United States Government Accountability Office

Report to Congressional Requesters

November 2020

TECHNOLOGY ASSESSMENT

5G Wireless

Capabilities and Challenges for an Evolving Network

Accessible Version

GAO-21-26SP

The cover image displays examples of a traditional cell tower (right) and a small cell (left), which can be installed on a utility pole or streetlamp to provide coverage to a relatively small area.

Cover source: GAO. | GAO-21-26SP

GAO Highlights

Highlights of GAO-21-26SP, a report to congressional requesters

November 2020

Why GAO did this study

GAO was asked to assess the technologies associated with 5G and their implications. This report discusses (1) how the performance goals and expected uses are to be realized in U.S. 5G wireless networks, (2) the challenges that could affect the performance or usage of 5G wireless networks in the U.S., and (3) policy options to address these challenges.

To address these objectives, GAO interviewed government officials, industry representatives, and researchers about the performance and usage of 5G wireless networks. This included officials from seven federal agencies; the four largest U.S. wireless carriers; an industry trade organization; two standards bodies; two policy organizations; nine other companies; four university research programs; the World Health Organization; the National Council on Radiation Protection and Measurements; and the chairman of the Defense Science Board's 5G task force. GAO reviewed technical studies, industry white papers, and policy papers identified through a literature review. GAO discussed the challenges to the performance or usage of 5G in the U.S. during its interviews and convened a one-and-a-half day meeting of 17 experts from academia, industry, and consumer groups with assistance from the National Academies of Sciences, Engineering, and Medicine.

GAO received technical comments on a draft of this report from six federal agencies and nine participants at its expert meeting, which it incorporated as appropriate.

View GAO-21-26SP. For more information, contact Hai Tran at (202) 512-6888, tranh@gao.gov or Vijay A. D'Souza at (202) 512-6240, dsouzav@gao.gov.

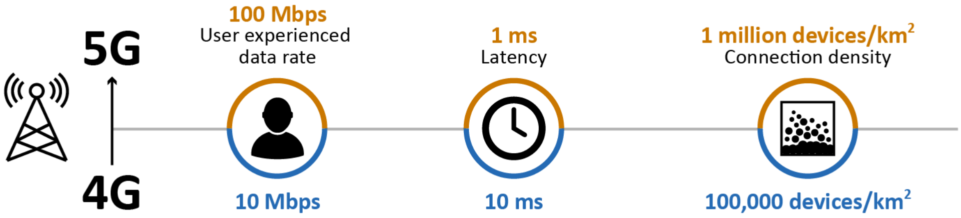
TECHNOLOGY ASSESSMENT

5G Wireless

Capabilities and Challenges for an Evolving Network

What GAO found

Fifth-generation (5G) wireless networks promise to provide significantly greater speeds and higher capacity to accommodate more devices. In addition, 5G networks are expected to be more flexible, reliable, and secure than existing cellular networks. The figure compares 4G and 5G performance goals along three of several performance measures.



Source: GAO depiction of International Telecommunication Union data. | GAO-21-26SP

Text of figure comparing 4 g and 5g networks

	5G	4G
Data Rate	100 Mbps User experienced data rate	10 Mbps
Latency	1 ms Latency	10 ms
Connection density	1 million devices/km^2 Connection density	100,000 devices/km^2

Note: Megabits per second (Mbps) is a measure of the rate at which data is transmitted, milliseconds (ms) is a measure of time equal to one thousandth of a second, and square kilometer (km^2) is a measure of area.

As with previous generations of mobile wireless technology, the full performance of 5G will be achieved gradually as networks evolve over the next decade. Deployment of 5G network technologies in the U.S. began in late 2018, and these initial 5G networks focus on enhancing mobile broadband. These deployments are dependent on the existing 4G core network and, in many areas, produced only modest performance improvements. To reach the full potential of 5G, new technologies will need to be developed. International bodies that have been involved in defining 5G network specifications will need to develop additional 5G specifications and companies will need to develop, test, and deploy these technologies. GAO identified the following challenges that can hinder the performance or usage of 5G technologies in the U.S.

Spectrum availability and efficiency Spectrum demand will likely continue to exceed supply.	- Research and development of technologies to make more efficient use of the spectrum (i.e., spectrum sharing technologies) are needed. - A thorough understanding of propagation in higher frequencies, under various operating conditions, is needed.
Cybersecurity 5G networks provide some network security enhancements, but many of those will not be realized until complete, or "standalone," 5G networks are deployed.	- 5G networks introduce new modes of cyberattack and expand the potential points of attack. - 5G does not eliminate existing concerns around supply chains for network hardware.

Privacy 5G networks will exacerbate existing privacy concerns.	- 5G networks introduce new kinds of user data, including more precise location data. - 5G networks are expected to produce far more data than current cellular networks.
Concern over possible health effects Deployment of 5G technology may intensify existing public concern that radio frequency energy exposure affects health.	- Decision makers need policy-relevant information on the effects of 5G technology. - Although there is no consistent evidence of health risks related to the radio waves used for 5G, responding to public concerns remains a challenge, in part due to the unknown long-term health effects.

GAO developed six policy options in response to these challenges, including the status quo. They are presented with associated opportunities and considerations in the following table. The policy options are directed toward the challenges detailed in this report: spectrum sharing, cybersecurity, privacy, and concern over possible health effects of 5G technology.

Policy options to address challenges to the performance or usage of U.S. 5G wireless networks

Policy option	Opportunities	Considerations
Spectrum-sharing technologies (report p. 47) Policymakers could support research and development of spectrum sharing technologies.	• Could allow for more efficient use of the limited spectrum available for 5G and future generations of wireless networks. • It may be possible to leverage existing 5G testbeds for testing the spectrum sharing technologies developed through applied research.	• Research and development is costly, must be coordinated and administered, and its potential benefits are uncertain. Identifying a funding source, setting up the funding mechanism, or determining which existing funding streams to reallocate will require detailed analysis.
Coordinated cybersecurity monitoring (report p. 48) Policymakers could support nationwide, coordinated cybersecurity monitoring of 5G networks.	• A coordinated monitoring program would help ensure the entire wireless ecosystem stays knowledgeable about evolving threats, in close to real time; identify cybersecurity risks; and allow stakeholders to act rapidly in response to emerging threats or actual network attacks.	• Carriers may not be comfortable reporting incidents or vulnerabilities, and determinations would need to be made about what information is disclosed and how the information will be used and reported.
Cybersecurity requirements (report p. 49) Policymakers could adopt cybersecurity requirements for 5G networks.	• Taking these steps could produce a more secure network. Without a baseline set of security requirements the implementation of network security practices is likely to be piecemeal and inconsistent. • Using existing protocols or best practices may decrease the time and cost of developing and implementing requirements.	• Adopting network security requirements would be challenging, in part because defining and implementing the requirements would have to be done on an application-specific basis rather than as a one-size-fits-all approach. • Designing a system to certify network components would be costly and would require a centralized entity, be it industry-led or government-led.
Privacy practices (report p. 50) Policymakers could adopt uniform practices for 5G user data.	• Development and adoption of uniform privacy practices would benefit from existing privacy practices that have been implemented by states, other countries, or that have been developed by federal agencies or other organizations.	• Privacy practices come with costs, and policymakers would need to balance the need for privacy with the direct and indirect costs of implementing privacy requirements. Imposing requirements can be burdensome, especially for smaller entities.
High-band research (report p. 51) Policymakers could promote R&D for high-band technology.	• Could result in improved statistical modeling of antenna characteristics and more accurately representing propagation characteristics. • Could result in improved understanding of any possible health effects from long-term radio frequency exposure to high-band emissions.	• Research and development is costly and must be coordinated and administered, and its potential benefits are uncertain. Policymakers will need to identify a funding source or determine which existing funding streams to reallocate.
Status quo (report p. 52)	• Some challenges described in this report may be addressed through current efforts.	• Some challenges described in this report may remain unresolved, be exacerbated, or take longer to resolve than with intervention.

Table of Contents

Figures

Abbreviations

3GPP	3rd Generation Partnership Project
5G	fifth-generation (wireless networks)
ATIS	Alliance for Telecommunications Industry Solutions
CBRS	Citizens Broadband Radio Service
CISA	Cybersecurity and Infrastructure Security Agency
CSRIC	Communications Security, Reliability, and Interoperability Council
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOD	Department of Defense
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FIPPs	Fair Information Practice Principles
GDPR	General Data Protection Regulation
ICT	information and communications technology
IEEE	Institute of Electrical and Electronics Engineers
IMT	international mobile telecommunications
IoT	Internet of Things
ITU	International Telecommunication Union
LTE	Long Term Evolution
MIMO	multiple input multiple output
NCI	National Cancer Institute
NCRP	National Council on Radiation Protection and Measurements
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development (program)
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration
R&D	research and development
RF	radio frequency

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

November 24, 2020

Congressional Requesters

Fifth-generation (5G) wireless networks promise to deliver significantly improved network performance and greater capabilities, such as greater speeds and higher capacity to accommodate more devices. These improvements will be achieved, in part, by the development and deployment of new technologies and by using additional radio frequency (RF) spectrum that will expand coverage areas and increase data transmission speed and capacity. Further, 5G could bring major investment from the wireless industry that can, over time, result in economic growth and creation of jobs. Recent studies have estimated that, based on the experience gained from the use of previous wireless generations, the U.S. could sustain major gains in employment and economic growth with widespread deployment of 5G.[1] According to studies on the socioeconomic benefits of 5G, additional potential benefits include increased access and availability to more advanced health care and education, reduced pollution and increased efficiency in transportation, and enhanced public safety response capabilities.[2] Studies have cited potential benefits in the billions of dollars, although it is unclear when and where the benefits will be realized.

In view of the anticipated worldwide deployment of 5G networks, you asked us to assess the technologies associated with 5G, as well as its broader impacts for the U.S. Earlier this year, we reported on challenges to deploying 5G and the ways the federal government is addressing those challenges.[3] Specifically, we found that the Federal Communications Commission (FCC) lacked comprehensive strategic planning to guide 5G spectrum policy and to mitigate the likelihood of 5G to widen the digital divide.[4] We also reported that the high cost of 5G infrastructure may affect its deployment, including costs associated with additional sites, such as fiber, power, and permitting. More recently, we reported on the extent to which the federal government has developed a national strategy to secure 5G.[5] We found that the current 5G national strategy fails to address costs and resources needed for implementation, and only

[1] See, for example: *Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities* (Accenture, 2017) and D.W. Sosa and G. Rafert, *The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States* (Analysis Group, February 2019).

[2] See, for example: GSM Association, *WRC Series: Study on Socio-Economic Benefits of 5G Services Provided in mmWave Bands* (2018) and Tech4i2, Real Wireless, Trinity College Dublin, and InterDigital, *Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe*, European Commission DG Communications Networks, Content & Technology (2016).

[3] GAO*, 5G Deployment: FCC Needs Comprehensive Planning to Guide its Efforts*, GAO-20-468 (Washington, D.C.: June 12, 2020).

[4] The digital divide refers to a disparity where different socioeconomic groups and groups in different geographic areas receive different levels of access to telecommunications services.

[5] GAO, *National Security: Additional Actions Needed to Ensure Effectiveness of 5G Strategy*, GAO-21-155R (Washington, D.C.: Oct. 7, 2020).

partially addresses other desirable characteristics of an effective national strategy. This report discusses (1) how the performance goals and expected uses are to be realized in U.S. 5G wireless networks; (2) the challenges that could affect the performance or usage of 5G wireless networks in the U.S.; and (3) policy options to address these challenges.

To address these objectives, we met with officials from selected federal agencies and companies involved with the development, deployment, or impacts of 5G networks. We also met with the four largest U.S. wireless carriers (AT&T Inc., Sprint Corporation, T-Mobile US, Inc., and Verizon Communications Inc.), industry organizations, standards bodies, and policy organizations.[6] Additionally, we met with four university wireless research programs and toured one of them.

During our interviews with officials and representatives, we discussed 5G performance goals; 5G applications; the status of key technologies that will enable the performance or usage of 5G networks; challenges to the performance or usage of 5G in the U.S.; and policy options to address these challenges.

To identify and understand challenges that may affect the performance and expected usage of 5G networks in the U.S., and to identify policy options to address these challenges, we convened a one-and-a-half day meeting of 17 experts from academia, industry, and consumer groups. We selected these experts with assistance from the National Academies of Sciences, Engineering, and Medicine to obtain a range of perspectives on 5G deployment.[7] In addition, we conducted a broad-based literature review of industry white papers, technical reports, and other documentation such as policy papers by think tanks. We also reviewed related technical reports on 5G and its broader impacts, such as industry white papers and the Institute of Electrical and Electronics Engineers (IEEE) Future Networks technology road maps.

To formulate the policy options, we gathered and assessed ideas from our literature review; interviews with agencies, industry, and researchers; and the expert meeting organized with the National Academies of Sciences, Engineering, and Medicine. See appendix I for a detailed description of our objectives, scope, and methodology.

We conducted our work from June 2019 to November 2020 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to technology assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work.

[6] Sprint Corporation merged with T-Mobile US, Inc. on April 1, 2020, and the merged company is known as T-Mobile. At the time of our interviews they were separate companies.

[7] We planned and convened this expert meeting in collaboration with our team examining 5G deployment challenges (GAO-20-468) and with the assistance of the National Academies of Sciences, Engineering, and Medicine to better ensure that a breadth of expertise was brought to bear in its preparation; however, all final decisions regarding meeting substance and expert participation were the responsibility of GAO. Any conclusions and recommendations in GAO reports are solely those of GAO.

We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

1 Background

1.1 Mobile wireless communication

Communication over the airwaves began about 130 years ago when wireless telegraphs replaced pigeons and flags for sending messages at sea. Since then, the technology has expanded dramatically to accommodate a multitude of uses, from emergency and medical services to video chats to industrial automation, many of which require the transmitting devices to be mobile.

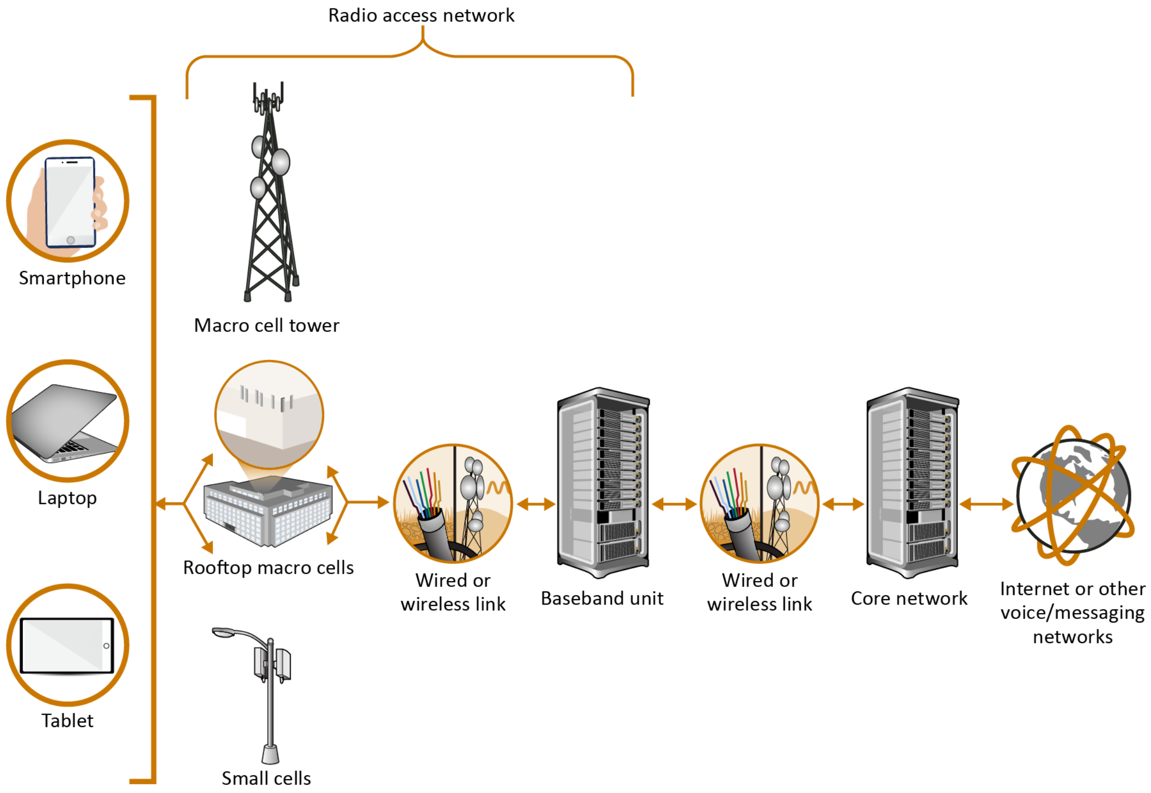
Mobile wireless technology for consumers developed in the 1980s as cellular communications.[8] *Cellular* refers to the division of a geographic area into smaller areas, known as cells. Phones within each cell send and receive radio signals from a base station, often called a cell tower, which connects users to other users on cellular and wired networks, such as landline telephones. The first-generation cellular network allowed for mobile phone calls using analog radio technology. The second generation introduced a greater range of frequencies, or bandwidth, along with digital radio technology. This enabled data communications in the form of text messaging. Continuing into the third and fourth generations, networks added capacity for more calls and for connectivity to the internet, which allowed for the transmission of increasingly larger amounts of data. The result is the current 4G era of mobile web browsing, mobile video, and smartphones. Each of these generations evolved gradually.

Figure 1 depicts a simplified architecture for a cellular network. Devices connect over the *radio access network*, which defines and manages the radio link between the customer device and the rest of the network. The radio access network comprises cellular base stations, wired or wireless links, and a *baseband unit* that processes the radio signals and manages interference. Base stations for 4G and 5G networks include traditional *macro cell* towers and rooftop installations as well as *small cells*, which can also be installed on utility poles or streetlamps to provide service to a smaller area. The hardware and software used to connect devices wirelessly to the baseband units are known as *radio access technology*, which includes “Long Term Evolution” (LTE) for 4G networks and “New Radio” for 5G.

Once a signal from the customer’s device reaches the base station, it is transmitted over a wired or wireless link to the baseband unit. The baseband unit connects over a wired or wireless link to the *core network*, which manages the radio access network and routes each connection to outside services, such as the internet, a land line, or back out through the radio access network to another wireless device.

[8] This report uses the term *mobile wireless* communication to refer to cellular technologies. We exclude distinct technologies such as walkie-talkies, even though they are both mobile and wireless.

