GSA®

U.S. General Services Administration

Acquisition Guidance for Procuring 5G Technology

Executive Summary

Acquisition Guidance for Procuring 5G Technology

Fifth generation (5G) wireless technology will be a primary driver of our nation's prosperity and security in the 21st century. "5G" is a shorthand term referring to the 5th generation cellular mobile network. It succeeds the 4G (LTE-A, WiMax), 3G (UMTS, LTE), and 2G (GSM) systems. The Secure 5G and Beyond Act of 2020 and the resulting National Strategy to Secure 5G detail how the United States will lead global development, deployment, and management of secure and reliable 5G infrastructure. As a part of this effort, GSA was directed to "establish government acquisition guidance for acquiring secure, open, interoperable advanced wireless systems and applications."

This document is a further evolution of the initial paper. It aims to provide government agencies basic information and guidance they need to procure 5G technology with appropriate security for government use cases.

There is an abundance of publicly available information about 5G technology. There are well-established reference sources and guidance for federal IT security, such as National Institute of Standards and Technology (NIST) documents, and ongoing efforts to specifically address cybersecurity for 5G. There are regulations and extensive, general guidance for federal acquisition. The Acquisition Guidance for Procuring 5G Technology fills the intersection of these three areas: technology, cybersecurity, and acquisition. It provides a primer on the 5G technology, references the most-relevant cybersecurity guidance, and describes acquisition considerations specific to 5G-related projects. The guidance is designed to help agencies identify their standards, security controls, and other requirements to provide a secure infrastructure for 5G-enabled technologies. This effort is also intended to reduce cost and eliminate acquisition redundancies. It is written in plain language and will be updated regularly as the technology matures.

The primary intended audience is the acquisition integrated project team (IPT) for an agency planning or performing a 5G-related project. This includes federal IT managers, procurement officers, and contracting officers. Agency executives may also find it valuable as an overview of the technology and key considerations. Although intended primarily for government readers, industry partners such as IT service providers, vendors, and manufacturers may also find the guidance useful for anticipating requirements in specific agency solicitations.

5G technology will improve mission delivery and business operations for government agencies. It offers faster performance and more capabilities, particularly for data-driven applications and machine-to-machine communication. Use cases include fixed wireless access, healthcare and medical, asset tracking, vehicle-to-vehicle communications, augmented and virtual reality, remote control of unmanned vehicles, and many others. Compared to earlier generations of wireless technology, 5G's features are highly customizable for specific applications. However, delivering 5G's capabilities requires significant changes to mobile communication systems. These changes can introduce security vulnerabilities and expand the attack surface. Security must be a major consideration for any acquisition and the appropriate requirements included. Supply Chain Risk Management (SCRM) and avoiding the prohibited sources specified by Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232) are important, related considerations.

The acquisition process for 5G technology is essentially the same as for other complex information technology. There may be 5G-specific architectural and performance requirements. These could include requirements for user equipment, the radio access network, the 5G core, and related services. Technical performance requirements could include those
for radio performance, such as coverage area, and spectrum utilization, among others.

Agencies can procure 5G technology through Other Transaction Authorities (OTAs), commercial contracts (FAR Part 12), or non-commercial negotiated acquisitions (FAR Part 15), depending on the agency's specific requirements and authorities. Several

OMB-designated Best-in-Class (BIC) contract vehicles allow for secure 5G services within their scope. BIC contracts provide a preferred governmentwide solution. Those relevant to 5G include:

- GSA Enterprise Infrastructure Solutions (EIS): **https://www.gsa.gov/technology/technology-purchasing-programs/telecommunications-and-network-services/enterprise-infrastructure-solutions**

- GSA Multiple Award Schedule (MAS) Wireless Mobility Solutions SIN 517312: **https://www.gsa.gov/technology/technology-purchasing-programs/mas-information-technology/sins-and-solutions-we-offer/wireless-mobility-solutions-sin-517312**

