U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests

January 5, 2022

Congressional Research Service
https://crsreports.congress.gov
R47012

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47012

January 5, 2022

Jill C. Gallagher
Analyst in Telecommunications Policy

U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests

Huawei Technologies Co., Ltd., is a China-based company that designs, manufactures, and sells telecommunications network equipment and devices. Founded in 1987, the company has grown from a small reseller of imported telephone switches into a multinational conglomerate with revenues of $138 billion in 2020 and a presence in over 170 countries. Huawei is estimated to be the largest of the four major global network equipment makers, which also include Finnish firm Nokia, Swedish firm Ericsson, and Zhong Xing Telecommunication Equipment (ZTE), a Chinese firm that is partially state-owned.

For more than two decades, U.S. government officials have raised national and economic security concerns about Huawei, citing its ties to the Chinese government and military, sanctions violations and unfair trade practices, preferential Chinese policies and financing that enabled its expansion globally, and the potential for espionage or sabotage of U.S. and global networks. With the emergence of fifth-generation (5G) telecommunications technologies that enable greater connectivity among billions of personal, business, and industrial devices and networks, U.S. concerns have become more pronounced.

There has been support in Congress for policies and restrictions aimed at securing U.S. networks and supply chains, and limiting Huawei's presence in global networks. In 2017, Congress passed legislation restricting the use of Huawei equipment in certain Department of Defense (DOD) networks. In 2018, it prohibited U.S. agencies from obtaining equipment, systems, and services that use Huawei equipment or services as a substantial or critical component, and prohibited the use of federal grants and loans for Huawei products. In 2019, the Department of Justice (DOJ) charged Huawei and its officials with financial fraud and sanctions violations. The Department of Commerce (DOC) subsequently added Huawei to the Entity List—a trade restriction list published by DOC's Bureau of Industry and Security—requiring companies to obtain a license to export goods to Huawei. In 2020, DOJ charged Huawei with racketeering, conspiracy to steal trade secrets, and sanction violations; DOC tightened restrictions on exports, limiting Huawei's access to foreign-produced semiconductors made with U.S. technologies; and Congress provided $1.9 billion to remove Huawei equipment from U.S. networks.

The Biden Administration upheld the Huawei-related restrictions imposed by the Trump Administration and tightened restrictions on sales of semiconductors for 5G devices. However, both Administrations allowed over $60 billion in transactions between U.S. firms and Huawei, which some lawmakers have questioned. The 117th Congress has acted to prohibit future use of Huawei equipment in the United States. P.L. 117-55 requires the Federal Communications Commission (FCC) to adopt rules clarifying it will no longer review or issue equipment licenses to companies that pose a national security threat, which include Huawei. Members have proposed legislation requiring DOC to certify certain conditions before removing Huawei from the Entity List (S. 568 and H.R. 4561). Other bills contain similar certifications, add certain Huawei affiliates to the Entity List, and require DOC to report on license applications and approvals (H.R. 1595 and H.R. 4792). S. 1260, which passed the Senate in June 2021, contains similar certifications and would also provide funding to bolster U.S. semiconductor manufacturing; foster the development of secure and trusted telecommunications technologies and supply chains; promote initiatives to increase U.S. participation in standards development bodies; and develop partnerships and programs to counter Huawei's global expansion.

As Congress considers new restrictions on Huawei, it may seek to examine the impact of the existing restrictions on national security, foreign policy, and the economic competitiveness of U.S. firms and develop policies that balance objectives in each of these areas. U.S. policies and restrictions require agencies and businesses to identify and remove Huawei equipment from telecommunications networks and to scrutinize supply chains, which many experts see as a necessary step to improving U.S. network security. However, some U.S. agencies argue the restrictions could disrupt U.S. agency work, businesses, and services to consumers, citing implementation challenges and the mandated timelines for compliance. Additionally, some experts warn the restrictions could reduce revenues for some U.S. suppliers to Huawei and lead to reduced funding for research and development, affecting U.S. competitiveness. China experts note that the restrictions may trigger retaliatory action by the Chinese government, which could move to exclude U.S. firms from the Chinese market and supply chains.

Contents

Figures

Contacts

Introduction

Huawei Technologies Co., Ltd., is a China-based company that designs, manufactures, and sells telecommunications network equipment and devices. For more than two decades, U.S. government officials have raised national and economic security concerns with Huawei, citing its ties to the Chinese government and military, preferential Chinese policies and financing that enabled its growth and expansion globally, and the potential for espionage.[1] There has been support in Congress for policies that prohibit use of Huawei equipment in U.S. networks,[2] restrict Huawei's access to U.S. technologies,[3] and promote the development and use of secure and trusted network equipment in the United States and globally.[4]

In 2017, the U.S. government began imposing restrictions on the use of Huawei equipment in the United States. In December 2017, Congress prohibited use of Huawei equipment in certain Department of Defense (DOD) networks (P.L. 115-91, §1656). In 2018, it prohibited U.S. agencies from obtaining Huawei equipment, systems, and services, and use of federal grants for Huawei equipment (P.L. 115-232, §889).

In January 2019, the Department of Justice (DOJ) brought criminal charges against Huawei and its officials for financial fraud and sanctions violations.[5] On May 15, 2019, President Trump signed Executive Order 13873, *Securing the Information and Communications Technology (ICT) Services Supply Chain*, prohibiting the purchase or use of any ICT produced by entities controlled by a foreign adversary that could create a risk of sabotage or catastrophic effects on critical infrastructure, and declaring a national emergency in regard to this threat.[6] While the executive order does not mention Huawei specifically, it directs the Department of Commerce (DOC) to identify technologies or countries that may warrant particular scrutiny and establish procedures to license transactions to mitigate concerns.

On May 21, 2019, in response to the criminal charges, DOC added Huawei and 68 of its affiliates to the Entity List—a trade restriction list published by DOC's Bureau of Industry and Security (BIS).[7] In its announcement, DOC stated that it reasonably believes the company to be involved

[1] See CRS Report R46693, *Huawei and U.S. Law*, by Stephen P. Mulligan and Chris D. Linebaugh.

[2] Senator Mark R. Warner, "Warner, Rubio Announce Growing Bipartisan Support to Combat Technology Threats from China," press release, January 29, 2019, at https://www.warner.senate.gov/public/index.cfm/2019/1/warner-rubio-announce-growing-bipartisan-support-to-combat-technology-threats-from-china.

[3] U.S. Congress, House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Cong., 2nd sess., October 8, 2012, pp. 27-29, at https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96. See also Robert D. Atkinson, "How China's Mercantilist Policies Have Undermined Global Innovation in the Telecom Equipment Industry," *Information Technology and Innovation Foundation*, June 22, 2020, at https://itif.org/sites/default/files/2020-china-mercantilist-telecom-equipment-industry.pdf.

[4] For example, see P.L. 116-124 and S. 604.

[5] DOJ, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud," press release, January 28, 2019, at https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial.

[6] Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," 84 *Federal Register* 22689, May 15, 2019.

[7] BIS administers Export Administration Regulations (EAR), export controls on commercial, dual-use, and less sensitive military items (15 C.F.R., subchapter C, parts 730–774). U.S. firms must obtain a license to export EAR items to Entity List organizations. See CRS In Focus IF11627, *U.S. Export Control Reforms and China: Issues for Congress*, by Ian F. Fergusson and Karen M. Sutter.

in activities contrary to the national security or foreign policy interest of the United States.[8] DOC, as the agency responsible for governing the export and re-export of certain commodities,[9] including technology and software, administers the Export Administration Regulations (EAR). The EAR impose licensing requirements on exports of certain products, buyers, and end destinations,[10] and DOC generally limits the availability of licenses for exports involving people or organizations on the Entity List.[11] On May 22, 2019, DOC created a Temporary General License (TGL) allowing some transactions to continue for 90 days, including operations of current networks, (e.g., software patches), support to existing devices, cybersecurity research and disclosure to Huawei of security vulnerabilities, and engagement in 5G standards development bodies.[12] From May 2019 through August 2020, DOC amended its rules, tightening restrictions on exports to Huawei, and extending the TGL several times.

In February 2020, DOJ charged Huawei with racketeering and theft of trade secrets, among other things.[13] In March 2020, Congress prohibited entities from using federal subsidies to purchase telecommunications equipment that poses a national security threat, which includes Huawei equipment, created a program to "rip and replace" untrusted equipment in U.S. networks (P.L. 116-124), and later appropriated $1.9 billion for the program (P.L. 116-260, §901). In May 2020, DOC amended its rules, imposing additional controls over certain foreign-produced items.[14] The rule applies specifically to Huawei and its listed non-U.S. affiliates, and intends to "restrict Huawei's ability to use U.S. technology and software to design and manufacture its semiconductors abroad."[15] In August 2020, DOC added several Huawei affiliates to the Entity List, discontinued the TGL, and tightened restrictions on use of U.S. technologies and software for foreign-made products manufactured for Huawei or its listed affiliates.[16]

[8] BIS, "Addition of Entities to the Entity List," 84 *Federal Register* 22961, May 21, 2019. (Note: DOC's End User Review Committee (ERC), composed of representatives of the Departments of Commerce, State, Defense, Energy, and, where appropriate, the Treasury, makes determinations to place entities on the Entity List.)

[9] See 15 C.F.R. §734.3, "Items Subject to Export Administration Regulations."

[10] International Trade Administration, "U.S. Export Regulations," at https://www.trade.gov/us-export-regulations-0.

[11] 15 C.F.R. subchapter C, parts 730-774.

[12] DOC, "Temporary General License," 84 *Federal Register* 23468-23471, May 22, 2019.

[13] DOJ, "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," press release, February 13, 2020, at https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.

[14] DOC, "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," 85 *Federal Register* 29849-29863, May 19, 2020.

[15] DOC, "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies," press release, May 15, 2020, at https://2017-2021.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts.html.

[16] BIS, "Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)," 85 *Federal Register* 51602, August 20, 2020. (Specifically, the rule applies to "foreign-produced items that are: the direct product of certain U.S. technology or software or produced by any plant or major component of a plant that is located outside the United States, when the plant or major component of a plant itself is a direct product of certain U.S.-origin technology or software; when the foreign-produced item will be incorporated into, or will be used in the 'production' or 'development' of any 'part,' 'component,' or 'equipment' produced, purchased, or ordered by Huawei or its listed non-U.S. affiliates; or Huawei or its listed non-U.S. affiliates is a party to any transaction involving the foreign-produced item, *e.g.*, as a 'purchaser,' 'intermediate consignee,' 'ultimate consignee,' or 'end-user.'" DOC cites the Export Control Reform Act of 2018 (ECRA), 50 U.S.C. Sections 4801-4852 as the legal basis for BIS's authority under which BIS issues this rule.)

While DOC permitted some transactions under the TGL, it imposed a license requirement for the export of other items to Huawei and its affiliates, including 5G technologies.[17] DOC adopted a "presumption of denial" policy, meaning DOC was unlikely to approve license requests.

The Biden Administration has upheld the policies of the Trump Administration, keeping Huawei on the Entity List and enforcing restrictions on 5G technologies. However, both Administrations approved some licenses, permitting some exports of U.S. products to Huawei—decisions that some lawmakers questioned.[18] In October 2021, the House Foreign Affairs Committee released data from DOC stating that from November 9, 2020, to April 20, 2021, DOC approved licenses authorizing at least $61 billion in exports of technology to Huawei.[19] In August 2021, DOC approved licenses authorizing exports of chips to Huawei for in-vehicle technologies, such as video screens and sensors, asserting that the chips are less sophisticated and pose less of a threat to U.S. foreign policy interests than more advanced 5G-capable chips.[20]

In November 2021, Congress acted to further restrict Huawei equipment use in the United States. Congress passed, and the President signed, legislation requiring the Federal Communications Commission (FCC) to adopt rules clarifying it would not authorize use of certain "covered" equipment in the United States,[21] which includes Huawei equipment (P.L. 117-55). Other legislative proposals would require DOC to certify a company is not involved in activities contrary to U.S. national security or foreign policy interests before removing it from the Entity List (S. 568 and H.R. 4561). H.R. 1595 includes a similar certification, adds certain Huawei affiliates to the Entity List, and requires DOC to report on export license applications.

Other legislative proposals focus less on restrictions and more on bolstering the U.S. telecommunications industry to help ensure the United States stays competitive in the global technology market. S. 1260 would provide funding to strengthen the U.S. semiconductor industry, and support advanced telecommunications technology research and alternatives to Huawei (e.g., Open Radio Access Network or ORAN technology development).

Still other legislation focuses on promoting the use of secure and trusted telecommunications equipment globally. S. 604 would build international partnerships among democratic nations to promote legal compatibility and democratic values in technology governance, to "avoid ceding leadership to authoritarian regimes and risking the growth of anti-democratic norms and standards around technologies," and promote coordination in investments to protect global networks. H.R.

[17] For example, see DOC, "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," 85 *Federal Register* 29849-29863, May 19, 2020 (imposing a control on certain "technology" or "software," including millimeter wave or 5G technologies).

[18] Michael Ruiz, "Republican Lawmakers Raise Flags over Report Biden Administration Greenlit Chip Sales to Huawei," *Fox Business*, August 26, 2021, at https://www.foxbusiness.com/politics/republicans-biden-chip-sales-huawei.

[19] "Export Control Licensing Decisions for Huawei (November 9, 2020-April 20, 2021)," data obtained by the House Foreign Affairs Committee from the Department of Commerce, released by the committee on October 21, 2021, available at https://gop-foreignaffairs.house.gov/wp-content/uploads/2021/10/Huawei-Licensing-Information.pdf.

[20] Karen Freifeld, "EXCLUSIVE: Huawei Get U.S. Approvals to Buy Auto Chips, Sparking Blow Back," Reuters, August 25, 2021, at https://www.reuters.com/business/autos-transportation/exclusive-us-approves-licenses-huawei-buy-auto-chips-sources-2021-08-25/.

[21] P.L. 117-55 states the FCC will no longer review applications for equipment that is on the list of "covered" communications equipment or services published by the FCC as directed under Section 2(a) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(a)). As directed in the act, the FCC published a list of covered equipment on March 12, 2021; see https://www.fcc.gov/supplychain/coveredlist.

3344 would provide project support and financing to certain Central and Eastern European nations to provide cost-effective alternatives to Huawei, and to improve global network security.

This report provides an overview of the global telecommunications market, a discussion of existing U.S. restrictions on Huawei, benefits and challenges in implementing restrictions, and considerations for Congress as it contemplates future policies concerning Huawei.

Global Telecommunications Networks and Equipment Market

This section provides brief background on network operators and ownership models in the United States and China, and on global network equipment manufacturers and their suppliers.

Network Operators and Ownership in the United States and China

In the United States, private-sector companies, such as AT&T, T-Mobile, Verizon, and many smaller telecommunications service providers, own and operate[22] telecommunications networks.[23] Network operators invest in their networks to improve coverage and service, retain existing customers, attract new customers, and increase revenue for the company and its shareholders.[24] The U.S. government provides some subsidies for network operators serving high-cost areas through its Universal Service Fund (USF),[25] and funding through federal grant programs,[26] to help ensure telecommunications services are available and affordable throughout the country.[27]

In China, the "Big Three" telecommunications network operators—China Mobile, China Telecom, and China Unicom—are state-owned enterprises.[28] The State-owned Assets Supervision

[22] One exception in the United States is FirstNet, the nationwide public safety network, funded with federal dollars, managed by the First Responder Network Authority, a government entity, and built by AT&T. See https://www.firstnet.gov/.

[23] Prior to 1984, the U.S. government recognized AT&T as a natural monopoly providing a public good; in turn, the U.S. government limited AT&T's rate-of-return (i.e., its profits). In 1984, in a DOJ antitrust suit, a U.S. District Court ordered AT&T to divest itself of subsidiaries—the Bell Operating Companies—providing local telephone service. The Bell Operating Companies were broken up into seven regional companies that would provide local service to ensure competition in the market. See Isaac J. Turk and Sabrina L. Montes, *The U.S. Telecommunications Services Industry*, Economics and Statistics Administration, August 1995, p. 11, at https://www.commerce.gov/sites/default/files/media/files/2018/the_u.s._ telecommunications_services_industry_assessing_competitive_advantage.pdf.

[24] Norbert Michel and James Gattuso, *Are U.S. Telecom Networks Public Property?*, The Heritage Foundation, April 8, 2004, at https://www.heritage.org/technology/report/are-us-telecom-networks-public-property.

[25] High-cost areas may be rural or remote areas where customers are limited and deployment costs are high. See CRS Report R46613, *The Digital Divide: What Is It, Where Is It, and Federal Assistance Programs*, by Colby Leigh Rachfal.

[26] See Jon Swartz, "How the Infrastructure Bill's $65 Billion in Broadband Spending Will Be Doled Out," *Market Watch*, November 9, 2021 (discussing funding available through the Infrastructure Investment and Jobs Act (P.L. 117-58)).

[27] CRS Report R46780, *Overview of the Universal Service Fund and Selected Federal Broadband Programs*, coordinated by Patricia Moloney Figliola.