Figure 1: Simplified cellular network architecture



Source: GAO. | GAO-21-26SP

Text for Figure 1: Simplified cellular network architecture

1. Technology
   a. Smartphone
   b. Laptop
   c. Tablet
2. Radio Access Network
   a. Macro cell tower
   b. Rooftop macro cells
   c. Small cells
3. Baseband unit
4. Core Network
5. Internet or other voice/messaging networks

1.2 The radio frequency spectrum

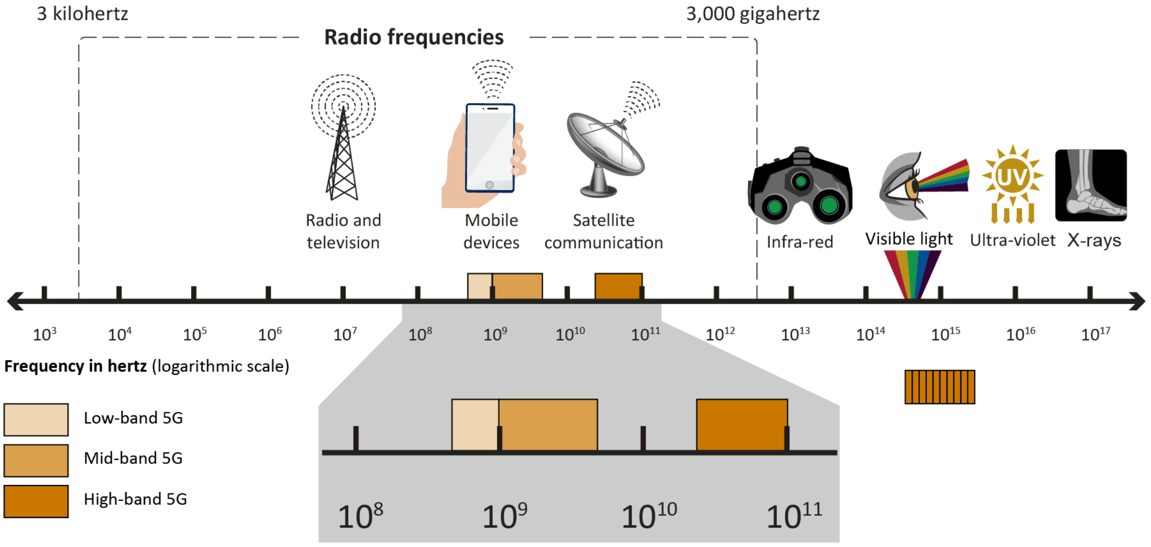
The radio access network uses radio signals, a form of electromagnetic waves, to communicate wirelessly. Electromagnetic waves transport energy and, unlike ocean waves, can travel through space without the need for wires or a physical medium. They include not only radio waves, but also infrared light, visible light, and X-rays, among others. The type of wave, along with its properties, depends on the frequency at which it oscillates.

Frequency is measured in hertz (Hz) and represents the number of cycles per second. Frequencies are also expressed in kilohertz (kHz, which is 1,000 Hz), megahertz (MHz, 1 million Hz), or gigahertz (GHz, 1 billion Hz). RF ranges from 3 kHz to a defined maximum of 3,000 GHz. For the purposes of cellular communications, the RF spectrum is generally split into three categories: low-band (under 1 GHz), mid-band (from about 1 GHz to about 6 GHz), and high-band (between 24 GHz and 100 GHz).[9] 4G mobile wireless networks use RF in the low- and mid-band, from 600 MHz to 3.5 GHz, while 5G will expand to higher frequencies. High-band frequencies are referred to as *millimeter wave*.[10] Figure 2 shows the parts of the electromagnetic spectrum typically used by various technologies, including the RF spectrum available and planned for 5G devices.

The frequency bands used for 5G offer complementary performance characteristics. Signals using low-band spectrum can cover larger areas, go around obstacles, and penetrate a range of materials more effectively than higher frequencies. High-band spectrum supports signals that have greater bandwidth and therefore can carry more information, but with a more limited range and poorer indoor coverage. The properties of mid-band spectrum are intermediate between low- and high-band.

Cellular data use is expected to increase over time (see fig. 3). This increasing demand for mobile data transmission will require additional spectrum, especially in the mid- and high-bands, for 5G networks.

Figure 2: Electromagnetic spectrum

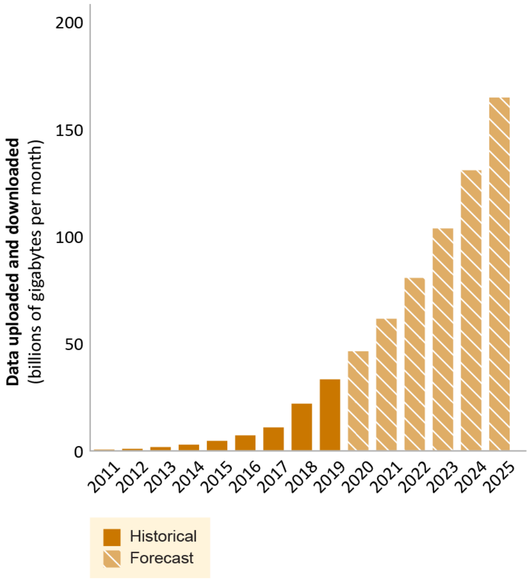


Source: Federal Communications Commission and GAO. | GAO-21-26SP

[9] The frequencies between 6 GHz and 24 GHz are referred to as mid-high band spectrum. According to NTIA officials, mid-high band spectrum could potentially be used for 5G purposes, but most 5G efforts have focused on low-, mid-, and high-band spectrum.

[10] This designation corresponds to their wavelength on the order of a millimeter. Wavelength is the length of the electromagnetic wave or the distance travelled in one cycle. It decreases as frequency increases. According to FCC officials, the agency chose 24 GHz as the lower boundary for millimeter-wave frequencies in its “Spectrum Frontiers” proceeding for practical reasons; see Use of Spectrum Bands Above 24 GHz for Mobile Radio Services, 81 Fed. Reg. 58,270 (proposed Aug. 24, 2016).

Figure 3: **Forecast of total worldwide mobile data usage**



Source: GAO analysis of Ericsson data. | GAO-21-26SP

Data table for Figure 3: Forecast of total world wide mobile data usage

Year	Data uploaded and downloaded (billions of gigabytes per month)
2011	0.234
2012	0.61
2013	1.446
2014	2.568
2015	4.379
2016	6.917
2017	10.603
2018	21.714
2019	33.038
2020	46.134
2021	61.245
2022	80.285
2023	103.388
2024	130.501
2025	164.399

1.3 Roles and responsibilities in the development of 5G

Various entities and agencies have responsibilities for developing 5G networks, including network deployment, spectrum management, health and safety, research and development (R&D), and technical specifications.

5G network deployment. The companies that own and operate mobile wireless networks—known as carriers—are in the process of deploying 5G wireless networks. The U.S. has three major wireless carriers that together command more than 90 percent of the market: AT&T, T-Mobile, and Verizon Communications. The five leading global firms offering equipment for 5G are Huawei, Nokia, Ericsson, Samsung, and ZTE.

Spectrum management. In the U.S., responsibility for managing spectrum—including allocating, assigning, regulating, and facilitating the sharing of spectrum for 5G—is divided between two agencies: the National Telecommunications and Information Administration (NTIA) within the Department of Commerce for federal government use, and the FCC for commercial and other nonfederal use, including cellular communications. NTIA is responsible for allocating spectrum for federal use, while the FCC is responsible for allocating and licensing spectrum for consumer, commercial, state, and local government purposes and for making unlicensed spectrum available for shared use by devices. Licensing assigns specific rights to specific frequency bands in a specific area and—generally speaking—to a specific entity, such as a wireless carrier.[11] In addition, the FCC and NTIA coordinate federal and non-federal use of shared spectrum pursuant to a memorandum of understanding between the agencies.

Health and safety. The FCC is also responsible for regulating the health and safety of RF exposure, including setting exposure limits for cellular communications. The *National Environmental Policy Act of 1969* requires the FCC to evaluate the effects of its actions on the quality of the human environment, including human exposure to RF energy emitted by FCC-regulated transmitters, devices, and facilities, such as those related to 5G.[12] The FCC sets standards intended to limit human exposure with technical input and collaboration from the Food and Drug Administration (FDA), Environmental Protection Agency, and other federal health and safety agencies. The National Institutes of Health conducts research on the potential health effects of RF exposure.

Research and development. Agencies including the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), NTIA, and the Departments of Defense (DOD), Energy, and Homeland Security (DHS) fund or conduct R&D for 5G and future mobile wireless technologies.[13] These agencies are to coordinate R&D priorities and investments through the Networking and Information Technology Research and Development (NITRD) program, a multiagency program that operates under the aegis of the White House Office of Science and Technology Policy. NITRD seeks to provide the R&D foundations for ensuring continued U.S. technological leadership, including accelerating development and deployment of advanced information technologies. Through the use of interagency working groups, NITRD coordinates federally funded R&D for advanced networking and information technology capabilities, such as 5G, as well as their transition to practical use.

Development of specifications and standards. Federal agencies—including the FCC, NIST, NTIA, DOD, DHS, and the Department of State—participate in the development of 5G technical specifications and standards through forums such as the International Telecommunication Union (ITU), a specialized agency of the United Nations that coordinates the standardization of international communications networks, and the Third Generation Partnership Project (3GPP), the international organization responsible for the development of technical specifications.[14] Technical specifications—

[11] The FCC generally does not mandate that spectrum licensees or commercial mobile radio service operators adopt a particular technology, according to FCC officials. The FCC takes a flexible-use, market-based approach, in which operators determine the best use of their spectrum licenses within FCC regulations that are designed to minimize the potential for harmful interference.

[12] Pub. L. No. 91-190, 83 Stat. 852 (1970), codified as amended at 42 U.S.C. §§ 4321–4347.

[13] DHS is also the sector-specific lead agency for the communications sector and, as such, has certain responsibilities to protect U.S. communications infrastructure from physical and cyber risks. See Presidential Policy Directive/PPD-21, Critical Infrastructure Security and Resilience (Feb. 12, 2013).

[14] Many other organizations are involved in developing specifications for 5G-related technologies. For example, the IEEE sponsors specification development activities that are directly related to the applications that will support the high-bandwidth, low-latency, and low-power requirements of 5G (and beyond) applications such as connected vehicles, massive Internet of Things, and industrial automation.

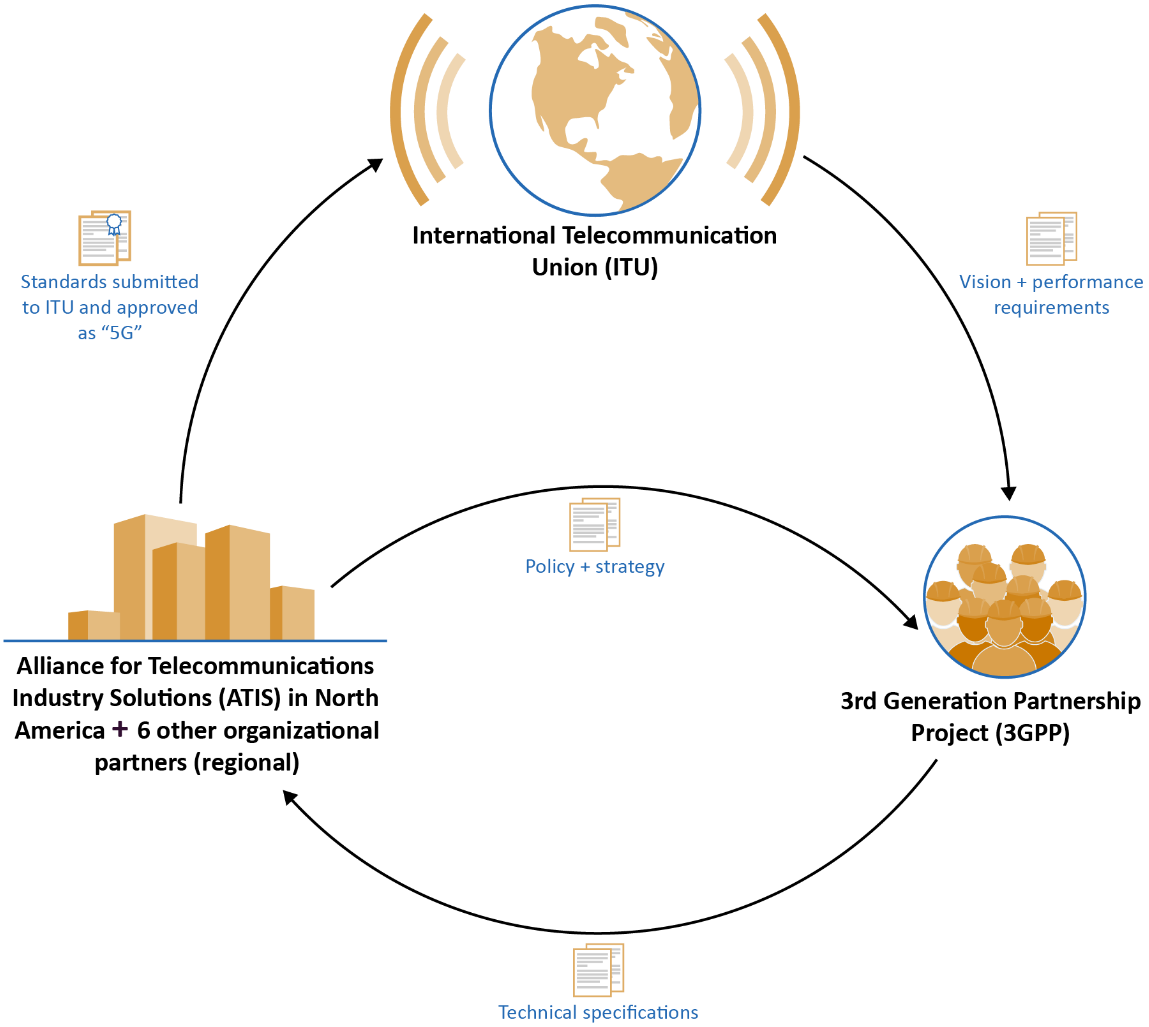
documented technical requirements that define a technology or set of technologies—are critical to developing and deploying 5G. A specification details the technical design, development, and procedures for developers and other stakeholders. In the context of 5G networks, technical specifications define how technologies enable network performance and network security protocols, and ensure interoperability among different aspects of the networks.[15] Standards are specifications that have been made official. ITU establishes its vision for each generation of mobile wireless communications, including the associated performance requirements, and 5G is 3GPP's specification that is responsive to this vision.[16]

3GPP comprises seven regional or national member organizations that represent industry interests, including the Alliance for Telecommunications Industry Solutions, the regional organization representing North America. These regional organizations are responsible for devising the policies and strategy under which 3GPP operates. In developing the technical specifications, 3GPP brings together more than 500 members from more than 40 countries, including from such diverse interests as mobile carriers, manufacturers, academics, and government agencies. Once 3GPP develops the technical specifications, the regional bodies transpose them into standards and submit them to ITU for approval as meeting the performance requirements of 5G. Figure 4 shows how these and other organizations are collaborating in the development and approval of 5G specifications.

[15] We use the term specifications to refer to both specifications and standards because the distinction is generally not necessary for understanding the issues in this report.

[16] ITU supports many activities, including development of technical specifications, and also more formally in its role to allocate global RF spectrum through a treaty-level process.

Figure 4: International bodies responsible for the development of 5G specifications


International Telecommunication Union (ITU)
Vision + performance requirements
3rd Generation Partnership Project (3GPP)
Technical specifications
Alliance for Telecommunications Industry Solutions (ATIS) in North America + 6 other organizational partners (regional)
Policy + strategy
Standards submitted to ITU and approved as "5G"

Source: GAO analysis of 3GPP, ATIS, ITU, and Qualcomm documentation. | GAO-21-26SP

2 Performance goals and use cases for 5G are expected to be realized over the next decade

5G network performance is expected to far exceed that of 4G/LTE as the technology develops over the next decade. 5G networks are expected to enable significantly higher data rates, massive increases in the number of connected devices, faster network response, and greater reliability, among other advancements. This improved network performance is expected to enhance many existing mobile broadband applications and also enable transformative new applications across industries and society.

Deployment of the necessary infrastructure has begun, although performance improvements will be achieved gradually, as network technologies incrementally evolve throughout the 2020s. Many of these technologies need further development, some of which is underway at federal and private research facilities known as test beds, and involve international partnerships that continue to develop technical specifications.

2.1 Network performance is expected to improve

5G networks are expected to provide far better performance than previous generations of wireless networks across many measures. ITU, as the United Nations agency that establishes a vision for each generation of mobile wireless communications, establishes key measures for performance that other standards setting bodies and carriers develop their vision and goals upon.[17] ITU lays out the following eight key performance measures for 5G:[18]

1. **Peak data rate.** The maximum achievable data rate under ideal conditions, usually measured in gigabits per second (Gbps).
2. **User-experienced data rate.** The data rate that is broadly available to a mobile device, measured in megabits per second (Mbps) to Gbps.
3. **Latency.** The time it takes from when the source sends a packet of data to when the destination receives it, usually measured in milliseconds. More precisely, latency for 5G is the contribution by the radio network to this time.[19] Low latency is especially important for applications, such as industrial automation or remote medicine, where delays in data transfers could be disastrous.
4. **Mobility.** The maximum speed a device can be traveling and still experience a defined quality of service. Mobility is important for applications that require

[17] Other standard settings organizations and wireless carriers have built out additional performance measures and goals to augment the ITU vision and adapt to the evolving needs of 5G. According to one carrier we spoke with, the ITU goals are important and operators look to those and additional measures, but these goals are often aspirational and may represent the peak performance that can be achieved under ideal conditions.

[18] ITU, *IMT Vision—Framework and overall objectives of the future deployment of IMT for 2020 and beyond*, Recommendation ITU-R M.2083-0 (September 2015).

[19] Latency is limited by the speed of light propagating either in air or in optical fiber and the processing time in the network.

reliable connection when moving, such as in transportation safety.

5. **Connection density.** The total number of connected and/or accessible devices that can be accommodated, measured in devices per unit area. Increased connection density will support customer use where there are a tremendous number of devices, such as in stadiums and warehouses.

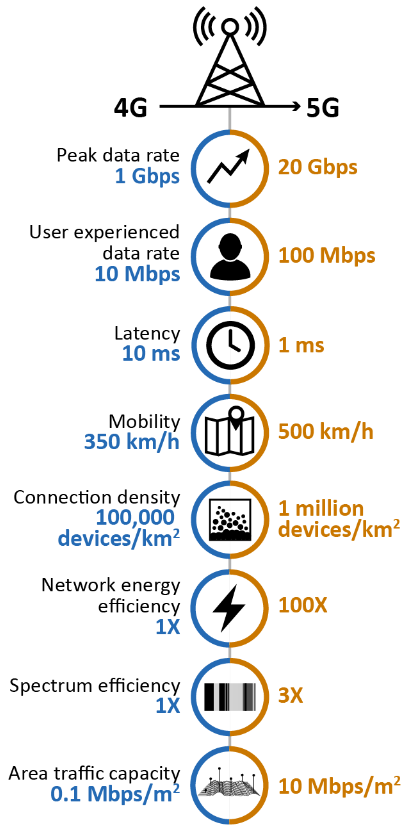
6. **Energy efficiency.** On the device side, the number of bits transmitted or received per unit of energy consumption. On the network side, energy efficiency refers to the quantity of information bits transmitted to or received from users, per unit of energy consumption of the radio access network (RAN), measured in bits per joule. Energy efficiency improvements are critical due to the expected massive increase in data use over time.