- GSA 2nd Generation IT Blanket Purchase Agreements (2GIT; equipment-only requirements): **https://www.gsa.gov/technology/technology-purchasing-programs/mas-information-technology/buy-from-mas-information-technology/2nd-generation-it-blanket-purchase-agreements**

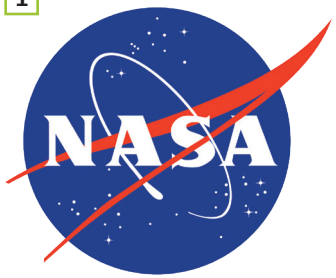
- NASA Solutions for Enterprise-Wide Procurement (SEWP): **https://www.sewp.nasa.gov**

- NITAAC Chief Information Officer – Commodities and Solutions (CIO-CS): **https://nitaac.nih.gov/gwacs/cio-cs**

Table of Contents

Acknowledgments

Contributing Departments, Agencies, and Organizations

1 

2 

3 

4 

5 

6 

7 

8 

9 

1. National Aeronautics and Space Administration
2. U.S. Department of Commerce, National Telecommunications and Information Administration
3. U.S. Department of Defense, Office of the Chief Information Officer
4. U.S. Air Force
5. U.S. Marine Corps
6. U.S. Navy
7. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency
8. U.S. Department of State
9. U.S. General Services Administration

Purpose and Scope

Fifth generation (5G) wireless technology will improve mission delivery and business operations for government agencies. 5G brings new applications and services to the federal workforce that older technology did not support.

5G offers faster performance and more capabilities, particularly for data-driven applications and machine-to-machine communication. These capabilities form the foundation for large networks that use sensors and machines, expanding the mobile networks' size and reliability. Compared to earlier generations of wireless technology, 5G's features are highly customizable for specific applications.

Acquiring secure 5G solutions is key to ensuring federal networks stay safe and resilient.

Delivering 5G's capabilities requires significant changes to mobile communication systems. These changes can introduce security vulnerabilities and expand the attack surface. They also provide opportunities for malicious actors who seek to:

- Illicitly obtain and use federal information
- Defraud government programs
- Disrupt operations

Such actions threaten how government agencies deliver essential services to the American people. Agencies considering buying 5G must also consider 5G's security risks when:

- Developing procurement packages
- Issuing solicitations
- Evaluating vendors
- Issuing awards

By following these best practices, incorporating them where appropriate into the procurement process, and effectively managing trusted vendors, the U.S. government can strengthen the security and resilience of its 5G networks and endpoints.

This document gives agencies the information and guidance they need to procure 5G technology with appropriate security for government use cases.

According to the Secure 5G and Beyond Act of 2020, Pub. L. 116-129 (03/23/2020), the executive branch developed a comprehensive implementation plan associated with the National Strategy to Secure 5G. Program offices and contracting activities must look for new approaches for communication systems, including advanced 5G features, to use to assess the acquisition risk. As new technologies and approaches arise, agencies need to judge whether they are good fits for their needs.

This guidance also gives agency leaders the strategies and tools to:

- Improve their security posture
- Reduce overall risk
- Support rapid delivery of 5G solutions

Given this broad scope and rapidly advancing technology, this document will not provide comprehensive guidance concerning requirement development but will rather serve as a common foundation and reference for a wide audience.

Background

What is 5G?

This section explains the historical factors and technical components that enable 5G capabilities. To help the reader, certain terms are accompanied by URLs to their definitions in the glossary that the Computer Security Resource Center of the National Institute of Standards and Technology (NIST) maintains.