[28] Like the United States, the Chinese government relied on a single provider that had a monopoly on telecom services in China. In 1999, the government broke up the monopoly and created smaller, state-owned enterprises (SOEs) to spur competition. In 2008, the Chinese government reversed course and consolidated the carriers, forming three SOEs: China Mobile, China Telecom, and China Unicom. See U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*, Staff Report, 116th Cong., 2nd sess., June 2020, pp. 20-21, at

and Administration Commission of the State Council, a government entity, holds a majority of the shares in and supervises Big Three operations.[29] The government selects the companies' leaders, many of which have "links to the [Ministry of Information Industry and Technology], the Government, or the [Communist] Party."[30] The Chinese government establishes target returns and growth rates,[31] and sets industry goals that align with Chinese national goals.[32] Further, Chinese law requires domestic and foreign companies operating in China to create a Communist Party of China Committee within each company to promote national and "social responsibility" goals.[33]

Chinese operators continually upgrade their networks to improve coverage and service, retain customers, attract new customers, and increase revenue.[34] However, as state-owned entities, they operate within a tightly controlled and closed domestic telecommunications market (one of the largest telecommunications markets in the world, in terms of subscribers),[35] and are compelled to support government goals such as "lower prices, higher speed and better coverage," at times ahead of growth and revenues.[36]

Global Network Equipment Manufacturers and Suppliers

To improve networks, operators purchase equipment from network equipment manufacturers. There are four major global network equipment makers: Chinese firm Huawei; Finnish firm Nokia; Swedish firm Ericsson; and Zhong Xing Telecommunication Equipment (ZTE), a Chinese firm that is partially state-owned. Huawei is the world's largest network equipment maker, based on estimates from the Dell'Oro Group, a telecom analysis firm. In first half of 2021, Huawei held about 30% of the $90 billion global network equipment market, Nokia and Ericsson each held about 15%, and ZTE held about 10%, according to Dell'Oro.[37]

---

https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.

[29] FCC, *In the Matter of China Unicom (Americas) Operations Limited* (DA-20-449), Order to Show Cause, April 24, 2020, pp. 3722-3723, at https://www.fcc.gov/document/china-unicom-americas-operations-limited-order-show-cause.

[30] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*, Staff Report, 116th Cong., 2nd sess., June 2020, p. 20, at https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.

[31] U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers*, Staff Report, 116th Cong., 2nd sess., June 2020, p. 2, at https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf.

[32] CRS In Focus IF10964, *"Made in China 2025" Industrial Policies: Issues for Congress*, by Karen M. Sutter.

[33] See, for example, China Unicom, *China Unicom Corporate Social Responsibility Report 2015*, p. 5, at https://www.unglobalcompact.org/participation/report/cop/create-and-submit/active/224671.

[34] U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, p. 19, at https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

[35] Robert D. Atkinson, "How China's Mercantilist Policies Have Undermined Global Innovation in the Telecom Equipment Industry," *Information Technology and Innovation Foundation*, June 22, 2020, at https://itif.org/sites/default/files/2020-china-mercantilist-telecom-equipment-industry.pdf. See also Daniel Slotta, "Telecommunications Industry in China—Statistics and Facts," *Statista*, April 21, 2021, at https://www.statista.com/topics/6577/telecommunications-industry-in-china/#dossierKeyfigures.

[36] Bien Perez, "Why Government Policy Has a Bigger Impact on China's Telecoms Industry Than Market Competition," *South China Morning Post*, March 11, 2017, at https://www.scmp.com/tech/china-tech/article/2077810/why-government-policy-has-bigger-impact-chinas-telecoms-industry.

[37] Stefan Pongratz, "Key Takeaways—1Q 2021 Total Telecom Equipment Market," Dell'Oro Group, June 15, 2021, at https://www.delloro.com/key-takeaways-total-telecom-equipment-market-2020/. See also Matt Kapko, "Ericsson,

Network equipment makers develop and deploy end-to-end network solutions for network operators (e.g., design, installation, integration of hardware and software). While the United States does not have a major network equipment manufacturer that provides end-to-end network solutions, it has many companies that supply these major manufacturers with essential parts (e.g., chips, software, switches, and other hardware).[38] For example, in 2018, Huawei announced that 33 of its top 92 suppliers were U.S. firms,[39] and in 2019 said it had purchased about $11 billion in supplies from U.S. companies in the past year.[40]

With the emergence of 5G technologies, industry analysts expect the equipment market to grow as network operators around the world upgrade networks. The Dell'Oro Group predicted the $90 billion equipment market to grow by 5% to 10% in 2021.[41] Analysts expect operators to upgrade to 5G, and network equipment manufacturers and their suppliers, including U.S. firms, to benefit from increased 5G spending.

Background on Huawei and U.S. Concerns with Huawei

Since 2000, the U.S. government has raised concerns about Huawei, citing its ties to the Chinese government and military, sanction violations, theft of intellectual property, and other offenses.[42] This section provides background on Huawei, and U.S. government concerns with Huawei.

Huawei Technologies Co., Ltd.

In 1986, the Chinese government initiated plans to improve its telecommunications infrastructure to develop its economy.[43] The government adopted a three-pronged policy to build its national telecommunications network, "including: (a) direct import of equipment; (b) technological transfer and absorbing; and (c) indigenous innovation with the hope that the Chinese homegrown firms would eventually catch up with multinational giants."[44] The government reduced tariffs on

Cisco, Samsung Gain Telco Gear Share as Huawei, Nokia Suffer Losses," *sdxcentral*, September 13, 2021, at https://www.sdxcentral.com/articles/news/ericsson-cisco-samsung-gain-telco-gear-share-as-huawei-nokia-suffer-losses/2021/09/.

[38] Sijia Jiang and Michael Martina, "Huawei's $105 Billion Business at Stake After U.S. Broadside," Reuters, May 16, 2019, at https://www.reuters.com/article/us-usa-trade-china-huawei-analysis/huaweis-105-billion-business-at-stake-after-u-s-broadside-idUSKCN1SM123.

[39] "Investment Intelligence: Huawei's 92 Core Suppliers Take Stock (source: China Business Industry Research Institute)," November 30, 2018, at http://finance.eastmoney.com/a/201811309968621 42.html.

[40] Sherisse Pham, "Losing Huawei as a Customer Could Cost U.S. Tech Companies $11 Billion," *CNN Business*, May 17, 2019, at https://www.cnn.com/2019/05/17/tech/huawei-us-ban-suppliers/index.html.

[41] Stefan Pongratz, "Key Takeaways—1H 2021 Total Telecom Equipment Market," Dell'Oro Group, September 13, 2021, at https://www.delloro.com/key-takeaways-1h21-total-telecom-equipment-market/.

[42] CRS Report R46693, *Huawei and U.S. Law*, by Stephen P. Mulligan and Chris D. Linebaugh.

[43] Eric Harwit, "Building China's Telecommunications Network: Industrial Policy and the Role of Chinese State-Owned, Foreign, and Private Domestic Enterprises," *The China Quarterly*, June 2007, p. 317, at https://www.jstor.org/stable/pdf/20192772.pdf.

[44] Yun Wen, "The Rise of Chinese Transnational ICT Corporations" (Dissertation, Simon Fraser University, 2017), pp. 66-67, at https://core.ac.uk/download/pdf/132453592.pdf.

imported telecommunications products,[45] supported joint ventures between domestic and foreign firms,[46] including U.S. firms,[47] and permitted private ownership of high-technology businesses.[48]

Ren Zhengfei, an engineer who served in the People's Liberation Army (PLA) Engineering Corps, started Huawei Technologies Co., Ltd. (Huawei) in 1987 as a private enterprise.[49] Initially, Huawei sold imported telephone switches.[50] By 1990, Huawei began making its own switches, and in 1993 released the C&C08, the most advanced digital switch in China at the time.[51]

While Huawei asserts its research and development (R&D) investments led to the invention of the switch, some researchers assert that the Chinese government assisted in its development. Specifically, a consortium of Chinese government agencies shared with domestic firms knowledge gained from joint ventures—business partnerships between Chinese and foreign firms that required foreign firms to transfer knowledge in exchange for access to the market—including knowledge of advanced switches.[52] Researchers say the shared knowledge helped domestic firms, including Huawei, "catch up" to foreign competitors.[53] The C&C08 gained the attention of the PLA, which contracted with Huawei to supply its telecommunications network.[54] The proceeds allowed Huawei to increase its R&D investments, develop new technologies, and expand in China,[55] with the support and protection of the Chinese government.[56]

In 1996, the Chinese government adopted policies to promote the development of domestic telecommunications technologies to counter the expansion of foreign firms in the Chinese telecommunications market, and to ensure security of Chinese networks.[57] It ended special import

[45] Eric Harwit, "Building China's Telecommunications Network: Industrial Policy and the Role of Chinese State-Owned, Foreign, and Private Domestic Enterprises," *The China Quarterly*, June 2007, p. 317, at https://www.jstor.org/stable/pdf/20192772.pdf.

[46] Ibid., pp. 318-321. (Discussing how foreign firms seeking to do business in China were required to form joint ventures with a local partner. The Chinese government required foreign firms to share their technologies and knowledge with Chinese firms to build indigenous capabilities.)

[47] Firms, including Lucent, Intel, AT&T, Motorola, and IBM, were eager to enter the Chinese market, but also recognized the risks of joint ventures—specifically, that Huawei could gain insight into their technologies and business strategies and compete with them in the future. See Bruce Gilley, "Huawei's Fixed Line to Beijing," *Far Eastern Economic Review*, December 28, 2000, p. 95, at https://web.pdx.edu/~gilleyb/Huawei_FEER28Dec2000.pdf.

[48] Yun Wen, "The Rise of Chinese Transnational ICT Corporations" (Dissertation, Simon Fraser University, 2017), p. 64, at https://core.ac.uk/download/pdf/132453592.pdf.

[49] Huawei Investment and Holding Co., Ltd., *2020 Annual Report*, March 2021, at https://www-file.huawei.com/minisite/media/annual_report/annual_report_2020_en.pdf.

[50] Switches are devices that enable the transmission (i.e., routing) of voice and data across telephone networks to facilitate communications between subscribers.

[51] Nathaniel Ahrens, *China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan*, Center for Strategic and International Studies, February 2013, pp. 3-4, at https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf.

[52] Qing Mu and Keun Lee, "Knowledge diffusion, market segmentation and technological catch-up: The case of the telecommunication industry in China," *Research Policy*, August 2005, p. 775, at https://www.sciencedirect.com/science/article/abs/pii/S0048733305000946?via%3Dihub.

[53] Ibid., p. 779.

[54] Nathaniel Ahrens, *China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan*, Center for Strategic and International Studies, February 2013, pp. 3-4, at https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf.

[55] Ibid.

[56] See Bruce Gilley, "Huawei's Fixed Line to Beijing," *Far Eastern Economic Review*, December 28, 2000, p. 95, at https://web.pdx.edu/~gilleyb/Huawei_FEER28Dec2000.pdf.

[57] Eric Harwit, "Building China's Telecommunications Network: Industrial Policy and the Role of Chinese State-

policies for telecommunications products, moved away from using foreign technologies in its networks, and adopted policies favoring domestic technology firms.[58] The government identified certain Chinese firms, including Huawei, as "national champions"—firms that could help it build a domestic telecommunications industry.[59] National champions, including Huawei, received preferential policy treatment, access to low-cost financing, R&D funding, and tax benefits.[60]

In 1998, the Chinese government established a "buy local" policy,[61] and offered domestic firms, including Huawei, access to low-cost loans and low-cost financing for their customers.[62] A number of researchers and journalists have attributed Huawei's rise in the telecommunications equipment industry to this support from the Chinese government.[63] Research in 1998 indicates "the Beijing headquarters of China Construction Bank lent Huawei [about $600 million] in buyer's credit, representing 45% of the total such credit it extended that year."[64] Chinese government financing allowed Huawei to offer low-cost equipment and financing to customers, win contracts, and gain market share in China. For example, Huawei's share of the Chinese switch market was about 20% in 1996[65] and grew to 42% in 2004, which scholars attribute to strong government support.[66]

With revenues it earned from the Chinese market, Huawei expanded globally. By the end of 2001, Huawei had established offices in 45 countries,[67] including the United States.[68] In the first quarter

Owned, Foreign, and Private Domestic Enterprises," *The China Quarterly*, June 2007, p. 327, at https://www.jstor.org/stable/pdf/20192772.pdf.

[58] Nathaniel Ahrens, *China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan*, Center for Strategic and International Studies, February 2013, p. 27, at https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf.

[59] Lindsay Maizland and Andrew Chatzky, *Huawei: China's Controversial Tech Giant*, Council on Foreign Relations, August 6, 2020, at https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

[60] Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019, at https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

[61] Eric Harwit, "Building China's Telecommunications Network: Industrial Policy and the Role of Chinese State-Owned, Foreign, and Private Domestic Enterprises," *The China Quarterly*, June 2007, p. 327, at https://www.jstor.org/stable/pdf/20192772.pdf.

[62] Alex Rubin, Alan Omar Loera Martinez, and Jake Dow, et al., *The Huawei Moment*, Center for Security and Emerging Technology, June 2021, p. 32, at https://cset.georgetown.edu/publication/the-huawei-moment/.

[63] Bruce Gilley, "Huawei's Fixed Line to Beijing," *Far Eastern Economic Review*, December 28, 2000, p. 96, at https://web.pdx.edu/~gilleyb/Huawei_FEER28Dec2000.pdf; Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019, at https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736; Robert D. Atkinson, "How China's Mercantilist Policies Have Undermined Global Innovation in the Telecom Equipment Industry," *Information Technology and Innovation Foundation*, June 22, 2020, at https://itif.org/sites/default/files/2020-china-mercantilist-telecom-equipment-industry.pdf; and Alex Rubin, Alan Omar Loera Martinez, and Jake Dow, et al., *The Huawei Moment*, Center for Security and Emerging Technology, June 2021, p. 32, at https://cset.georgetown.edu/publication/the-huawei-moment/.

[64] Bruce Gilley, "Huawei's Fixed Line to Beijing," *Far Eastern Economic Review*, December 28, 2000, p. 96, at https://web.pdx.edu/~gilleyb/Huawei_FEER28Dec2000.pdf.

[65] Eric Harwit, "Building China's Telecommunications Network: Industrial Policy and the Role of Chinese State-Owned, Foreign, and Private Domestic Enterprises," *The China Quarterly*, June 2007, p. 329, at https://www.jstor.org/stable/pdf/20192772.pdf.

[66] Eric Harwit, "Telecommunications and the Internet in Shanghai: Political and Economic Factors," *Urban Studies*, vol. 42, no. 10 (September 2005), p. 1849, at https://www.jstor.org/stable/pdf/43197202.pdf.

[67] Evan S. Medeiros, Roger Cliff, and Keith Crane, et al., *A New Direction for China's Defense Industry* (RAND Corporation, 2005), p. 219, at https://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG334.pdf.

[68] Dan Steinbock, "The Case for Huawei in America (a report prepared for Huawei)," July 15, 2012, p. 12, at https://huawei.mediaroom.com/download/20120904+Case+for+Huawei+in+America-Huawei+%28ds%29.pdf.

of 2009, analysts reported Huawei doubled its share of the global network equipment market to 15%, surpassing Alcatel-Lucent (14%) and coming in third behind Ericsson (33%) and Nokia-Siemens (21%).[69] By the end of 2009, Huawei surpassed Nokia in revenue to become the second-largest equipment maker in the world.[70] In 2012, it surpassed Ericsson to become the largest.[71]

Huawei asserts it was able to expand globally due to investments in R&D, improved products, low pricing, and customized service—an assertion supported by some carriers.[72] However, many analysts attribute some of Huawei's growth to Chinese government assistance.

Researchers at the Institute of Developing Economies, a Japanese research center affiliated with the Japan External Trade Organization, which conducts economic studies on developing regions, attributes Huawei's growth to state-supported financing. According to its research, in 2004, the China Development Bank (CDB) provided Huawei a credit line of $10 billion, and the Export-Import Bank of China gave an additional $600 million to expand globally.[73] Researchers at the Center for American Progress, a U.S.-based public policy institute, assert Huawei "owes its rise to Chinese industrial policies that have suppressed global competition for nearly two decades," and to state-supported financing.[74] According to its research, the CDB provided an additional $30 billion in 2009 for Huawei's expansion globally.[75] Scholars at the Center for Strategic and International Studies (CSIS), a Washington, DC, public policy research center, found Huawei "slashed prices well below that of its competitors, purportedly sometimes by as much as 70 percent, and provided vendor-financed loans to their customers" to win global market share.[76]

Some analysts attribute Huawei's growth to questionable trade practices, including forced technology transfer.[77] According to a July 2021 report by the Center for Security and Emerging Technology (CSET) at Georgetown University, "Huawei has also benefitted during its rise from the business environment fostered by Beijing that normalized technology transfer from foreign firms."[78] In addition to forced technology transfer, CSET also notes legal challenges by

[69] "Huawei Passes Alca-Lu in Mobile Vendor Rankings," *Fierce Wireless*, March 24, 2009, at https://www.fiercewireless.com/europe/huawei-passes-alca-lu-mobile-vendor-rankings.

[70] Tarmo Virki, "UPDATE 1-China's Huawei Takes No. 2 Spot in Mobile Gear," Reuters, November 13, 2009, at https://www.reuters.com/article/telecom-gear/update-1-chinas-huawei-takes-no-2-spot-in-mobile-gear-idUSLD56804020091113.

[71] Cyrus Lee, "Huawei Surpasses Ericsson as World's Largest Telecom Equipment Vendor," *ZDNet*, July 25, 2012, at https://www.zdnet.com/article/huawei-surpasses-ericsson-as-worlds-largest-telecom-equipment-vendor/.

[72] Reply Comments of the Rural Wireless Association to the Federal Communication Commission (FCC) Public Notice, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs* (WC Docket No. 18-89), December 7, 2018, p. 15.

[73] Institute of Developing Economies, *China in Africa*, Chapter 11, "The Role of China's Financial Institutions," October 2009, p. 77, at https://www.ide.go.jp/English/Data/Africa_file/Manualreport/cia_11.html.https://www.ide.go.jp/ English/Data/Africa_file/Manualreport/cia_11.html.

[74] Melanie Hart and Jordan Link, "There Is a Solution to the Huawei Challenge," *Center for American Progress*, October 14, 2020, at https://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge/.

[75] Ibid. Table 1 provides a list of Huawei global equipment deals funded with Chinese state bank export financing.

[76] Nathaniel Ahrens, *China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan*, Center for Strategic and International Studies, February 2013, p. 10, at https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf.