7. **Spectrum efficiency.** The amount of information transmitted within a given amount of spectrum, measured in bits per second per hertz. Spectrum efficiency is important because spectrum is a scarce and limited resource.

8. **Area traffic capacity.** The total traffic throughput served per geographic area, measured as data rate per unit area. Area traffic capacity increases will enable better network performance in densely populated areas.

Figure 5 depicts how 5G is expected to perform compared to 4G/LTE across these eight performance measures. Both 5G and 4G/LTE networks continue to evolve toward these goals, as we discuss later in this chapter.

Figure 5: 5G performance goals compared to 4G/LTE across key measures



Source: GAO analysis of International Telecommunication Union documentation. | GAO-21-26SP

Note: Gigabits per second (Gbps) and Megabits per second (Mbps) are measures of the rate at which data is transmitted, milliseconds (ms) is a measure of time equal to one thousandth of a second, and square meter (m^2) and square kilometer (km^2) are measures of area.

In addition to these eight measures, the ITU identifies several other performance measures that aim to make 5G more flexible, reliable, and secure:[20]

- **Spectrum and bandwidth flexibility.** The flexibility of the network design to handle

[20] ITU, *IMT Vision*.

different scenarios, such as the capability to operate at different frequency ranges.

- **Reliability.** The capability to provide a given service with a very high level of availability. Reliability is compromised if too much data are lost, late, or have errors. Improving the reliability of the network is critical for time-sensitive, mission-critical applications like automation and healthcare.
- **Resilience.** The ability of the network to continue operating correctly during and after a natural or man-made disturbance, such as the loss of power.
- **Security and privacy.** The ability to encrypt and protect user data and signaling, and enhance network security against cyberattacks, such as unauthorized user tracking, hacking, fraud, sabotaging, and denial of service, which can be detrimental to national security and the safeguarding and privacy of users' data.
- **Operational lifetime.** Operation time per stored energy capacity, which is particularly important for Internet of Things (IoT) devices requiring a very long battery life whose regular maintenance is difficult for physical or economic reasons.[21]

2.2 5G supports enhanced mobile broadband and may enable new applications across industries

5G network performance improvements are expected to enable new kinds of applications that are to significantly improve mobile broadband experiences, enable communication among a massive number of devices, and introduce faster and more reliable communications between devices, among other things. Together, these improvements will help to enable applications such as 3D video, augmented or virtual reality, smart cities, and automated vehicles.[22] These types of end-user applications will be enabled by improvements in three use case categories—enhanced mobile broadband, ultra-reliable and low-latency communications, and massive machine-type communications.[23]

Enhanced mobile broadband addresses the human-centric use cases for access to multi-media content, services, and data, primarily through faster connections, higher data throughput, and greater capacity compared to previous wireless generations. The throughput improvements should significantly change the user experience with hand-held devices, virtual reality, and video streaming,

[21] IoT refers to the technologies and devices that sense information and communicate it to the internet or other networks and, in some cases, act on that information. These *smart* devices are increasingly being used to communicate and process new quantities and types of information and respond automatically to improve industrial processes, public services, and the well-being of individual consumers. For example, a fitness tracker can monitor a user's vital statistics, store the information in the cloud, and present insights on a smartphone. See GAO*, Internet of Things: Status and Implications of an Increasingly Connected World*, GAO-17-75 (Washington, D.C.: May 15, 2017).

[22] Smart cities may use sensors, cameras, and other technologies to improve city operations and management. For example, these technologies may be used to improve traffic flow, public safety, and energy efficiency. Automated vehicles are those in which at least some aspect of a safety-critical control function, such as steering, throttle, or braking, occurs without direct driver input. Automated vehicles may improve driving safety, energy consumption, environmental sustainability, and land use.

[23] These use case categories are commonly known as eMBB, URLLC, and mMTC, respectively.

which will account for around three-quarters of mobile data traffic by 2025, according to industry estimates.[24] It is also expected to enable new applications, such as 3D video streaming and extended reality.[25] According to a 5G Americas white paper on 5G services innovation, extended reality applications are expected to impact a wide range of industries, including healthcare, education, military, emergency response, and industrial manufacturing, among others.[26] For example, extended reality applications have been developed to help fighter pilots fly better in poor visibility or darkness.

Enhanced mobile broadband will help enable applications that require high data rates and a seamless user experience, but performance requirements will vary across applications. For example, wide-area coverage applications, such as connected vehicles, require performance improvements over 4G/LTE in coverage and mobility. In contrast, high density applications will be used in areas, such as arenas or dense urban areas that requires less coverage and mobility, but greater connection density and higher throughput. Similar performance requirements to high density applications will also be needed for fixed wireless access, which provides a cost effective opportunity to provide broadband wireless for homes and businesses use in rural and underserved areas because it eliminates the need for costly deployment of deep-fiber fixed access infrastructure to homes.[27] This could help close the wireless access gap between geographic and socioeconomic groups, known as the digital divide, a subject on which we previously reported.[28]

Ultra reliable and low-latency communications has stringent requirements for capabilities, such as throughput, latency, and availability. This use case category requires time-sensitive, ultra-reliable connections to support applications where network failure could lead to disastrous consequences, such as mission-critical applications like communications for first responders or remote medicine, ranging from sharing video for diagnostic purposes to controlling an insulin pump or performing robotic surgery. This use case can also enhance novel industrial applications, such as factory automation using advanced robots to increase efficiency and worker safety. In addition to low-latency and high reliability, some applications will also require high mobility, as in the case of connected vehicles.

Massive machine type communications is characterized by a very large number of connected devices typically transmitting a relatively low volume of delay non-sensitive data. This use case category will enable a large, spatially dense number of devices to be connected. This density is especially

[24] Ericsson, *Ericsson Mobility Report* (Stockholm, Sweden: June 2020). Cisco, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022* (February 2019).

[25] Extended reality is an umbrella term for different types of digital realities, including virtual reality, augmented reality, and mixed reality. Virtual reality is a fully immersive digital reality experienced through a headset, while augmented and mixed reality create interactive, digital realities layered on real world experiences.

[26] 5G Americas, *5G Services Innovation White Paper* (November 2019).

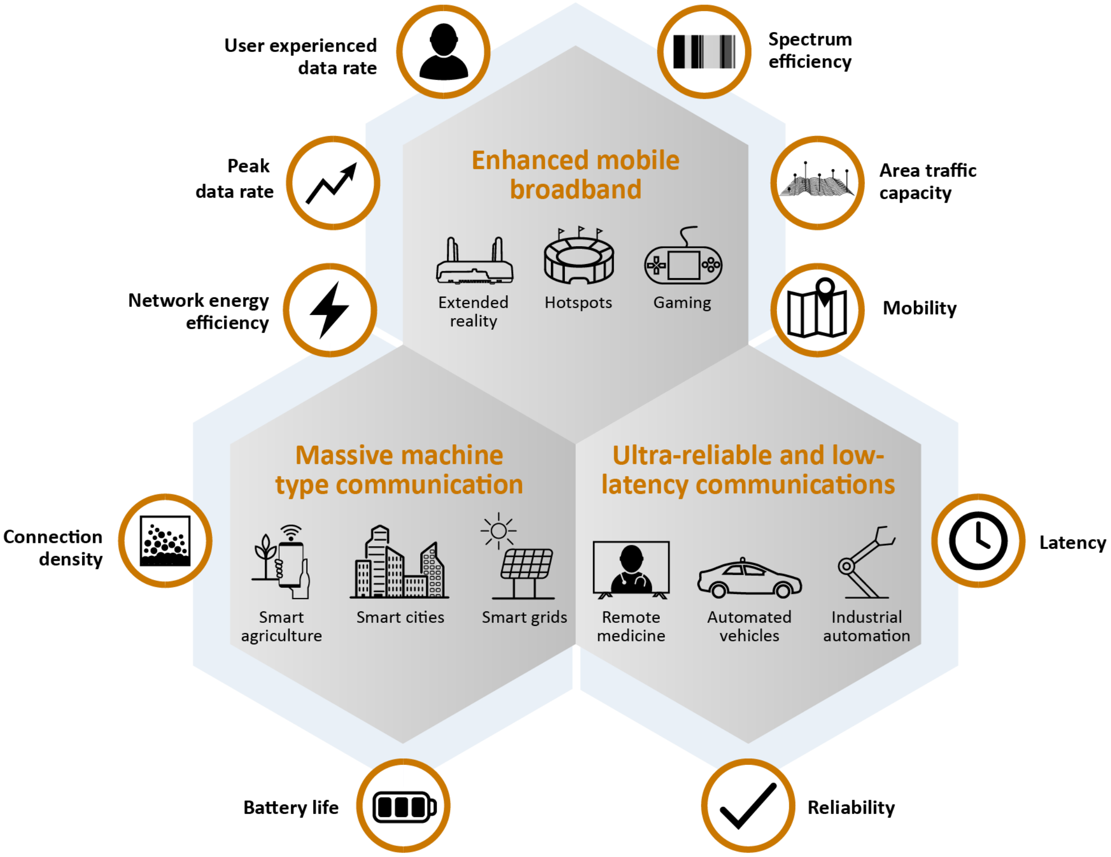
[27] The *Ericsson Mobility Report* estimates that fixed wireless will account for 25 percent of total mobile network data traffic globally by 2025.

[28] GAO-20-468, 14–17.

important in enabling IoT applications like smart phones, cameras and sensors, which can help enable applications across a wide spectrum of government and industrial uses. For example, energy and utility management may employ smart grids, which include smart meters, sensors, monitoring, and data management systems. These will be enhanced by 5G and are expected to contribute to economic growth and environmental gains. These technologies can also be used to enable smart logistics, smart cities, and smart agriculture to realize similar economic and environmental benefits.[29] Applications in this use case category require high connection density, energy efficiency, and long operational lifetime; however, they do not require high data rates or mobility.

Figure 6 shows how select applications align with use case categories and the improvements in performance measures that enable them.

Figure 6: Applications of 5G



Source: GAO. | GAO-21-26SP

[29] Smart logistics use data to optimize traffic and logistics management systems to improve the flow of vehicles and goods. Smart agriculture is the use of IoT and other technologies to more effectively produce food, such as through improving crop yields and saving natural resources.

2.3 Deployment has begun with a focus on enhanced mobile broadband

U.S. wireless carriers began deploying 5G infrastructure and services in late 2018, with a focus on enhanced mobile broadband. Carriers are initially pursuing different deployment strategies based on the spectrum assets they have licensed from the FCC. For example, some carriers are deploying 5G broadly and are focused on improving service using low-band spectrum. Low-band spectrum typically has relatively low data capacity but can travel over longer distances and through physical barriers better than higher bands, resulting in better coverage but lower speeds. Other carriers are focused on enabling services that require higher data rates with high-band spectrum, such as in dense urban environments. As of August 2020, two carriers had announced nationwide 5G coverage. However, most customers will likely not experience significant improvements over 4G/LTE in coverage and performance immediately.

In order to enable the rapid introduction of some 5G capabilities, 5G components have been designed to work with existing 4G/LTE components or even independent of carrier-managed networks. According to a carrier representative, recent 4G/LTE hardware can support 5G with either a software upgrade or a minor hardware upgrade at the base station. Some solutions enable a dynamic allocation of radio resources between 4G/LTE and 5G New Radio and are able to transition in as little as a few milliseconds to adapt to changes in users' needs. In addition to deployments by carriers, organizations can use private networks, independent of carrier-managed networks, to ensure they have the most control over the performance and security over their networks and are not dependent on the pace of carrier deployment of 5G technologies. According to Deloitte, private 5G may become the preferred wireless choice for many of the world's largest businesses, particularly for manufacturing plants, logistics centers, and ports, as private 5G will allow them to better customize the networks for their particular needs.[30] In July 2020, Nokia announced the rollout of new 5G wireless networks for industrial clients and an order to build a private 5G wireless network for a mining technology firm.

2.4 Additional technology development is needed to meet the requirements of all 5G use cases

Some of the technologies necessary to deliver on the full potential of 5G are not yet fully developed. Two technologies in particular—high-band technology and end-to-end network slicing—are important for network performance, but subject to further development, as detailed here. High band provides more bandwidth for greater capacity, while end-to-end network slicing dedicates network resources to better meet the needs of particular customers or applications.

5G is also building on or making greater use of several technologies already present in 4G/LTE. One such technology is active

[30] Deloitte Insights, "Private 5G Networks: Enterprise Untethered," in *Technology, Media, and Telecommunications Predictions 2020* (Deloitte Development LLC, December 2019), 30–45.

antennas, which consist of many individual antenna elements and can electronically steer radio signals to reduce interference, allowing more devices to share a given frequency band. Active antennas allow beamforming, in which signals are focused into beams and steered to serve customers. A related technology that 5G is to improve is Multiple Input Multiple Output (MIMO) architecture—the use of multiple signals from as many as hundreds of antenna elements. 5G MIMO offers improvements in spectrum efficiency over 4G/LTE MIMO. Further, while existing MIMO is optimized to provide a few users with optimal throughput for enhanced mobile broadband, 5G MIMO may eventually be optimized to alternatively provide low-data rate connectivity to a large number of users for massive machine type communications.

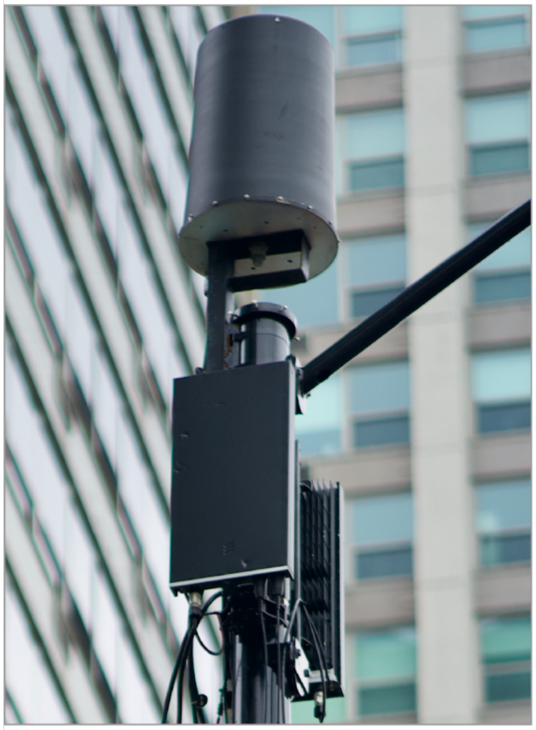
2.4.1 High-band technology

5G introduces high-band technology: antennas, radios, and modems that are designed to send and receive high-band signals to mobile wireless networks. High-band frequencies are on the order of 10 times higher than those frequencies used by 4G/LTE. The use of high-band technology has historically focused on the aerospace sector, including satellite communications, remote sensing, and radar systems.

High band provides wider bandwidth in the large amount of available spectrum, which is particularly important for enhanced mobile broadband applications that require extremely high data rates. Of the nearly 6 GHz the FCC has made available for licensed use for commercial mobile wireless services, nearly 5 GHz is at high-band frequencies. This high-band spectrum may offer capacity for carriers to support growing demand.

High-band technology is generally limited by a shorter effective range than lower bands and thus requires a higher density of infrastructure. As we previously reported, high-band small cells may be limited to high-density areas.[31] Densely deployed small cells can boost network capacity without the need for additional spectrum. Figure 7 shows an example of a 5G small cell with two high-band antennas facing away from each other.

Figure 7: 5G high-band small cell



Source: GAO. | GAO-21-26SP

[31] GAO-20-468, 18.

High-band technology is relatively underdeveloped, according to IEEE, with challenges including cost, energy efficiency, and complexity of high-band infrastructure and devices.[32] For example, techniques are needed to optimize beamforming and MIMO to provide the mix of coverage, throughput, reliability, and energy efficiency demanded by a variety of applications. Energy efficiency will also be a challenge for high-band infrastructure generally. According to IEEE, the telecommunications industry is already concerned about power consumption in low-band and mid-band infrastructure, and how it will be difficult to achieve even these current levels of efficiency using high-band technology. NSF has funded a city-scale advanced wireless test bed to overcome challenges particular to MIMO implementation (see next section).

Another challenge to deploying enhanced mobile broadband services is understanding how high-band signals travel through their environment; that is, how they propagate. Propagation modeling—which helps carriers plan what infrastructure is needed to provide desired coverage levels—is less mature for high-band technology, which may impact carriers' planning for coverage and spectrum use. According to an FCC official, industry does not have much experience studying issues of propagation at high-band frequencies—how signals reflect off of buildings, for example—when planning a network deployment. NIST is one federal entity working to address this research gap, in part through an international consortium that studies high-band signal propagation. NTIA is another federal agency working to address this research gap. According to NTIA officials, its Institute for Telecommunication Sciences is developing a millimeter-wave measurement capability that includes propagation, spectrum, and noise measurements.