"5G" is a shorthand term referring to the 5th generation cellular mobile network. It succeeds the 4G (LTE-A, WiMax), 3G (UMTS, LTE), and 2G (GSM) systems. 5G performance targets include:

- High data rate
- Reduced latency
- Energy saving
- Cost reduction
- Higher system capacity
- Massive device connectivity within a specific coverage area

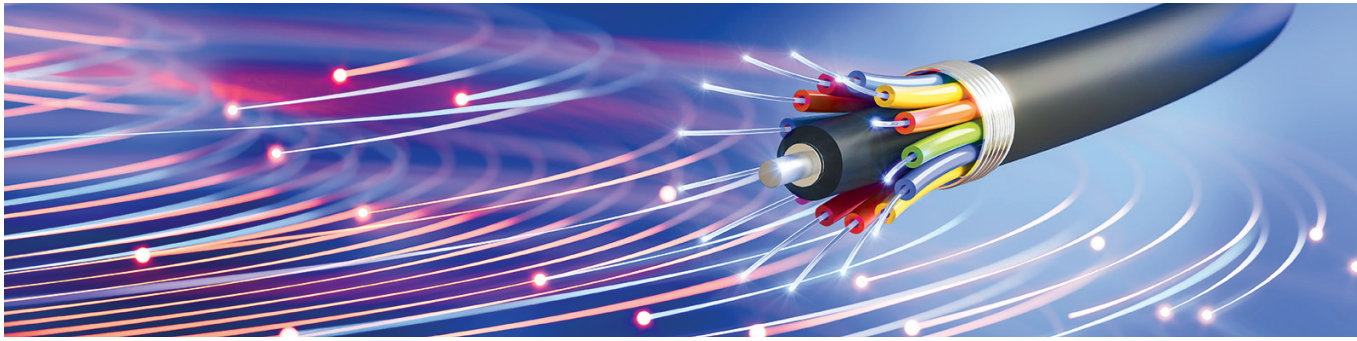
5G is a global standard set by the 3rd Generation Partnership Project (3GPP), a consortium of organizations that develop mobile telecommunications protocols structured as numbered releases.

- The first 5G standard was Release-15 in mid-2018.
- 3GPP completed Release-16 specifications in 2020 to accommodate early commercial deployment.
- Release-17 was completed in late 2022.
- Release-18 is also in development.

Release-16 was adopted by the International Telecommunication Union (ITU) as a candidate for its 5G standard, IMT-2020. The ITU IMT-2020 specification demands speeds up to 20 Gbps achievable with wide channel bandwidths and massive multiple input, multiple output (MIMO) architectures.

Most U.S. nationwide carriers currently use Release-15 but are expected to deploy Release-16 features into their networks.

5G networks are digital cellular networks composed of a patchwork of cells within a larger service area covered by one or more providers. Mobile devices in a cell communicate by radio waves with a local antenna array containing a low-power automated transceiver. The transceiver assigns channels from a common pool of frequencies reused in geographically separated cells. The local antennas are connected with the telephone network and the internet by a high bandwidth optical fiber or a wireless backhaul connection. When a user crosses from one cell to another, their mobile device is automatically handed off seamlessly to the antenna in the new cell.



Advantages of 5G

One of the major advantages of 5G is that 5G networks have:

- Much higher specified peak data rates than previous cellular networks
- Multiple Gbps, which is faster than current cable internet and many times faster than earlier cellular technology

Because of the higher data rates, 5G networks will serve not just cellphones but could also provide a general home and office networking solution, competing with wired internet providers. Previous cellular networks provided low data rate internet access suitable for cell phones, but a cell tower could not economically provide enough bandwidth to serve as a general internet provider for home computers.

Similarly, 5G may also complement or replace Wi-Fi in some scenarios.

Higher Frequency Radio Waves

5G networks achieve these higher data rates by using higher-frequency radio waves in or near the millimeter wave band around 28 and 39 GHz. Previous cellular networks used frequencies in the microwave band between 700 MHz and 3 GHz.

5G providers also use a second lower frequency range in the microwave band, below 6 GHz, but this will not have the high speeds of the new frequencies. Orthogonal frequency division multiplexing (OFDM) modulation is used, in which multiple carrier waves are transmitted in the frequency channel, so multiple bits of information are transferred at the same time.

Gasses absorb millimeter waves in the atmosphere, are less tolerant of diffraction and deflection, and have a shorter range than microwaves. Therefore, the size of the cells is smaller.

