. 4, 2020), https://www.law360.com/articles/1250204/huawei-denies-rico-trade-secret-theft-charges-in-ny-case?te_pk=97fb4a2a-382f-4f2e-8ebf-ecb90855ae1a&utm_source=user-alerts&utm_medium=email&utm_campaign=tracked-entity-alert.

[257] Complaint at ¶ 2, Huawei Technologies Co. Ltd. et al. v. U.S. Immigration and Customs Enforcement et al., No. 20-cv-03155 (D.D.C. Oct. 30, 2020). *See also* Kelcee Griffis, *Huawei Sues Trump Admin. For 'Stonewalling' FOIA Requests*, LAW360 (Nov. 2, 2020), https://www.law360.com/articles/1325126/huawei-sues-trump-admin-for-stonewalling-foia-requests.

[258] *See generally* Robert J. Palladino, Deputy Spokesperson, U.S. Dep't of State, Press Statement, Canada's Legitimate Arrest of Huawei CFO Meng Wanzhou (Dec. 21, 2018), https://www.state.gov/canadas-legitimate-arrest-of-huawei-cfo-meng-wanzhou/.

[259] *See, e.g.*, Chun Han Wong, et al., *'No Coincidence': China's Detention of Canadian Seen as Retaliation for Huawei Arrest*, WALL ST. J. (Dec. 12, 2018), https://www.wsj.com/articles/no-coincidence-chinas-detention-of-canadian-seen-as-retaliation-for-huawei-arrest-11544619753; Chris Buckley et al., *China Arrests 2 Canadians on Spying Charges, Deepening a Political Standoff*, N.Y. TIMES (May 16, 2019), https://www.nytimes.com/2019/05/16/world/asia/china-canadian-arrested.html.

[260] Meng reportedly is discussing a potential "deferred prosecution agreement" with U.S. authorities that would permit her return to China in exchange for an admission of wrongdoing *See, e.g.*, Jacquie McNish et al., *U.S. in Talks With Huawei Finance Chief Meng Wanzhou About Resolving Criminal Charges*, WALL ST. J. (Dec. 4, 2020), https://www.wsj.com/articles/u-s-in-talks-with-huawei-finance-chief-meng-wanzhou-about-resolving-criminal-charges-11607038179?st=zc6p8p07ewhsda7&reflink=article_gmail_share.

[261] *See, e.g.*, Peter Zimonjic, Vassy Kapelos, *Support of Canadians gives Michael Kovrig Hope, Says His Wife on 2nd Anniversary of Arrest*, CAN. BROADCASTING CORP. (Dec. 9, 2020), https://www.cbc.ca/news/politics/kovrig-spavor-china-two-year-anniversary-1.5835373.

[262] *See* H.Res. 521, 116th Cong. (2019).

The United States has also pursued charges against at least one Chinese national, Bo Mao, for conspiring with an unnamed company, which media outlets reported to be Huawei, to steal intellectual property (IP) from a U.S. company.[263] Mao, a Chinese professor working at a Texas university, pled guilty as part of plea agreement to one count of making false statements to the Federal Bureau of Investigation during its investigation into the alleged IP theft.[264] Mao was sentenced to time served with three years supervised release and has been permitted to return to China.[265]

Visa Restrictions

In July 2020, the United States stated it would use existing provisions in U.S. immigration law to restrict the ability of Huawei and other Chinese telecommunication company employees to obtain U.S. visas.[266] Under the Immigration and Nationality Act, an alien is inadmissible to the United States if the Secretary of State has reasonable grounds to believe the alien's entry "would have potentially serious adverse foreign policy consequences for the United States . . . ."[267] Secretary of State Pompeo announced that the United States was imposing visa restrictions on "employees of Chinese technology companies that provide material support to regimes engaging in human rights abuses globally."[268] Secretary Pompeo described Huawei as an "arm of the [Chinese Communist Party's] surveillance state that censors political dissidents and enables mass internment camps . . . ."[269] Huawei denies that it participates in human rights violations.[270]

Diplomacy and Foreign Aid

Some in Congress have expressed interest in whether U.S. allies abroad permit Huawei products in their communications networks.[271] Executive branch officials in the Trump Administration