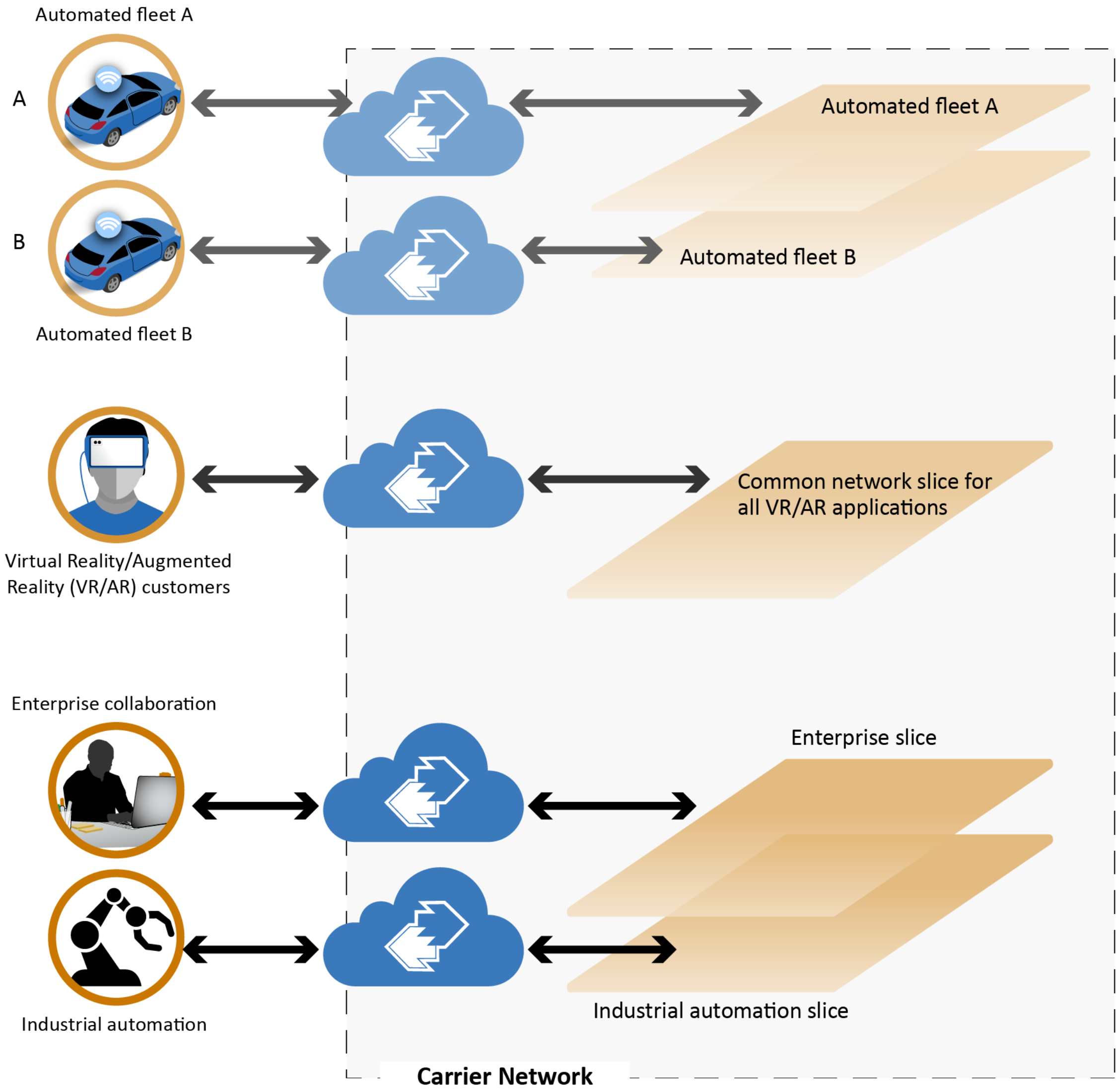
2.4.2 End-to-end network slicing

End-to-end network slicing allows 5G carriers to provide different levels of service and performance for specific customers or applications over the same network. Carriers can split the resources of physical network infrastructure into independent *logical* networks, or *network slices*, which run on shared infrastructure. 5G can slice across every part of the network, from customer devices through applications, thus enabling *end-to-end network slicing*. This technology may be particularly important for applications beyond enhanced mobile broadband—namely, for ultra-reliable and low-latency communications and for massive machine type communications.[33] For example, a carrier can simultaneously provide isolated networks for different fleets of vehicles, optimization for virtual reality applications, high data rate for videoconferencing, high reliability and low latency for automating industrial machines, and basic voice or internet access using the same underlying network infrastructure (see fig. 8).

[32] IEEE Future Networks Initiative, *International Network Generations Roadmap*, 1st ed. (2019).

[33] See, for example, FCC Technological Advisory Council 5G IoT Working Group, *5G Network Slicing Whitepaper* (March 2019).

Figure 8: Diverse set of applications offered through network slicing



Source: GAO, based on Federal Communications Commission and Ericsson documentation. | GAO-21-26SP

End-to-end network slicing is enabled by virtualization—the use of software instead of hardware to manage configurable network resources. Instead of designing or configuring a piece of hardware—a server, for example—to operate the same way for all users, virtualization allows network components to be configured to meet the needs of different users. In virtualized networks, the functions previously confined to dedicated systems now run as software code on generic hardware.

Cloud computing provides the virtualized platform for end-to-end network slicing across the radio access network and core network.[34] 5G continues a trend from hardware-centric to software-defined, virtualized architectures, and from centralized, dedicated hardware to distributed, generic systems. Network functions can run in cloud infrastructure across multiple, geographically distributed locations, which allows the network to provide connectivity and services simultaneously to more users without overloading. Generic hardware can be located remotely and allocated on demand (i.e., “in the cloud”). A distributed cloud computing architecture locates some resources close to the user, at the network *edge*.[35] Cloud computing resources located at the edge can meet more diverse demands, such as low latency, as well as better serve the needs of the radio access network. This architecture allows for more flexible use of the network in 5G, which is needed to provide different services while potentially serving billions of devices. Additionally, efforts are underway to optimize the energy efficiency of the cloud computing resources used by cellular networks.[36]

However, end-to-end network slicing requires 5G *standalone* networks. Standalone networks comprise a 5G radio access network atop a 5G core network; in contrast, current hybrid—or non-standalone—networks use a 4G core network. Standalone networks introduce greater security and functionality, including enabling applications beyond enhanced mobile broadband that use end-to-end network slicing. While carriers have begun to deploy 5G core networks, the timeline for the full rollout of U.S. standalone 5G networks is uncertain. In addition, more R&D is needed to improve and optimize the performance of distributed cloud computing architectures. NSF officials identified achieving low-latency as a particular challenge, and the agency continues to fund early-stage R&D in this area. IEEE predicts that networks with latency of 1 to 2 milliseconds will be achieved in the latter half of the 5G development timeline—that is, between 2024 and 2029.

2.5 Development of 5G technologies and applications uses 5G test beds

Test beds are research facilities that enable testing theories, tools, and technologies that are relevant to 5G in more real-world settings. Test beds are critical for development and testing of the new network technologies in 5G, as well as the applications that the networks will enable, and many such test beds—federally funded and private—are in operation already. Federally funded test beds are pursuing R&D into applications of 5G and future wireless networks. Private test beds are similarly pursuing 5G technology and applications.

[34] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[35] One example of a standard for distributed cloud computing is multi-access edge computing. This is a dynamic, on-demand architecture that provides the hardware resources that meet the application’s requirements and responds to changes in traffic.

[36] The IEEE Green ICT (Information and Communications Technology) Standards Committee published its first standard in 2020 and has eight additional standards in development.

Test beds help facilitate experimentation outside of a laboratory in a real-world setting, as many parameters cannot be simulated in a laboratory, according to an NSF official. The following examples illustrate factors needing real-world testing for 5G network technologies:

- The amount of RF noise in the live environment is highly variable; while it can be approximated, it cannot be replicated in a laboratory setting, according to an NSF official.
- The virtualization of communications infrastructure increases the need for testing and verification, according to an NSF official.
- The development and verification of 5G security requires test beds to emulate the attack environment, according to IEEE.

DOD, the Department of Energy, the Department of Commerce's NTIA, and NSF all operate federal 5G test beds.[37] DOD test beds are exploring 5G for military uses, working on methods to improve 5G security, and evaluating spectrum-sharing techniques. At test beds at 12 U.S. bases, DOD is experimenting with applying 5G to logistics and asset management, augmented combat training, warehouse management, and bidirectional spectrum sharing between 5G and DOD systems. These test beds evaluate techniques and prototypes to improve the security of 5G for adversarial environments, including dynamic spectrum utilization and zero-trust architecture.[38] Idaho National Laboratory, one of the Department of Energy's National Laboratories, operates a Wireless Test Range, Wireless Security Institute, and a Spectrum Innovation Department. These facilities are funded by the Departments of Defense, Energy, Homeland Security, and Justice to study system security, spectrum sharing, software defined and virtual networking, and radio access networks. For example, the Idaho National Laboratory is evaluating the security vulnerabilities of 5G devices, developing jam-resistant and spectrum-sharing devices, and building a capability to monitor spectrum and identify its users. NTIA has granted the laboratory's Wireless Test Range an experimental station authorization to locally manage its use of spectrum for government testing purposes. According to Department of Energy officials, INL currently operates three 5G systems across an 890 square mile range. In addition, the NTIA Institute for Telecommunication Sciences develops spectrum-sharing models, publishes propagation modeling tools, and operates a 5G test bed that focuses on open radio access networks and virtualization and open source implementations, according to NTIA officials.

In addition to test beds operated by the Departments of Defense, Energy, and Commerce, NSF is funding three test beds in diverse environments to study 5G and other advanced wireless technologies under real-

[37] The NITRD Wireless Spectrum Research and Development Interagency Working Group maintains a public inventory of test beds, all of which officials anticipate will incorporate 5G capabilities.

[38] Zero-trust architecture treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized; see NIST, *Zero Trust Architecture*, Special Publication 800-207 (Gaithersburg, Md.: August 2020).

world conditions.[39] The test beds are designed to accelerate development and commercialization of promising technologies, ensure continued U.S. leadership in wireless communications, and prepare the U.S. workforce for new job opportunities. The test beds are studying and demonstrating a broad set of technologies that span wireless devices, communication techniques, networks, systems, and services. The following describes the three NSF test beds:

- In New York City, the Cloud Enhanced Open Software-Defined Mobile Wireless test bed focuses on testing high-bandwidth and low-latency 5G communications with distributed cloud computing. The test bed has begun to deploy a macro cell and small cells that experiment with fixed and mobile wireless technologies across one tenth of a square mile in Manhattan. FCC licensed the test bed to operate in mid-band spectrum, and the test bed supports licensed and unlicensed use and experimentation across low-, mid-, and high-band spectrum. According to FCC officials, a request is pending at the FCC to augment the geographic zone of experimentation in New York City.
- In Salt Lake City, the Platform for Open Wireless Data-driven Experimental Research test bed is developing protocols or technologies for 5G and future wireless networks. The test bed focuses on improving components of 5G—such as dynamic spectrum sharing, MIMO, and distributed cloud computing—for applications beyond enhanced mobile broadband. The project has deployed fully-programmable radios attached to a user-configurable network across about four contiguous square miles. The FCC licensed this test bed to operate mobile wireless technologies using about 2.5 GHz of low- and mid-band spectrum.
- In North Carolina, the Aerial Experimentation and Research Platform for Advanced Wireless test bed focuses on the integration of unmanned systems into the national airspace and enables advanced wireless features for unmanned aircraft systems operating in low- and mid-band spectrum. According to FCC officials, a request is pending at the FCC to add to the research conducted at this facility by modifying the license to approve experimentation similar to that conducted in New York City and Salt Lake City mentioned above.

Private test beds are also being used to develop and test new 5G technologies and applications. For example, Verizon Communications has partnered with the University of Michigan on a test bed for automated vehicles. In another case, AT&T and Samsung partnered to create a manufacturing-focused 5G test bed in Austin, Texas, with the goal of providing a real-world understanding of how 5G can impact manufacturing and provide insight into the future of a smart factory. Similarly, Verizon Communications and Corning Inc. have partnered on a factory test bed in Hickory, North Carolina, to test connected vehicles

[39] The NSF Platforms for Advanced Wireless Research program is collaborating with 30 private-sector companies, including AT&T, Ericsson, Nokia Bell Labs, Qualcomm, Samsung, T-Mobile, and Verizon Communications.

(e.g., robotic forklifts), wireless inventory tracking, and video surveillance for preventative maintenance.

2.6 5G technology development requires additional technical specifications

The ongoing development of 5G technologies requires the continued development of 5G specifications by 3GPP. The 3GPP specifications define the end-to-end system, including the radio access network and the core network, and define the parameters for interoperable 5G network technologies, ensuring that technologies from one vendor can work seamlessly with those from another. The specifications are important for an open and competitive market for the technologies offered by different vendors.

Compliance with 3GPP specifications is not mandatory and is not governed or enforced by any independent entity. In general, wireless carriers require that technology vendors adhere to the 3GPP specifications as part of their equipment purchase agreements. The specifications ensure interoperability between different network components, so equipment that does not adhere to the specifications may not function within the network. However, some specifications, such as many related to cybersecurity, are optional and may not be implemented if the carrier does not require or enable them or appropriately configure them.

Work on 5G specifications began in 2016. 3GPP, the international partnership project that develops specifications, split this development into a series of separate *releases*, each introducing new, and revising existing, technical specifications. Based on past releases and projected schedules, the work on a specification release typically takes about 18 months—starting with steps to define the content and ending with the completion of a technical specification release. Given these timeframes, 3GPP staggered the initial three releases for 5G and carried out work on more than one release at the same time.

Two of the releases of 5G specifications are now complete, with the next expected in late 2021. Several 5G network capabilities will likely not be enabled until 2022 or later because deployment lags the release of specifications.[40] Stakeholders suggested that it is appropriate to think about the 3GPP specifications and the commercialization of technologies as a continuous evolution. Aspects of the 5G goals that are ultimately unmet in the 2020s will likely remain objectives for mobile wireless systems beyond 5G.

[40] Technology commercialization generally takes 1 to 2 years after the completion of a specification release, according to an equipment vendor we interviewed. The length of the process may vary depending on factors such as technological complexity and importance to stakeholders, according to FCC officials.

The following provides details of the first three releases of 5G specifications:[41]

- Release 15 was completed—or frozen—in June 2019 and included specifications for 5G New Radio with non-standalone network architecture.[42] This release included specifications to enable enhanced mobile broadband and specifications for technologies necessary for massive machine-type communications and network slicing. It also began defining technologies to enable the first aspects of standalone 5G networks. This initial set of specifications was important for component suppliers to begin design and implementation of some 5G network components, including chipsets.
- Release 16 was completed in July 2020 and, according to 3GPP, marked the completion of the full vision of 5G networks. It included specifications for technologies related to ultra-reliable and low-latency communications, Industrial IoT, use of unlicensed spectrum, private networks, and improvements to network efficiency. The release met the ITU's technical performance requirements of 5G networks and, if approved by the ITU, as planned, in November 2020, will define the specifications for 5G networks.[43]
- Release 17 is scheduled for completion in late 2021.[44] It focuses on a series of 5G network enhancements, including additional specifications related to network slicing, distributed cloud computing, and dynamic spectrum sharing.

Figure 9 gives a general timeline of the key 5G specifications in 3GPP releases 15, 16, and 17.

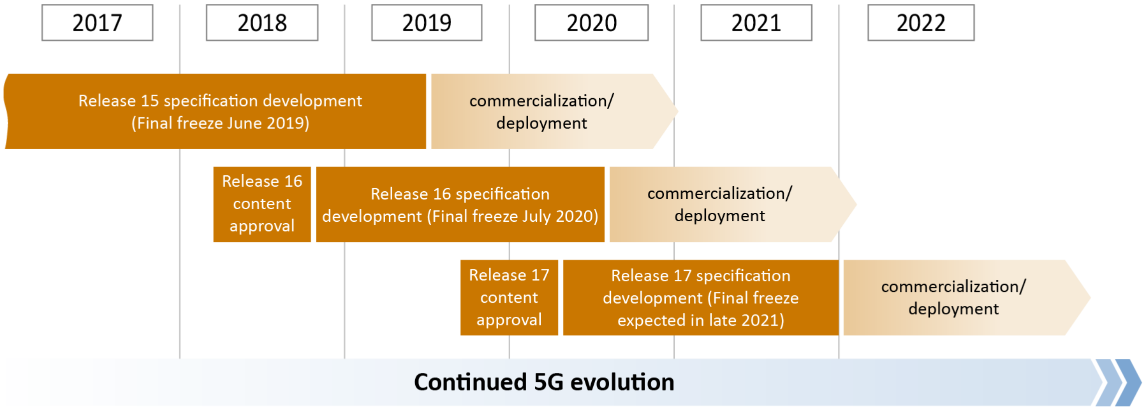
[41] 3GPP releases 13 and 14 included some specifications related to 5G networks, but release 15 is considered the first specification set focused on 5G network development. In addition to specifying aspects of 5G, releases 15 and 16 also continued to update 4G/LTE network requirements. Prior 3GPP releases defined specifications for the earlier, third generation of wireless networks.

[42] Each specification set is completed over a period of about 18 months. The process begins with a step to define content, followed by the development of the specifications, and ending with the completion—or freeze—of the specifications. As specifications are developed, they are frozen in phases (known as early drop, main drop, and late drop) as the specifications are finalized. When a specification set is frozen, only essential corrections are allowed, but introduction of additional functions, or modification to existing functions, is forbidden.

[43] ITU does not use the term 5G, but refers to 5G as "IMT [international mobile telecommunications] for 2020 and beyond."

[44] In September 2020, 3GPP stated that a delay in the release 17 schedule will be necessary, but it will not make a firm decision on the freeze date until December 2020.

Figure 9: General timeline of 3rd Generation Partnership Project specification development


2017
2018
2019
2020
2021
2022
Release 15 specification development (Final freeze June 2019)
commercialization/ deployment
Release 16 content approval
Release 16 specification development (Final freeze July 2020)
commercialization/ deployment
Release 17 content approval
Release 17 specification development (Final freeze expected in late 2021)
commercialization/ deployment
Continued 5G evolution

Source: GAO analysis of Nokia, Qualcomm, and 3rd Generation Partnership Project documentation. | GAO-21-26SP

Note: When a specification set is approved, or frozen, only essential corrections are allowed.

According to two industry representatives that we spoke to and reports discussing the development of 5G networks, it is important that the U.S. government and its domestic 5G vendors remain active in the specification development process. Specification development at 3GPP will continue beyond release 17, adding specifications for technologies to enable more advanced network performance and applications beyond those that define existing or planned 5G networks. The specification development process, according to two industry representatives, is meant to be open, transparent, and meritocratic. Under this process, the technology best suited to address a specific technological challenge generally becomes part of the specification set. However, industry representatives and reports discussing the development of 5G have raised concerns that China has in recent years been more aggressively asserting influence over the process in an attempt to bolster its domestic industry and attain control over network technologies that may have serious implications for U.S. network security. Nevertheless, according to other industry representatives, western companies continue to lead the standardization of 5G.

In addition to the specifications being developed by 3GPP, many other organizations are developing specifications related to different aspects of the broader 5G ecosystem. These organizations include IEEE, which develops specifications for Wi-Fi;[45] the Internet Engineering Task Force, which is developing specifications for enhancing internet protocols to support the 5G architecture and security features; and the O-RAN Alliance, which is developing specifications to support a virtualized radio access network.

[45] 5G networks also provide access from non-3GPP networks, such as Wi-Fi. Wi-Fi 6, the latest generation of Wi-Fi technology standardized by IEEE, could serve all of the key applications of 5G with comparable performance to 5G, with the exception of mobility. Consumer cellular devices may continue to offload data to available Wi-Fi networks, an approach that is supported by 3GPP specifications.

3 Key challenges to the performance or usage of 5G in the U.S.

While 5G is expected to deliver significantly improved network performance and greater capabilities, challenges may hinder the performance or usage of 5G technologies in the U.S. We grouped the challenges into the following four categories:

- availability and efficient use of spectrum
- security of 5G networks
- concerns over data privacy
- concerns over possible health effects

3.1 Spectrum availability and efficiency

We have reported that the lack of sufficient mid-band spectrum is a key challenge to deploying 5G.[46] As demand for spectrum outpaces supply, it will be difficult to realize 5G capabilities without more effective access to and use of mid-band and high-band spectrum. Spectrum sharing is one proposed solution to increasing spectrum availability and efficiency, but implementing it has challenges: (1) a lack of flexible and adaptive spectrum-sharing technologies and (2) an incomplete scientific understanding of the propagation of high-band frequencies.

3.1.1 Spectrum-sharing technologies

Increasing usage of limited spectrum will require additional R&D to keep pace with accelerating customer demand. While there are efforts being made to improve simple sharing techniques to increase use of limited spectrum, according to a 2018 NIST report, more innovative spectrum-sharing techniques are required to better use occupied or new spectrum bands at a reasonable cost, for increasingly diverse wireless customers.[47] One set of simple methods for sharing is to allocate spectrum access in one dimension, such as geography or time. With geographic sharing, users access the same frequencies in different locations to avoid interference. With temporal sharing, users access the same frequencies at different times. See figure 10 for examples of geographic and temporal sharing.