5G cells will be the size of a city block, unlike the cells of previous cellular networks, which could be many miles across. Due to their shorter wavelengths, millimeter waves also have trouble passing through solid objects such as the walls of buildings, requiring multiple antennas to cover a cell.

Optimizing the Network

5G technologies will enable a range of advanced techniques to optimize the performance of mobile devices and their networks. Millimeter wave antennas are much smaller than those used in previous cellular networks, measuring only a few inches long.

Instead of relying on a single cell tower, 5G cells will be covered by many antennas, mounted on objects such as telephone poles and buildings. One technique that will be used to increase the data rate in 5G cells is using massive MIMO antennas.

Instead of relying on a single signal to transfer data to and from a device, 5G technology will transfer data through multiple signals. Each cell will have multiple antennas communicating with the wireless device, each over a separate frequency channel, received by multiple antennas in the device. Thus, multiple bitstrings of data will be transmitted simultaneously, in parallel.

Another technique called "beamforming" will provide targeted coverage when and where it is needed. In beamforming, a base-station computer continuously calculates the best route for radio waves to reach each wireless device and organizes multiple antennas to work together as a phased array. This creates a beam of millimeter waves that can be electronically steered to devices lacking coverage.

Drawbacks

5G technologies have drawbacks as well. The smaller, more-numerous millimeter wave cells make 5G network infrastructure more expensive to build per square kilometer of coverage than previous cellular networks. 5G deployment is currently limited to cities that have enough users per cell to provide an adequate return on investment.

Architecture

In a non-stand-alone architecture, commonly used by wireless carriers in their initial deployments, the 5G-capable device can connect to a 4G LTE antenna and a 5G antenna, where available. Both routes would connect to a 4G Evolved Packet Core architecture.

In a stand-alone architecture, once deployed by carriers, the devices will connect to a 5G antenna and 5G core network, thereby increasing the data-rate dramatically.

Non-stand-alone architecture enables a smooth application transition from 4G LTE to 5G New Radio (NR). Stand-alone architecture enables newer services such as network slicing and private routing.

Emerging Technologies

The high data rate and low latency of 5G will power many applications and unlock several emerging technologies soon:

- Practical virtual
- Augmented reality
- Fast machine-to-machine (M2M) interaction in the Internet of Things (IoT)

There are a few key differences between the legacy 4G technologies and future 5G technologies:

- First is the virtualization and containerization of the 5G core. This method allows for more flexibility and efficiencies in how the core can be deployed, reducing how much computational power is required to support it.

Stand-alone architecture enables newer services such as network slicing and private routing.

- Second is the separation of the control plane, which carries signal traffic, and the user plane, which carries network user traffic.
  - This new architecture allows the user plane traffic to be locally routed, localizing and privatizing the traffic. This new network configuration reduces latency and jitter. It also moves the application closer to the network's edge, enabling use cases such as augmented and virtual reality (AR/VR), the tactile Internet, and autonomous systems.
- Third is the potential widespread adoption of what is typically referred to as a private cellular network (PCN), which includes a private SIM and a private core.
- This new type of network architecture was further enhanced when Citizens Broadband Radio Spectrum (CBRS) was introduced. CBRS is a band of spectrum available for anyone to use. As a result, any agency can now create a PCN. PCNs give an agency a high degree of control over how its devices, applications, and solutions are deployed, secured, and supported.

Securing 5G

While the deployment of 5G presents new opportunities for better services, agencies need to consider several risks. Secure 5G implementation requires planning for resilience at the design phase and mitigating network exposure to untrustworthy elements.

The Cybersecurity and Infrastructure Security Agency (CISA), in coordination with the National Security Agency (NSA) and the Office of the Director of National Intelligence, sees five dangers:

1 Threat actors may try to influence 5G networks' design and architectures.

5G will use more information and communication technology components than previous generations of wireless networks. Municipalities, companies, and organizations building their PCNs will at the same time increase their own network vulnerabilities.