[77] Generally, when a government forces foreign businesses to share their technology in exchange for market access.

[78] Alex Rubin, Alan Omar Loera Martinez, and Jake Dow, et al., *The Huawei Moment*, Center for Security and Emerging Technology, June 2021, p. 34, at https://cset.georgetown.edu/publication/the-huawei-moment/.

competitors, including U.S. firms Cisco Systems in 2003 and T-Mobile in 2014, accusing Huawei of theft of intellectual property.[79]

A June 2020 report by the Information Technology and Innovation Foundation (ITIF), a Washington, DC, think tank, attributes Huawei's rise in the global market to "mercantilist Chinese government policies."[80] ITIF analysts assert Chinese government policies forced technology transfer from foreign firms through joint ventures, restricted foreign access to the Chinese market, incentivized purchase of domestic products, guaranteed domestic market share to Chinese firms, and provided low-cost government financing that allowed Huawei to undercut competitor pricing and contributed to its growth. Still other researchers say that Huawei's success in the highly competitive global telecommunications market likely required "both high entrepreneurial achievements as well as state support."[81]

A key concern of the U.S. government centers on Huawei's growing presence in global networks and the potential risk of espionage or sabotage by the Chinese government, using Huawei equipment. Huawei asserts that it is the most scrutinized technology company in the world and that since its founding in 1987, "not one of Huawei's customers has ever experienced a major cybersecurity breach."[82] Nonetheless, some security experts caution that there is a possibility that the Chinese government could exploit a hidden vulnerability and allow theft of U.S. national security information, personal information, or intellectual property from U.S. businesses.[83]

U.S. Government Concerns with Huawei

Huawei first attracted U.S. government attention in the early 2000s, when United Nations (UN) observers accused it of violating sanctions by providing fiber-optic technology and switching equipment to Iraq.[84] The Chinese government applied to a UN sanctions committee in 1999 for approval for Huawei to supply Baghdad with telecommunications technologies. DOD raised concern that Iraq could use the technologies for military purposes; in response, the United States and United Kingdom placed holds on the contracts.[85]

---

[79] The U.S. Department of Justice would later accuse Huawei of theft of intellectual property of six U.S. companies. See DOJ, "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," press release, February 13, 2020, at https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering; see also Chuin-Wei Yap, Dan Strumpf, and Dustin Volz, et al., "Huawei's Yearslong Rise Is Littered with Accusations of Theft and Dubious Ethics," *Wall Street Journal*, May 25, 2019, at https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858.

[80] Robert D. Atkinson, "How China's Mercantilist Policies Have Undermined Global Innovation in the Telecom Equipment Industry," Information Technology and Innovation Foundation, June 22, 2020, at https://itif.org/sites/default/files/2020-china-mercantilist-telecom-equipment-industry.pdf.

[81] Peter Nolan, *China and the Global Business Revolution* (London: Palgrave McMillan, 2001), p. 863.

[82] Huawei, "5G Security. Huawei: Facts, Not Myths," *Voice of Huawei* (blog), December 17, 2019, at https://www.huawei.com/en/facts/voices-of-huawei/5g-security.

[83] U.S. Department of State, "Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications," Remarks by Dr. Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, Multilateral Action on Sensitive Technologies Conference, September 11, 2019, at https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/index.html.

[84] U.S.-China Economic and Security Review Commission, *2002 Report to Congress of the U.S.-China Security Review Commission*, July 2002, p. 139, at https://www.uscc.gov/sites/default/files/annual_reports/2002%20Annual%20Report%20to%20Congress.pdf.

[85] Colum Lynch, "Chinese Firm Probed on Links with Iraq," *Washington Post*, March 17, 2001, at

On December 11, 2001, China became a member of the World Trade Organization (WTO), agreeing through its membership to remove trade barriers, open its markets to foreign companies and their exports, and update its legal framework to add transparency, predictability, and protections into business dealings.[86] Subsequently, the Chinese equipment makers Huawei and ZTE sought to expand to the United States. However, when the companies attempted to win contracts with major U.S. network operators (e.g., AT&T, Verizon, Sprint), U.S. officials raised security concerns. In a 2010 letter to the FCC Chair, a bipartisan group of lawmakers stated,

> We are very concerned that these companies 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 so that communications can be disrupted, intercepted, tampered with, or purposely misrouted.[87]

Shortly thereafter, the parties abandoned the deals.[88] Huawei also pursued acquisitions of U.S. technology firms; however, the Committee on Foreign Investment in the United States (CFIUS) identified national security concerns, and the parties abandoned the deals before CFIUS recommended that the President block the transactions.[89] While Huawei was unsuccessful in its attempts to secure a contract with a major U.S. telecommunications provider, or to acquire U.S. technology firms, it was successful in winning work in the U.S. rural market. By offering low prices, low-cost financing, and enhanced customer service to small and rural providers, Huawei was able to gain a foothold in the U.S. telecommunications market.[90]

In 2012, the U.S. House of Representatives Permanent Select Committee on Intelligence released a report on Huawei and ZTE. The committee expressed concern with Huawei's ties to the Chinese government and military; Chinese Communist Party involvement in the Huawei organization; China's support of Huawei as a national champion advancing Chinese national goals; Huawei's growing presence in telecommunications networks globally; and the potential for espionage.[91] The committee also raised concerns over accusations from U.S. businesses that Huawei engaged in theft of trade secrets and other proprietary data.[92] The committee expressed concern that Huawei could use its presence in telecommunications networks to engage in undetected espionage against the U.S. government and businesses.[93]

---

https://www.washingtonpost.com/archive/politics/2001/03/17/chinese-firm-probed-on-links-with-iraq/87495bb6-a6d6-44a1-9d60-42813559493e/.

[86] United States Trade Representative, *2020 Report to Congress on China's WTO Compliance*, 2021, p. 5, at https://ustr.gov/sites/default/files/files/reports/2020/2020USTRReportCongressChinaWTOCompliance.pdf.

[87] Letter from Senator Jon Kyl, Senator Joseph Lieberman, and Senator Susan M. Collins, et al., to Julius Genachowski, Chairman, Federal Communications Commission, October 19, 2010, at https://www.hsgac.senate.gov/media/minority-media/congressional-leaders-cite-telecommunications-concerns-with-firms-that-have-ties-with-chinese-government.

[88] Christopher Rhoads and Rebecca Buckman, "A Chinese Telecom Powerhouse Stumbles on Road to the U.S.," *Wall Street Journal*, July 28, 2005, at https://www.wsj.com/articles/SB112250344291097987.

[89] CRS Report R46693, *Huawei and U.S. Law*, by Stephen P. Mulligan and Chris D. Linebaugh, pp. 3-5.

[90] Mike Dano, "Huawei Equipment Currently Deployed by 25% of U.S. Rural Wireless Carriers, RWA Says," December 11, 2018, at https://www.fiercewireless.com/wireless/huawei-equipment-currently-deployed-by-25-u-s-rural-wireless-carriers-rwa-says.

[91] U.S. Congress, House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Cong., 2nd sess., October 8, 2012, p. 32, at https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96.

[92] Ibid., pp. 31-32.

[93] Ibid., pp. 13-30.

In 2017, as companies began testing 5G technologies,[94] U.S. officials again raised security concerns with integrating Huawei technologies in U.S. networks and systems.[95] U.S. officials raised specific concerns about a 2017 National Intelligence Law in China,[96] which requires that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law."[97] U.S. officials, including members of Congress, expressed concern that the law would require Huawei to turn over data to the Chinese government upon request,[98] an assertion Huawei denies.[99]

U.S. Government Restrictions on the Use of Huawei Equipment

Starting in 2017, the U.S. government began imposing restrictions on Huawei. It restricted the use of Huawei equipment in DOD networks, prohibited federal agencies from purchasing or using Huawei equipment, prohibited the use of federal grant and loan funds for Huawei equipment, restricted exports to Huawei, and funded the replacement of Huawei equipment in U.S. networks.

Restrictions on DOD's Use of Huawei Equipment

At a June 22, 2016, hearing before the House Armed Services Committee, Representative Rogers questioned DOD officials about the department's use of Huawei equipment. Acting Assistant Secretary of Defense for Homeland Defense and Global Security Thomas Atkin stated, "There are currently no Huawei or ZTE products on the DOD Unified Capabilities Approved Products List (APL)."[100] The DOD later clarified, "[t]he fact that a product does not appear on an APL does not mean contractors cannot offer bids or that the government can still select outside the APL. Short of suspension and debarment, federal contractors and vendors are not precluded from competing on DOD contracts."[101] The hearing was one of the first indicators that the U.S. government did

[94] Huawei Investment and Holding Co., Ltd., 2017 Annual Report, March 22, 2018, p. 8, at https://www.huawei.com/-/media/corporate/pdf/annual-report/annual_report2017_en.pdf?la=en. See also Afif Osseiran, "What Are 5G Systems For?," *Ericsson* (blog), February 23, 2017, at https://www.ericsson.com/en/blog/2017/2/what-are-5g-systems-for.

[95] Senator Marco Rubio, "Rubio, Cotton, Van Hollen, Schumer Introduce NDAA Amendment on Huawei, ZTE," press release, June 7, 2018, at https://www.rubio.senate.gov/public/index.cfm/press-releases?ID=D49158AB-DA0F-4C89-BFD6-02C7DF35A536. See also Federal Communications Commission, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs—Huawei Designation*, June 30, 2020, pp. 2-10, at https://docs.fcc.gov/public/attachments/DA-20-690A1.pdf.

[96] S.Con.Res. 10. See also FCC, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs—Huawei Designation*, June 30, 2020, p. 6, at https://docs.fcc.gov/public/attachments/DA-20-690A1.pdf.

[97] Chinese National People's Congress Network, "National Intelligence Law of the People's Republic (Adopted at the 28th meeting of the Standing Committee of the 12th National People's Congress)," June 27, 2017, at http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

[98] S.Con.Res. 10.

[99] Arjun Kharpal, "Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice," *CNBC*, March 5, 2019, at https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

[100] U.S. Congress, House Committee on Armed Services, *Military Cyber Operations*, 114th Cong., 2nd sess., June 22, 2016, H.A.S.C. No. 114-128.

[101] Ibid.

not have a clear picture of its own use of Huawei equipment, or clear policies on Huawei use in U.S. networks.

On December 12, 2017, Congress enacted the National Defense Authorization Act (NDAA) for Fiscal Year 2018 (P.L. 115-91). Section 1656(a) directs the Secretary of Defense to certify to congressional defense authorization and appropriations committees[102] whether DOD uses "covered defense telecommunications equipment or services" in its nuclear command, control, and communications, ballistic missile defense, and continuity of government systems. Congress named Huawei equipment as equipment "covered" under the act. Section 1656(b) prohibited the Secretary from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses Huawei equipment or services as an essential component of that system, effective one year from the date of enactment.[103]

After President Trump signed the FY2018 NDAA into law, DOD officials reported that the department was screening contracts for Huawei equipment and services. In a Senate Armed Services Committee hearing on April 19, 2018, Secretary of the Navy Richard Spencer testified the Navy had halted a contract because it found that a division of the company with which DOD was contracting listed Huawei as a joint venture partner.[104] Further, following February 2018 testimony from intelligence officials expressing concern about Huawei devices at a hearing of the Senate Select Committee on Intelligence,[105] DOD banned the sale of Huawei devices at military exchanges in April 2018 due to reported concerns from military officials that the Chinese government could use the devices to track the movement and location of soldiers.[106] Thus, after the passage of the FY2018 NDAA, DOD increased its efforts to identify and restrict use of Huawei equipment in DOD supply chains and networks, and on military bases.

Restrictions on Federal Agency Use of Huawei Equipment

On August 8, 2018, as DOD was drafting rules for implementing Section 1656 of the FY2018 NDAA, Congress passed and the President signed the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (P.L. 115-232). The law has three major provisions that limit the use of Huawei equipment:

- Section 889(a)(1)(A) prohibits federal agencies from procuring equipment, systems, or services that use "covered" telecommunications equipment or services as a substantial or essential component of a system.
- Section 889(a)(1)(B) prohibits federal agencies from entering into a contract with an entity that uses "covered" equipment, system, or service.

[102] The Committee on Armed Services and the Committee on Appropriations of the Senate; and the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

[103] P.L. 115-91, Title XVI, Subtitle D, §1656.

[104] U.S. Congress, Senate Committee on Armed Services, Hearing to Receive Testimony on the Posture of the Department of the Navy in Review of the Defense Authorization Request for Fiscal Year 2019 and the Future Years Defense Program, 115th Cong., 2nd sess., April 19, 2018, p. 19 (transcript), at https://www.armed-services.senate.gov/hearings/18-04-26-department-of-defense-budget-posture.

[105] U.S. Congress, Senate Select Committee on Intelligence, *Open Hearing on Worldwide Threats*, 115th Cong., 2nd sess., February 13, 2018, S. Hrg. 115-278.

[106] Stu Woo and Gordon Lubold, "Pentagon Orders Stores on Military Bases to Remove Huawei, ZTE Phones," *Wall Street Journal*, May 2, 2018, at https://www.wsj.com/articles/pentagon-asking-military-bases-to-remove-huawei-zte-phones-1525262076.

- Section 889(b)(1) of the NDAA prohibits agencies from using federal grants and loans for "covered" telecommunications equipment.
- In the act, Congress defined "covered" equipment as equipment produced by Huawei and other China-based equipment manufacturers that Congress identified as companies that pose a threat to U.S. national security.[107] Congress mandated Section 889(a)(1)(A) to take effect August 13, 2019, one year after enactment of the FY2019 NDAA, and Sections 889(a)(1)(B) and Section 889(b)(1) to take effect two years after the date of enactment of the FY2019 NDAA or August 13, 2020.

Similarities and Differences Between FY2018 and FY2019 NDAAs

While Section 1656 of the FY2018 NDAA and Section 889(a)(1)(A) of the FY2019 NDAA are similar, there are several notable differences:

- Section 1656 in the NDAA for FY2018 is DOD-specific. It applies to equipment, systems, or services to carry out the DOD nuclear deterrence or homeland defense missions. Section 889 pertains to all federal executive agency systems.
- Section 889 exempts certain activities (e.g., services that enable connections to the facilities of a third party, such as backhaul, roaming, or interconnection arrangements; or telecommunications equipment that cannot route or redirect user data traffic).[108] Section 1656 has no such exemptions.
- Section 1656 (b)(2) provides the Secretary of Defense with authority to waive the prohibitions on a case-by-case basis for an additional year if the waiver is in the national interest, and if the Secretary certifies to the congressional committees[109] that the Secretary is removing the covered equipment. Section 889 provides agency heads with the authority to issue a one-time waiver to an entity for no more than two years if the entity provides a compelling justification for the additional time; a description of the presence of covered telecommunications equipment or services in its supply chain; and a phase-out plan to eliminate use of such covered equipment, which the agency head must provide to certain

[107] P.L. 115-232, §889(f).

[108] General Services Administration (GSA), "GSA Implementation of Section 889, Frequently Asked Questions 3.0," September 21, 2020, at https://www.gsa.gov/cdnstatic/Section%20889%20-%20FAQs%2030.pdf. (*Backhaul* generally means the links between the edge of a network and the core network, such as the link between cell towers and the core network; the links can be wired or wireless. *Roaming* means the cellular communications received by a visited network when the caller cannot reach the home network, which may occur when there is lack of coverage or because traffic is too high on the home network, and is usually through agreement between the carriers. *Interconnection agreements* are agreements between two carriers to hand off traffic from customer A's network to customer B's network.) See Letter from Christopher D. Roberti, Senior Vice President, U.S. Chamber of Commerce, et al., to Dr. Michael E. Wooten, Administrator, Office of Federal Procurement Policy, Office of Management and Budget, September 14, 2020, at https://www.uschamber.com/assets/archived/images/200914_us_chamber_comment_letter_sec_889_part_b_interim_rule_final_1.0.pdf (stating generally that these activities were exempt to "enable the section 889 prohibition to exist alongside the routine traffic exchanges and interconnection agreements that are necessary for global communications … which carriers are legally obligated to interconnect with (47 U.S.C §251) and offer voice and data roaming to (47 CFR §20.12) other domestic providers that may have covered equipment or services in their networks or facilities.").

[109] As defined in 10 U.S.C., §101(a)(16), which includes the Committee on Armed Services and the Committee on Appropriations of the Senate and of the House of Representatives.

congressional committees.[110] Section 889 also grants the Director of National Intelligence authority to provide a waiver to an agency, extending the date, if the Director determines the waiver is in the U.S. national security interest.

- Section 1656 lists both the People's Republic of China (PRC) and the Russian Federation as "covered countries." Section 889 lists only the PRC as a "covered foreign country."
- Section 1656 defines "covered telecommunications equipment" as equipment produced or provided by Huawei or ZTE, or using such equipment, or from any entity that the Secretary reasonably believes to be owned or controlled by a foreign government. Section 889 names Huawei, ZTE, and three additional companies,[111] and allows the Secretary of Defense in consultation with the Office of the Director of National Intelligence and Federal Bureau of Investigation to identify other companies controlled by or connected to a foreign government for purposes of this section.