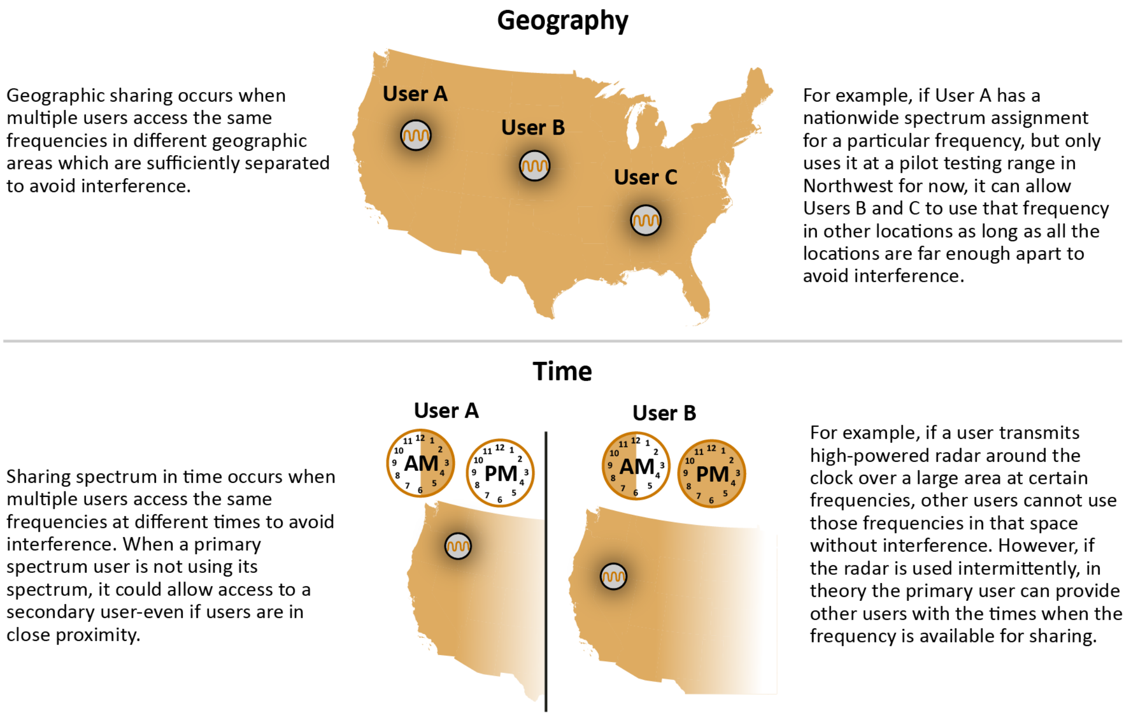
Simple access sharing methods, such as those that use time or geography macroscopically (i.e., over large time scales or large geographies), are not efficient because these methods are static and do not adapt to variations in usage demands. For example, a frequency may be allocated to a single license holder in a large geographic area, but the license holder may not need access to the frequency at all times. When the license holder is not using the frequency, other users would not have access to the frequency.

Dynamic spectrum access technologies could improve the use of licensed frequencies by allowing equipment to sense and select among available frequencies over shorter time scales and smaller geographic areas. In addition, dynamic spectrum access

[46] GAO-20-468, 7.

[47] NIST, *Future Generation Wireless Research and Development Gaps*, Special Publication 1219 (Gaithersburg, Md.: February 2018).

Figure 10: **Examples of simple spectrum-sharing methods**



Geographic sharing occurs when multiple users access the same frequencies in different geographic areas which are sufficiently separated to avoid interference.

For example, if User A has a nationwide spectrum assignment for a particular frequency, but only uses it at a pilot testing range in Northwest for now, it can allow Users B and C to use that frequency in other locations as long as all the locations are far enough apart to avoid interference.

Sharing spectrum in time occurs when multiple users access the same frequencies at different times to avoid interference. When a primary spectrum user is not using its spectrum, it could allow access to a secondary user-even if users are in close proximity.

For example, if a user transmits high-powered radar around the clock over a large area at certain frequencies, other users cannot use those frequencies in that space without interference. However, if the radar is used intermittently, in theory the primary user can provide other users with the times when the frequency is available for sharing.

Source: GAO and Map Resources. | GAO-21-26SP

technologies would reduce the need for human intervention and support flexible and adaptive spectrum sharing. Two such technologies are a tiered access system using a centralized database and an autonomous collaboration system based on artificial intelligence and machine learning. The following further explains these technologies.

The FCC created the Citizens Broadband Radio Service (CBRS) framework to increase commercial access to mid-band spectrum at 3,550–3,700 MHz while preserving existing federal use.[48] The framework prioritizes access to the band in three tiers. Top priority tier one users have protection from interference from lower tier users and include current federal users (e.g., U.S. Navy radar systems) and a number of licensed commercial users (e.g., fixed satellite service). New commercial entrants have either tier two (licensed) or tier three (unlicensed) access, which is managed by commercial Spectrum Access Systems that use databases to manage and coordinate access to a frequency. Tier-two users—which can include wireless carriers—will have access to the same mid-band spectrum when a tier-one user is not using it; if the frequency is in use by a nearby tier-one user, the tier-two users will be required to move to a different frequency. Tier-three users, which include the widest possible group of potential users, can access the band when it is not being used by either tier-one or tier-two users. According to NTIA, the Spectrum Access System and the

[48] For the regulations governing the use of devices in CBRS, see 47 C.F.R. pt. 96.

environmental sensors that alert the system when Navy radar systems are in use were certified by the FCC, following testing by NTIA's Institute for Telecommunication Sciences. Commercial systems must use only certified, FCC-approved devices and register with the Spectrum Access System. The technology supporting this spectrum-sharing framework was authorized for full commercial operation in January 2020. According to NTIA, CBRS has seen successful deployments of tier-three commercial general access unlicensed use and will see deployments of tier-two commercial priority access licensed used in fiscal year 2021, completing the transition to full three tiered spectrum access sharing.

Another example of dynamic spectrum access technologies are Collaborative Intelligent Radio Networks that use autonomous collaboration based on artificial intelligence and machine learning to increase access to spectrum. The DARPA Spectrum Collaboration Challenge competition led to the development of some of these radio networks, which demonstrated the application of recent advances in artificial intelligence and machine learning to spectrum sharing. The competition was announced in 2016 and ran until 2019. According to DARPA, the Spectrum Collaboration Challenge aimed to ensure that the increasing number of military and civilian wireless devices would have full access to the increasingly crowded electromagnetic spectrum. The competition aimed to challenge innovators in academia and business to produce breakthroughs in collaborative artificial intelligence and help create increased spectrum availability through sharing. Each competitor developed radio networks capable of autonomous collaboration to automate the spectrum management process. Specifically, the radio networks determined the best way to share congested radio frequencies among independent systems that were not using the same radio communications standard and were able to dynamically adapt as the situation changed.

Although these examples show progress is possible, more R&D is needed to adequately demonstrate dynamic spectrum access technology. A 2019 NITRD report noted that secure autonomous spectrum decision making is one of three overarching spectrum R&D priorities.[49] Further, according to FirstNet, an independent authority within NTIA, additional R&D of advanced spectrum-sharing technologies could allow for more efficient use of the limited spectrum available for 5G and for future generations of wireless networks.

According to DOD officials, the department has several ongoing efforts to facilitate spectrum sharing through dynamic spectrum access and sharing. For example, in 2020 the department began funding work to experiment with dynamic spectrum-sharing technology at Hill Air Force Base in Utah. According to DOD officials, this pilot could

[49] NITRD Wireless Spectrum R&D Interagency Working Group, *Research and Development Priorities for American Leadership in Wireless Communications* (Washington, D.C.: May 2019). The NITRD program is the nation's primary source of federal R&D in advanced computing, networking, and software. It is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the federal R&D enterprise. The work of the National Science and Technology Council is organized under committees that oversee subcommittees and working groups focused on different aspects of science and technology. Federal agency members of the Wireless Spectrum R&D Interagency Working Group coordinate spectrum-related R&D activities both across the federal government and with the private sector and academia.

help open additional mid-band spectrum for 5G usage without requiring an expensive and time-consuming relocation of military radar systems that are the current users of this spectrum. Additionally, dynamic spectrum sharing, as opposed to an exclusive non-federal or federal allocation, could increase the overall spectrum usage of the band.

3.1.2 Improved understanding of high-band propagation would enable more efficient spectrum sharing

Sharing approaches will need to consider use of higher frequencies to meet future spectrum demand; however, effectively sharing spectrum in higher frequencies is challenging due to the lack of understanding of high-band signal propagation in a cellular communications network setting. According to a NIST report, a thorough understanding of propagation in higher frequencies under various operating conditions is a critical first step to designing systems that take advantage of higher frequencies.

Improved characterization of the propagation of high-band frequencies could lead to more innovative and efficient spectrum sharing through wireless system design. For example, better signal propagation models can allow for optimal placement of small cells to optimize capacity and limit interference, according to the Small Cell Forum.[50] The 5G Millimeter-Wave Channel Model Alliance, a NIST-sponsored international research consortium, recently released two white papers that serve as technical best practice documents for wireless research laboratories investigating high-band propagation.

3.2 Securing 5G networks

The challenges associated with securing 5G networks can be divided into three areas. First, although the 5G specifications have the potential to increase security over prior generations, most of these security enhancements will not be realized until there are wide-scale deployments of standalone 5G networks. Second, 5G potentially introduces new modes of cyberattack and an expanded number of points of attack. Third, 5G requires continued assessments to identify future security vulnerabilities, as well as public-private collaboration to mitigate them.

3.2.1 Key security enhancements require standalone deployments and proper implementation

3GPP specifications for 5G include security enhancements that could address some existing 4G/LTE vulnerabilities. However, most of these enhancements will only be realized when standalone 5G is deployed on a large scale, which may take a decade. Additionally, security vulnerabilities identified in legacy specifications and mitigated in 5G are not implemented in legacy standards, such as 4G/LTE, since prior standard releases are no longer updated. Moreover, the 3GPP security enhancements are not activated by default; some are optional for carriers to

[50] Small Cell Forum, *Precision Planning for 5G Era Networks with Small Cells* (United Kingdom: Oct. 1, 2019). If small cells are placed too far apart, the carrier could experience capacity loss and if small cells are placed too close together, the carrier could experience interference and increased capital costs.

implement. If carriers do not implement these options, 5G networks will be susceptible to existing 4G/LTE vulnerabilities.

The following are examples of key security enhancements that 3GPP has designed and specified for 5G, and challenges to implementation:

- **Subscriber identifier.** The specifications include features that enhance subscriber privacy, such as the ability to encrypt the 5G subscriber identifier. Each device with a cellular connection, such as a cellphone, tablet, laptop, or mobile hotspot, has an identifier, known as the Subscriber Permanent Identifier in 5G networks and the International Mobile Subscriber Identity in 4G networks, which correlates to a specific subscriber. In 4G/LTE networks, the identifier is sent in clear (i.e., unencrypted) text, in some cases, when a mobile device is establishing a connection. In 5G networks, the device's identifier is always transmitted over the radio interfaces in an encrypted form, which would make the subscriber identity unavailable to rogue base stations, which are cellular devices that are not owned and operated by legitimate carriers. With the subscriber identifier, the operator of the rogue network may be able to infer the location of a specific individual without their knowledge. This poses a significant threat to user privacy, and potentially safety as users rely on operators' privacy practices. Although 3GPP specifications require equipment vendors to support this security enhancement, carriers are not required to implement it.
- **Authentication enhancements.** The 3GPP specifications introduce a new framework for authentication, which is a process for verifying the identity of a user or device before allowing access to the network. The new framework will, among other things, use the same authentication methods for both 3GPP (namely, 5G radio access) and non-3GPP (e.g., Wi-Fi) networks, allowing carriers to use the same authentication framework for both networks instead of using different frameworks. In addition, when a user device needs to authenticate over an untrusted non-3GPP access network, such as Wi-Fi, the device will connect via a function called the non-3GPP interworking function, which establishes an encrypted connection when the device is connected to the 5G core.

  Another example of an authentication enhancement involves increased home network control. Prior to 5G, when a user's device was roaming, the home carrier network of the subscriber had to trust the visited network through which the authentication took place. This vulnerability allowed networks to be spoofed and to send false signaling messages to the home carrier in an effort to request the 4G/LTE subscriber identifier and location of the device, which could then be used to intercept voice calls and text messages. In 5G networks, the home carrier will obtain proof that the device has been successfully authenticated and enable the home carrier network to verify device location to determine that the device actually is in a visited network, preventing spoofing attacks. The specifications define both of these authentication enhancements as mandatory functions for carriers to implement.

- **Integrity protection for user data.** While there has been protection for the integrity of the control plane (signaling communication needed to connect user equipment) since 3G, the 3GPP specifications also allow carriers to apply integrity protection to user plane (user data) traffic, such as voice communication, Short Message Service, and application traffic, in 5G networks.[51] While integrity protection of user data imposes additional demands on networks and devices, this demand is offset by the ability to mitigate known attacks methods that exploit the lack of user data integrity protection, such as attacks that can manipulate and redirect traffic.[52] Although 3GPP specifications require equipment vendors to support this security enhancement, carriers are not required to implement it.
- **Increased roaming security.** The 3GPP specifications are to increase inter-operator network connections (roaming) security with a network function called the Security Edge Protection Proxy. The proxy helps protect the network edge (boundary between two networks) and provide confidentiality of sensitive information as it is passed between two mobile networks. In addition, the proxy will help mitigate a number of internetworking and roaming threats in 4G/LTE networks. Specifically, in prior generation networks, carriers use protocols such as Signaling System 7 and Diameter to interconnect their networks to support long distance and international calling. However, both protocols have many security vulnerabilities, such as susceptibility to denial-of-service attacks, location tracking, fraud, and subscriber and network information disclosure.[53] The specifications state that the proxy is a mandatory function for carriers to implement.

For all of these security enhancements to be effective, carriers and 5G equipment vendors will need to properly implement, configure, and manage the 3GPP specifications—actions that are voluntary in some cases, complex, and potentially costly. Further, there is concern that some carriers may not comply with 3GPP specifications or may incorrectly implement them. According to a report by DHS's Cybersecurity and Infrastructure Security Agency (CISA), advanced security features in 5G protocols and technologies will improve communications security but will require proper configuration and implementation.[54] The report noted that, as

[51] Each protocol within the air interface performs a series of functions and operates on one of two logical planes: the user plane or the control plane. The user plane is the logical plane responsible for carrying user data being sent over the network while the control plane is responsible for carrying all of the signaling communication needed for the user equipment to be connected. Short Message Service is a wireless messaging service that enables users to send and receive short text messages, typically 160 characters or fewer, to or from mobile phones and can support a host of applications.

[52] Exploitation of certain vulnerabilities in the mutual authentication process allows an attacker to manipulate data between the phone and the network and redirect traffic to another destination.

[53] A denial-of-service attack prevents or impairs the authorized use of networks, systems, or applications by flooding the system with data and exhausting resources.

[54] CISA, *Critical Infrastructure Security and Resilience Note: Overview of Risks Introduced by 5G Adoption in the United States* (July 31, 2019). CISA is a component of DHS with the mission to act as the Nation's risk advisor, collaborate with stakeholders to secure critical infrastructure, and provide cybersecurity tools and services to protect the federal government's network infrastructure.

municipalities, companies, and organizations build their own local 5G networks, it is possible they will not properly implement 5G security enhancements, making equipment and networks vulnerable to interception, disruption, and manipulation.

Furthermore, once a carrier has migrated its entire network core to 5G, the carrier still may include 4G/LTE protocols alongside 5G for backward compatibility, which may allow some of the older security vulnerabilities to persist. Carrier officials we spoke with stated that they did not have a specific plan or timeline for when they would remove older technologies, such as 4G/LTE, from their network core.

To address concerns regarding implementation of 3GPP security enhancements, there are efforts under development to help facilitate both implementation and configuration. Specifically, the National Cybersecurity Center of Excellence, a part of NIST, is developing a cybersecurity practice guide using a phased approach to align with the development of 5G specifications.[55] One goal of the guide is to help organizations increase their understanding of 5G standards-based security features. The guide will identify several 5G applications and demonstrate for each one how to strengthen the underlying 5G architecture components to mitigate risks. In addition, the FCC has directed the Communications Security, Reliability, and Interoperability Council (CSRIC), which is charged with providing recommendations to ensure the security and reliability of the nation's communications systems, to evaluate the standards for 3GPP releases 15 and 16. The evaluation is to identify potential areas of risk, recommend best practices to mitigate the risks, recommend appropriate updates to the 3GPP security specifications, and identify optional and legacy features in 3GPP specifications that could diminish the effectiveness of 5G security, along with recommendations to address these gaps.

3.2.2 5G networks may introduce new cybersecurity risks and expand existing ones

Some of the technologies introduced by the development and deployment of 5G may increase cybersecurity risks. We have ongoing work enumerating national security risks related to 5G and reviewing agency processes to identify and assess 5G risks. We have previously reported on federal strategies for 5G security.[56] This section covers risks related to three facets of 5G: network architecture, expansion of IoT, and the supply chain.

5G network architecture risks

One potential source of increased security risks in 5G network architecture is Network Function Virtualization. Network Function Virtualization allows carriers to virtualize network functions traditionally managed by specific pieces of equipment, such as routers and firewalls, on cloud-based servers using

[55] The National Cybersecurity Center of Excellence is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the National Cybersecurity Center of Excellence develops examples of cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

[56] GAO-21-155R.

specialized software. Virtualization will eliminate the need for purpose-built hardware and will push core functions towards the radio access network or network access edge to allow for a flexible and elastic network more capable of meeting the demands of network traffic in real time. Unlike prior technologies, in which a given piece of hardware can be optimized for only one application at a time, a 5G network would use virtualization to optimize performance of multiple applications, even those that require very different levels of bandwidth, latency, availability, and security.

However, virtualization of network functions will increase the network's vulnerability to attackers due to the increased reliance on software. Software typically requires frequent updates and could present vulnerabilities that attackers will seek to exploit. For example, the software that supports virtualization may be vulnerable to attacks that could bring down or compromise an entire network. According to a 5G Americas report, vulnerabilities in software components have often surfaced in the past and securing the software that virtualizes network functions remains a major challenge.[57] In addition, a CSRIC report states that the virtualization of network functions introduces a new risk because virtualization is still a comparatively new architecture and carriers may still be unfamiliar with the risks inherent in networks that are more defined by software than hardware.[58] According to the report, a lack of staff with the skillsets needed to operate virtualized networks may represent the largest threat in telecommunication networks utilizing this new architecture.

Increased virtualization also introduces challenges for network monitoring. Due to the virtualized architecture of 5G networks and deployment of network functions closer to the radio access network or network access edge, it will be more difficult to detect and recognize the types of traffic crossing these networks and mitigate against any new threats.