Improperly deployed, configured, or managed 5G systems are more vulnerable to disruption and manipulation.

2 The 5G supply chain is vulnerable to threats whether due to malice or accident.

The presence of more components increases the complexity of 5G systems. It also complicates the supply chains that produce them. A 5G supply chain is vulnerable to the malicious or unintentional introduction of risks such as malicious software and hardware, possibly through counterfeit components. Poor designs, manufacturing processes, and maintenance procedures also contribute to these risks.

Open Radio Access Network (O-RAN), defined further on page 17, is one 5G architecture that is expected to be increasingly adopted. It allows multiple new smaller vendors implementing O-RAN-compliant standards.

This has benefits, but it also could introduce a new set of supply-chain vulnerabilities. 5G hardware, software, and services provided by untrusted entities could compromise network assets. A compromised network may damage data confidentiality, integrity, and availability.

3 Current 5G deployments that use legacy infrastructure and untrusted components with known vulnerabilities.

5G builds upon previous generations of wireless networks. It is currently being integrated with 4G LTE networks. These older elements may contain vulnerabilities that the new 5G systems risk inheriting. Legacy vulnerabilities of this type include:

- Exfiltration risks
- Distributed denial-of-service attacks
- Signaling System 7/Diameter challenges

Some legacy vulnerabilities, accidental or maliciously inserted by untrusted suppliers, may affect 5G equipment and networks despite integrating more security enhancements.

4 Limited competition in key segments of the 5G marketplace results in more proprietary solutions from untrusted vendors being utilized by 5G providers.

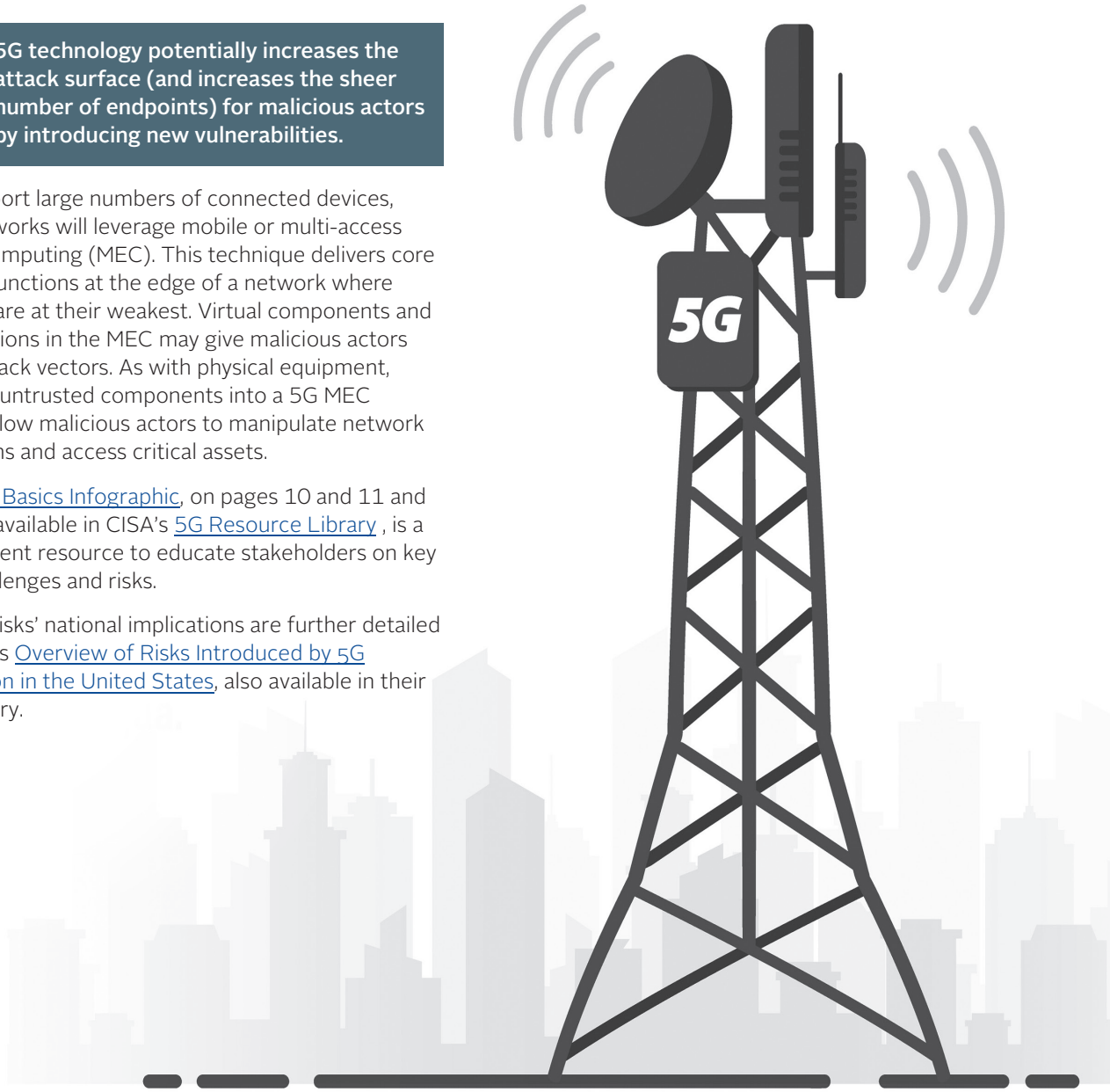
Despite developing standards designed to encourage interoperability, some companies, such as Huawei, build proprietary interfaces into their technologies. This limits customers' choices to use alternative equipment. If their products won't work with other technologies and services, trusted companies can't compete in the 5G market.

