Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Next Steps For Regulation Of The US Telecom Sector

By **Zack Harmon, Rod Rosenstein, Dan Coats, Christine Savage, Sumon Dantiki and Alex Early**

(May 7, 2020, 6:44 PM EDT) - On April 4, President Donald Trump issued an executive order creating the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector.

Zack Harmon

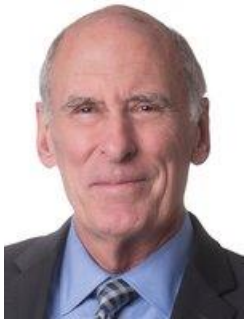
The new executive order and other recent developments reflect growing government scrutiny that requires companies that are part of the nation's digital infrastructure and telecommunications supply chain to review how they incorporate cybersecurity and counterintelligence risk into their operations and strategic planning.

The committee replaces an informal interagency working group known as Team Telecom, which assisted the Federal Communications Commission in licensing decisions involving foreign ownership or control for national security and law enforcement risks. For new applications, the committee is empowered to recommend denying licenses or imposing mitigation conditions.

Rod Rosenstein

For current licenses, it is empowered to review existing mitigation agreements — including in cases where a company is in full compliance — and recommend modifying them or revoking the license entirely.

The establishment of this Telecom Committee highlights growing governmental concern about the national security risks posed by foreign participation or control across a broad range of U.S. critical infrastructure. The evolving telecommunications sector is a particular focus: A senior U.S. Department of Justice official pointedly warned in congressional testimony that the department is "increasingly concerned with supply chain threats, especially to [the] telecommunications sector."[1]



Dan Coats

The concern is reflected in a series of related developments. The Committee on Foreign Investment in the United States in the past few years has both expanded its jurisdictional scope and taken a much more aggressive approach to enforcement, including proactively reviewing more closed transactions.[2]

Similarly, in December 2019, the U.S. Department of Commerce issued a proposed rule on Securing the Information and Communications Technology and Services Supply Chain,[3] or the

ICTS proposed rule, that would empower the secretary to conduct national security reviews of foreign communications equipment and services acquisitions for use in the U.S. telecommunications supply chain, defined broadly to include cloud service providers, software as a service and connected medical and video devices in addition to traditional telecommunications service providers.

Christine Savage

The ICTS proposed rule would allow the Commerce Department to block transactions affecting critical infrastructure or the digital economy or condition them on risk mitigation measures.[4]

Taken together, the new Telecom Committee and the ICTS proposed rule signify a robust approach to a broad set of potential telecommunications supply chain threats. When both initiatives are implemented, the U.S. government will be able to review, modify, block or potentially unwind a broad range of telecommunications and digital infrastructure transactions throughout the telecommunications supply chain.

Sumon Dantiki

Telecom Committee: Structure and Process

Chair, Members and Advisers

The attorney general chairs and funds the new committee, with "the exclusive authority to act, or to authorize other Committee Members to act, on behalf of the Committee," elevating the attorney general's authority beyond his previous Team Telecom leadership role.[5]

Alex Early

The committee includes the secretaries of defense and homeland security (who composed the prior informal Team Telecom), along with any other department/agency head or White House assistant that the president designates.[6] The order also enumerates advisers to the committee, including the secretaries of state, treasury and commerce, as well as the director of national intelligence, the U.S. trade representative and the president's national security adviser.[7]

Review Timelines

Under the new process, once an FCC application is deemed complete and referred to the committee for review, the committee must complete an initial review of an application within 120 days, with the option of a secondary assessment to further examine potential risks within 90 days.[8] The DOJ has stated that even complex applications would be reviewed within about a year under this process,[9] potentially eliminating the lengthy delays that sometimes resulted from Team Telecom review.

Formalized, Timely Intelligence Analysis

The Office of the Director of National Intelligence under the executive order must produce a written threat analysis assessment of each license or application that the committee reviews within 30 days of a request by the chair.[10] The ODNI already plays a similar role in the CFIUS review process.

Recommendation Process

In deciding whether to accept, deny, revoke or impose mitigation conditions on a specific license, the executive order includes several provisions and internal deadlines to encourage consensus among members. If such consensus cannot be found, the attorney general will present any issue directly to Telecom Committee members for a majority vote, with the power to break ties and determine the committee recommendation.[11]

Consensus Telecom Committee recommendations to approve an application outright or with any mitigation measures go directly to the
Federal Communications Commission via the National Telecommunications and Information Administration.

If consensus cannot be found, the committee may then take a vote; for committee votes which are not unanimous, the executive order appears to require the chair to give notice the president within seven days and then wait at least more 15 days before notifying the FCC.[12]

The executive order does not clarify what will happen after the president receives notice, but it terms a nonunanimous recommendation as an intended recommendation, suggesting that the goal is give the president an opportunity to overrule it.