[263] *See* United States Sentencing Memorandum, U.S. v. Mao, No. 1:19-cr-00392 (E.D.N.Y. Dec. 10, 2020), ECF No. 82 [hereinafter U.S. v. Mao Sentencing Memorandum]. While the United States uses a pseudonym for Huawei in its filings, referring to it as "Company 1," its allegations mirror a civil suit in which a jury found Huawei misappropriated the trade secrets of a U.S. company, and media outlets publically identified "Company 1" as Huawei. *See* Stewart Bishop, *Professor Charged in IP Theft Case Related to Huawei Rap*, LAW360 (Sep. 3, 2019), https://www.law360.com/articles/1195086; Karen Freifield, *Chinese Professor Pleads Guilty to Lying to FBI in Huawei-related Case*, REUTERS (Dec. 4, 2020), https://www.reuters.com/article/us-huawei-tech-usa/chinese-professor-pleads-guilty-to-lying-to-fbi-in-huawei-related-case-idUSKBN28E394; *see also* Verdict Form at Question No. 41, Huawei Technologies Co. LTD. v. Huang, No. 4:17-cv-893 (E.D. Tex., June 26, 2019), ECF No. 476 (jury verdict form in misappropriation civil case against Huawei).

[264] U.S. v. Mao Sentencing Memorandum, *supra* note 263, at 2.

[265] Judgment, U.S. v. Mao, No. 1:19-cr-00392 (E.D.N.Y. Dec. 14, 2020), ECF No. 74.

[266] Michael R. Pompeo, U.S Sec'y of State, *Press Statement, U.S. Imposes Visa Restrictions on Certain Employees of Chinese Technology Companies that Abuse Human Rights* (July 15, 2020), https://www.state.gov/u-s-imposes-visa-restrictions-on-certain-employees-of-chinese-technology-companies-that-abuse-human-rights/ [hereinafter Visa Restrictions Statement].

[267] 18 U.S.C. § 1182(a)(3)(c).

[268] Visa Restrictions Statement, *supra* note 266.

[269] *Id.*

[270] *See Huawei's Commitment to Human Rights 2020*, HUAWEI.COM, https://www-file.huawei.com/-/media/corporate/local-site/uk/pdf/huawei_human-rights-commitment_2020.pdf (last visited Dec. 14, 2020). For more background on human rights issues in China, see CRS Report R45956, *Human Rights in China and U.S. Policy: Issues for the 116th Congress*, by Thomas Lum and Michael A. Weber.

[271] *See infra* note 279–280.

encouraged foreign countries not to use Huawei equipment in their 5G networks,[272] with some success.[273] For example, after announcing that it would permit Huawei products in noncritical elements of its 5G networks,[274] the United Kingdom changed course in July 2020 and announced that it would bar domestic telecommunications operators from using Huawei equipment when building the country's 5G networks.[275] The Trump Administration launched or engaged in other multilateral efforts to promote construction and use of global 5G networks that do not use Huawei systems.[276]

Some observers contend that Huawei's access to Chinese financial state support has allowed Huawei to sell its products and services at discounted prices worldwide.[277] Media outlets have reported that the Trump Administration considered using foreign aid and development programs to help wireless carriers in foreign countries buy equipment from Huawei's major non-Chinese rivals—Sweden's Ericsson AB, Finland's Nokia Corp., and South Korea's Samsung Electronics Co.[278] Some Members of the 116th Congress introduced bills that would have prohibited the United States from sharing intelligence with any country that uses Huawei technology in its 5G

[272] *See, e.g.*, Michael R. Pompeo, U.S. Sec'y of State, *Europe Must Put Security First with 5G*, POLITICO EUROPE (Dec. 2, 2019), https://www.politico.eu/article/europe-must-put-security-first-with-5g-mike-pompeo-eu-us-china/.