5 5G technology potentially increases the attack surface (and increases the sheer number of endpoints) for malicious actors by introducing new vulnerabilities.

To support large numbers of connected devices, 5G networks will leverage mobile or multi-access edge computing (MEC). This technique delivers core traffic functions at the edge of a network where signals are at their weakest. Virtual components and applications in the MEC may give malicious actors new attack vectors. As with physical equipment, putting untrusted components into a 5G MEC could allow malicious actors to manipulate network functions and access critical assets.

The 5G Basics Infographic, on pages 10 and 11 and readily available in CISA's 5G Resource Library , is a convenient resource to educate stakeholders on key 5G challenges and risks.

Those risks' national implications are further detailed in CISA's Overview of Risks Introduced by 5G Adoption in the United States, also available in their 5G library.

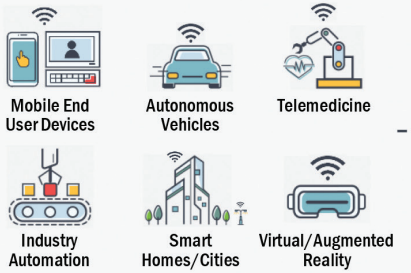


5G: The Basics

What is 5G?

The fifth generation (5G) of wireless technology represents a complete transformation of telecommunication networks, introducing a wealth of benefits that will pave the way for new capabilities and support connectivity for applications like smart cities, autonomous vehicles, remote healthcare, and much more. Here's how it will work:

USE CASES



5G networks will enable the connection for billions of new devices, sensors, and systems that will intelligently connect to the network, based on their time sensitivity and computational needs.

RADIO ACCESS NETWORK (RAN)

Small Cells

Macro Towers

5G networks will leverage low-, mid-, and high-band spectrum, requiring the deployment of smalls cells in addition to macro towers. These small cells will serve as signal repeaters, providing improved speed, greater network capacity, and stronger reliability in high-density areas.

Baseband Unit (BBU) Pool

The centralized BBU Pool implements software-defined networking and multi-access edge computing to allocate the network, based on need and connects to remote radio units located on macro towers through mobile fronthaul (optical fiber).