Authority for Retrospective Review and Compliance Monitoring

The executive order explicitly contemplates that the Telecom Committee may reexamine existing licenses for risk — even if a mitigation agreement is in place and the company is complying with it.[13]

The committee also has broad authority to monitor any mitigation measures the FCC imposes as a condition on a license and to develop methods of monitoring compliance with mitigation measures, including by requiring member entities to report any material noncompliance to the committee. The DOJ, moreover, may request the ODNI to provide analyses of threats to risk mitigation, compliance monitoring and enforcement to committee member and advisor entities.[14]

Recent Past as Prelude: Google and China Telecom

Within a few days of the executive order forming the new Telecom Committee, the DOJ publicly announced decisions on two significant pending FCC national security reviews of Google Inc. and China Telecom Corp Ltd. Although all these reviews occurred under the prior Team Telecom regime, the rationales used in their dispositions highlight the concerns that will drive the new committee process.

China Telecom

In 2007, China Telecom signed a letter of assurance with the DOJ, including the FBI, and the U.S. Department of Homeland Security pledging to make U.S. records available in response to legal requests and not to disclose those U.S. records to foreign governments as conditions of its authority to operate in the U.S. under Section 2014 of the Communications Act.[15]

The conditions did not include any requirement to provide detailed information about China Telecom's supply chain. Thirteen years later, in an April 2020 decision to revoke the license, the DOJ cited among its considerations a markedly changed understanding of the cyber threat posed by China, inaccurate

statements by China Telecom about its cybersecurity and data storage practices, and concerns about exploitation by the Chinese government.[16]

Following the DOJ decision, the FCC issued a show cause order on April 24, giving China Telecom Americas, China Unicom Americas, Pacific Networks Corp., and ComNet USA LLC 30 days to demonstrate that they are not subject to the influence and control of the Chinese government.[17]

Google

Along with a Chinese partner, Google and Facebook (both acting through subsidiaries) applied for FCC authority to operate the Pacific Light Cable Network System connecting the United States to Taiwan and Hong Kong via undersea data cables.

In April 2020 the Department of Justice, with concurrence from the Departments of Homeland Security and Defense, decided not to object to a six-month temporary approval for Google to operate the portion of the PCLN connecting the United States and Taiwan, but did not approve the portion connecting to Hong Kong.[18]

The decision is conditioned on a national security agreement that requires immediate, and likely recurring, supply chain disclosures, as well as ongoing requirements to report attempted data breaches and changes in foreign ownership, an annual compliance report, and possible auditing requirements.[19]

In addition, Google committed to "pursue diversification of interconnection points in Asia," and to establish network facilities that deliver traffic "as close as practicable" to its ultimate destination.[20] The DOJ also pointedly warned that "there is a significant risk that the grant of a direct cable connection between the United States and Hong Kong would seriously jeopardize the national security and law enforcement interests of the United States."[21]

Future Impact

The creation of a standing national security review committee for telecommunications licenses is in many ways a formalization of the preexisting ad hoc Team Telecom. But the executive order formalizing these functions in the new Telecom Committee elevates national security equities, establishes the DOJ's leadership authority and cements the trend toward more robust supply chain monitoring and ongoing compliance obligations.

The initiative clearly is part of a broader effort; indeed, even when acting in its Team Telecom advisory role to enter into a provisional national security agreement with Google, the DOJ cited the executive order concerning the ICTS proposed rule.[22] That 2019 executive order found that "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services."

Viewed alongside the ICTS proposed rule and other significant related developments, the new Telecom Committee signals that the government will exercise broad authority to review, mitigate and reject transactions affecting digital infrastructure. Accordingly, companies supporting digital infrastructure and the telecommunications supply chain should proactively review their operations and strategic planning to make sure they appropriately incorporate cybersecurity and counterintelligence risk, including through:

- Threat awareness: Ensuring that processes for understanding a fast-moving threat landscape are robust and defensible.

- Supply chain vetting/due diligence: Ensuring a rigorous and updated vetting and due diligence process for key suppliers.

- IT vendor (hardware and software) due diligence: Ensuring a rigorous and updated vetting and due diligence process for information technology hardware and software used in critical infrastructure.

- Monitoring, documenting and analyzing attempted data breach attempts: Tracking, understanding and mitigating attempts to gain unauthorized digital access to key systems.

- Insider threat program: Having a comprehensive and muscular insider threat program in place with technical, HR, compliance and physical elements.