[273] *Compare*, *e.g.*, WILLIAMS, *supra* note 5 ("[A] growing number of countries have either formally banned or otherwise taken steps to exclude Huawei from their 5G networks. These include Australia, Japan, the United States, the United Kingdom, France, Sweden, India, Vietnam, and Taiwan."); *and* Amy Kazmin and Stephanie Findlay, *India Moves to Cut Huawei Gear from Telecoms Network*, Fin. TIMES (Aug. 24, 2020), https://www.ft.com/content/55642551-f6e8-4f9d-b5ba-a12d2fc26ef9; *with*, *e.g.*, Lindsay Maizland and Andrew Chatzky, *Huawei: China's Controversial Tech Giant*, COUNCIL FOREIGN RELATIONS (Aug. 6, 2020), https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant ("Russia's 5G network will be built with Huawei's help, and Malaysian telecommunications firms have signed preliminary agreements with Huawei."); *and* William Boston and Stu Woo, *Huawei Gets Conditional Green Light in Germany as Government Approves Security Bill*, WALL ST. J. (Dec. 16, 2020), https://www.wsj.com/articles/huawei-gets-conditional-green-light-in-germany-as-government-approves-security-bill-11608117504 ("A bill approved by Chancellor Angela Merkel's cabinet that would allow Huawei's continued presence in Germany still requires parliamentary approval.").

[274] *See* Dominic Raab, U.K. Foreign Sec'y, Foreign Secretary's Statement on Huawei (Jan. 28, 2020), https://www.gov.uk/government/speeches/foreign-secretary-statement-on-huawei; Mike Cherney and Dan Strumpf, *Taking Cue from the U.S., Australia Bans Huawei from 5G Network*, WALL ST. J. (Aug. 23, 2018), https://www.wsj.com/articles/australia-bans-chinas-huawei-from-5g-network-rollout-1534992631.

[275] *Press Release: Huawei to Be Removed from UK 5G Networks by 2027*, GOV.UK (July 14, 2020), https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027.

[276] *See* U.S. Dep't of State, *The Clean Network*, STATE.GOV, https://www.state.gov/the-clean-network/ (last visited Dec. 21, 2020) (describing the United States' Clean Network program, which foreign countries and corporations can join, as a "comprehensive approach to safeguarding the nation's assets including citizens' privacy and companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party"); Paul Triolo and Kevin Allison, *In Struggle with China, US Advances Industrial Policy of its Own*, EURASIA GROUP (June 11, 2020), https://www.eurasiagroup.net/live-post/struggle-china-us-advances-industrial-policy (discussing U.S. participation in multilateral fora designed to counter Chinese influence, such as the Economic Prosperity Network and Blue Dot Network).

[277] *See supra* note 24. *See also* Maizland and Chatzky, *supra* note 273.

[278] *See* Stu Woo, *Facing Pushback from Allies, U.S. Set for Broader Huawei Effort*, WALL ST. J. (Jan. 28, 2020), https://www.wsj.com/articles/facing-pushback-from-allies-u-s-set-for-broader-huawei-effort-11579775403?mod=article_inline&mod=article_inline ("Washington plans to use the State Department's Digital Connectivity and Cybersecurity Partnership, the U.S. Agency for International Development, the Export-Import Bank of the U.S. and U.S. International Development Finance Corporation . . . [to] help wireless carriers in foreign countries buy equipment from Huawei's rivals . . . .").

networks.[279] Other Members proposed resolutions encouraging U.S. allies not to use Huawei systems and equipment in their infrastructure.[280]

National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA)

The most recently passed Huawei-related legislation came in the National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA), passed over President's Trump's veto in December 2020.[281]

Section 1058

Section 1058 of the FY2021 NDAA limits the Secretary of Defense's ability to locate a major weapons systems or permanently assign forces in a country with "at risk" 5G or sixth generation (6G) wireless network equipment, software, or services if U.S. military personnel and their families will be directly connected to the "at risk" networks.[282] Executive branch officials previously have voiced concern about Huawei equipment installed near U.S. military bases.[283] Prior to making a base or forces assignment that falls within Section 1058's parameters, the Secretary of Defense must consider risks in the host country posed by "at-risk vendors," which is defined to include Huawei and ZTE.[284]

Section 9202

Some officials in the Trump Administration and Members of the 116th Congress expressed the desire to encourage development of information and communications companies in the United States or allied nations that can better compete with and serve as alternatives to Huawei.[285] U.S. companies do not manufacture certain key elements of the infrastructure necessary for 5G

[279] *See* H.R. 5661, 116th Cong. § 1(a) (2020); S. 3153, 116th Cong. § 1(a) (2020).