The developing Open Radio Access Network Alliance may be the source of another potential vulnerability in 5G architecture. This alliance promotes competition and specialization among a variety of 5G component and software providers, similar to how modern computers use specialized vendors for memory, processing, and software. While this initiative strives to improve performance and reduce costs, the attack surface of the network expands considerably.

Another source of increased security risks in 5G network architecture is network slicing. If implemented properly, network slicing should limit an attacker's ability to access critical areas within a network by isolating the attack to the infected network slice and not the entire network. However, according to a 5G Americas report, if the slices and the components within a slice are not adequately isolated, an attacker could attack the slice using components from another slice.[59]

Features that increase reliance on software, such as Network Function Virtualization, will need to be monitored for vulnerabilities and

[57] 5G Americas, *The Evolution of Security in 5G* (July 2019).

[58] FCC CSRIC, *Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks v14.0* (September 2018).

[59] 5G Americas, *The Evolution of Security in 5G*.

patched as quickly as possible to address evolving risks and ensure security and functionality. According to the Cyberspace Solarium Commission report, patch development and distribution—the process whereby a software developer creates a fix to a vulnerability and distributes it to users—is key to eliminating the risk that a given vulnerability can pose.[60] The report recommends, among other things, that software and hardware component developers and manufacturers establish a publicly accessible process for vulnerability reporting, retain records documenting when a vulnerability was made known or discovered by the company, and maintain a vulnerability disclosure and patching policy for their products. In addition, the report recommends that the U.S. government study the potential effectiveness of directing NIST to develop guidance or expectations about how quickly patches should be implemented once released.

Expansion of the Internet of Things (IoT)

IoT devices will be major users of 5G networks, bringing new capabilities while also creating significant security risks.[61] According to a CSRIC report, cellular-connected IoT devices are expected to number in the billions, which will increase points of entry to wireless networks.[62] In addition, many IoT devices may be unable to protect themselves due to limited processing power, and some devices may be more vulnerable because they will be connected to networks for long periods (e.g., automated vehicles and medical devices). Further, manufacturers of many types of IoT devices are sometimes small companies with few resources, limiting their ability to conduct security testing.

IoT devices have been used in the past to inject and spread malware, including ransomware, to other parts of the network used by the devices.[63] In addition, because many IoT devices are designed without security in mind, they are often a route for attacks on other targets, such as the radio access network, the 5G core, infrastructure devices, web servers, and other IoT devices.

We have also previously reported on the potential implications of the use of the IoT.[64] According to the report, these implications include challenges to the development of the IoT, such as ensuring:

- **Information security.** The IoT brings the risks inherent in potentially unsecured information technology systems into homes, factories, and communities. IoT devices, networks, or the cloud servers where they store data can be compromised in a cyberattack. For example, in 2016, hundreds of thousands of weakly-secured IoT devices were accessed and hacked, disrupting traffic on the internet.

[60] U.S. Cyberspace Solarium Commission (March 2020).

[61] We previously reported on IoT cybersecurity risks; see GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-668 (Washington, D.C.: July 27, 2017).

[62] FCC, *Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks*.

[63] S.R. Zahra and M.A. Chishti, "Ransomware and Internet of Things: A New Security Nightmare," in *Proceedings of the 9th International Conference on Cloud Computing, Data Science & Engineering* (IEEE, January 2019).

[64] GAO-17-75.

- **Safety.** Researchers have demonstrated that IoT devices such as connected automobiles and medical devices can be hacked, potentially endangering the health and safety of their owners. For example, in 2015, hackers gained remote access to a car through its connected entertainment system and were able to disable the brakes and disable the transmission.
- **Standards.** IoT devices and systems must be able to communicate easily. Technical standards to enable this communication will need to be developed and implemented effectively.

Supply chain and other network cybersecurity risks

According to an April 2019 Defense Innovation Board report, a compromised supply chain poses a serious threat to national security by introducing vulnerabilities into networks and systems.[65] According to the report, supply chains for 5G wireless telecommunications will expand on the existing global supply chain for wireless technology and be highly complex. Tracking the source of components in the supply chain is extremely difficult due to the complexity and increased geographic distribution for 5G technologies. The Cyberspace Solarium Commission, led by Members of Congress, senior executive agency leaders, and non-federal experts, also reported on supply chain risks in 2020.[66] The report noted that securing supply chains is one of the five strategic objectives to reshape the cyber ecosystem toward greater security.[67] The report also stated that the U.S. has grown more dependent on suppliers from countries, such as China, that may come under malign influence, introducing vulnerability into the ecosystem. We have previously reported that federal agencies need to take urgent action to manage information and communications technology supply chain risks.[68]

The global reach of the 5G supply chain, as well as the technological complexity of the components of 5G technologies, present the risk that components from suppliers whose quality and security cannot be fully guaranteed may be used in 5G networks. According to a CISA report, carriers and equipment vendors may use 5G components manufactured by untrusted companies, likely, in part, because of the relatively low costs or the components may already exist as part of the current LTE infrastructure.[69] The report stated that the use of 5G components manufactured by untrusted companies could expose U.S. entities to risks introduced by malicious software and hardware, counterfeit components, and component flaws caused by

[65] Defense Innovation Board, *The 5G Ecosystem: Risks & Opportunities for DOD* (Washington, D.C.: April 2019).

[66] The *John S. McCain National Defense Authorization Act for Fiscal Year 2019* established the Cyberspace Solarium Commission to "…develop a consensus on a strategic approach to defending the U.S. in cyberspace against cyber attacks of significant consequences." Pub. L. No. 115-232, § 1652, 132 Stat. 1636, 2140-41 (2018). The report was published March 11, 2020.

[67] U.S. Cyberspace Solarium Commission.

[68] GAO, *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* GAO-21-164SU (Washington, D.C.: Oct. 27, 2020).

[69] CISA, *Critical Infrastructure Security and Resilience Note*.

poor manufacturing processes and maintenance procedures.

The CISA report also described steps that could increase the development and use of trusted components and lower the risks of using malicious untrusted components. These steps included national investment in R&D, economic incentives for manufacturing and buying trusted components, and economic deterrents for purchasing and installing untrusted components.

Various federal statutes, regulations, and policies attempt to mitigate some of the risks to the supply chain. For example, the *John S. McCain National Defense Authorization Act for Fiscal Year 2019* prohibits executive branch agencies and government contractors from procuring, obtaining, extending, or renewing a contract to procure or obtain, 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.[70] The act defines "covered telecommunications equipment or services" to include telecommunications equipment produced by Huawei Technologies Company (Huawei), ZTE Corporation, or any of their subsidiaries or affiliates. In May 2019, the Department of Commerce added Huawei and certain non-U.S. affiliates to the Entity List[71] (with additional affiliates added in August 2019 and August 2020) as entities who may have engaged in activities that are contrary to U.S. national security or foreign policy interests. Also in May 2019, the President issued an executive order prohibiting transactions involving information and communications technology and services originating in foreign adversaries, which pose an undue risk to critical infrastructure or to U.S. national security.[72]

In 2020, the FCC published a final rule in response to ongoing concerns about the integrity of the communications supply chain.[73] The rule prohibits the use of money from the Universal Service Fund to purchase or obtain equipment or services from any communications equipment or service provider identified by the FCC's Public Safety and Homeland Security Bureau as posing a national security risk to communications networks or the communications supply chain, such as Huawei Technologies Company and ZTE Corporation.[74] Additionally, the *Secure and Trusted Communications Networks Act of 2019* was signed into law in March 2020 and prohibits the use of certain federal funds to obtain communications equipment or services from a company that poses a national security risk to U.S. communications networks.[75]

[70] Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917 (2018). *See also* FAR 52.204-24.

[71] The Entity list is found at Supplement No. 4 to Part 744 of the Export Administration Regulations.

[72] Executive Order No. 13873, 84 Fed. Reg. 22,689 (May 15, 2019). In May 2020, the President extended the national emergency declaration under that executive order through May 2021.

[73] See 47 C.F.R. § 54.9 (2020).

[74] The Universal Service Fund, which is paid for by contributions from telecommunications providers based on an assessment of interstate and international end-user revenue, provides funding for projects and services in pursuit of the goal that all Americans have access to advanced communication services.

[75] Pub. L. No. 116-124, 134 Stat. 158 (2020).

3.2.3 5G networks will require continuous monitoring of security threats and increased coordination

Not all 5G security threats are known, and new threats will evolve as deployment progresses and attackers get access to 5G networks. According to CISA officials, it is impossible to fully identify 5G vulnerabilities due to the limited rollout of 5G infrastructure in the U.S. to date. In addition, according to 5G Americas, the increase in the volume of devices and the complexity of the infrastructures in 5G are likely to also increase threats.

5G security will, therefore, require continued monitoring of the threat landscape and increased public and private coordination. In response to concerns about 5G's potential effect on national security, the *Secure 5G and Beyond Act of 2020* was signed into law in March 2020.[76] It, among other things, requires the President, in consultation with relevant federal agencies, to develop a strategy to secure and protect 5G systems and infrastructure in the U.S. and provide technical assistance on 5G security to mutual defense treaty allies, strategic partners and other countries. In March 2020, the White House issued the *National Strategy to Secure 5G* to provide direction on how the U.S. government will secure 5G infrastructure domestically and abroad.[77] The strategy states that the U.S. Government, in partnership with state, local, and tribal governments as well as private sector partners, will seek to continuously identify and characterize economic, national security, and other risks posed by cyber threats to and vulnerabilities in 5G infrastructure. The *Secure 5G and Beyond Act of 2020* also requires the President, within 180 days of the enactment of the act (enacted March 23, 2020), to develop and submit an implementation plan for this strategy. As we reported last month, the 5G national strategy does not contain information regarding an implementation plan.[78] The plan is to include an identification and assessment of potential security threats related to 5G, along with development of an ongoing capability to identify security vulnerabilities in 5G and future generations of wireless communications systems.

According to a July 2019 CISA report, there is a need for increased coordination with the private sector. The report noted that the private sector could provide insights on where government support or intervention will help secure 5G technologies and the 5G network.[79] In addition, the Cyberspace Solarium Commission report stated that one way to enable rapid detection and identification of cyber threats is through coordinated network monitoring and threat detection programs.[80] According to the report, voluntary programs, through which the U.S. government provides sensors or funding to monitor private-sector networks, can help identify if cyber threats are isolated incidents or part of a larger, coordinated campaign. The report recommended that the government build and communicate a better understanding of threats, with the specific aim of informing private-sector security operations, directing

[76] Pub. L. No. 116-129, 134 Stat. 223 (2020).

[77] White House, *National Strategy to Secure 5G* (Washington, D.C.: March 2020). We have reviewed this strategy; see GAO-21-155R.

[78] GAO-21-155R, 8.

[79] CISA, *Critical Infrastructure Security and Resilience Note*.

[80] U.S. Cyberspace Solarium Commission.

government operational efforts, and ensuring better common situational awareness for coordinated action between government and the private sector.

In August 2020, CISA released its 5G strategy that establishes five strategic initiatives to advance the deployment of a secure and resilient 5G infrastructure.[81] According to the strategy, the initiatives stem from the four lines of effort defined in the *National Strategy to Secure 5G* and include associated objectives to ensure there are policy, legal, security, and safety frameworks in place to use 5G technology while managing significant associated risks. The strategy notes that each of the initiatives should address critical risks to secure 5G deployment, such as physical security concerns; attempts by threat actors to influence the design and architecture of the network; vulnerabilities within the 5G supply chain; and an increased attack surface for malicious actors to exploit weaknesses.

3.3 Privacy

5G technology will likely exacerbate privacy concerns due to (1) the increased precision of location data and (2) the proliferation of IoT devices. Whether the privacy of user information will be adequately protected is a significant question in the deployment of 5G, in part because there is no comprehensive federal legislation addressing privacy requirements for non-federal enterprises. We have previously recognized the need for the limitation of the collection and use of personal information with knowledge and consent, as well as the need to improve federal privacy efforts, as critical actions to address challenges related to data privacy.[82]

5G is changing the ability to precisely collect and aggregate location data. 4G/LTE networks can determine a device's location using three or four base stations to within about 150 feet. 5G is expected to allow a single base station to determine location within a few inches outdoors and within a few feet indoors.

One motivation for improving location data has been to enhance services such as emergency calling, traffic reports, ride sharing, and roadside assistance. These services will help meet the requirements for Enhanced 911, which is dedicated solely to first responders. Other uses of location data collected by devices are for entertainment or personal services, including social media, shopping, augmented reality, and fitness monitors. In addition, user location data also could provide auto insurers with information to determine premiums and advertisers with information to target content based on location.

5G networks will also significantly increase the amount of IoT data, because devices will connect to vast networks of sensors that are located not only in workplaces, but also in home technology such as security systems and appliances. Privacy advocates have expressed concerns about the use and storage of vast amounts of data without consent, including location data, which could compromise user privacy and lead to issues including identity theft, discrimination, and other harm. Data could be linked across

[81] CISA, *5G Strategy: Ensuring the Security and Resilience of 5G Infrastructure In Our Nation* (Washington, D.C.: August 2020).

[82] GAO, *High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

devices and profiles, giving data aggregators the ability to track user habits and activities. Furthermore, unsecured, highly detailed information could be used by foreign adversaries to gather intelligence and by other entities to monitor persons of interest. According to findings by the FCC, at least one location aggregator used location data to locate any cell phone on major mobile networks in the U.S. without the knowledge and consent of the phone's owner.[83]

These changes could exacerbate existing issues related to privacy, including the absence of comprehensive federal privacy laws and the management of data privacy protections through a patchwork of state laws and industry guidelines.

Two federal laws relate broadly to the privacy of location data.[84] First, section 222 of the *Communications Act of 1934* generally only permits carriers to disclose certain types of data, such as location data, for purposes associated with that user's service, unless they receive permission to use that data for other purposes.[85] Second, the *Children's Online Privacy Protection Act* requires that covered websites publish privacy policies detailing the operators of the website and how data is collected and used and also limits data that can be collected about children.[86] Neither of these laws, however, comprehensively addresses data storage, data use, or other data privacy measures in the U.S. By contrast, several other nations have created overarching privacy laws, and a few U.S. states have created laws directly related to consumer data privacy.[87] For example, the *California Consumer Privacy Act of 2018* created requirements that businesses disclose, on request, what personal information is being collected and to whom it is being sold and allowed consumers to prohibit the sale or request the deletion of personal information, with exceptions.[88]

The *Privacy Act of 1974*, which governs the collection, use, and dissemination of personal information maintained by the federal government, does not deal directly with location data privacy, but the law did introduce the basic concepts embodied in the "Fair Information Practice Principles" (FIPPs) that have been used to further develop possible overarching federal privacy

[83] FCC Notice of Apparent Liability for Forfeiture and Admonishment. *FCC 20-24* (Washington, D.C.: February 2020), FCC Notice of Apparent Liability for Forfeiture and Admonishment. *FCC 20-25* (Washington, D.C.: February 2020), FCC Notice of Apparent Liability for Forfeiture and Admonishment. *FCC 20-26* (Washington, D.C.: February 2020), FCC Notice of Apparent Liability for Forfeiture and Admonishment. *FCC 20-27* (Washington, D.C.: February 2020). Location aggregators are companies that purchase location data from carriers and then use that data to create and sell products for advertising or tracking purposes.

[84] In addition to those laws, which specifically address the privacy and security of location data, the Federal Trade Commission has general authority under 15 U.S.C. § 45 to prevent unfair or deceptive commercial practices which can include practices related to the collection, use, or disclosure of data. FCC officials also highlighted the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986), as protecting location information from access by government entities.

[85] Pub. L. No. 73-416, 48 Stat. 1064 (1934), amended and codified in relevant part at 47 U.S.C. § 222.

[86] Pub. L. No. 105-277, §§ 1301–1308, 122 Stat 2681-728 (1998) codified at 15 U.S.C. §§ 6501–6506, and implementing regulations at 16 C.F.R. §§ 312.1–312.13.

[87] For example, the *General Data Protection Regulation* (GDPR) is directly applicable to European Union members. This law requires affirmative consent from users to allow the collection of personal data, as well as requirements that users receive notice of their data rights. By default, data may only be used for specified purposes.

[88] Cal. Civ. Code §§ 1798.100 to 1798.199.

legislation.[89] The principles provide a framework for organizations to use to address privacy in their business practices and include principles related to limiting the collection of personal data, specifying the purpose of the collection, limiting the use of collected data, safeguarding collected data, and providing users the choice of whether to have their data collected.

As we have previously reported, gaps exist in the federal privacy framework regarding consumers' right to know about or control the collection of their data. In addition, current privacy frameworks do not address new technologies such as mobile technology.[90]

In the absence of comprehensive privacy legislation, individual companies are a primary source of policies related to the storage and use of data. For example, CTIA published *Best Practices and Guidelines for Location-Based Services* in 2010 to guide mobile carriers and others in protecting location data.[91] These best practices focus on two fundamental principles: notice to users explaining how location information will be used, disclosed, and protected, and informed consent from users allowing providers to use or disclose location information. The guidelines discuss general information regarding the safeguarding of location information and adherence to laws related to data use, particularly data connected to minors. These guidelines were last updated in 2010 and are voluntary for location-based service providers.

We have previously recommended that Congress consider developing comprehensive legislation to enhance consumer protections related to securing the privacy of their personal information. Specifically, we suggested consideration of agency responsibilities and authority to oversee internet privacy and the balance between internet privacy for consumers and the ability for industry to provide desired services and innovation.[92]

3.4 Concern over possible health effects

The deployment of 5G technology, including the numerous small cell base stations needed to transmit and receive high-band frequencies, may exacerbate existing public concerns that RF energy exposure may cause

[89] Pub. L. No. 93-579, 88 Stat. 1896 (1974); 5 U.S.C. § 552a. A U.S. government advisory committee first proposed the FIPPs for protecting the privacy and security of personal information. While FIPPs are not legal requirements, they provide a framework for balancing privacy with other interests. For a revised version of the FIPPs that has been widely adopted, see Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Paris: Sept. 23, 1980).

[90] GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

[91] CTIA, *Best Practices and Guidelines for Location-Based Services* version 2.0 (March 23, 2010). CTIA is a trade association representing the wireless communications industry in the U.S.

[92] GAO, *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility*, GAO-19-52 (Washington, D.C.: Jan. 15, 2019), 38.

cancer[93] or otherwise endanger human health, although there is limited evidence to support these concerns. Several U.S. localities, private citizens, and non-profits have filed lawsuits involving the deployment of 5G, including claims that the FCC has failed to update its RF exposure limits in light of the new technology.[94] Health concerns have also interrupted 5G deployment abroad, with several Swiss communities delaying rollouts, and protesters in the United Kingdom and the Netherlands damaging 5G towers.

To respond to public concerns, decision makers need policy-relevant information on the long-term health effects of 5G technology. Although there is currently no consistent evidence of health risks related to 5G RF exposure in humans, responding to public concerns remains a challenge, in part due to the possibility of unknown long-term health effects and the challenges in researching this topic.