Benefits and Challenges with Section 1656 and Section 889

A key benefit of Section 1656 and Section 889 is that they restrict the use of U.S. government funding to foreign companies that the U.S. government determined to have engaged in activities contrary to U.S. national security and foreign policy interests. Additionally, they require U.S. agencies and entities (e.g., grantees, businesses) to gain visibility into their supply chains to identify the presence of untrusted equipment in U.S. networks. Supply chain experts note that visibility into supply chains is the first step in assessing and mitigating security risks.[112] U.S. agencies have acknowledged the value of the activities required under Sections 1656 and 889. For example, DOD officials supported the provisions, citing challenges they had in gaining visibility into their supply chains during their response to the COVID-19 pandemic, and recognized the value of examining telecommunication supply chains for risks.[113]

Agencies also recognized the complexity of the task, and expressed concern for the timelines. Before agencies published rules to implement Section 1656 and Section 889, the Office of Management and Budget (OMB) requested an extension on the timeline.[114] On June 4, 2019, the then-Acting Director of OMB submitted a legislative proposal to Vice President Pence, for consideration by the Senate in the FY2020 NDAA. The OMB Director requested a two-year extension on implementation of Section 889(a)(1)(B), which prohibits the federal government from contracting with an entity that *uses* covered equipment, and Section 889(b)(1), which

[110] The term "appropriate congressional committees" is defined in Section 889 as the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Homeland Security and Governmental Affairs of the Senate; and the Committee on Financial Services, the Committee on Foreign Affairs, and the Committee on Oversight and Government Reform of the House of Representatives.

[111] The three additional companies are Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company.

[112] Cybersecurity and Infrastructure Security Agency, *Building a More Resilient ICT Supply Chain: Lessons Learned During the Covid-19 Pandemic*, p. 30, November 2020, at https://www.cisa.gov/sites/default/files/publications/lessons-learned-during-covid-19-pandemic_508_2.pdf.

[113] U.S. Congress, House Committee on Armed Services, *Department of Defense COVID-19 Response to Defense Industrial Base Challenges*, 116th Cong., 2nd sess., June 10, 2020, H.A.S.C. No. 116-84 (Washington: GPO, 2021), p. 27, at https://www.congress.gov/event/116th-congress/house-event/LC66027/text.

[114] P.L. 115-232, Section 889(f).

prohibits the use of federal grant and loan funds for covered equipment. In a letter to the Vice President, the OMB Director stated,

> While the Administration recognizes the importance of these prohibitions to national security, a number of agencies have heard significant concerns from a wide range of potentially impacted stakeholders who would be affected by section 889, which the Administration believes could be addressed with a modified implementation schedule. Challenges that could arise under the current schedule potentially include a dramatic reduction in the available industrial base (including small business suppliers), who will no longer be able to sell to the Government, either because their non-government business is more valuable, or due to the cost of the potential regulatory burdens associated with compliance with subsections (a)(l)(B) and (b)(l).[115]

The intent of the request, according to a White House spokesperson, was to give federal contractors and grantees, including rural federal grant recipients, "time to extricate themselves from doing business with Huawei and other Chinese tech companies listed in the NDAA."[116] The OMB Director pressed for greater stakeholder engagement, and stated that the "Administration believes, based on feedback from impacted stakeholders, that this additional preparatory work will better ensure the effective implementation of the prohibition without compromising desired security objectives."[117] However, a few days later, Reuters reported that the OMB Director told Congress it could meet the two-year deadline. In a letter to Senator Jim Inhofe, then-chair of the Senate Armed Services Committee, the OMB Director stated, "Congress has made it clear in recent days the importance of implementing the law within the two years provided, and we will," according to reports from Reuters.[118]

While OMB focused on implementation of Section 889(b), the Federal Acquisition Regulations (FAR) Council was working on Section 889(a), the acquisition-related restrictions. The FAR Council is the federal body responsible for writing and revising the Federal Acquisition Regulations—policies and procedures federal agencies follow during procurements. The FAR Council is composed of DOD, the General Services Administration (GSA), the National Aeronautics and Space Administration (NASA), and OMB, which serves as chair.

On August 13, 2019, the FAR Council published rules implementing Section 889(a)(1)(A)—the rules prohibiting federal agencies from procuring covered equipment.[119] The rules, effective immediately, prohibit contractors from providing any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or a waiver applies. Under the rules, contractors must report any such equipment, systems, or services discovered

[115] Letter from Russell T. Vought, Acting Director, Office of Management and Budget, to Honorable Michael R. Pence, President of the Senate, June 4, 2019, pp. 3-4, at https://www.whitehouse.gov/wp-content/uploads/2019/06/Pence-Proposal.pdf.

[116] Dan Strumpf, "Acting U.S. Budget Chief Seeks Reprieve on Huawei Ban," *Wall Street Journal*, June 10, 2019, at https://www.wsj.com/articles/acting-budget-chief-seeks-reprieve-on-huawei-ban-11560108418.

[117] Letter from Russell T. Vought, Acting Director, Office of Management and Budget, to Honorable Michael R. Pence, President of the Senate, June 4, 2019, p. 3, at https://www.whitehouse.gov/wp-content/uploads/2019/06/Pence-Proposal.pdf.

[118] Roberta Rampton, "White House Says It Will Meet Two-Year Deadline for Huawei Ban for Contractors," Reuters, June 12, 2019, at https://www.reuters.com/article/us-usa-trade-huawei/white-house-says-it-will-meet-two-year-deadline-for-huawei-ban-for-contractors-idUSKCN1TE033.

[119] DOD, GSA, and NASA, "Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment," 84 *Federal Register* 40216, August 13, 2019.

during contract performance; the requirement flows down to subcontractors.[120] As permitted under Section 889, the rules allow agency heads to grant entities a one-time waiver on a case-by-case basis for up to two years; in other circumstances, the DNI may grant a waiver to an agency if the Director determines the waiver is in the U.S. national security interest.[121]

In the public comment period, vendors and industry associations generally expressed concern with the rules and the timeline. The Professional Services Council (PSC), an association of over 400 companies that provide federal agencies with products and services, said the rules require contractors to engage in a "time-consuming, burdensome and costly exercise" to determine whether products they use are from a banned company.[122] The U.S. Chamber of Commerce noted that "contractors need a reasonable amount of time to investigate and determine with relative confidence that the equipment in question is actually covered under ... the rule."[123]

On December 13, 2019, the FAR Council published a second interim rule, effective immediately, amending the FAR to require contractors to certify annually whether they offer covered equipment, systems, or services to the government, including Huawei equipment or services.[124] Only contractors who answer affirmatively in their annual certification are required to disclose more information on a contract-by-contract basis.

While the intent of the second interim rule was to reduce regulatory burden, vendors would still need to assess their supply chains to determine whether they offer covered products or services to the government. The FAR Council acknowledged challenges with visibility in the supply chain, noting, "[d]ata on the extent of the presence of the covered telecommunications equipment and services in the global supply chain is extremely limited, as is information as to the costs of removing and replacing covered equipment or services where it does exist."[125] Nonetheless, vendors were required to affirm that they conducted a "reasonable inquiry" into whether they use covered equipment or services, and report on covered equipment use annually.[126]

Industry associations continued to express concerns on implementation challenges. On March 12, 2020, the PSC and the National Defense Industrial Association (NDIA), a trade association for the U.S. government and defense industry, wrote a joint letter to Senator Jim Inhofe, Senate Armed Services Committee Chair, expressing concern with the timeline for Section 889(a)(1)(B). This section prohibits federal agencies from entering into a contract with an entity that *uses* covered equipment, systems, or services. The industry associations requested that Congress extend the timeline on Section 889(a)(1)(B) implementation from August 2020 to February 2021, citing challenges presented by the COVID-19 pandemic. The organizations noted,

> Part B will impose significant financial and operational costs on medium and small-sized firms at a moment of substantial uncertainty and hardship. While we agree that Part B addresses a significant problem in defense supply chains, and that additional measures are

[120] DOD, GSA, and NASA, "Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment," 84 *Federal Register* 40216, December 13, 2019.

[121] Ibid.

[122] Daniel Wilson, "Huawei Ban's Compliance Rules Too Taxing for Contractors," *Law360*, November 1, 2019, at https://www.law360.com/articles/1215716/huawei-ban-s-compliance-rules-too-taxing-for-contractors.

[123] Ibid.

[124] DOD, GSA, and NASA, "Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment," 84 *Federal Register* 68314, December 13, 2019.

[125] DOD, GSA, and NASA, "Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment," 85 *Federal Register* 42671, July 14, 2020.

[126] Ibid., p. 42666.

> needed to protect DOD information assets from covered equipment, COVID-19 has made the current implementation timeline infeasible.[127]

In May 2020, Senators Rubio and Cardin urged OMB to consider the impact to small business contractors when crafting guidance or regulations related to Section 889(a)(1)(B).[128] They asked OMB to provide clear processes and adequate time for small businesses to comply.

DOD officials also expressed concern with the implementation of Section 889. In June 2020, then-Under Secretary of Defense for Acquisition and Sustainment Ellen Lord testified that the COVID-19 pandemic required DOD to accelerate its understanding of its supply base, the vendors involved, and whether companies associated with adversaries were key suppliers.[129] The Under Secretary noted the value in conducting an inquiry into its supply chain, and the difficulty in identifying all suppliers for all components and all tiers of its supply chain; in a subsequent discussion on Section 889(a)(1)(B), the Under Secretary stated Section 889 may have unintended consequences to the Defense Industrial Base, noting, "The thought that somebody six or seven levels down in the supply chain could have one camera in a parking lot, and that would invalidate one of our major primes being able to do business with us, gives us a bit of pause."[130]

On July 14, 2020, the FAR Council issued an interim rule implementing Section 889(a)(1)(B).[131] The new rule took effect August 13, 2020, for all federal agencies and contractors, unless an agency head granted a waiver or there was a previous exemption. Entities had 60 days to provide comments on the interim rule that the Council could consider before it issued final rules.

Some industry stakeholders submitted comments to the FAR Council on the interim rules, seeking clarification on language in Section 889(a)(1)(B) prohibiting an agency head to "enter into a contract … with an entity that uses any equipment, system, or service that uses covered telecommunications equipment" as an essential component of any system. Industry associations appealed to Congress to clarify the language in Section 889(a)(1)(B), including terms such as "uses" and "essential component," and to allow agencies to grant blanket waivers or extensions, or extend the timeline so that entities had time to reasonably assess use of covered equipment.[132]

Some in Congress proposed amendments to the FY2021 NDAA to extend the deadlines for compliance with Section 889(a)(1)(B). In June 2020, Senator Ron Johnson proposed an amendment (2193) to the FY2021 NDAA that would have extended the deadline for Section 889(a)(1)(B) compliance to August 2021.[133] In July 2020, Representative Virginia Foxx proposed

---

[127] Letter from Herbert J. Carlisle, General, USAF (Ret.), President and CEO, NDIA, and David J. Berteau, President and CEO, PSC, to U.S. Senator James Inhofe, Senate Armed Services Committee, Chairman, et al., March 31, 2020, at https://www.pscouncil.org/a/Resources/2020/PSC_and_NDIA_Letter_for_Extension_to_NDAA_Section_889_Effective_Date.aspx.

[128] U.S. Senator Marco Rubio, "Rubio, Cardin Urge OMB to Consider Small Business Contractors When Issuing Regulations to Secure the Supply Chain," press release, May 4, 2020, at https://www.rubio.senate.gov/public/index.cfm/2020/5/rubio-cardin-urge-omb-to-consider-small-business-contractors-when-issuing-regulations-to-secure-the-supply-chain.

[129] U.S. Congress, House Committee on Armed Services, *Department of Defense COVID-19 Response to Defense Industrial Base Challenges*, 116th Cong., 2nd sess., June 10, 2020, H.A.S.C. No. 116-84 (Washington: GPO, 2021), p. 10, at https://www.congress.gov/event/116th-congress/house-event/LC66027/text.

[130] Ibid.

[131] DOD, GSA, and NASA, "Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment," 85 *Federal Register* 42665, July 14, 2020.

[132] Lauren C. Williams, "DOD Looks for Extension on Huawei Ban," *FCW*, June 16, 2020, at https://fcw.com/articles/2020/06/16/williams-ndaa-huawei-DOD.aspx; Letter from Industry Organizations to Congress, July 15, 2020, at https://www.uschamber.com/sites/default/files/200715_coalition_sec.889delay_congress.pdf.

[133] Professional Services Council, "Senator Ron Johnson Amendment to the Fiscal Year 2021 NDAA," June 2020, at

an amendment to Section 889(a)(1)(B) that would have extended the timeline through January 1, 2022.[134] Congress did not consider either amendment in its deliberations on the FY2021 NDAA.

On August 12, 2020, a day before the effective date, the DOD Under Secretary for Acquisition and Sustainment requested that the DNI Director grant DOD a waiver to the prohibitions listed in Section 889 (a)(1)(B), as permitted under Section 889(d)(2) of the NDAA for FY2019.[135] The DNI granted DOD a temporary waiver until September 30, 2020. On September 29, 2020, the DNI extended the waiver through September 30, 2022. The waiver allows DOD to continue to execute procurement actions for specified items deemed to be of "low-risk potential"[136] and necessary to execute the DOD mission, which the DNI asserts is in the national interest.[137] Further, the DNI requested that DOD provide information and updates on risks related to the waiver and mitigation measures.[138] DOD is the only agency that received a blanket extension; thus, contractors supplying other agencies are still required to meet the provisions in Section 889(a)(1)(B), unless they receive an individual waiver from an agency.

On January 15, 2021, DOD issued final rules for DOD agencies that included provisions to ensure compliance with Section 1656 and Section 889,[139] effective immediately.[140] DOD required its vendors to stipulate annually whether "covered defense telecommunications equipment or services" are included in their product offerings to the U.S. government.[141] If a vendor answers affirmatively, it must report for each contract with DOD use of any covered equipment or services; DOD extended the reporting from one to three business days and extended the mitigation from 10 to 30 business days.[142] Generally, failure to submit required information to the government constitutes a breach of contract that can lead to cancellation, termination, and financial consequences. DOD urged contractors to develop a compliance plan that will allow them to submit accurate representations to the government in the course of their offers.[143] Major

https://www.pscouncil.org/a/Resources/2020/Sen._Johnson_889_Amendment_to_FY21_NDAA.aspx.

[134] "Amendment to Rules Committee Print 116-57, Offered by Ms. Foxx of North Carolina," July 13, 2020, at https://amendments-rules.house.gov/amendments/FOXX_057_xml713201211421142.pdf.

[135] Memorandum from John Ratcliffe, Director of National Intelligence, to Ellen M. Lord, Under Secretary for Acquisition and Sustainment, Department of Defense, August 12, 2020, at http://thecgp.org/images/08-12-20_Memo_DNI-Response-to-DOD-Waiver-Request_20-00733_U-FOUO_SIGNED-.... pdf.

[136] The Office of the Director of National Intelligence (ODNI) provided guidance to executive agencies for use when evaluating the risk associated with granting a waiver. Specifically, the ODNI Strategic Supply Chain Security Guidance identifies "high risk" Product Service Codes (PSCs). If the procurement associated with a waiver request contains any "high risk" PSCs, ODNI has instructed that additional scrutiny and analysis should be undertaken before the agency head grants the waiver.

[137] Memorandum from John Ratcliffe, Director of National Intelligence, to Ellen Lord, Under Secretary for Acquisition and Sustainment, Department of Defense, September 29, 2020, at https://thecgp.org/images/Memo-20-00823_DOD-Request-for-Section-889-Waiver-2.pdf.

[138] Ibid.

[139] Defense Acquisition Regulations System (DFARS), DOD, "Defense Federal Acquisition Regulation Supplement: Covered Defense Telecommunications Equipment or Services (DFARS Case 2018-D022)," 86 *Federal Register*, January 15, 2021.

[140] The DNI granted DOD a waiver through September 30, 2022, to continue to do business with companies that manufacture "low-risk, high-volume" items (e.g., food, clothing, transportation) needed to support DOD's mission.

[141] DFARS 252.204-7016, Covered Defense Telecommunications Equipment or Services-Representation, at https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7016.

[142] DFARS 252.204-7018, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services, at https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7018.

[143] DOD, GSA, and NASA, "Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment," 85 *Federal Register* 42670, July 14, 2020.

vendors advised their suppliers to ensure they are in full compliance and to convey the requirement down to their suppliers at all tiers of their supply chain.[144]

Media reports indicate implementation is proving challenging for some businesses, and raising some legal questions.[145] For example, companies working on international development contracts, where there may be limited choices in terms of telecommunications services, may need to file for a waiver, a process that can reportedly take four to six weeks and delay vendor start dates.[146] Small businesses may need to hire staff to review supply chains, creating additional cost burdens.[147] Legal experts advised contractors on extensions, noting that the law allows for an extension on a case-by-case basis that could give vendors until August 13, 2022, to comply.[148] Other legal analysts advised contractors to conduct "reasonable inquiries" and education of employees and suppliers on a regular basis to ensure compliance.[149] Some vendors raised legal questions as to whether the U.S. government may be liable for costs incurred by contractors due to required changes to existing contracts.[150]

The Acquisition Reform Working Group (ARWG)—a stakeholder body composed of large industry associations that provide goods and services to DOD, including the Computing Technology Industry Association Technology Industry Council, NDIA, and the U.S. Chamber of Commerce, submitted a letter to House and Senate Armed Services Committee leadership on June 15, 2021. The ARWG expressed its support for initiatives to improve DOD systems security, but recommended that in the future Congress require input from stakeholders, a transition period or phased implementation to ensure effective compliance, and specific guidance from agencies, such as a detailed list of covered equipment, alternative equipment, and mitigation techniques.[151]

Restrictions on Federal Grants for Huawei Equipment

As the FAR Council focused on the implementation of Section 889(a)—the acquisition-related provisions in Section 889—OMB created rules for Section 889(b) that prohibit agency heads

[144] For example, see Memo from Vice President, Corporate Supply Chain, Northrop Grumman, to Northrop Grumman Supply Base, Prohibition on Procurement for Certain Telecommunication and Video Surveillance Services or Equipment, May 18, 2020, at https://www2.northropgrumman.com/suppliers/OASISDocuments/.May2020_%20MemoInterimRulingCommsSurv-SupplierComm.pdf.

[145] Theresa Hitchens, "U.S. Industry Struggles to Strip Chinese Tech from Networks," *Breaking Defense*, February 22, 2021, at https://breakingdefense.com/2021/02/us-industry-struggles-to-strip-chinese-tech-from-networks/.