[280] *See*, *e.g.*, H.Res. 827, 116th Cong. § 1 (2020) ("[T]he Parliament of the United Kingdom of Great Britain and Northern Ireland is encouraged to reject or amend the National Security Council's decision on telecommunications security in a manner that excludes high-risk vendors, such as Huawei, from the country's 5G infrastructure . . . ."); S.Con.Res. 10, 116th Cong. (2019) (calling on the United States and its allies to limit risks associated with use of Huawei and other Chinese communications companies' products). *See also* Letter from 20 U.S. Senators to Members of Parliament, U.K. House of Commons, (Mar 3, 2020), https://www.sasse.senate.gov/public/_cache/files/040d4bec-953e-49fd-866c-3f44785b2134/03.03.20-sasse-schumer-letter-to-uk-parliament.pdf (letter from 20 U.S. Senators to the U.K. House of Commons urging the United Kingdom to revisit its recent decision to allow Huawei in certain portions of its telecommunications network).

[281] *See* FY2021 NDAA, *supra* note 13.

[282] *Id.* § 1058(a).

[283] *E.g.*, *FCC Wants to Know if Huawei Gear is Near U.S. Military Bases*, BLOOMBERG LAW (Nov. 5, 2019), https://news.bloomberglaw.com/tech-and-telecom-law/fcc-wants-to-know-if-huawei-gear-is-near-u-s-military-bases.

[284] *Id.*

[285] *See*, *e.g.*, Ellen Nakashima and Jeanne Whalen, *Barr Suggests U.S. Consider Investing in Nokia, Ericsson to Counter Huawei*, WASH. POST. (Feb. 6, 2020), https://www.washingtonpost.com/national-security/barr-warns-against-chinese-dominance-of-5g-super-fast-networks/2020/02/06/1da26794-48ec-11ea-9164-d3154ad8a5cd_story.html; Press Release, Office of Senator Mark Warner, National Security Senators Introduce Bipartisan Legislation to Develop 5G Alternatives to Huawei, (Jan 14, 2020), https://www.warner.senate.gov/public/index.cfm/2020/1/national-security-senators-introduce-bipartisan-legislation-to-develop-5g-alternatives-to-huawei.

telecommunications systems.[286] At the same time, some observers believe Chinese state support of Huawei and other communications companies have helped those companies develop their products, gain market share, and reinvest profits in research and development.[287] In response to this dynamic, the 116th Congress included provisions in the FY2021 NDAA that authorize funds to support 5G research and promote telecommunications equipment providers that can act as alternatives to Huawei in the United States and abroad.[288]

Section 9202 of the FY2021 NDAA establishes a Public Wireless Supply Chain Innovation Fund (Innovation Fund), which can make grants of up to $50 million to support, among other things, the promotion and deployment of certain communications network technology, including 5G technology and equipment.[289] The Administrator of the National Telecommunications and Information Administration (NTIA) is to administer the Innovation Fund with the advice of an interagency advisory board.[290]

Section 9202 also creates a Multilateral Telecommunications Security Fund (Multilateral Telecom Fund) to be administered by the Secretary of State, in consultation with an interagency group.[291] The provision authorizes the Secretary of State to create a common funding mechanism with the United States' foreign partners to "support the development and adoption of secure and trusted telecommunications technologies."[292] It also calls for the Secretary of State "to secure commitments and contributions from trusted foreign partners such as the United Kingdom, Canada, Australia, New Zealand, and Japan" while pursuing three objectives:

> (i) Advancing research and development of secure and trusted communications technologies;
>
> (ii) Strengthening supply chains; and
>
> (iii) Promoting the use of trusted vendors.[293]

Finally, Section 9202 requires the executive branch to consider how to enhance U.S. representation at international 5G standards-setting bodies, such as the International Telecommunication Union (ITU).[294] Some observers believe that the Chinese government exerts influence over international bodies that set 5G technical standards to benefit Huawei and other

[286] For discussion of the "race to 5G," see CRS Report R45485, *Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress*, by Jill C. Gallagher and Michael E. DeVine, at 8. Some observers question the ability of U.S. technology companies to offer viable alternatives to Huawei. *See, e.g.*, Henry Kressel, *O-Ran No Near-Term Challenger to Huawei, Ericsson*, ASIA TIMES (Dec. 29, 2020), https://asiatimes.com/2020/12/opening-the-telecom-equipment-market-wont-be-easy/.