Our nation's telecommunications backbone — always significant to recent national economic life — is set to both rapidly transform and be at the heart of growing and indispensable digital infrastructure. For example, the development of 5G (and successor) technology, portends data rates hundreds of times faster than current ones.[23]

Next-generation wireless networks would also facilitate much greater connectivity of a range of connected devices, by one estimate projected to be 41.6 billion devices by 2025.[24]

This level of connectivity would accelerate the use of a variety of connected products and services with security effects, such as cloud providers, telemedicine, smart cities blanketed by sensors, smart homes with monitoring and security mechanisms, automated logistics operations, autonomous vehicles, drones and delivery robots, medical devices, facial recognition and other biometric technologies, and virtual/augmented reality.[25]

It would also likely have important effects on the development of artificial intelligence and other transformative technological efforts.[26]

While there is agreement that current telecommunications infrastructure needs to be dramatically upgraded to fully realize this potential, how this will be accomplished is not clear.[27] However, given that this networked future will lead to novel dependence, counterintelligence risks and cybersecurity challenges it will undoubtedly bring even more U.S. government scrutiny on telecommunications providers, entities within their supply chain, and other companies that could be considered part of our digital critical infrastructure.

Zack Harmon is a partner at King & Spalding LLP and former chief of staff at the FBI.

Rod Rosenstein is a partner at the firm and former deputy attorney general.

Dan Coats is a partner at the firm and former director of national intelligence.

Christine Savage, Sumon Dantiki and Alex Early are partners at the firm.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Statement of John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice, Before the Committee on the Judiciary, U.S. Senate, For A Hearing On China's Non-Traditional Espionage Against The United States: The Threat And Potential Policy Responses, U.S. Dep't of Justice, at 8 (Dec. 12, 2018), available at https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2018/12/18/12-05-2018_john_c._demers_testimony_re_china_non-traditional_espionage_against_the_united_states_the_threat_and_potential_policy_responses.pdf.

[2] Statement of Christopher Wray, Director, Federal Bureau of Investigation, Before the Committee on the Judiciary, U.S. House of Representatives, At A Hearing Entitled "FBI Oversight," U.S. Dep't of Justice (Feb. 5, 2020), available at https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2020/02/06/fbi18.doc_.pdf ("As a result of the Foreign Investment Risk Review Modernization Act, which was enacted last year, the FBI anticipates its workload to increase dramatically."); Deputy Assistant Attorney General Adam S. Hickey of the National Security Division Delivers Remarks at the Fifth National Conference on CFIUS and Team Telecom, U.S. Dep't of Justice (Washington D.C. April 24, 2019), available at https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-adam-s-hickey-national-security-division-delivers-0 ("FIRRMA represents the most significant reform of the CFIUS process in more than a decade. . . . Most significantly, in my view, [FIRRMA] expands the Committee's authority to address emerging national security risks that fall outside foreign control thresholds . . . or any deal structured to circumvent CFIUS review.").

[3] Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65,318-65,319 (Nov. 27, 2019) (to be codified at 15 C.F.R. pt. 7).

[4] Id.

[5] Executive Order 13913 of April 4, 2020 Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, at §§3(c), 4(b), 11(b) (emphasis supplied), 85 Fed. Reg. 19,643 (Apr. 8, 2020), https://www.govinfo.gov/content/pkg/FR-2020-04-08/pdf/FR-2020-04-08.pdf.

[6] Id. at §3(b).

[7] Id. at §3(d). Committee Members and Advisors are authorized to designate a senior executive to perform their functions

[8] Id. at §§5(b)(iii), 5(c).

[9] Attorney General Will Chair Committee to Review Foreign Participation in the U.S. Telecommunications Sector, U.S. Dep't of Justice, Press Release No. 20-363 (Apr. 7, 2020), available at https://www.justice.gov/opa/pr/attorney-general-will-chair-committee-review-foreign-participation-us-telecommunications.

[10] Supra note 5 "Exec. Order 13913" at §§7(a), (b); see supra note 1 at 5 ("As part of this process, the FBI provides input and analysis to the National Intelligence Council within eight days of a CFIUS filing and a risk assessment to the Department of Justice within 30 days of a CFIUS filing.").

[11] Supra note 5 "Exec. Order 13913" at §9(e).

[12] Id. at §9(g).

[13] Id. at §§6(a), (b).

[14] Id. at §7.

[15] Letter of Assurance from China Telecom to DOJ, FBI, and DHS (July 17, 2007), available at https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=-133273&f_number=ITCT/C2007072500285.

[16] Executive Branch Agencies Recommend the FCC Revoke and Terminate China Telecom's Authorizations to Provide International Telecommunications Services in the United States, U.S. Dep't of Justice, Press Release No. 20-269 (updated Apr. 10, 2020), available at https://www.justice.gov/opa/pr/executive-branch-agencies-recommend-fcc-revoke-and-terminate-china-telecom-s-authorizations.