CORE NETWORK

Core Network Infrastructure

The Core Network is the backbone of the U.S. communications infrastructure that routes data and connects the different parts of the access network.

How does 5G compare to 4G?

5G promises an array of enhancements, providing higher data rates (extremely fast download speeds), ultra-low latency (near real-time interactivity), and increased network capacity (allowing for the connectivity of many more devices at once).

100x

Faster Download Speeds

While a 3GB movie would take 40 minutes to download on 4G, it would take only 35 seconds on a 5G network.

10x

Decrease in Latency

Data response times will be as low as 1 millisecond, providing endless possibilities from remote surgery to self-driving cars.

100x

Network Capacity

5G promises greater traffic capacity, allowing for millions of devices to be connected on the same network within a small area.

What are the risks?

The Cybersecurity and Infrastructure Security Agency (CISA) leads 5G risk management efforts to ensure that the U.S. can fully benefit from all the advantages 5G connectivity promises to bring. The following risks depict some of the focus areas that CISA is examining as part of this effort.

Susceptibility of the 5G supply chain, due to the malicious or inadvertent introduction of vulnerabilities

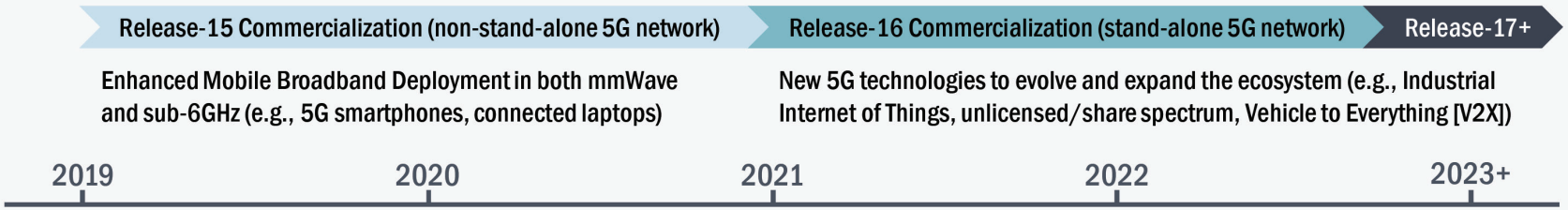
Initial 5G deployments leveraging legacy infrastructure and untrusted components with known vulnerabilities

Limited competition in the 5G marketplace resulting in more proprietary solutions from untrusted vendors

5G technology potentially increasing the attack surface for malicious actors to introduce new vulnerabilities

When will 5G be available?

The 3rd Generation Partnership Project (3GPP), a telecommunications standards organization, develops a series of *Releases* that provide developers with a stable platform for the implementation of cellular telecommunications features. Releases 15, 16, and 17 focus on 5G features.



Source: Yost, S. (2019). "Should We Even Be Talking About 6G?" Semiconductor Engineering. https://semiengineering.com/should-we-even-be-talking-about-6g/. Accessed on March 2, 2020.

For more information, visit www.cisa.gov/5g.

Standards

As noted in Section II, the 3GPP establishes standards that provide a complete system description for mobile telecommunications. A list of all 5G-related 3GPP specifications (including core network and system aspects) is provided in Specification 3GPP TR 21.205 or by searching the 5G Specification Set at the 3GPP website.

Key specifications include:

- Radio-related specifications addressing only NR: 38 series specifications (**https://www.3gpp.org/DynaReport/38-series.htm**)
- Radio-related specifications addressing only LTE: 36 series specifications (**https://www.3gpp.org/dynareport?code=36-series.htm**)
- Radio-related specifications addressing aspects affecting both LTE and NR: 37 series specifications (**https://www.3gpp.org/dynareport?code=37-series.htm**)
- Service requirements for next-generation new services and markets: 3GPP TS 22.261 (**https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107**)
- System Architecture for the 5G system (stage 2): 3GPP TS 23.501 (**https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144**)
- Procedures for the 5G System (stage 2): 3GPP TS 23.502 (**https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145**)
- NR; NR and NG-RAN Overall Description (stage 2): 3GPP TS 38.300 (**https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3191**)
- NR; Multi-connectivity; Overall description (stage 2): 3GPP TS 37.340 (**https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3198**)
- NG-RAN; Architecture description: 3GPP TS 38.401 (**https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3219**)