[287] *See supra* note 25. Huawei denies that it has achieved success because of state support, claiming that government subsidies account for less than one percent of total revenue. *See Huawei: Facts, Not Myths*, *supra* note 4.

[288] FY2021 NDAA, *supra* note 13, § 9202(a). *See also Press Release: Warner & Rubio Applaud Passage of 5G Legislation* (Dec. 11, 2020), https://www.warner.senate.gov/public/index.cfm/2020/12/warner-rubio-applaud-passage-of-5g-legislation ("The [legislation from which Section 9202 is derived] seeks to encourage and support U.S. innovation in the race for 5G by providing funds to support research and development in Western-based alternatives to Chinese equipment providers Huawei and ZTE.").

[289] FY2021 NDAA, *supra* note 13, § 9202(a)(1).

[290] *Id.*

[291] *Id.* § 9202(a)(2).

[292] *Id.* § 9202(a)(2)(B).

[293] *Id.*

[294] *Id.* § 9202(b).

domestic Chinese firms.[295] Some Members of the 116th Congress and officials in the Trump Administration described American leadership in these standards-setting bodies as important for advancing U.S. national security, foreign policy, and economic interests.[296]

Title XCIX: Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America

Title XCIX of the FY2021 NDAA, titled Creating Helpful Incentives to Produce Semiconductors for America Act (commonly referred to as the CHIPS for America Act),[297] requires the Secretary of Commerce to establish a program to provide financial assistance to incentivize investment in the U.S. semiconductor manufacturing industry.[298] Grants are not to exceed $3 billion per project unless the President certifies to Congress that a larger investment is necessary to "significantly increase . . . reliable domestic supply of semiconductors relevant for national security and economic competitiveness[,]" and to meet national security needs.[299] Title XCIX also requires, among other things: (1) establishment of public-private partnerships to incentivize domestic microchip production;[300] (2) a study of the U.S. industrial base to support microelectronic production;[301] (3) the creation of a Multilateral Semiconductors Security Fund;[302] and (4) funding for microelectronic research and development in federal agencies.[303] While these provisions do not target Huawei or its products directly, some observers view federal support for the microchip industry as part of a broader effort to ensure U.S. companies maintain a foothold in technology supply chains that are essential for products made by Huawei and other foreign technology companies.[304]

---

[295] *See*, *e.g.*, Hart and Link, *supra* note 24; Alan Beattie, *How the US, EU, and China Compete to Set Industry Standards*, FIN. TIMES (July 25, 2019), https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271; Brett. D. Schaefer, Dean Cheng, and Klon Kitchen, *Chinese Leadership Corrupts Another U.N. Organization*, HERITAGE FOUND. (May 11, 2020), https://www.heritage.org/global-politics/commentary/chinese-leadership-corrupts-another-un-organization.

[296] U.S. Dep't of Commerce, *Commerce Clears Way for U.S. Companies to More Fully Engage in Tech Standards-Development Bodies*, (June 15, 2020), https://www.commerce.gov/news/press-releases/2020/06/commerce-clears-way-us-companies-more-fully-engage-tech-standards (quoting U.S. Secretary of Commerce as stating, "The Department is committed to protecting U.S. national security and foreign policy interests by encouraging U.S. industry to fully engage and advocate for U.S. technologies to become international standards."); Letter from Senator James M. Inhofe et al. to Wilbur Ross, U.S. Sec'y of Commerce, et al. (Apr. 14, 2020), https://www.rubio.senate.gov/public/_cache/files/4565c857-270a-4375-abb7-4d65ad416ebc/B99D3ED832787BD956653CC3A4176071.20200414-letter-to-secretary-of-commerce-on-5g-standards-final.pdf ("It is critical for U.S. companies to participate fully in these standards-setting bodies to ensure that their technologies are represented in the standards.").

[297] Title XCIX includes provisions that originated in two bills introduced in the 116th Congress: (1) the CHIPS for America Act, S. 3933, 116th Cong. (2020) and H.R. 7178, 116th Cong. (2020), and (2) the American Foundries Act of 2020, S. 4130, 116th Cong. (2020).