[146] Jared Serbu and Scott Maucione, "Second Stage of Chinese Telecom Ban Producing Unintended Consequences," *Federal News Network*, March 29, 2021, at https://federalnewsnetwork.com/DOD-reporters-notebook-jared-serbu/2021/03/second-stage-of-chinese-telecom-ban-producing-unintended-consequences/.

[147] DOD, GSA, and NASA, "Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment," 85 *Federal Register* 42672, July 14, 2020.

[148] Michael Mortorano and Paul Ghazaryan, "Coping with Chinese Telecom Ban's Unclear Requirements," *Law360*, August 19, 2020, at https://www.law360.com/articfraudles/1302625/coping-with-chinese-telecom-ban-s-unclear-requirements.

[149] Trayce Winfrey Howard, "Section 889 Part B Redux: What Are Contractors' Compliance Obligations in 2021?," *Wiley Newsletter*, July 2021, at https://www.wiley.law/newsletter-Section-889-Part-B-Redux-What-Are-Contractors-Compliance-Obligations-in-2021.

[150] Scott S. Sheffler, "Section 889, the 'Huawei Ban' in Federal Contracts: General Scope and Considerations," Feldesman Tucker Leifer Fidell LLP (blog), August 10, 2020, at https://www.feldesmantucker.com/section-889-the-huawei-ban-in-federal-contracts-general-scope-and-considerations/.

[151] Letter from Acquisition Reform Working Group Members to Senator Jack Reed, Chairman, Senate Armed Services Committee, et al., June 15, 2021, at https://www.ndia.org/about/media/press-releases/2021/6/17/-/media/sites/press-releases/documents/arwg-fy-2022-proactive-letter-final-06152021.ashx.

from obligating or expending grant and loan funds to obtain or enter into a contract to obtain covered equipment, systems, or services. After industry input,[152] OMB refined its grant regulations, added a new section, 2 C.F.R. 200.216, to reflect the Section 889 restrictions, and published final guidance on August 13, 2020, which applies to all U.S. agency grants.[153]

Benefits and Challenges of Grant Restrictions

A benefit of the grant restrictions is that they apply to all federal granting agencies. Granting agencies integrate OMB rules into grant guidance and agreements; grantees incorporate rules into subgrantee agreements. Thus, with one set of rules from OMB, which are applicable to all agencies, there is a greater chance for consistent application of the rules related to prohibitions on covered equipment. Further, with federal grants exceeding $750 billion annually, the restrictions could significantly reduce use of untrusted equipment across many missions (e.g., homeland security, education, overseas programs).[154]

Some agencies have faced challenges implementing Section 889(b) rules, including U.S. agencies that support overseas programs through grants. Recipients of U.S. Agency for International Development (USAID) funding reported that "some 70% of missions in Africa and 65% of missions in Asia are apparently relying on service providers with prohibited equipment [e.g., Huawei, ZTE]."[155] USAID, which formed a task force on Section 889(b), surveyed current use of prohibited equipment, and requested an agency-level waiver from the DNI that would allow it, for a limited time, to permit use of affected internet and phone services. The waiver was due to expire on September 30, 2020; USAID obtained a waiver extension through September 30, 2022.[156]

In guidance to grantees, USAID emphasized its waiver does not alter the FAR requirements for contractors to disclose use of covered equipment. Individual contractors seeking a waiver are still required to provide a compelling justification for the additional time to implement the requirements under Section 889, calling for a "full and complete laydown of the presence of covered telecommunications or video surveillance equipment or services in the entity's supply chain, and a Phase-Out Plan for eliminating the covered equipment or services."[157] The agency emphasized in guidance to recipients that "it is in the best interest of the contractor to replace covered technology, if it wants to continue to receive U.S. government contracts."[158] Although Section 889(b)(2) requires agencies to prioritize funding to "rip and replace" covered equipment, USAID stipulates that grant funds can be used to remove and replace covered equipment only when the equipment is used in support of the award.[159]

---

[152] Jake Parker, "Here's What NDAA Section 889 Really Means for Federal Grants," *Security Industry Association*, August 13, 2020, at https://www.securityindustry.org/2020/08/13/heres-what-ndaa-section-889-really-means-for-federal-grants/.

[153] Office of Management and Budget, "Guidance for Grants and Agreements," 85 *Federal Register* 49515, August 13, 2020.

[154] CRS Report R40638, *Federal Grants to State and Local Governments: A Historical Perspective on Contemporary Issues*, by Robert Jay Dilger.

[155] USAID, Section 889 Task Force, "Section 889 Frequently Asked Questions (FAQs) for Contractors and Recipients of USAID awards," October 23, 2020, p. 4, at https://www.usaid.gov/sites/default/files/documents/Partner_FAQs_Master_10232020.pdf.

[156] Ibid., p. 5.

[157] Ibid.

[158] Ibid., p. 4.

[159] USAID, Section 889 Task Force, "Section 889 Frequently Asked Questions (FAQs) for Contractors and Recipients of USAID awards," October 23, 2020, p. 13, at https://www.usaid.gov/sites/default/files/documents/

Like industry stakeholders, grantees have sought clarity on Section 889(b), asking for a definitive list of banned equipment, processes on waivers, clarification on whether individual projects funded with nonfederal funds must comply, and whether funding is available for replacement equipment.[160] In May 2021, the U.S. Chief Financial Officers Council (CFOC)—an organization of CFOs and Deputy CFOs of the largest federal agencies, and senior officials from OMB and the Department of the Treasury who work together to improve financial management in the U.S. government—provided additional guidance on Section 889. The CFOC issued a list of frequently asked questions (FAQs), which provided details on covered entities, foreign countries, and equipment; processes for certifying compliance; allowable and unallowable costs; and waivers.[161]

Huawei Challenges Section 889 Restrictions in Court

On March 7, 2019, Huawei challenged the U.S. government in U.S. district court, arguing that Section 889 is unconstitutional.[162] Among other things, Huawei claimed that the U.S. government inflicted punishment on it through legislation, without provision of the protections of a judicial trial or due process.[163] In February 2020, the federal court rejected Huawei's claim, and noted, "What Huawei pejoratively labels as Congress unconstitutionally adjudicating facts is better characterized as a thorough congressional investigation into a potential threat against the nation's cybersecurity. Congress's investigation led to the passing of a defense-appropriations bill as a prophylactic response to that threat."[164]

Restrictions on USF Subsidies for Huawei Equipment

In April 2018, the FCC proposed rules prohibiting the use of the USF monies for purchase of equipment and services from companies that pose a national security risk.[165] The FCC stated that it issued the rules in response to a letter from lawmakers expressing concern about the use of Huawei equipment in U.S. telecommunications networks,[166] and to requirements in Section 1656 of the FY2018 NDAA. The USF, a fund the FCC oversees, provides subsidies to telecommunications providers to serve high-cost areas, to make available, without discrimination, communications services at reasonable charges, to all people.[167]

Partner_FAQs_Master_10232020.pdf.

[160] For example, see guidance from Brown University, "Compliance Notice," June 2, 2021, at https://compliance.brown.edu/sites/g/files/dprerj446/files/NDAA_Sec_889_Compliance_Notice_6.2.21.pdf.

[161] U.S. Chief Financial Officers Council, *2 C.F.R. Frequently Asked Questions*, May 3, 2021, pp. 10-14, at https://www.cfo.gov/assets/files/2CFR-FrequentlyAskedQuestions_2021050321.pdf.

[162] CRS Report R46693, *Huawei and U.S. Law*, by Stephen P. Mulligan and Chris D. Linebaugh.

[163] *Huawei Technologies USA, Inc., et al. v. The United States of America, et al.*, 13 (U.S. District Court for the Eastern District of Texas 2019).

[164] CRS Report R46693, *Huawei and U.S. Law*, by Stephen P. Mulligan and Chris D. Linebaugh.

[165] FCC, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket 18-89, Notice of Proposed Rulemaking, April 16, 2018, pp. 2-3, at https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

[166] Letter from Senator Tom Cotton et al., U.S. Senate, to Hon. Ajit Pai, Chairman, FCC, December 20, 2017, at https://apps.fcc.gov/edocs_public/attachmatch/DOC-349859A2.pdf.

[167] 47 U.S.C. §151.

Benefits and Challenges with USF Restrictions

A key benefit to restrictions on USF subsidies is that they target telecommunications operators, Huawei's key U.S. customers. Targeting the $8 billion USF fund—a program that subsidizes telecommunications network deployment and upgrade—and offering replacement funds through the Secure and Trusted Communications Networks Reimbursement Program,[168] provides incentives for telecommunications operators to remove untrusted equipment from U.S. networks. Further, restrictions on USF funds, which support small and rural network operators, could eliminate Huawei's last remaining foothold in the United States, which U.S. officials see as necessary to secure U.S. networks.[169]

A challenge is in implementing the restrictions. In comments to the FCC on the proposed rule, the Rural Wireless Association (RWA) stated many of its members—small and rural wireless network operators—rely on USF subsidies to build out networks and provide services in high-cost areas.[170] The RWA estimated that about 25% of U.S. rural providers use some Huawei equipment, and restricting the use of USF funds could affect network buildout and services in rural areas.[171] The FCC's proposed rule would, if adopted, "significantly and negatively impact small and rural wireless carriers' ability to operate," and the cost of compliance would overwhelm rural operators, according to the RWA.[172] The RWA argued that Section 889(b)(1) restricts use of federal grants and loan funds, not subsidies, and thus should not be applied to USF subsidies.[173]

While the RWA and others contested the FCC's proposed rule, Congress acted to codify the FCC's proposed rules, and restrict the use of USF funds for equipment that could pose a national security threat. In March 2020, Congress passed and the President signed the Secure and Trusted Communications Network Act of 2019 (P.L. 116-124). The law requires the FCC to develop a list of covered equipment—that is, equipment that poses a threat to national security—adopt rules to prohibit the use of subsidies administered by the FCC (i.e., USF) for covered equipment, and create a program to make reimbursements to providers to replace covered equipment from networks of small, rural providers. Congress authorized $1 billion to fund the replacement of covered equipment, and stipulated that if the FCC finds $1 billion is not enough to replace the covered equipment, it should notify the appropriate congressional committees.

On June 30, 2020, the FCC designated Huawei and its affiliates, along with several other firms, as covered entities.[174] In September 2020, the FCC announced that, after an extensive data survey of operators, it determined replacement costs to be in the range of $1.8 billion.[175] In December 2020,

[168] CRS Insight IN11663, *Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions*, by Jill C. Gallagher.

[169] Jeffrey Starks, Commissioner, FCC, "The Huawei Threat Is Already Here (Op-Ed)," *The Hill*, May 26, 2019, at https://thehill.com/opinion/technology/445493-the-huawei-threat-is-already-here.

[170] Generally, rural areas are expansive and require deployment across a wider region, and yield fewer customers to support operations, expansion, and upgrades; thus, many rural regions are high-cost regions.

[171] Reply Comments of the Rural Wireless Association to the FCC, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket 18-89, December 7, 2018, at https://ecfsapi.fcc.gov/file/12080817518045/FY%202019%20NDAA%20Reply%20Comments%20-%20FINAL.pdf.

[172] Ibid., p. 14.

[173] Ibid., pp.4-8.

[174] FCC, "FCC Designates Huawei and ZTE," press release, June 30, 2020, at https://docs.fcc.gov/public/attachments/DOC-365255A1.pdf.

[175] FCC, "FCC Releases Results of Supply Chain Data Request," press release, September 4, 2020, at https://docs.fcc.gov/public/attachments/DOC-366702A1.pdf.

in the Consolidated Appropriations Act, 2021 (P.L. 116-260), Congress appropriated $1.9 billion for the reimbursement program.[176] The FCC plans to allocate funds to reimburse entities for costs related to the removal and replacement of Huawei and ZTE equipment from U.S. networks.[177]

On July 13, 2021, the FCC adopted final rules for the program to align with the Consolidated Appropriations Act, 2021, amendments, which extends eligibility to carriers with 10 million or fewer customers and authorizes reimbursement to include all communications equipment and services produced or provided by Huawei or ZTE.[178] The FCC announced it would accept applications for reimbursement on October 29, 2021, through January 14, 2022.[179]

On December 21, 2021, the RWA and NTCA – The Rural Broadband Association (NTCA)[180] requested a one-month extension of the filing deadline, stating that "collecting the necessary cell site data, filling out the numerous entries in the location, equipment, and cost estimate excel sheets, and attaching necessary documentation is a massive undertaking that requires substantial work."[181] The groups noted that the task is particularly challenging for small providers, given their limited workforce, and staffing challenges, especially during the holiday season and due to the COVID-19 Omicron variant.[182] On December 29, 2021, the FCC extended the deadline two weeks, to January 28, 2022.[183]

While U.S. officials see "rip and replace" as necessary to ensure the security of U.S. networks, some small carriers have expressed concern that the task is complex and the directive may disrupt service in rural areas, including 911 service.[184] The president and chief executive officer (CEO) of the Competitive Carriers Association, which represents many smaller and regional carriers, stated, "Directives are being issued with no idea of the complexity. In some cases, our members must replace everything from antennas and remote radio heads (RRHs) down to baseband units (BBUs) and the core without interrupting service. It's really 'replace, then rip' rather than 'rip and replace' that is often bandied about inside the Beltway."[185]

---

[176] CRS Insight IN11663, *Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions*, by Jill C. Gallagher.

[177] Statement of Acting Chairwoman Jessica Rosenworcel, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Third Further Notice of Proposed Rulemaking (February 17, 2021), at https://www.fcc.gov/document/implementing-secure-and-trusted-communications-networks-act-0.

[178] FCC, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Third Report and Order, WC Docket No. 18-89, adopted July 13, 2021, at https://docs.fcc.gov/public/attachments/FCC-21-86A1.pdf.

[179] FCC, "Supply Chain Reimbursement Program: Webinar for Broadband Providers," September 27, 2021, p. 9, at https://www.fcc.gov/sites/default/files/supply-chain-webinar-presentation-09272021.pdf.

[180] The organization's name was the National Telephone Cooperative Association. In 2002. It changed its name to the National Telecommunications Cooperative Association, and is now called NTCA—the Rural Broadband Association.

[181] FCC, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Motion for Extension of Time of the Rural Wireless Association, Inc. and NTCA – The Rural Broadband Association, WC Docket No. 18-89, December 21, 2021, pp. 1-2, at https://www.ntca.org/sites/default/files/documents/2021-12/RWA-NTCA%20Filing%20Deadline%20Extension%20Request_12.21.21_FINAL.docx.pdf.

[182] Ibid.

[183] FCC, *In the Matter of Protecting against National Security Threats to the Communications Supply Chain Through FCC Programs, Motion for Extension of Time of the Rural Wireless Association, Inc. and NTCA—The Rural Broadband Association*, Order, WC Docket No. 18-89, adopted December 29, 2021,

[184] John Celentano, "What 'Rip and Replace' Really Means," *Inside Towers*, March 31, 2020, at https://insidetowers.com/cell-tower-news-what-rip-and-replace-really-means/.

[185] Ibid.

The FCC expects to issue funding allocation decisions, based on submitted reimbursement requests, in the second quarter of 2022.[186] Some operators have raised concerns over eligible costs that are not fully covered (e.g., customer equipment such as routers), possible workforce shortages that may affect their ability to install new equipment, and the one-year timeline for implementation.[187]

Huawei Challenges Restrictions on USF Subsidies

On July 30, 2020, Huawei petitioned the FCC to reconsider its decision to ban the use of USF funds for Huawei equipment and services; in December 2020, the FCC upheld its decision.[188] On February 8, 2021, Huawei filed a petition in the U.S. Court of Appeals for the Fifth Circuit, challenging the FCC's decision and authority.[189]

Huawei argued that in its cost-benefit analysis, the FCC ignored the benefits of Huawei's service to rural U.S. communities; according to Huawei, it exerts competitive pressure on prices in the United States. The company contends that removing its equipment from U.S. networks could create long-term interoperability problems and affect service in rural regions where it is often the sole supplier, and that excluding its equipment could cause some carriers to go out of business, raise prices, widen the digital divide, and slow 5G deployment.[190] In June 2021, the federal court denied Huawei's petition for review, finding that "the [FCC] reasonably acted within the broad authority Congress gave it to regulate communications."[191]

Restrictions on Exports to Huawei

On May 21, 2019, the DOC Bureau of Industry and Security (BIS) published rules that added Huawei and 68 of its non-U.S. affiliates to the Entity List,[192] citing long-standing U.S. government concerns that Huawei has been engaged in activities contrary to national security and foreign policy interests of the United States.[193] DOC stated that Huawei raised sufficient concern, and that prior review of exports, re-exports, or transfers of items, and the possible imposition of conditions or denials on shipments to the listed entities, would enhance BIS's ability to prevent activities contrary to the national security or foreign policy interests of the United States.[194]

The Entity List specifies the license requirements it imposes on each listed person or entity.[195] BIS imposed a license requirement for all items subject to the Export Administration Regulations

---

[186] FCC, *Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions*, September 24, 2021, at https://docs.fcc.gov/public/attachments/DOC-376062A1.pdf.

[187] Bevin Fletcher, "FCC Sets Timelines for Huawei Rip and Replace Reimbursement," Fierce Wireless, September 28, 2021, at https://www.fiercewireless.com/regulatory/fcc-sets-timelines-for-huawei-rip-and-replace-reimbursement.

[188] FCC, "FCC Affirms Designation of Huawei as National Security Threat," press release, December 10, 2020, at https://docs.fcc.gov/public/attachments/DOC-368700A1.pdf.

[189] *Huawei Technologies USA, Inc., and Huawei Technologies Co., Ltd., v. Federal Communications Commission, United States of America*, Case 21-60089, p. 3 (United States Court of Appeals for the Fifth Circuit 2021).