[17] Order to Show Cause, In the Matter of China Telecom (Americas) Corporation, FCC, GN Docket 20-109; No. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, (Apr. 24, 2020); Order to Show Cause, In the Matter of China Unicom (Americas) Corporations Limited, FCC, GN Docket 20-110; No. ITC-214-20020728-00361, ITC-214-20020724-00427 (Apr. 24, 2020); Order to Show Cause, In the Matter of Pacific Networks Corp. and ComNet (USA) LLC, FCC, GN Docket 20-111; No. ITC-214-20090105-00006, ITC-214-20090424-00199 (Apr. 24, 2020).

[18] Department of Justice Clears on Google's Application to the Federal Communications Commission to Operate a Portion of the Pacific Light Cable Network System, U.S. Dep't of Justice, Press Release No. 20-367 (Apr. 8, 2020), available at https://www.justice.gov/opa/pr/department-justice-clears-google-s-application-federal-communications-commission-operate.

[19] Petition To Adopt Conditions For Special Temporary Authority, In the Matter of GU Holdings Inc., et al., Application for a License to Construct, Land, and Operate an Undersea Fiber Optic Cable Connecting the United States, Hong Kong, Taiwan, and the Philippines, FCC, No. SCL-LIC-20170421-00012, SCL-AMD-20171227-00025, SCL-STA-20200402-00015 (Apr. 8, 2020).

[20] Id. at 11, Provisional National Security Agreement For Requested Special Temporary Authority, §C(7).

[21] Id. at 3.

[22] Id. at 5 (quoting Exec. Order 13873).

[23] Ian King and Scott Moritz, Why 5G Mobile Is Arriving with a Subplot of Espionage, Bloomberg (Jan. 8, 2020), available at https://www.bloomberg.com/news/articles/2020-01-08/why-5g-mobile-is-

arriving-with-a-subplot-of-espionage-quicktake (noting that 5G "could end up being 100 times faster" than 4G); but see Bob O'Donnell, Real-World 5G Speeds Are Slower Than Expected, Forbes (Nov. 22, 2019), available at https://www.forbes.com/sites/bobodonnell/2019/11/22/real-world-5g-speeds/#65a2f1244f96 (noting that "as early experience has shown, real-world [5G] speeds don't come close to the many theoretical throughput numbers that vendors have talked about.").

[24] The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast, International Data Corporation (June 18, 2019), available at https://www.idc.com/getdoc.jsp?containerId=prUS45213219; see also What Is 5G, and When Do I Get It?, Wired (Feb. 13, 2017), available at https://www.wired.com/2017/02/what-is-5g-and-when-do-i-get-it/ ("Because it's designed for a world in which tens of billions of gadgets depend on constant connectivity, 5G networks will be engineered to adapt to the needs of individual devices.").

[25] CP Gurnani, Perspectives: 5G will have an enormous impact on the world, CNN Business (Jan. 18, 2019), available at https://www.cnn.com/2019/01/18/perspectives/davos-5g-tech-mahindra/index.html (noting that 5G, and connected devices that rely on it, will "disrupt the way we live and work. It will go beyond mobile broadband and impact self-sustaining modern human establishments like smart cities, robotics and self-driving cars, and foster innovation in critical sectors such as health care, agriculture and education."); Nick Huber, A Hacker's Paradise? 5G and Cyber Security, Financial Times (Oct. 14, 2019), available at https://www.ft.com/content/74edc076-ca6f-11e9-af46-b09e8bfe60c0 (highlighting the increasing security challenges when "everything from cars and factory assembly lines to baby monitors and traffic lights have embedded internet-connected sensors"); Sue Halpern, The Terrifying Potential of the 5G Network, The New Yorker, (Apr. 26, 2019), available at https://www.newyorker.com/news/annals-of-communications/the-terrifying-potential-of-the-5g-network ("[E]verything from toasters to dog collars to dialysis pumps to running shoes will be connected. Remote robotic surgery will be routine, the military will develop hypersonic weapons, and autonomous vehicles will cruise safely along smart highways. . . . A totally connected world will also be especially susceptible to cyberattacks.").

[26] James Rundle and Angus Loten, The Power of Combining 5G and AI, Wall Street Journal (Nov. 8, 2019), available at https://www.wsj.com/articles/the-power-of-combining-5g-and-ai-11573234753 (noting the increasing use of AI in many industries, including food and beverage, medicine, retail, manufacturing, and automotive).

[27] David E. Sanger, Julian E. Barnes, Raymond Zhong and Marc Santora, In 5G Race With China, U.S. Pushes Allies to Fight Huawei, N.Y. Times (Jan. 26, 2019), available at https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html ("In an age when the most powerful weapons, short of nuclear arms, are cyber-controlled, whichever country dominates 5G will gain an economic, intelligence and military edge for much of this century.").