[298] FY2021 NDAA, *supra* note 13, tit. XCIX, §§ 9901-08.

[299] *Id.* § 9902(a)(3)(B).

[300] *Id.* § 9903.

[301] *Id.* § 9904.

[302] *Id.* § 9905.

[303] *Id.* § 9906.

[304] *See*, *e.g.*, Robert A. Manning, *The U.S. Finally Has a Sputnik Moment with China*, FOREIGN POLICY (Oct. 29 2020) https://foreignpolicy.com/2020/10/29/us-china-sputnik-moment-technology-competition-semiconductors/; Hirsh Chitkara, *A Newly Proposed Bipartisan Bill Would Earmark $22 Billion to Lure Chip Manufacturers to US*, BUS. INSIDER (June 12, 2020), https://www.businessinsider.com/chips-for-america-act-will-shift-chip-manufacturing-to-us-

Conclusion

The federal government's legal actions involving Huawei have evolved from straightforward spending restrictions to a multifaceted effort to ban the company from telecommunications networks in the United States and internationally. What began as appropriations restrictions in 2013 evolved in the FY2018 NDAA into a procurement ban in DOD's sensitive nuclear and national defense missions.[305] That narrow procurement ban expanded in the FY2019 NDAA to an executive branch-wide ban on procuring from any company that uses Huawei products and services.[306] In 2019, legal actions transitioned from the procurement context to the realm of international trade as the executive branch added Huawei to the Entity List and invoked the President's IEEPA authority.[307] In 2019 and 2020, the FCC took steps to limit Huawei's presence in U.S. telecommunications networks, and Congress provided additional direction for these efforts with the Secure Networks Act, enacted in early 2020.[308] As the Trump Administration pursued diplomatic efforts to convince allied countries to ban Huawei from their 5G networks in 2020, the 116th Congress passed the FY2021 NDAA, which contemplates using federal funds to support private competitors to Huawei domestically and abroad.[309]

Some observers view the increasing complexity of the legal actions involving Huawei as a microcosm of the broader challenges presented by China's rise on the global stage.[310] At the same time, U.S. officials have sought to account for potential negative impacts of these escalating actions by, for example, calibrating U.S. export regulations to allow American companies to work with Huawei when identifying cybersecurity vulnerabilities or working in international standards-setting organizations.[311] The United States also has shown willingness to take increasingly strict actions—such as narrowing the foreign direct product rule for Huawei and its affiliates or instituting a "rip and replace" program—when this is deemed necessary for national security and American interests.[312] Given the competing considerations in Huawei policy, a balancing of interests may continue in the 117th Congress and in the Biden Administration.

2020-6.

[305] *See supra* § Federal Spending Restrictions.

[306] *See id.*

[307] *See supra* §§ Export Restrictions, Executive Orders Under the International Emergency Economic Powers Act (IEEPA).

[308] *See supra* § Federal Communications Commission's Actions.

[309] *See supra* § National Defense Authorization Act for Fiscal Year 2021.

[310] *See, e.g.*, WILLIAMS, *supra* note 5, at 1 ("Washington's growing focus on the risks posed by Chinese technology companies operating in the United States embodies the complexity of the challenges confronting U.S. policymakers in responding to China's rise in technological, economic, and geopolitical power."); Lu Chuanying and Nicolas Huppenbauer, *What the Huawei Case Can Teach Us About the U.S-China Power Game*, *in* PERSPECTIVES ON THE GLOBAL ECONOMIC ORDER IN 2019: A U.S.-CHINA ESSAY COLLECTION 36, 39 (2019) ("The Huawei dispute is one case in point against the backdrop of the larger power game between the United States and China, and it reflects [a] . . . trend toward securitization and economic competition in the bilateral relationship."). For a discussion of China's economic rise, see CRS Report RL33534, *China's Economic Rise: History, Trends, Challenges, and Implications for the United States*, by Wayne M. Morrison.

[311] *See supra* notes 95 and 96.

[312] *See supra* §§ Foreign Direct Product Rule and *De Minimis* Rules, Federal Communications Commission's Actions.

Author Information

Stephen P. Mulligan
Legislative Attorney

Chris D. Linebaugh
Legislative Attorney

Disclaimer