[190] Ibid., p. 47.

[191] Ibid., p. 2.

[192] BIS administers the Export Administration Regulations (15 C.F.R., subchapter C, parts 730-774), export controls on commercial, dual-use, and less sensitive military items. See CRS In Focus IF11627, *U.S. Export Control Reforms and China: Issues for Congress*, by Ian F. Fergusson and Karen M. Sutter.

[193] BIS, "Addition of Entities to the Entity List," 84 *Federal Register* 22961, May 21, 2019.

[194] Ibid.

[195] CRS In Focus IF11627, *U.S. Export Control Reforms and China: Issues for Congress*, by Ian F. Fergusson and

(EAR),[196] which comprises most U.S.-made products, including technology and software, and certain foreign-produced items, such as items that contain a certain percentage of controlled U.S.-origin content,[197] and items that are a "direct product" of controlled U.S. technologies.[198] Under the rules, the export, re-export, or transfer of any such item to Huawei or its listed affiliates requires a license (i.e., approval from DOC); however, BIS adopted a license review policy of "presumption of denial," meaning that it is unlikely to approve such license applications.[199]

On May 22, 2019, DOC created a temporary general license (TGL), effective May 20, 2019, that temporarily authorized engagement in "certain transactions, involving the export, re-export, or transfer of items subject to the EAR"; the TGL allowed U.S. companies to temporarily provide certain products and services to Huawei and its affiliates.[200] The TGL allowed for some exports from U.S. parties to Huawei to "assure the continued secure operation of portions of telecommunications systems while allowing time for affected companies and persons to identify and shift to other sources of equipment, software, and technology."[201] It allowed U.S. software providers that support Huawei to send software patches to ensure networks and devices are secure; gave U.S. companies that supply component parts to Huawei time to adjust their business strategy; and allowed rural carriers that rely on Huawei equipment time to determine their path forward to ensure continuity of services for customers.[202] The TGL was valid for 90 days. DOC extended the TGL several times, from May 2019 through August 13, 2020.[203]

On May 15, 2020, BIS issued interim rules tightening restrictions on Huawei and its affiliates. The restrictions apply to certain foreign-made items produced or developed by Huawei that are a direct product of certain controlled U.S. technologies and software, or a direct product of a plant outside the United States where the plant itself uses certain controlled U.S. technologies and software.[204] DOC noted that while companies seeking to export U.S. items to Huawei and its affiliates are required to obtain a license, "Huawei has 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."[205] The rules apply when there is knowledge the items made with U.S. technologies

---

Karen M. Sutter.

[196] For items subject to the EAR, see 15 C.F.R. §734.3. For a list of BIS-controlled items (also called the Commerce Control list, or CCL), see 15 C.F.R. §774.

[197] Also known as the de minimis rules, see 15 C.F.R. §734.4.

[198] See 15 C.F.R. §736.2(b)

[199] BIS, "Addition of Entities to the Entity List," 84 *Federal Register* 22962, May 21, 2019.

[200] BIS, "Temporary General License," 84 *Federal Register* 23468-23471, May 22, 2019.

[201] BIS, "Huawei Temporary General License Extension Frequently Asked Questions," May 18, 2020, at https://www.bis.doc.gov/index.php/documents/pdfs/2446-huawei-entity-list-temporary-general-license-extension-faqs/file.

[202] Jeanne Whalen and Felicia Sonmez, "Huawei Business Ban Leaves Rural Wireless Companies with Few Alternatives," *Washington Post*, April 19, 2019, at https://www.washingtonpost.com/business/2019/08/19/huawei-business-ban-leaves-rural-wireless-companies-with-few-alternatives/.

[203] On August 21, 2019, BIS published an extension of the temporary general license (TGL), effective August 19, 2019, that extended the validity of the TGL another 90 days, through November 18, 2019, and added 46 additional affiliates to the Entity List. BIS extended the TGL for another 90 days, through February 16, 2020, then again through April 1, 2020, then May 15, 2020, and then through August 13, 2020, when the TGL expired.

[204] DOC, "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," 85 *Federal Register* 29849, May 19, 2020.

[205] DOC, "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies," press release, May 15, 2020, at https://2017-2021.commerce.gov/news/press-releases/2020/

and software are destined for specified entities (i.e., Huawei and its affiliates). In its rules, DOC provided some time for entities to adjust, allowing foundries to continue shipments without a license until September 14, 2020.[206]

On August 17, 2020, DOC issued final rules, tightening restrictions on Huawei.[207] First, DOC added 38 Huawei affiliates to the Entity List, "because they present a significant risk of acting on Huawei's behalf contrary to the national security or foreign policy interests of the United States."[208] Second, DOC allowed the TGL to expire, discontinuing its approval for transactions supporting continued operations of networks and for support and service of Huawei devices; DOC allowed companies to continue to engage in cybersecurity research and vulnerability disclosures involving Huawei. Third, DOC tightened restrictions on foreign-produced items.

DOC amended its rules to close loopholes that Huawei was using to obtain advanced chipsets, such as leveraging overseas foundries that use U.S. software or technology to design and develop its advanced chips,[209] and shipping chips directly to the end-user avoid requirements for a license for items produced or developed by Huawei.[210] The August rules impose a license requirement on foreign-made items (1) when the item is produced using certain controlled U.S. technology and software, or produced in a plant that uses such technology and software, and (2) when there is knowledge the item will be incorporated into the "production or development of any part, component, or equipment produced, purchased, or ordered" by Huawei or its affiliates, or when they are a party to such transactions (e.g., a purchaser, end-user).

In its August 2020 rules, BIS adopted a "presumption of denial" license review policy. However, it also noted that "[s]ophistication and capabilities of technology in items is a factor in license application review," and that it would review on a case-by-case basis license applications for items capable of supporting the development or production of telecom systems, equipment, and devices below the 5G level (e.g., 3G, 4G).[211] Thus, while the rules restricted Huawei's access to U.S.-made semiconductors and foreign-produced semiconductors made with U.S. technologies, and tightened restrictions on advanced (e.g., 5G) chipsets specifically, they allowed some flexibility for BIS to approve transactions for less-advanced (e.g., 3G, 4G) technologies.

In December 2020, DOC placed additional entities, including Chinese chipmaker Semiconductor Manufacturing International Corporation (SMIC), a supplier of Huawei, on the Entity List. DOC added SMIC and 10 of its affiliates due to "evidence of activities between SMIC and entities of concern in the Chinese military industrial complex."[212] The rules limit SMIC's ability to acquire

05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts.html.

[206] Ibid.

[207] DOC, "Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds another 38 Affiliates to the Entity List," press release, August 17, 2020, at https://2017-2021.commerce.gov/ news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and.html.

[208] Ibid.

[209] BIS, "Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)," 85 *Federal Register* 51602, August 20, 2020, at https://www.govinfo.gov/content/pkg/FR-2020-08-20/pdf/2020-18213.pdf.

[210] Lori E. Scheetz, John R. Shane, and Daniel P. Brooks, "Commerce Tightens Huawei Restrictions; Aims to Close Loopholes," *Wiley Alert*, August 18, 2020, at https://www.wiley.law/alert-Commerce-Tightens-Huawei-Restrictions-Aims-to-Close-Loopholes.

[211] BIS, "Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)," 85 *Federal Register* 51602, August 20, 2020, at https://www.govinfo.gov/content/pkg/FR-2020-08-20/pdf/2020-18213.pdf.

[212] BIS, "Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities from the

certain U.S. technology by requiring companies seeking to export such technologies to SMIC to apply for a license (i.e., gain approval) to sell to the company. DOC stipulated that items uniquely required to produce advanced semiconductors are subject to a presumption of denial "to prevent such key enabling technology from supporting China's military modernization efforts."[213] In the rules, DOC adopted a presumption of denial policy for items uniquely required to produce more advanced technologies (e.g., 5G chips), but allowed for case-by-case review for all other items.[214]

Market analysts say that placing SMIC on the Entity List could "choke China's semiconductor supply chain," affect its ability to develop and produce advanced (5G) semiconductors used in smartphones and network equipment, and affect Huawei's smartphone business.[215] Some analysts contend that restricting SMIC's access to U.S. technologies and equipment could accelerate Chinese efforts to develop its chip-making capabilities.[216] In December 2021, Chinese media reported that Huawei's CEO stated it is continuing to invest in its flagship smartphones; however, with restrictions limiting its access to U.S. chipsets and technologies, the next release (expected in 2022) would use Huawei's HarmonyOS operating system (replacing Google Android), and would not have 5G capability, but would instead use 4G chipsets. The CEO noted that its Shanghai R&D Center is working to bring 5G chipsets to Huawei smartphones in the future, but did not provide specific dates.[217]

Benefits and Challenges in Restrictions on Exports

In its May 2019 Public Notice adding Huawei to the Entity List, DOC identified Huawei as an entity acting contrary to the national security and foreign policy interests of the United States, citing the indictment filed by DOJ in January 2019, charging Huawei and its officials with financial fraud, sanctions violations, obstruction of justice, and other offenses.[218] DOC asserts that the restrictions on exports to Huawei enhance DOC's ability to prevent activities contrary to the national security or foreign policy interests of the United States—a key benefit of the restrictions on exports.[219] There is bipartisan support in Congress for restrictions on exports, without exceptions, to limit U.S. exports to a company that the U.S. government has identified as engaging in activities contrary to U.S. national security and foreign policy interests.[220]

Entity List" 85 *Federal Register* 83416-83432, December 22, 2020.

[213] Ibid., p. 83416.

[214] BIS, "Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List," 85 *Federal Register* 83416, December 22, 2020.

[215] Xiuxi Zhu, "Potential US Ban on SMIC Could Choke China's Semiconductor Supply Chain," *Standard and Poor's Global Market Intelligence*, September 20, 2020, at https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/potential-us-ban-on-smic-could-choke-china-s-semiconductor-supply-chain-60375095.

[216] Ian King, "Biden Faces a Policy Dilemma with China's Biggest Chipmaker," *Bloomberg*, December 22, 2021, at https://www.bloomberg.com/news/newsletters/2021-12-22/smic-poses-policy-dilemma-for-biden-s-china-chip-crackdown.

[217] Efe Udin, "Huawei Will Continue to Work on Its Kirin Chip Design," *GizChina*, December 7, 2021, at https://www.gizchina.com/2021/12/07/huawei-self-developed-5g-chip-solution-will-arrive-soon/.

[218] DOJ, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud," press release, January 28, 2019, at https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial.

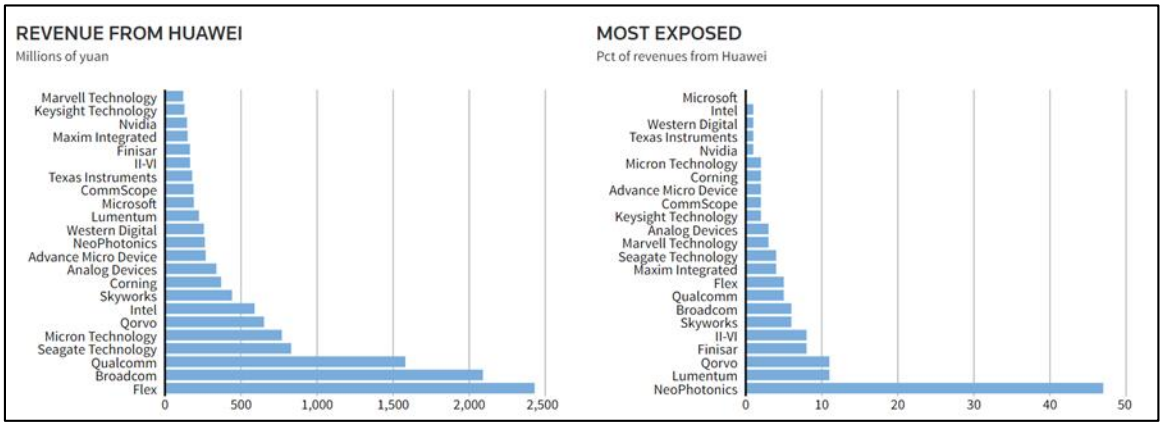
[219] BIS, "Addition of Entities to the Entity List," 84 *Federal Register* 22961, May 21, 2019.

[220] Maggie Miller, "Trump Reversal on Huawei Get Bipartisan Pushback," *The Hill*, July 2, 2019, at https://thehill.com/policy/cybersecurity/451260-trump-reversal-on-huawei-gets-bipartisan-pushback; also Karen Freifeld, "Huawei Gets U.S. Approvals to Buy Auto Chips, Sparking Blow Back," Reuters, August 25, 2021.

A key challenge to restrictions on exports is in balancing U.S. national security interests with U.S. economic interests, including potential losses to U.S. businesses that supply Huawei with parts. At its 2018 Core Supplier Convention, Huawei reported that 33 of its top 92 suppliers are U.S. companies.[221] In 2018, Huawei reported that it had purchased $70 billion in parts from 13,000 global suppliers, including about $11 billion in products from U.S. businesses, such as semiconductors from Qualcomm and Broadcom, and software from Microsoft and Google.[222]

In 2018, Goldman Sachs assessed the revenues of Huawei's U.S. suppliers (examining the percentage of their revenues that come from Huawei), and their exposure should business with Huawei cease or diminish (**Figure 1**).

Figure 1. U.S. Suppliers to Huawei (2018)



Source: Sijia Jiang and Michael Martina, "Huawei's $105 billion business at stake after U.S. broadside," Reuters, May 16, 2019, at https://www.reuters.com/article/us-usa-trade-china-huawei-analysis/huaweis-105-billion-business-at-stake-after-u-s-broadside-idUSKCN1SM123. The graphic was created by Reuters Graphics on December 13, 2018, available at https://fingfx.thomsonreuters.com/gfx/editorcharts/USA-CHINA-HUAWEI/0H001GSE93H2/index.html (used with permission from Reuters).

Notes: This graphic shows some U.S. suppliers to Huawei, created after the arrest of Huawei's Chief Financial Officer (CFO) in December 2018. Goldman Sachs, the investment firm, used company data (Q32018) to determine U.S. firms' revenues from Huawei (in yuan) and their exposure to risk if that business were to cease or diminish. Reuters created this graphic from the Goldman Sachs data. The yearly average exchange rate in 2018 for converting Chinese Yuan to U.S. Dollars was 6.620, per the U.S. Internal Revenue Service. Pct=percent.

In May 2019, after DOC added Huawei to the Entity List, many U.S. telecommunications technology companies that supply Huawei with component parts adjusted their revenue projections. The adjustments provide some insight into the business relationships and interdependencies between U.S. firms and Huawei.

For example, Qorvo Inc., a U.S. chipmaker and provider of wireless technology solutions, reported that sales to Huawei and its affiliates accounted for approximately $469 million or 15% of its total revenue in its fiscal year ending March 30, 2019.[223] Due to restrictions on exports, it

[221] Zhang Yushuo, "Huawei Exposes Its Surprising Group of Key Suppliers for the First Time," *Yicai*, November 30, 2018, at https://www.yicaiglobal.com/news/huawei-exposes-its-surprising-group-of-key-suppliers-for-the-first-time.

[222] Sherisse Pham, "Losing Huawei as a Customer Could Cost U.S. Tech Companies $11 Billion," *CNN Business*, May 17, 2019, at https://www.cnn.com/2019/05/17/tech/huawei-us-ban-suppliers/index.html.

[223] Qorvo, "Qorvo® Updates Financial Guidance Due to U.S. Department of Commerce Action Against Huawei," press release, May 21, 2019, at https://www.qorvo.com/newsroom/news/2019/qorvo-updates-financial-guidance-due-to-us-department-of-commerce-action-against-huawei.

expected a $50 million loss in revenue in the first quarter of 2020 (April to June 2019).[224] Analog Devices Inc., a large U.S. chipmaker, projected a decline in revenue for its third quarter (June to August 2019) that fell below what some financial analysts expected, due to an estimated $60 million in lost sales to Huawei.[225] Lumentum Holdings Inc., which makes advanced optical networking products, reported in May 2019 that Huawei represented 18% of its total revenue in its third quarter of 2019, ending March 30, 2019.[226] It projected its fourth-quarter revenue for 2019 (April to June 2019) at $405 million to $425 million; in May 2019, the company adjusted its fourth-quarter revenue, projecting revenues in the range of $375 million to $390 million, due to restrictions on sales to Huawei.[227] In June 2019, U.S. chipmaker Broadcom—a supplier to Huawei—projected that it would make $2 billion less in annual sales due to the restrictions on exports; it reduced its 2019 end-year revenue forecast from $24.5 billion to $22.5 billion.[228]

U.S. companies and industry associations expressed their concerns to the Trump Administration about the restrictions. On July 1, 2019, Bloomberg reported that the Semiconductor Industry Association (SIA) met with the Commerce and Treasury Secretaries to convey that the restrictions would hurt the U.S. semiconductor industry by cutting off access to their largest market and hurting their ability to invest in R&D, and U.S. national and economic security.[229] In response to industry concerns, the Trump Administration loosened some restrictions on exports. In July 2019, President Trump, in a press conference at the conclusion of the G-20 summit in Japan, mentioned U.S. businesses were "not exactly happy" with the restrictions and announced he would allow certain exports to Huawei.[230] In August 2019, DOC extended the TGL for 90 days, permitting certain transactions with Huawei to continue through November 2019.

Many U.S. companies noted the complexities and uncertainties of the restrictions in their quarterly financial statements.[231] Some companies reported publicly that they had halted sales to

[224] Ibid.

[225] Catherine Larkin, "Analog Devices Earnings Forecast May Be Blunted by Huawei Ban," *Bloomberg Quint*, May 20, 2019, at https://www.bloombergquint.com/onweb/analog-devices-earnings-forecast-may-be-blunted-by-huawei-ban.