3.4.1 Unknown long-term health effects

While research on the biological effects of RF energy has been underway for decades, research on the long-term health effects of pre-5G technology is ongoing and research on the possibility of long-term health effects of 5G technology is largely unknown because the technology is still new and has not been widely deployed.

Officials from federal regulatory and research agencies did not indicate any cause for alarm due to these unknowns because of the research from observational studies on pre-5G technology and from experimental studies of high-band 5G technology.[95] The National Cancer Institute (NCI) reviewed three large observational studies and several smaller observational studies of humans exposed to pre-5G technology.[96] The results of the large studies were inconsistent in linking cell phones and cancer outcomes and methodological challenges may have affected the findings. A few of the smaller studies showed a relationship with non-malignant tumors. 5G technology introduces RF energy at higher frequencies than used for existing cellular communications systems. However, higher frequencies have less penetration into the human body and therefore are thought to be less of a concern than lower frequencies.

[93] The RF spectrum used in cellular communications has not been definitively linked to cancer or other health outcomes, according to FCC and FDA. The lower frequencies of the radio frequency spectrum that are used for wireless communication, including 5G communication, are considered “nonionizing radiation” because these frequencies lack sufficient energy to remove electrons from atoms and molecules. In contrast, X-rays are considered “ionizing” radiation, which can have significant human health effects and are known to increase the risk of cancer. The radio frequencies used by cellular communications systems can lead to tissue heating, but is not thought to emit enough RF energy to cause harmful heating.

[94] The U.S. Court of Appeals for the Ninth Circuit dismissed a challenge claiming that FCC failed to reassess its RF exposure limits, because, by the time of the decision, FCC had completed its evaluation of the effects of 5G technology on its RF standards and concluded that the RF limits did not need to be updated. City of Portland v. United States, 969 F.3d 1020, 1046-47 (9th Cir. 2020). FCC’s evaluation and decision not to update its RF exposure limits is currently being challenged in the D.C. Circuit Court of Appeals. Brief of Petitioners at 65-69, Environmental Health Trust v. FCC, No. 20-1025 (D.C. Cir. July 29, 2020).

[95] Experimental studies are those in which the exposure to RF energy is determined by the investigator. Observational studies are those where exposure to RF energy is observed (usually reported or measured).

[96] NCI reviewed the Interphone, Million Women Study, Danish Registry Linkage Study, which all evaluated 2G and 3G technologies; RF exposure from high-band 5G technology was not evaluated in these studies.

FDA officials do not expect changes to the current safety standards from 5G technology.

According to officials, the unknown long-term health effects and R&D opportunities related to 5G technology include the following:

- **High-band 5G frequencies.** The latest IEEE standard on electromagnetic safety published in 2019 focused on the effects of frequencies above 6 GHz in experimental studies. However, no studies have been carried out on the long-term health effects of high-band 5G frequencies in observational studies, such as those in settings experienced by the general public, because the technology has not been deployed for long enough or widely enough to conduct these studies. According to an NCI scientist, even after high-band 5G technology has been put into use in the coming years, the long-term health effects on people, if any, may not be known for many years later because some health outcomes could take decades to develop. The high-band frequencies used in 5G will only be available for observational studies once 5G technology has been deployed widely. A National Institutes of Health scientist noted that the 5G frequencies are still not clearly defined, making it difficult to understand the impact on human exposure.
- **Active antennas with beamforming.** FCC stated that RF exposure below the exposure limits are safe. However, no research has been conducted to characterize long-term exposure to the multiple active antennas with beamforming that are a feature of 5G. It is unknown how the signals from these antennas may affect human health in the long-term. It could be computationally intensive to study the long-term exposure to these antennas due, in part, to their many possible configurations, which may increase or decrease the RF energy exposure. According to NIST experts, a statistical model is needed to study these configurations, and it will be necessary to evaluate this model against measurements of actual systems. NSF officials believe that artificial intelligence techniques have the potential to better address this modeling challenge.
- **Certain high-risk populations, cancer, and non-cancer outcomes.** In 2008, a committee convened by the National Research Council (part of the National Academies of Sciences, Engineering, and Medicine) reported that further research was needed to characterize exposure to RF energy in juveniles, young children, and pregnant women and fetuses in observational studies.[97] An NCI scientist we interviewed reiterated these unknown long-term health effects for pre-5G technology and with respect to 5G. Further research was also needed for non-cancer outcomes, such as developmental and behavioral outcomes, according to the committee proceedings and the NCI scientist. Observational studies may be used to study health outcomes that take years and decades to

[97] National Research Council, *Identification of Research Needs Relating to Potential Biological or Adverse Health Effects of Wireless Communication Devices*, National Academies Press (Washington, D.C.: 2008).

develop, such as developmental, behavioral, and cancer outcomes. However, as mentioned above, there have been no observational studies on the long-term health effects of high-band 5G frequencies because the technology is still new.

3.4.2 Research challenges

Challenges in understanding research on the possibility of long-term health effects of exposure to RF energy from pre-5G and 5G technology include: (1) measuring RF exposure to populations, and (2) synthesizing research for decision makers and for the public.

Measuring population exposure to RF

Measuring RF exposure in observational studies is a challenge, but these types of studies are of interest in making policy relevant recommendations. Observational studies ask participants to report their current cell phone use, or attempt to measure RF exposure. Yet asking participants about their current cell phone use or using cell phone call logs may not be a good proxy for RF exposure, since people may use phones for more than voice calls and call logs do not account for potential exposure to surrounding small cells and base stations, Wi-Fi networks, and other environmental exposures. NCI scientists noted that cancer and other chronic exposures require collection of not only current RF exposures, but past RF exposures that may contribute to total exposure. The type of RF exposure relevant to health outcomes is also unknown whether it be peak exposure or cumulative, according to NCI scientists. However, none of the recent observational studies attempted to estimate the entire accumulated RF dose in the individual environments of the study subjects.

To better address the measurement of RF exposure in future studies involving high-band frequencies, an NCI scientist noted that studies that measure exposure to RF energy and the amount of RF energy deposited into the body (dosimetry) would first need to be performed to prepare for human observational studies and to help understand how exposure is different with 5G technology.

Synthesizing research for decision makers and the public

Due to the challenges of measuring long-term exposure to RF energy and unavailability of the evidence at this time, assessments of 5G technology will likely be based on human or animal experimental studies (usually short-term) and human observational studies that rely on self-reporting exposure to RF energy, all of which have limitations. The experimental studies may not be relevant to long-term human exposure to RF energy as studies conducted over a shorter period may not detect outcomes that take decades to develop. As noted above, self-reporting may not be a good proxy for total, peak, or cumulative exposure to RF energy.

Because there is a large and evolving body of relevant research, it is important that the results be regularly synthesized for Congress and the public. The FCC relies on the FDA as well as other organizations—principally IEEE and the National Council on Radiation Protection and Measurements (NCRP)—to review scientific research and provide recommendations for setting RF safety standards.[98] However, each of these organizations has only reviewed a subset of the relevant research and, of these organizations, only IEEE updates its formal assessments regularly. Specifically:

- According to officials, the FDA monitors peer-reviewed science regarding RF energy and health. The agency does not typically make its assessments publicly available, but released one assessment publicly in February 2020.[99] The assessment focused on cancer-related animal and human studies of frequencies below 6 GHz. The assessment did not include non-cancer outcomes or frequencies above 6 GHz. The agency does not have plans to update this review for the FCC unless it becomes aware of research that would lead it to change its current assessment, that the current scientific evidence has not linked RF energy from cell phones with health problems in humans.
- IEEE has periodically published standards for RF energy exposure in 1991, 2005, and 2019.[100] While IEEE does include reviews of observational studies of frequencies below 6 GHz in its latest standard, its assessment of those studies was that many were weak in terms of their design and exposure assessment. The IEEE noted, "while the available results do not indicate a strong causal association, they cannot establish the absence of a hazard." The review did not include observational studies above 6 GHz because the technology has not been deployed for long enough or widely enough to conduct these studies, as mentioned above.
- NCRP reviewed two larger observational studies in its 1986 review; however, it has not published an update since.[101] The studies reviewed included a retrospective study of U.S. naval personnel conducted by the National Academies of Sciences and a retrospective study of American embassy personnel in Moscow conducted

[98] While other organizations synthesize the literature on RF energy and health outcomes, we focus on the three organizations (FDA, IEEE, and NCRP) that FCC principally relies on for synthesizing the literature and providing recommendations for setting RF safety standards. NCRP was chartered in law by the U.S. Congress in 1964 to collect, analyze, and disseminate information and recommendations about radiation protection in the public interest. Pub. L. No. 88-376, 78 Stat. 320 (1964). The International Commission on Non-ionizing Radiation Protection (ICNIRP) also synthesizes experimental and observational studies. It is an independent, non-governmental organization chartered in Germany that provides guidelines followed by several European Union countries. IEEE and ICNRP have been working to harmonize their standards.

[99] FDA, *Review of Published Literature between 2008 and 2018 of Relevance to Radiofrequency Radiation and Cancer* (Silver Spring, Md.: February 2020).

[100] According to IEEE officials, the standards have a 10-year revision cycle. However, the standard is a "living" document that may be revised sooner, for example, if the conclusions of an ongoing World Health Organization Environmental Health Criteria systematic review reveal any significant results.

[101] NCRP Report No. 86, Biological Effects and Exposure Criteria for Radiofrequency Electromagnetic Fields, 1986. According to an NCRP official, NCRP produces reports at the request and funding of federal agencies. NCRP has not been funded to update Report No. 86.

by Johns Hopkins University.[102] Neither study found evidence of an association between RF energy and adverse outcomes. The naval study used occupation as a proxy for exposure to RF energy, and the embassy study was not able to obtain complete information on exposures and outcomes for participants. These studies focused on persons occupationally exposed to RF energy and may not be relevant to public exposure to RF energy.

[102] Observational studies may be prospective or retrospective. In prospective studies, participants are enrolled and data are collected on their current exposures. Then, participants are followed up over a period of time (some cohort studies have been ongoing for years) to observe outcomes that develop. In retrospective studies, participants are enrolled and asked about exposures and outcomes that have already occurred. The benefit of a prospective study is that it is less subject to recall bias, which may be present in retrospective studies where outcomes are known and participants are asked to report past exposure.

4 Policy options to address challenges to the performance and usage of 5G networks in the U.S.

Achieving the expected performance and usage of 5G networks in the U.S. has potentially wide-ranging ramifications for the U.S. economy and society. We identified six policy options in response to the challenges discussed in the previous chapter. In this chapter, we first present policy options that address availability and efficient use of spectrum, security of 5G networks, concerns over data privacy, and understanding the possibility of long-term health effects of 5G technology—each of which could affect the nation's ability to achieve the expected performance and usage of 5G networks. We then describe the potential implications if policymakers choose to maintain the status quo; that is, they do not take active steps to counter the identified challenges to the performance and usage of 5G technologies in the U.S.[103] For each policy option, including the status quo, we present potential opportunities and considerations.[104]

[103] We consider policymakers broadly to include Congress, federal agencies, academic and research institutions, private companies, and industry trade groups, among others.

[104] We present policy options that were within the scope of this technology assessment. They are not an exhaustive list of all potential policy options, nor are they recommendations to federal agencies or matters for congressional consideration. They are not listed in a specific rank or order, and we are not suggesting that they be completed individually or combined in any particular fashion. We did not conduct the detailed additional analysis that would be needed to fully implement a specific policy option or combination of options—for instance, on potential design and legal issues—nor did we assess how effective the options may be. We express no view regarding the extent to which legal changes would be necessary to implement them.

Policy option: Spectrum sharing technologies

Policymakers could promote R&D of spectrum-sharing technologies.

Potential opportunities

Additional R&D of advanced spectrum-sharing technologies could allow for more efficient use of the limited spectrum available for 5G and for future generations of wireless networks. As discussed earlier in this report, ensuring the efficient use of spectrum is important for 5G network performance and usage as the networks continue to evolve and as they give way to the next generations of wireless networks. R&D could help solve the many remaining challenges related to spectrum sharing. For example, NITRD's Wireless Spectrum R&D Interagency Working Group and NIST have identified the need for effective automation of interference detection and mediation as especially important as highly directional, active antennas become more common.[105] Development of sharing technologies will also be important for use in unlicensed spectrum, where multiple users are allowed to operate simultaneously. Unlicensed spectrum is not centrally managed, so each device makes its own determination to transmit and every user has the same priority.

According to reports by the Center for a New American Security, the National Security Commission on Artificial Intelligence, and NIST, there are opportunities to use recent advances in machine learning and artificial intelligence for advancing spectrum-sharing techniques.[106] Policymakers could promote R&D in multiple ways, including through grants to academic and research institutions, by setting up a public-private partnership, or as tax credits for industry. For testing and development in real-world settings, new 5G test beds may be necessary, according to NIST, or it may be possible to use existing test beds.

Potential considerations

R&D can be costly; it is generally considered a long-term investment, and its potential benefits are uncertain. Analysis will be required to identify funding sources, set up funding mechanisms, or determine from which existing funding streams to reallocate funds. In addition, the respective roles for government, the private sector, and academia in researching and developing new spectrum-sharing technologies would need to be defined, planned, and coordinated to ensure that research and costs are not duplicative.

Furthermore, spectrum sharing presents a complex set of R&D needs, and extensive field testing would likely be necessary to prove its feasibility in various operating environments, according to NIST and the Wireless Spectrum R&D Interagency Working Group. For example, performance characteristics at different frequency bands would need to be studied and understood because each spectrum band has its own nuance and therefore may need its own technological solution.

In addition, the feasibility of using spectrum-sharing technologies to free up spectrum is dependent on how heavily a given spectrum band is used. This is of particular concern in mid-band, according to FCC officials, where much of the spectrum is in use by incumbents, but may also affect higher frequency bands as they become more congested over time. Furthermore, as we recently reported, FCC has not clearly identified specific and measurable performance goals for managing spectrum demands for 5G, which may make it difficult to determine when and where it is appropriate to use spectrum-sharing technologies in the mid-band.[107]

Source: GAO. | GAO-21-26SP

[105] See NITRD, *Research and Development Priorities* and NIST, *Future Generation Wireless*.

[106] See Center for a New American Security, *Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy* (November 2019); National Security Commission on Artificial Intelligence, *First Quarter Recommendations* (March 2020); NIST, *Future Generation Wireless*.

[107] GAO-20-468.

Policy option: Coordinated cybersecurity monitoring

Policymakers could support nationwide, coordinated cybersecurity monitoring of 5G networks.

Potential opportunities

As discussed in chapter 3, as 5G networks develop and are deployed the security threat landscape will evolve and expand, exacerbating existing cybersecurity issues. To address this challenge, policymakers could support the development and implementation of a coordinated, nationwide monitoring program to continuously identify and manage cybersecurity risks. Such a program could help ensure the entire U.S. wireless ecosystem—including carriers, vendors, software developers, network administrators, and other stakeholders—stays knowledgeable about evolving cybersecurity threats, in close to real time, identify cybersecurity risks on a continuous basis, and allow stakeholders to act rapidly in response to emerging threats or actual network attacks.

To support the nationwide program, carriers could develop and implement a continuous network monitoring program aimed at ensuring that threats, attacks, or vulnerabilities are quickly identified and reported. These monitoring programs would provide assurance that network traffic is tracked, devices are monitored, and data are collected to help maintain network security. While the major U.S. carriers have some monitoring programs in place, these efforts may not be consistent in implementation.

A nationwide program could also include a centralized clearinghouse where carriers, vendors, government agencies, and other stakeholders would report cybersecurity incidents, threats, and other relevant information. These monitoring and reporting efforts could be assisted by automation and automated tools.[108] The program could include a transparent, open threat database that would allow all reporting entities—from small IoT device manufacturers to large carriers—to be on equal footing with regard to understanding the evolving threat landscape. This type of coordinated, centralized program could be modeled on existing efforts by entities such as within DHS's Cybersecurity and Infrastructure Security Agency, which plays a role in for sharing cybersecurity-related information with federal and nonfederal entities, or the Communications Information Sharing Analysis Center, a non-profit, member-driven organization formed by critical infrastructure owners and operators to share information between government and industry. The program could allow stakeholders to better coordinate responses to evolving threats, including preemptive countermeasures. In addition, the program could provide data and statistics to inform policymakers and help them understand the nature and scope of cybersecurity attacks from a broad perspective.

Potential considerations

Implementing continuous monitoring programs would have associated development and implementation costs for the carriers and others. The monitoring programs would also require an independent entity, either public or private, to certify or validate that the programs are meeting requirements.

A centralized, nationwide clearinghouse would require an independent body or government agency to administer it and to provide oversight and enforcement. A source of ongoing funding would need to be developed. If a federal agency were involved, questions of jurisdiction would need to be resolved, in part because the system would need to gather and share information. Carriers may not be comfortable reporting incidents or vulnerabilities, especially if that information could be shared with regulators and competitors.[109] In addition, carriers may not want to share what they consider proprietary information specific to their network operations. To address such concerns, determinations would need to be made about what information is to be disclosed, how the information will be used and reported, and how companies would be protected from liability associated with disclosing sensitive information.

Source: GAO. | GAO-21-26SP

[108] We recently reported on the use of automation for monitoring of federal government networks. See GAO*, Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-598 (Washington, D.C.: Aug. 18, 2020).

[109] FCC is the federal regulatory agency for communications, and it develops and administers policies and rules to advance the security and reliability of the nation's communications infrastructure. DHS is responsible for coordinating the federal effort to promote the security and resilience of the nation's critical infrastructure, which includes the communications sector, and serves as the lead agency for coordinating and prioritizing security and resiliency activities in the communications sector. See GAO, *Telecommunications: FCC Should Improve Monitoring of Industry Efforts to Strengthen Wireless Network Resiliency*, GAO-18-198 (Washington, D.C.: Dec. 12, 2017).

Policy option: Cybersecurity requirements

Policymakers could adopt cybersecurity requirements for 5G networks.

Potential opportunities

Adoption of specific requirements to enhance the security of 5G networks could help reduce cybersecurity risks and improve the performance and usage of 5G networks in the U.S. Specifically, policymakers could require (1) the implementation of specific cybersecurity standards and recommended practices for 5G networks, some of which already exist, and (2) the use of trusted network components and vendors.

A first step that could enhance cybersecurity of 5G networks would be requiring the implementation of specific cybersecurity standards by carriers and private networks, a step that some cybersecurity researchers have suggested. Without a baseline set of security requirements, the implementation of network security practices across the 5G network is more likely to be piecemeal and inconsistent. Instead, if requirements are developed and agreed on by a broad coalition of stakeholders and are built from specifications developed by standards bodies (e.g., 3GPP), best practices developed by government agencies (e.g., NIST), through efforts of the private sector (e.g., the carriers), or a combination of these, there may be an increased chance of broad stakeholder agreement and buy-in. In addition, using existing specifications or best practices and developing a best practices guide to assist with configuration and implementation may decrease the time and cost of implementing complex requirements. As discussed in chapter 3, NIST's National Cybersecurity Center of Excellence is developing a cybersecurity best practices guide, in part to help organizations increase their understanding of 5G standards-based security features. Furthermore, implementation of cybersecurity requirements could be flexible rather than designed as a one-size-fits-all approach to facilitate implementation. For example, some security practices could be mandatory only as needed to address a mission-critical concern.

A second step that could enhance cybersecurity is to ensure the use of trusted network components and vendors, as has been recommended by CISA, the Cyberspace Solarium Commission, and others.[110] Implementing a well-designed front-end validation and certification system for hardware and software vendors would give buyers a way to know which network components are trusted. Furthermore, requiring the use of trusted network components would help ensure that security is built into 5G networks rather than patched together on a piecemeal basis, making the entire network more secure, as outlined in the Cyberspace Solarium Commission report. Under such a system, 5G vendors and specific network equipment would be independently assessed, certified, and labeled as being acceptable for use in 5G networks in the U.S.

Potential considerations

These steps face challenges. Defining and implementing specific cybersecurity standards and recommended practices will be challenging because requirements will need to be defined on an application-specific basis rather than as a one-size-fits-all approach. Because of the sheer volume of specific applications, one official suggested that mission-critical parts of the network should be the focus, at least initially. In addition, the specific security controls will need to be continually updated as 5G systems develop and evolve and as network designs change, so this effort will need to take place continuously over time. Furthermore, outlining specific requirements is not the only step. Even if certain security controls are mandatory, they are often complex and will need to be properly configured, implemented, and managed. Accomplishing this would require best practice "how to" guides, which may be time-consuming and costly to develop.

In addition, adoption of cybersecurity requirements will impose costs, such as costs associated with additional network elements, added latency, and administrative overhead. Some smaller carriers and private enterprise network operators may not have the resources to fully implement new cybersecurity requirements, according to CSRIC. According to officials from a major carrier, security requirements can also have other negative consequences, such as stifling innovation. These officials stated that there is a need to balance any new security requirements with possible negative effects.

Setting up a system to certify network components would be costly and require a centralized entity to administer it. If such a system were voluntary and led by the private sector, it is unclear whether industry has the proper incentives to develop and implement such a system. Therefore, a system to certify network components may be best situated within a federal agency.

Source: GAO. | GAO-21-26SP

[110] CISA, *Critical Infrastructure Security and Resilience Note*. U.S. Cyberspace Solarium Commission.

Policy option: Privacy practices

Policymakers could adopt uniform privacy practices for 5G user data.

Potential opportunities

Adopting uniform privacy practices could help enhance protection of consumers' personal information. These practices would address (1) the collection, storage, and use of 5G user data and (2) uniform practices for informing users and obtaining their consent for the collection, storage, and use of such data. Policymakers could also choose to apply the practices to ensure the policy framework addresses other new technologies, such as biometric data collection.

Uniform practices could help consumers better understand the privacy of their data and inform their decisions on what information to provide. Such practices could help overcome the privacy concerns exacerbated by 5G networks and applications because they could reduce consumer uncertainty about data collection, use, and storage, and they could increase user control over their data, according to CTIA and the Federal Trade Commission.

In addition, policymakers could adapt existing privacy practices that have been implemented at the state level or in other countries, or those that have been developed by federal agencies or other organizations, as described in chapter 3. Uniform privacy practices, implemented nationally, could also forestall the need for further state-by-state efforts.

Potential considerations

Policymakers would need to balance the need for privacy with the direct and indirect costs of implementing privacy practices. Complying with privacy requirements can be burdensome, especially for smaller entities, because technology, legal, and personnel costs to do so can be extensive. Implementation of privacy requirements may need to be flexible because different entities collect and use data in different ways and because some technologies do not have the ability to easily inform users of how their data is used and get their consent. For example, it may be extremely difficult for manufacturers of smart devices, such as refrigerators and light bulbs, to get informed consent in the same way that carriers would do so because their devices may not have interfaces to communicate and secure consent from the user.

In addition, companies may not wish to disclose how they use data, as some uses may be business sensitive or proprietary. Furthermore, industry may argue that costly or burdensome privacy practices are not, on balance, needed.

It could also be challenging for policymakers to determine how to oversee and enforce the implementation of privacy practices. One option would be mandatory reporting requirements, which may forestall the need for significant added oversight, and could be a simple, flexible mechanism to maximize transparency and ensure consumers are more fully informed. Alternatively, policymakers could assign an oversight body the responsibility to enforce the adoption of privacy practices; currently, the Federal Trade Commission has broad enforcement authority to protect consumers from unfair and deceptive trade practices, which can include practices that affect consumer privacy and data security.[111] Any additional oversight or compliance mechanism would come with added cost.

As outlined in our 2019 report on internet privacy, it can be difficult to balance consumers' need for privacy—including ensuring users have control over their data and understand how such data is collected and used—with industry's ability to provide low-cost services, innovate, and customize user experiences.[112] Existing privacy principles, such as the FIPPs, are intended to achieve this balance. Regardless, comprehensive privacy practices may be difficult to design in a way that all interested parties would support.

Source: GAO. | GAO-21-26SP

[111] The common carrier exception in the Federal Trade Commission Act, codified in relevant part at 15 U.S.C. § 45(a)(2), however, prohibits the Federal Trade Commission from taking action against common carriers, such as providers of telecommunications services, which are generally regulated by the FCC under the Communications Act, codified in relevant part at 47 U.S.C. § 151 et seq.

[112] GAO-19-52.

Policy option: High-band research

Policymakers could promote R&D for high-band technology.

Potential opportunities

Policymakers could promote R&D of advanced high-band technology—including the properties of active antennas—to better understand and characterize signal propagation characteristics. Research into high-band technology could also help close the knowledge gaps and increase understanding of any possible health effects, including the effects of long-term exposure to high-band RF energy; characterizing exposure to highly directional beams and multiple antennas; and characterizing high-band exposure for high-risk populations, including pregnant women, and young children.

Antenna research in laboratory settings could result in improved statistical modeling of antenna characteristics and the generation of data to more accurately represent signal propagation, according to NIST.[113] These data could help optimize geographic placement in small-cell deployments and minimize interference, resulting in a more efficient use of spectrum. Understanding signal propagation and other characteristics of advanced antenna systems is critical for current high-band 5G antennas and will remain critical as future generations of wireless communications increasingly use high-band spectrum.

Policymakers could promote R&D of advanced high-band technology in multiple ways, including through grants to academic institutions, research performed by federal laboratories, public-private partnerships, or tax credits for industry. To better understand propagation characteristics and exposure levels in real-world settings, test beds may be necessary. Multiple 5G test beds are in operation, and it may be possible to use these existing sites with ongoing technology investments for field testing 5G high-band technology, according to NIST. For example, according to NTIA officials, NTIA operates an existing high-band test bed focused on propagation, spectrum, and noise measurements up to 110GHz, and expanding and enhancing such a test bed would prove far less costly than the establishment of a new test bed. As an added benefit, new test beds could also be used to test new 5G applications and use cases, which could, in turn, spur demand for new products and services. In addition, a thorough understanding of high-band transmission could benefit future wireless networks, which will operate in spectrum bands higher than those allocated for 5G.

Potential considerations

R&D can be costly, must be coordinated and administered, is generally considered a long-term investment, and its potential benefits are uncertain. Policymakers would need to identify a new funding source for research or determine which existing funding streams to reallocate. Similarly, funding development work at new test bed facilities would involve significant costs. On the other hand, adapting existing test bed facilities would not require a significant capital outlay, but may require significant coordination.

Complicating high-band technology research is the likelihood that each frequency band will have different characteristics that will need to be independently studied and understood, which will add to the cost of R&D. Propagation modeling and understanding exposure modalities are complex topics and will require significant testing and validation. Because the private sector is carrying out R&D of high-band technology, promoting additional research would require an understanding of ongoing research and coordination with the private sector to understand the proper role of government. The precise roles of government, the private sector, and academia would need to be assessed and understood, and it would take planning and coordination to assure that research is not duplicative. However, potential costs borne by any one actor could be reduced if multiple entities combined their resources.

Source: GAO. | GAO-21-26SP

[113] NIST, *Future Generation Wireless*.

Policy option: Status quo

Policymakers could maintain the status quo
(i.e., allow current efforts to proceed without intervention).

Potential opportunities

As 5G networks continue to evolve, some of the challenges identified in this report may be addressed without any intervention from policymakers. Governments and the cellular communications industry will continue to carry out 5G R&D, carriers will continue deploying 5G networks, and vendors will offer new 5G-enabled devices. The resources directed toward 5G networks and toward more advanced networks are difficult to quantify, and it is impossible to predict how 5G networks will evolve over the next decade. Without intervention, 5G network and technology development and deployment will continue, including R&D in laboratories, component and application testing at test beds, and network deployment across the U.S. If policymakers allow current efforts—public, private, and joint—time to solve the problems they are targeting, they could avoid spending additional time and money to address these challenges.

Potential considerations

Maintaining the status quo will likely not fully address the challenges identified in this report, and ongoing efforts to address these types of challenges may take longer and lack strategic focus. In addition, maintaining the status quo may contribute to other 5G challenges. For example, we identified challenges to 5G deployment in a recent report, and we have ongoing work into the national security risks related to 5G.[114] As 5G technologies and networks continue to evolve to enable more advanced cellular applications, policymakers must determine the extent to which this development is optimally led by private entities and market forces, or whether a more unifying, strategic direction is needed. Coordination and planning may be required to ensure that research is targeted appropriately and aimed at known knowledge gaps. If efforts lack strategic focus, addressing these key challenges may take longer or may not occur at all, putting the achievement of expected capabilities and uses of 5G networks in the U.S. at risk.

Source: GAO. | GAO-21-26SP

[114] GAO-20-468.

5 Agency comments

We provided a draft of this product to the Departments of Commerce, Energy, and Health and Human Services; DHS; DOD; FCC; and NSF for their review. DOD told us that they had no technical comments on the draft report; the remaining six agencies provided technical comments, which we incorporated as appropriate. Participants in our expert meeting from CTC Technology & Energy, CTIA, Google, Illinois Institute of Technology, National Consumer Law Center, Nokia—North and South America, PwC, University of Colorado, and U.S. Cellular also reviewed a draft of this product; we incorporated their technical comments as appropriate.

We are sending copies of this report to the appropriate congressional committees and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov/.

If you or your staff have any questions about this report, please contact Hai Tran at (202) 512-6888 or tranh@gao.gov or Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

Hai Tran

Hai Tran
Senior Level Technologist
Science, Technology Assessment,
and Analytics

Vijay A. D'Souza

Vijay A. D'Souza
Director
Information Technology and Cybersecurity

List of Requesters

The Honorable James M. Inhofe
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Marco Rubio
Acting Chairman
The Honorable Mark R. Warner
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Eddie Bernice Johnson
Chairwoman
Committee on Science, Space, and
Technology
House of Representatives

The Honorable Adam B. Schiff
Chairman
The Honorable Devin Nunes
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

The Honorable Bill Foster
Chairman
Subcommittee on Investigations and
Oversight
Committee on Science, Space, and
Technology
House of Representatives

The Honorable Richard Burr
United States Senate

The Honorable Mikie Sherrill
House of Representatives

Appendix I: Objectives, scope, and methodology

In view of the anticipated worldwide deployment of 5G networks, you asked us to assess the technologies associated with 5G, as well as expected economic and social impacts. This report discusses:

1. how the performance goals and expected uses are to be realized in U.S. 5G wireless networks;
2. the challenges that could affect the performance or usage of 5G wireless networks in the U.S.; and
3. policy options to address these challenges.

To address these objectives, we met with officials from selected federal agencies and entities involved with the development or impacts of 5G networks. These agencies were:

- Air Force Research Laboratory, Department of Defense (DOD),
- Cybersecurity and Infrastructure Security Agency, Department of Homeland Security (DHS),
- Defense Advanced Research Projects Agency, DOD,
- Federal Communications Commission (FCC),
- Food and Drug Administration (FDA), Department of Health and Human Services,
- Idaho National Laboratory, Department of Energy,
- National Institutes of Health, Department of Health and Human Services,
- National Institute of Standards and Technology (NIST), Department of Commerce,
- National Oceanic and Atmospheric Administration, Department of Commerce,
- National Science Foundation (NSF),
- National Telecommunications and Information Administration (NTIA), Department of Commerce,
- Networking and Information Technology Research and Development Program, White House Office of Science and Technology Policy,
- Office of the Secretary of Defense, DOD, and
- Science and Technology Directorate, DHS.

In addition, we interviewed representatives from five 5G equipment or component vendors, which included some of the largest companies by industry revenue.[115] We also

[115] We interviewed representatives from some of the largest firms by industry revenue in the communications components and systems sub-sectors, as identified using Bloomberg data: Samsung Electronics America, Inc.; QUALCOMM Incorporated; Nokia Corporation; Telefonaktiebolaget LM Ericsson; and Broadcom Inc.

interviewed representatives from the four largest U.S. wireless carriers (Verizon Communications Inc., Sprint Corporation, T-Mobile US, Inc., and AT&T Inc.); an industry trade organization (5G Americas); small businesses (Celona, Inc., Edge Compute, Inc., Prime Lime Consulting, and Wickr); standards bodies (the Institute of Electrical and Electronics Engineers and the Alliance for Telecommunications Industry Solutions); and policy organizations (Electronic Frontier Foundation and R Street Institute).[116] Additionally, we met with four university wireless research programs and toured one of them.[117] Furthermore, we met with the study chairman of the Defense Science Board Quick Task Force on Defense Applications of 5G Network Technology.[118] During our interviews with officials and representatives, we discussed topics such as 5G performance goals; 5G applications; the status of key technologies that will enable the performance or usage of 5G networks; challenges to the performance or usage of 5G in the U.S.; and options to address these challenges.

To identify and understand challenges that may affect the performance and expected usage of 5G networks in the U.S., we discussed the challenges to the performance or usage of 5G in the U.S. with officials from FCC, NTIA, NIST, NSF, DOD, Department of Energy, and DHS. We also convened a one-and-a-half day meeting of 17 experts from academia, industry, and consumer groups to discuss challenges and potential actions the federal government could take to address those challenges. We selected these experts with assistance from the National Academies of Sciences, Engineering, and Medicine to obtain a range of perspectives on 5G deployment.[119] We also conducted a broad-based literature review using articles and reports identified in the following three ways:

1. searches of databases using Scopus, IEEE Xplore, and Google Scholar;
2. interviews with agency officials, U.S. cellular carriers, and other communications industry stakeholders; and
3. references in literature.

For the literature search, we used terms including 5G and performance, framework, network design, policy, or governance. We refined our search terms and used the same three databases with additional search terms including edge computing, radio access

[116] Sprint Corporation merged with T-Mobile US, Inc. on April 1, 2020, and the merged company is known as T-Mobile. At the time of our interviews they were separate companies.

[117] We interviewed officials from NYU WIRELESS, the Cloud Enhanced Open Software-Defined Mobile Wireless Testbed, a collaboration among Rutgers University, Columbia University, and New York University; the Platform for Open Wireless Data-driven Experimental Research, a collaboration between the University of Utah and Rice University; the Aerial Experimentation and Research Platform for Advanced Wireless, a partnership led by North Carolina State University.

[118] Defense Science Board, *Defense Science Board Task Force: Defense Applications of 5G Network Technology* (Washington, D.C.: June 24, 2019).

[119] We planned and convened this expert meeting in collaboration with our report on 5G deployment, GAO-20-468, and with the assistance of the National Academies of Sciences, Engineering, and Medicine to better ensure that a breadth of expertise was brought to bear in its preparation; however, all final decisions regarding meeting substance and expert participation were the responsibility of GAO. Any conclusions and recommendations in GAO reports are solely those of GAO. For details on the shared methodology for a questionnaire on 5G deployment sent to 146 stakeholders, which we identified as having knowledge of 5G networks, and expert meeting, including a list of meeting participants, see GAO-20-468, pp. 28–30.

network, network slicing, New Radio, millimeter wave, and cyber. We filtered the search by the highest cited authors and studies published since 2016. We reviewed reports on 5G and its broader impacts, including industry white papers and technical reports, such as the IEEE Future Networks technology road maps. To understand the health effects of wireless technology, we interviewed officials from the Department of Health and Human Services, the National Council on Radiation Protection and Measurements, and the World Health Organization; reviewed safety standards; and reviewed assessments published by DOD, FDA, and the National Institutes of Health. We also requested and reviewed a DOD bibliography of peer-reviewed articles, technical notes, technical reports, and special reports published in fiscal years 1997 through 2019 on the physiological effects of microwave or millimeter wave energy.

We formulated policy options around the policy objective of achieving expected capabilities and uses of 5G networks in the U.S. To develop the policy options, we conducted a literature review of articles and reports using Scopus, IEEE Spectrum, Harvard Kennedy School's Think Tank Search, and Google Scholar. We used search terms including 5G and federal government, public administration, public sector, policy, decision, risk, or spectrum management. We gathered and assessed policy ideas from our literature review of the policy implications of 5G; interviews with agencies, industry, and researchers; the results from a brief questionnaire on challenges to 5G deployment sent to 146 stakeholders that we identified as having knowledge of 5G networks; and the National Academies of Sciences, Engineering, and Medicine expert meeting mentioned above. After identifying a preliminary list of policy options, we analyzed these options to eliminate those deemed to be beyond the scope of the assessment, its policy objective statement, and our reporting objectives. We removed ideas that were not likely to achieve the policy objective or did not fit into the overall scope of our work. For example, we removed policy ideas related to FCC's role in spectrum allocation because those issues were within the scope of a related GAO engagement. We grouped the remaining ideas based on themes related to our identified challenges. We analyzed each policy option by identifying and discussing potential benefits and considerations of implementing them. The policy options and analyses were supported by documentary and testimonial evidence from sources including the literature review, industry white papers, the 5G expert meeting, and interviews with 5G stakeholders.

We conducted our work from June 2019 to November 2020 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to technology assessments. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations to our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

Appendix II: GAO contacts and staff acknowledgments

GAO contacts

Hai Tran, (202) 512-6888 or tranh@gao.gov

Vijay A. D'Souza, (202) 512-6240 or dsouzav@gao.gov

Staff acknowledgments

In addition to the contacts named above, Richard Hung (Assistant Director), Neela Lakhmani (Assistant Director), Jonathan Felbinger (Analyst in Charge), Saar Dagani, Matt Hunter, Mike Krafve, Bruce Rackliff, Ben Shouse, Andrew Stavisky, Sirin Yaemsiri, and AJ Yohn made key contributions to this report. Chris Businsky, Wayne Emilien, Nancy Glover, Elma Hajric, Patrick Harner, Kaelin Kuhn, Dan Luo, Lisa Maine, Anika McMillon, and John Pham also contributed to this report.

(103593)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact: Website: https://www.gao.gov/fraudnet/fraudnet.htm
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, YoungC1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

Strategic Planning and External Liaison

Stephen Sanford, Acting Managing Director, spel@gao.gov, (202) 512-9715
U.S. Government Accountability Office, 441 G Street NW, Room 7B37N, Washington, DC 20548