[226] Lumentum, "Lumentum Provides Update on U.S. Department of Commerce Entity List Designation of Huawei and Affiliates and the Impact to Fiscal Fourth Quarter Ending June 29, 2019 Outlook," May 20, 2019, press release, at https://www.lumentum.com/en/media-room/news-releases/lumentum-provides-update-us-department-commerce-entity-list-designation.

[227] Reuters Staff, "Lumentum says halting all Huawei shipments, cuts quarterly forecast," Reuters, May 20, 2019, at https://www.reuters.com/article/us-huawei-suppliers/lumentum-says-halting-all-huawei-shipments-cuts-quarterly-forecast-idUSKCN1SQ1B5.

[228] Asa Fitch, "Broadcom to Take $2 Billion Hit from Huawei Ban," *Wall Street Journal*, June 13, 2019, at https://www.wsj.com/articles/broadcom-lowers-revenue-outlook-amid-trade-tensions-11560459528?mod=article_inline; see also Mike Dano, "U.S. Government's Huawei Ban Pushes Business to Qualcomm's Rival," *Light Reading*, March 26, 2021, at https://www.lightreading.com/security/us-governments-huawei-ban-pushes-business-to-qualcomms-rival/d/d-id/7683202067.

[229] Jenny Leonard and Ian King, "How U.S. Chipmakers Pressed Trump to Ease China's Huawei Ban," *Bloomberg*, July 1, 2019, at https://www.bloomberg.com/news/articles/2019-07-02/how-u-s-chipmakers-pressed-trump-to-ease-huawei-export-controls.

[230] C-Span, "President Trump Closing News Conference at G-20 Summit," press conference (video, starting 00:14:52), June 29, 2019, at https://www.c-span.org/video/?462171-1/president-trump-holds-news-conference-20-summit-japan.

[231] See, for example, Qualcomm, Form 10-Q, July 31, 2019, p. 57, at https://investor.qualcomm.com/sec-filings/quarterly-reports?form_type=&year=2019. (See "Risks Related to Our Businesses," where Qualcomm states: "Import/export regulations, such as the U.S. Export Administration Regulations administered by the U.S. Department of Commerce, are complex, change frequently, have generally become more stringent over time and have intensified under the current U.S. administration. If our customers or suppliers fail to comply with these regulations, we may be required to suspend activities with these customers or suppliers, which could negatively impact our results of operations. Additionally, we may be required to incur significant expense to comply with, or to remedy violations of,

Huawei, and were assessing the impact of the restrictions on their revenues, examining the TGL to determine what they could legally sell to Huawei, and were preparing to submit license applications that would permit longer-term sales of some products to Huawei.[232]

While SIA warned that restricting sales to Huawei would hurt the U.S. telecommunications technology industry and impact U.S. national and economic security,[233] some Members of Congress expressed concern that lifting the restrictions, as President Trump planned, would create national security risks. In a letter to President Trump dated November 21, 2019, a group of 10 lawmakers urged the President to suspend approval of licenses, and take steps to "ensure Congress is appropriately informed about the license approval process and related national security implications going forward."[234] In November 2020, Representative Michael McCaul, ranking member of the House Foreign Affairs Committee, in a letter to the Commerce Secretary, also requested detailed information on licenses to assess the implementation of the restrictions, and fulfill Congress's duty to protect U.S. national security.[235] Although license information is deemed confidential under Section 1761(h) of the Export Control Reform Act of 2018 (P.L. 115-232), Representative McCaul noted that license information had appeared in the press, and thus should be released to Congress.[236]

For example, in November 2019, the *Washington Post* reported information it received from industry sources, which stated that DOC approved the first licenses, authorizing exports to listed entities; DOC approved one-quarter of 300 license applications submitted, according to the *Post*.[237] In March 2021, Reuters reported that, based on DOC documents it had seen, between 2019 and 2020, DOC approved licenses for companies to sell $87 billion worth of goods to Huawei, and that licenses had a term of four years.[238] According to Reuters, in the month of

these regulations.")

[232] Angela Moon, "Exclusive: Google Suspends Some Business with Huawei After Trump Blacklist—Source," Reuters, May 19, 2019. See also Lumentum, "Lumentum Provides Update on U.S. Department of Commerce Entity List Designation of Huawei and Affiliates and the Impact to Fiscal Fourth Quarter Ending June 29, 2019 Outlook," press release, May 20, 2019, at https://ir.qorvo.com/news-releases/news-release-details/qorvor-updates-financial-guidance-due-us-department-commerce; and Qorvo, Inc., Q1 2020 Results (Earning Call Transcript), August 1, 2019, https://seekingalpha.com/article/4280496-qorvo-inc-qrvo-ceo-robert-bruggeworth-on-q1-2020-results-earnings-call-transcript.

[233] Jenny Leonard and Ian King, "How U.S. Chipmakers Pressed Trump to Ease China's Huawei Ban," *Bloomberg*, July 1, 2019, at https://www.bloomberg.com/news/articles/2019-07-02/how-u-s-chipmakers-pressed-trump-to-ease-huawei-export-controls.

[234] Letter from Senators Charles E. Schumer, Tom Cotton, and Chris Van Hollen, et al., to President Donald J. Trump, November 21, 2019, at https://www.democrats.senate.gov/imo/media/doc/11.21.19%20POTUS-Huawei%20Letter.pdf.

[235] Letter from Michael T. McCaul, Ranking Member, House Foreign Affairs Committee, to Honorable Wilbur Ross, Secretary of Commerce, November 9, 2020, at https://gop-foreignaffairs.house.gov/wp-content/uploads/2021/02/11.9.20-Letter-to-Secretary-Ross-re-Oversight-of-Export-Control-Licensing.pdf.

[236] House Foreign Affairs Committee, "McCaul Calls Out Misleading Answers from Under Secretary Pelter at U.S.-China Economic and Security Review Commission Hearing," press release, September 9, 2021, at https://gop-foreignaffairs.house.gov/press-release/mccaul-calls-out-misleading-answers-from-under-secretary-pelter-at-u-s-china-economic-and-security-review-commission-hearing/.

[237] Jeanne Whalen, Joseph Marks, and Ellen Nakashima, "U.S. Approves First Licenses for Tech Sales to Huawei," *Washington Post*, November 20, 2019, at https://www.washingtonpost.com/technology/2019/11/20/us-said-approve-first-licenses-tech-sales-huawei/.

[238] Karen Freifeld, "Biden Administration Adds New Limits on Huawei's Suppliers," Reuters, March 11, 2021, at https://www.reuters.com/article/us-usa-huawei-tech/biden-administration-adds-new-limits-on-huaweis-suppliers-idUSKBN2B3336.

January 2021, DOC denied 116 licenses worth $119 billion and approved four worth $20 million; 300 applications worth $296 million were still pending in January 2021.[239]

In October 2021, the House Foreign Affairs Committee requested licensing information from DOC and published it.[240] From November 9, 2020, to April 20, 2021, U.S. companies submitted 169 license requests to sell products to Huawei. DOC approved 113 licenses worth $61 billion; DOC returned 48 licenses worth $28 million with no further action, and denied two licenses worth $57 million.[241] The documents show that while DOC instituted restrictions in May 2019, it continued to allow some exports to Huawei—first under the TGL and then through individual licenses. Thus, both the Trump and Biden Administrations issued approvals on sales of products to Huawei, which some Members of Congress assert are contrary to U.S. national security and foreign policy objectives. Consequently, Congress has pressed for greater transparency into and reporting on licenses, license criteria, and approvals.[242]

The restrictions affected U.S. businesses in different ways. Some companies halted sales to Huawei, while others continued to export certain items to Huawei under the TGL or through longer-term licenses. Nonetheless, many U.S. companies saw reductions in sales and revenues because of the restrictions on exports to Huawei. For example, North Carolina-based Qorvo, Inc., reported that it received a license to sell some products to Huawei; however, in October 2021, Qorvo reported Huawei accounted for less than 5% of its revenue for the year ending 2021 (down from 15% in 2019).[243] Since then, Qorvo appears to have shifted its focus to emerging technologies to offset loss in revenue, reporting success in sales of gallium nitride (GaN) semiconductors and 5G base stations.[244]

Other firms have reported they are no longer doing business with Huawei, but have increased business outside of China and expanded their work in emerging technologies to offset losses in revenue. Cree, a North Carolina-based chipmaker and provider of wireless technologies, noted in 2019 that sales to Huawei generated $15 million a quarter for the company.[245] In August 2019, after DOC added Huawei to the Entity List, Cree's CEO stated the restrictions created uncertainties for the business, "because a substantial portion of the semiconductor market is in China, and a substantial percentage of the growth is there as well."[246] In August 2020, Cree (now Wolfspeed) reported it was no longer doing business with Huawei, but was able to repurpose products intended for Huawei, and increase its business outside of China, which helped to offset losses.[247] It also invested in GaN and silicon carbide semiconductors, and in October 2021

[239] Ibid.

[240] Export Control Licensing Decisions for Huawei (November 9, 2020-April 20, 2021)," data obtained by the House Foreign Affairs Committee from the Department of Commerce, released by the Committee on October 21, 2021, at https://gop-foreignaffairs.house.gov/wp-content/uploads/2021/10/Huawei-Licensing-Information.pdf.

[241] Ibid.

[242] For example, see H.R. 1595 and H.R. 4792.

[243] Qorvo, Inc., FY21 Annual Report (for the fiscal year ending April 3, 2021), June 29, 2021, p. 7, at https://ir.qorvo.com/static-files/660e1b53-4846-4008-bfb3-00b86658f34f.

[244] Ibid.

[245] Rick Smith, "What If China 'Just Never Came Back?' Cree CEO Warns of Trade War, Huawei Ban Impact," *WRAL TechWire*, August 21, 2019, at https://www.wraltechwire.com/2019/08/21/what-if-china-just-never-came-back-cree-ceo-warns-of-trade-war-huawei-ban-impact/.

[246] Ibid.

[247] Cree, Inc., CEO Gregg Lowe on Q4 2020 Results—Earnings Call Transcript, August 18, 2020, at https://seekingalpha.com/article/4369598-cree-inc-cree-ceo-gregg-lowe-on-q4-2020-results-earnings-call-transcript.

announced it had entered into a strategic supplier agreement with General Motors (GM) to provide silicon carbide chips for GM's electric vehicle programs.[248]

Other companies saw slowed growth after DOC announced the restrictions. In September 2019, after California-based Broadcom projected a $2 billion reduction in revenues due to the restrictions on exports, the CEO noted in a quarterly earnings call that it is managing business "with an expectation that we will continue to operate in a very low growth uncertain macro environment for the foreseeable future."[249] In December 2019, Broadcom financial reports indicated that its revenues diminished, due to restrictions on sales to Huawei, but were slightly higher than the $22.5 billion projected ($22.597 billion), driven by increased 5G deployments.[250] Its rate of growth in terms of revenues year-over-year had slowed from 18.21% in 2018 to 8.39% in 2019 to 5.71% in 2020, due in part to the restrictions, according to some market analysts.[251] In September 2021, the CEO stated its revenues were up 16.44% year-over-year for the quarter, which he attributed to upticks in sales to global network operators deploying 5G networks, increased demand from business customers and device makers, and strategic investments in software and cloud services that helped to offset restrictions on sales of semiconductors.[252] Like other firms, Broadcom saw gains in other areas, which helped to offset some of the loss in revenue.

Some U.S. chipmakers saw loss of market share. In March 2021, industry analysts from the consulting firm Omdia reported that Taiwan's Mediatek surpassed California-based Qualcomm as the world's largest supplier of chips for smartphones, which some market analysts attribute to U.S. government restrictions on the sale of supplies to Huawei.[253] In September 2021, Counterpoint Research, a technology market research firm, reported that Mediatek continues to gain market share, capturing a 43% share of the global smartphone System on Chip market in the second quarter of 2021 compared to a 35% share in the first quarter of 2021, while Qualcomm accounted for 24% market share in the second quarter of 2021, compared to 29% in the previous quarter.[254]

In some cases, U.S. firms may benefit from the restrictions by potentially gaining market share once held by Huawei. As the leading global supplier of network switching equipment, California-

[248] Wolfspeed, Inc., "General Motors and Wolfspeed Forge Strategic Supplier Agreement to Leverage Silicon Carbide for GM's Future Electric Vehicle Programs," press release, October 4, 2021, at https://www.wolfspeed.com/company/news-events/news/general-motors-wolfspeed-forge-strategic-supplier-agreement-to-leverage-silicon-carbide-for-electric-vehicle-programs.

[249] Broadcom, Inc. (AVGO), CEO Hock Tan on Q3 2021 Results (Earnings Call Transcript), September 2, 2021, at https://seekingalpha.com/article/4453351-broadcom-inc-avgo-ceo-hock-tan-on-q3-2021-results-earnings-call-transcript.

[250] AVGO, "Broadcom Revenue 2009-2021," accessed November 29, 2021, at https://www.macrotrends.net/stocks/charts/AVGO/broadcom/revenue. See also Sophia Nicholson, "The Worst Is Over for Broadcom Stock—Can It Rally?," Market Realist, December 26, 2019, at https://marketrealist.com/2019/12/worst-over-broadcom-stock-can-it-rally/.

[251] Ibid.

[252] Broadcom, Inc. (AVGO), CEO Hock Tan on Q3 2021 Results (Earnings Call Transcript), September 2, 2021, at https://seekingalpha.com/article/4453351-broadcom-inc-avgo-ceo-hock-tan-on-q3-2021-results-earnings-call-transcript.

[253] Mike Dano, "US Government's Huawei Ban Pushes Business to Qualcomm's Rival," *Light Reading*, March 26, 2021, at https://www.lightreading.com/security/us-governments-huawei-ban-pushes-business-to-qualcomms-rival/d/d-id/768367.

[254] Counterpoint, "MediaTek Captures Record 43% Share of Smartphone AP/SoC Shipments in Q2 2021," press release, September 6, 2021, at https://www.counterpointresearch.com/mediatek-captures-record-43-share-smartphone-apsoc-shipments-q2-2021/.

based Cisco Systems could increase its global market share,[255] as the United States and potentially other foreign governments restrict use of Huawei equipment in telecommunications networks and business systems.[256] Companies that receive U.S. government licenses to do business with Huawei, such as California-based Intel, may also gain market share.[257]

Other U.S. companies have shifted strategies to offset losses in revenue. For example, California-based Marvell Technology reported an 11% decline in revenues in the first quarter of its FY2020 (February 2019 to May 2019) due to export restrictions, according to analysts at BMO Capital Markets.[258] Marvell pivoted to 5G technologies, data centers, and storage solutions for telecom operators, and collaborated with 5G telecom equipment makers (e.g., Ericsson, Nokia, and Samsung) to support 5G deployments. In its June 2021 earnings call, Marvell reported it "delivered the fourth straight quarter of double-digit year-on-year revenue growth despite industry-wide supply constraints that have tightened considerably over the same time period."[259]

Some U.S. companies were hard-hit by the restrictions. In October 2020, California-based Neophotonics, which derived more than 40% of its revenues from Huawei in 2018, announced cost-cutting measures, including reductions in its workforce by approximately 4%.[260] In November 2021, Lumentum announced plans to acquire Neophotonics for $918 million to strengthen its offerings in high-speed optical components for cloud and telecom network infrastructure, including 5G, Internet of Things (IoT), and next-generation networks.[261]

While the restrictions on exports limit Huawei's access to U.S. technologies—to prevent it from engaging in activities that are contrary to U.S. national security and foreign policy interests—they have also resulted in reduced revenues for some U.S. businesses, which some business groups warn could lead to reduced investments in R&D and diminished competitiveness of U.S. firms.[262] A challenge for Congress is in balancing U.S. national and economic security interests.

[255] Eric J. Savitz, "Huawei Faces Increased Scrutiny. Apple, Cisco, and Other Tech Stocks Could Benefit," *Barron's*, July 9, 2020, at https://www.barrons.com/articles/huawei-sanctions-apple-cisco-and-other-tech-stocks-51594321329.

[256] Harsh V. Pant, "India Draws a Line in the 5G Sand," *Foreign Policy*, May 18, 2021, at https://foreignpolicy.com/2021/05/18/india-draws-a-line-in-the-5g-sand. See also Joe Panettieri, "Huawei Banned in Which Countries," *CHANNELe2e*, December 27, 2021, at https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/3/ (discussing actual and de facto bans on Huawei use in 5G networks in Australia, New Zealand, United Kingdom, Sweden, and Japan, and other countries considering restrictions or band on Huawei).

[257] Mario McKellop, "Intel Receives U.S. Commerce Department Approval to Sell Select Products to Huawei," *The Burn-In*, September 25, 2020, at https://www.theburnin.com/featured/intel-receives-us-approval-sell-products-huawei-2020-09-25/.

[258] Priya Nigam, "Marvell Prospects Affected by Loss of Huawei Revenue, BMO Says," *Benzinga*, May 31, 2019, at Benzinga, https://www.benzinga.com/analyst-ratings/analyst-color/19/05/13841173/marvell-prospects-affected-by-loss-of-huawei-revenue-bmo-says.

[259] Marvell Technology Group, Ltd., Q1 2022 Earnings Call Transcript, June 7, 2021, at https://news.alphastreet.com/marvell-technology-group-ltd-mrvl-q1-2022-eamings-conference-call-transcript/.

[260] Stephen Hardy, "NeoPhotonics Looks to Cut Costs, Including Layoffs," *Lightwave*, October 5, 2020, at https://www.lightwaveonline.com/business/earnings-statements/article/14184704/neophotonics-looks-to-cut-costs-including-layoffs.

[261] Lumentum, "Lumentum to Acquire NeoPhotonics to Accelerate Optical Network Speed and Scalability," press release, November 4, 2021, at https://www.lumentum.com/en/media-room/news-releases/lumentum-acquire-neophotonics-accelerate-optical-network-speed-and.

[262] U.S. Chamber of Commerce, *Understanding U.S.-China Decoupling*, February 17, 2021, p. 3, at https://www.uschamber.com/international/understanding-us-china-decoupling-macro-trends-and-industry-impacts.

Considerations for Congress

In response to concerns about Huawei and other Chinese telecommunications firms, the 117th Congress has enacted legislation to protect U.S. networks, and proposed legislation to address implementation challenges, ensure security of U.S. networks and supply chains, protect U.S. competitiveness in the global telecommunications market, and improve global network security. The following section discusses challenges raised by these issues and proposals to address those challenges.

Ensuring Security of U.S. Networks

Congress may seek to assess the effectiveness of these policies, programs, and restrictions to determine whether they are making U.S. networks more secure.

Challenges Assessing Impact of Restrictions

Since implementation of U.S. policies related to Huawei is still under way, it is difficult to assess their impact on network security. For example, while DOC added Huawei to the Entity List in May 2019, it permitted billions of dollars in sales of technology to Huawei under the TGL and individual licenses through at least April 2021. Additionally, while many agencies have implemented rules to restrict federal agency purchases of Huawei equipment, in some cases, such as with DOD, timelines for compliance were extended, which would affect an assessment of impact. Finally, the Reimbursement Program, while funded in December 2020, is set to release funding in the first quarter of 2022; thus, Congress may not see the removal of Huawei equipment from U.S. networks until 2023 or later. As a result, Congress may not see the full impact of restrictions for several years.

Congress could hold oversight hearings with a wide array of agencies and their stakeholders (e.g., contractors, grantees, overseas vendors, small businesses, universities) on their progress in implementing the existing restrictions, challenges, and impact on U.S. network security.

Congress may gain some insight on implementation of Section 889 through oversight hearings and reports required under Section 889. Section 889 requires entities seeking a waiver (e.g., extended time to comply), to provide the federal contracting agency with a full and complete description of the presence of covered equipment in its network and a phase-out plan, which the federal agency must provide to the congressional oversight committees. Congress could use these reports to gain insight into Huawei use, and to inform future policies regarding Huawei.

Congress may also monitor implementation through review of DOC licenses. Legislation in the 117th Congress proposes greater transparency to enable Congress to monitor transactions with Huawei. H.R. 1595 would prohibit DOC from removing Huawei (or its subsidiaries or affiliates) from the Entity List unless DOC certifies that Huawei (1) has not engaged in activities that are contrary to U.S. national security or foreign policy interests; and (2) is not owned, controlled, or influenced by the Communist Party of China. The bill would also require DOC to submit a monthly report identifying and describing all license applications and approvals. Through greater transparency, Congress may be in a better position to assess the implementation and effectiveness of U.S. restrictions on exports to Huawei, and their impact on U.S. network security.

Challenges in Identifying and Addressing Continually Emerging Risks

A key challenge rests in the fact that the U.S. network is part of a larger interconnected global network; thus, a breach of one network could affect all others. Experts assert that removing

Huawei equipment from U.S. networks may remove some risks, but that other risks remain. Former FCC Chairman Tom Wheeler agrees that Huawei equipment poses a risk to U.S. network infrastructure due to its ties to the Chinese government, its theft of trade secrets, and obligations to assist the Chinese government with intelligence work, but argues that "keeping Chinese hardware out of most U.S. network infrastructure does not equate to successfully preventing foreign espionage or sabotage of those networks…. The internet, after all, is about the interconnection of disparate networks; keeping Chinese hardware out does not translate into keeping Chinese-originated digital code out."[263]

Wheeler asserts that foreign adversaries have exploited non-Chinese telecommunications infrastructure, and that the U.S. government should remain focused on promoting an open economic model and leading 5G cybersecurity standards.[264] S. 1260, which passed the Senate in June 2021, would address some of these issues, providing funding to bolster the U.S. semiconductor industry, create test beds for open, interoperable network solutions,[265] and support 5G R&D and domestic and international efforts to secure the information and communications technology (ICT) supply chain and global networks.

An ongoing challenge in ensuring network security is the fact that new companies and technologies continually enter the market, which may present new risks to networks. Congress may be interested in continual monitoring and oversight of U.S. network security through hearings or investigative reports. Congress hears from U.S. intelligence agencies on network security concerns in annual hearings. Other agencies and advisory councils that study network security may also provide useful information to Congress. For example, the National Security Technical Advisory Council to the President (NSTAC) provides recommendations to the President on network security. The FCC Communications Security, Reliability, and Interoperability Council (CSRIC) provides reports on aspects of network security. The Department of Homeland Security (DHS) works with federal agencies to help ensure federal networks are secure. Hearings that include interagency advisory committees may help Congress gain awareness of network security issues and mitigation recommendations, which may inform future policies aimed at securing U.S. and global networks.

In the past, Congress has gained insight on entities posing security risks through hearings and investigations. Congress first documented its concerns about Huawei in the 2012 HPSCI investigative report. While Congress did not restrict use of Huawei equipment at the time, the report signaled to U.S. telecommunications providers that Congress was concerned with Huawei's ties to the Chinese government and its business practices. Major U.S. telecom operators noted that they opted not to use the equipment in their networks because of the concerns raised in the 2012 report, and were not as affected by the restrictions on Huawei use.[266]

Thus, while the 2012 report identified entities of concern, it did not recommend or impose restrictions on use, timelines for transitioning away from untrusted equipment, or actions for businesses. As a result, smaller U.S. operators and other entities (e.g., universities) made

[263] Tom Wheeler, "Keeping Huawei Hardware Out of the U.S. Is Not Enough to Secure 5G," *Lawfare*, February 20, 2019, at https://www.lawfareblog.com/keeping-huawei-hardware-out-us-not-enough-secure-5g.

[264] Ibid.

[265] For example, Open Radio Access Network (ORAN) architecture would allow operators to move away from single-vendor network solutions and toward open, interoperable architectures that would enable operators to select component parts from various vendors. A security advantage would be that if one part posed security risks, it could be replaced with the equipment of another vendor without replacement of the entire network.

[266] Jessica Bursztynsky, "Verizon CEO: We're Doing Just Fine Without Using Any Equipment from Chinese Tech Giant Huawei," *CNBC*, July 11, 2019, at https://www.cnbc.com/2019/07/11/ceo-hans-vestberg-says-verizon-does-not-use-any-huawei-equipment.html.

decisions to use the equipment. Thus, identifying the entity of risk may not halt its use; education, mitigation strategies, or restrictions may be needed to address security risks from entities or equipment that poses a threat to U.S. networks.

Since 2017, Congress has identified foreign adversaries in legislation and restricted use of equipment from listed entities; however, the list has varied in individual legislation and agency implementation. For example, Section 1656 of the FY2018 NDAA lists both the People's Republic of China (PRC) and the Russian Federation as covered countries, while Section 889 of the FY2019 NDAA lists only the PRC as a covered foreign country. Similarly, while the DOC Entity List covers Huawei and its more than 150 affiliates, the FCC "covered" list includes only Huawei and no affiliates. Further, multiple lists of entities and equipment are emerging, such as the DOC Entity List, FCC covered list, DHS National Risk Management Center list of equipment categories that may pose a risk, and the DOD List of Chinese Military Companies. Having multiple lists of countries, entities, and equipment that pose a threat to U.S. national security may present challenges to agencies and vendors and may hinder effective implementation.

Further, while there are lists of foreign adversaries, covered entities, affiliates, and equipment, the lists reside in multiple agencies. Responsibilities are dispersed across federal agencies. For example, Executive Order 13873 assigns responsibility to the Commerce Secretary to coordinate with other agencies to identify and mitigate risks posed by transactions; the DNI to continue to assess ICT threats; and the DHS Secretary to assess and identify entities, hardware, software, and services that pose the greatest potential consequences to U.S. national security. Legislation in the 117th Congress (H.R. 2685) would require DOC's National Telecommunications and Information Administration to examine and report on the cybersecurity of mobile service networks and their vulnerability to cyberattacks. Another bill (H.R. 4067) would require the FCC's CSRIC to provide biennial reporting to the FCC, Congress, and the public on recommendations to improve network security.

While some applaud the whole of government approach to assessing, identifying, and addressing risks, others, including some Members of Congress, have recognized a need to clarify governance responsibilities with regard to network security, to "ensure the United States can mount coordinated and efficient responses to security incidents and also identify new risks."[267]

Ensuring U.S. Competitiveness

Some scholars assert the restrictions on trade with Huawei could backfire, and hurt U.S. businesses, the U.S. economy, and U.S. competitiveness.[268] These scholars assert that the global telecommunications market is interdependent, with "coupled global networks of trade, production, knowledge, innovation, finance, regional and global institutions, and security," and that the "global system generates shared benefits for cooperation, [and] shared costs for non-cooperation."[269] Some foreign policy experts assert there are economic and diplomatic tools that could ensure security of networks and counter Huawei's growth and dominance in the global

[267] U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Communications and Technology, *A Safe Wireless Future: Securing our Networks and Supply* (June 25, 2021 Memorandum for Subcommittee Staff, in preparation of June 30, 2021 hearing), 117th Cong., 1st sess., June 30, 2021, p. 2, at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Briefing%20Memo_CAT%20Hrg_2021.06.30.pdf.

[268] James Andrew Lewis, "Selling to Huawei," Center for Strategic and International Studies, August 19, 2019, at https://www.csis.org/analysis/selling-huawei.

[269] Thomas D. Lairson, David Skidmore, and Wu Xinbo, "Why the U.S. Campaign Against Huawei Backfired," *The Diplomat*, May 13, 2020, at https://thediplomat.com/2020/05/why-the-us-campaign-against-huawei-backfired/.

telecommunications market. They say deep engagement and a "coordinated and well-funded effort to enhance U.S. competitiveness" are better able to protect national security, foreign policy, and economic interests than trade restrictions.[270]

Some policymakers have called for a government-led assessment of ICT markets, so the U.S. government has a better sense of companies leading the market. For example, H.R. 4028 would direct the Secretary of Commerce to submit to Congress within one-year a report analyzing the state of economic competitiveness of trusted vendors in the ICT supply chain, identify which components or technologies are critical or vulnerable, and identify components or technologies on which U.S. networks depend. It would also require the Commerce Secretary to submit to Congress a strategy to ensure the competitiveness of trusted vendors in the United States.

Some analysts suggest the U.S. government could help U.S. businesses advance 5G technologies through funding for R&D, low-cost financing for product development, policies and programs to help small businesses bring 5G products to market faster, and export credits for firms seeking to sell products globally.[271] They, and some lawmakers, argue government intervention may be necessary to compete with Huawei—a multinational conglomerate that leverages low-cost state-supported financing and other Chinese government subsidies and policies to undercut competitors' prices.[272] Scholars at the ITIF have encouraged the Biden Administration to document China's unfair trade practices, including Huawei's domestic market guarantees and state-supported financing that enables Huawei to undercut competitor pricing, and decide whether the United States should bring any of these concerns before the WTO for action.[273]

In the 117th Congress, Members have introduced legislation to provide U.S. government funding to the telecommunications industry for R&D on advanced technologies and 5G applications, to assure U.S. leadership and competitiveness in the global telecommunications industry. Experts assert that federal funding for R&D could counter China's investment in its domestic telecommunications technology firms, including Huawei, which invests heavily in R&D. In order to increase the competitiveness of U.S. businesses in the global 5G market, some scholars call for increased funding from the U.S. government for the semiconductor industry, 5G deployment, development of 5G "use cases" U.S. businesses can offer globally,[274] and 6G technologies.[275] The U.S. Innovation and Competition Act (S. 1260), which passed the Senate on June 8, 2021, would fund investment in U.S.-based semiconductor fabrication facilities and equipment, and test beds

[270] Ibid.

[271] Center for Strategic and International Studies, *Accelerating 5G in the United States*, March 2021, at https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210301_Lewis_Accelerating_5G_0.pdf?klP.hknBLh2uJBCPMkxs5_wRNzFiMbdO.

[272] Jeanne Whalen, "To Counter China, Some Republicans Are Abandoning Free-Market Orthodoxy," *Washington Post*, August 26, 2020, at https://www.washingtonpost.com/business/2020/08/26/republicans-favor-industrial-policy/.

[273] Stephen Ezell, *False Promises II: The Continuing Gap Between China's WTO Commitments and Its Practices*, Information Technology and Innovation Foundation, July 26, 2021, at https://itif.org/publications/2021/07/26/false-promises-ii-continuing-gap-between-chinas-wto-commitments-and-its.

[274] Some, including Huawei's founder, see the development of 5G use cases (e.g., smart cars, private networks for businesses, consumer applications) and Internet of Things technologies (e.g., sensors, wearable devices) that will run on 5G networks as phase 2 of 5G. These systems and devices are expected to generate new revenues for companies. See Yuan Yang, James Kynge, Sue-Lin Wong, and Nian Liu, "Huawei Founder Predicts Internet of Things Is Next US Battle," *Financial Times*, July 3, 2019, at https://www.ft.com/content/716181ce-9bd8-11e9-9c06-a4640c9feebb.

[275] Center for Strategic and International Studies, *Accelerating 5G in the United States*, March 2021, at https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210301_Lewis_Accelerating_5G_0.pdf?klP.hknBLh2uJBCPMkxs5_wRNzFiMbdO.

for open, interoperable network solutions,[276] 5G R&D, and domestic and international efforts to secure the wireless communication supply chain and global networks.

Some analysts call for U.S. government leadership, coordination, and funding for 6G, both domestically and internationally, which they assert could help the United States lead 6G standards and technology development.[277] Experts suggest that the U.S. government should target funding to 6G technologies through U.S. government funding of government R&D projects, R&D centers at universities, and tax incentives to support private-sector investment in R&D focused on 6G technologies to ensure the U.S. companies are positioned to be competitive in 6G.[278] Engagement in 6G development and standards setting could help ensure that U.S. interests and values are represented and U.S. national security and foreign policy interests are protected in 6G standards development organizations. In the 117th Congress, H.R. 4045 would require the FCC to create a 6G Task Force of government, industry representatives, and public interest groups to submit a report to Congress on 6G opportunities and challenges.

Ensuring Secure Global Networks and Communications

Some analysts encourage continued formation of international coalitions to advance security requirements and agreements through standards development and other international organizations (e.g., the International Telecommunication Union). International coordination on 5G security began under the Trump Administration, through such efforts as the Prague Proposals, where 22 nations agreed on a set of security recommendations for 5G networks, [279] and the State Department's Clean Networks initiative.[280] The Biden Administration is engaging allies and partners in 5G security and training and education on 5G security, and sharing approaches and options for restricting use of untrusted equipment, including Huawei.[281]

Some analysts urge the U.S. government to expand[282] funding and financing of secure 5G networks globally.[283] The Transatlantic Telecommunications Security Act (H.R. 3344) would authorize the U.S. International Development Finance Corporation (DFC) to provide financing

[276] For example, ORAN architecture would allow operators to move away from single-vendor network solutions and toward open, interoperable architectures that would enable operators to select component parts from various vendors. A security advantage would be that if one part posed security risks, it could be replaced with the equipment of another vendor without replacement of the entire network.

[277] Ali Khayrallah and Hugo Tullberg, "U.S. and EU Approaches to 6G," *Wilson Center*, July 15, 2021, at https://www.wilsoncenter.org/article/us-and-eu-approaches-6g.

[278] David Sacks, "China's Huawei Is Winning the 5G Race. Here's What the United States Should Do to Respond," *Council for Foreign Relations* (blog), March 29, 2021, at https://www.cfr.org/blog/china-huawei-5g.

[279] Government of the Czech Republic, "Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals," press release, March 5, 2019, at https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[280] U.S. Department of State, "The Clean Network," retrieved August 28, 2021, archived at https://2017-2021.state.gov/the-clean-network/index.html.

[281] Stu Woo and Drew Hinshaw, "U.S. Fight Against Chinese 5G Efforts Shifts From Threats to Incentives," *Wall Street Journal*, June 14, 2021, at https://www.wsj.com/articles/u-s-fight-against-chinese-5g-efforts-shifts-from-threats-to-incentives-11623663252.

[282] Melanie Hart and Jordan Link, "There Is a Solution to the Huawei Challenge," *Center for American Progress*, October 14, 2020, at https://www.americanprogress.org/issues/security/reports/2020/10/14/491476/solution-huawei-challenge/.

[283] Stu Woo, "U.S. to Offer Loans to Lure Developing Countries Away from Chinese Telecom Gear," *Wall Street Journal*, October 18, 2020, at https://www.wsj.com/articles/u-s-to-offer-loans-to-lure-developing-countries-away-from-chinese-telecom-gear-11603036800?mod=article_inline; and Stu Woo and Drew Hinshaw, "U.S. Fight Against

Chinese 5G Efforts Shifts From Threats to Incentives," *Wall Street Journal*, June 14, 2021, at https://www.wsj.com/articles/u-s-fight-against-chinese-5g-efforts-shifts-from-threats-to-incentives-11623663252.

for 5G network development to U.S. allies and partners in Central and Eastern Europe for networks that do not incorporate technology that poses security risks, such as Huawei equipment.

Conclusion

The U.S. government has taken steps to remove Huawei from U.S. networks, restrict exports to Huawei, and cease providing Huawei—an entity identified as engaging in activities contrary to U.S. national security and foreign policy interests—with essential parts that it needs to grow and expand globally. In the short term, Congress may focus on monitoring the implementation of policies and restrictions to increase their effectiveness and mitigate unintended impacts on U.S. agencies and businesses. In the long term, options for Congress include assessing the impact of the restrictions on security of U.S. networks and supply chains, retaining or refining restrictions against Huawei to protect foreign policy interests, and investing in U.S businesses and industries to advance U.S. economic interests and competitiveness.

Author Information

Jill C. Gallagher
Analyst in Telecommunications Policy

Disclaimer