Examples of Government 5G Use Cases

In addition to the commonly conceived use case of smartphone connectivity, 5G is expected to enable a wide range of use cases and IoT applications. While many use cases are already possible with other wireless technologies – such as Bluetooth, Wi-Fi 6.0, LoRa, and 4G – 5G technology magnifies their potential. Some use cases require the higher data rate, lower latency, or the ability to connect many more devices in a small area that 5G provides.

For example, the Department of Defense (DOD) is developing 5G military tactical requirements. DOD invests heavily in smart warehouses, dynamic spectrum sharing, and AR/VR for military use. In addition to the military use, there are other use cases for 5G that apply to the government.

5G Service Provider

- Fixed Wireless Access
- Healthcare and medical
- Internet of Things – asset tracking, remote monitoring
- Mission-critical emergency services and public-safety networks
- Public-utility power management
- Sensors
- Ship-to-shore
- Smart base
- Smart city
- Traffic control
- Vehicle-to-vehicle

5G Enterprise Systems

- Augmented and virtual reality
- High-precision supervisory control and data acquisition
- High-speed telemetry from tethered government systems
- Intelligent video
- Local area network (LAN) and cable replacement
- Remote control of unmanned vehicles

Federal Mobility Group

The Federal Mobility Group (FMG) worked with several federal agencies and collected more examples of federal 5G use-cases in the Framework to Conduct 5G Testing (Section 3.1):

Contracting for 5G: Tools and Strategies

Acquisition Process

Determine Application Requirements, Purpose, and Connectivity

Before you take any action, determine your requirements. Pay particular attention to:

- Bandwidth
- Application-specific security
- Latency, the time delay in processing data packets
- Jitter, the amount of inconsistency in latency across the network
- Location or locations where the application needs to run

Does the application need to work locally on the private network, or must it be able to roam and work domestically and abroad? Private networks allow a device to work only while on the LAN. They will not permit roaming outside their cellular network unless an agreement is in place with one or more public mobile network operators.

Use Cases

5G technologies will power a wide ecosystem of devices and services. Once you have identified your requirements, review the use cases you want to address next.

A "use case" is any instance in which the enhanced capabilities of 5G will be used to support a given need and the circumstances surrounding that deployment. As with requirements, the location of a use case will determine its ultimate architecture.

First, decide whether the 5G will reside on a private network, a public network, or both.

Network Connectivity

Network connectivity introduces cybersecurity risks. The purpose and type of connection determine the appropriate security controls to use.

Describe the following:

- Access purpose, including network performance requirements such as:
  - Throughput
  - Latency
  - Signal-to-noise ratio
  - Potential risk
- Connections, not limited to persistent connections over airwaves but may also include the possible sharing of data between mobile devices and network connected systems
- Life-cycle-based approach to ensure security controls are in place before activating and effective during operational use

Acquisition Planning and Requirements Development

Request a detailed description of the requirements from the agency requirements developer. That description must include who, what, when, where, why, and how to ensure that a device that fully meets the use case and location considerations previously described is requested.

For security reasons, you will need to limit connectivity. If you require the ability to turn off or limit connectivity, the device should still function, or at least function enough to fulfill your needs.

Next, develop appropriate security and privacy requirements. The acquisition must include any required service. If the use case involves sensitive or protected privacy information, these security and privacy requirements must conform to your internal policies or applicable legal or regulatory requirements.

A "use case" is any instance in which the enhanced capabilities of 5G will be used to support a given need and the circumstances surrounding that deployment.

You or your providing vendor must be able to patch devices to protect against identified vulnerabilities. If you use a patching service available through a vendor or manufacturer, compare that service to the expected life cycle of the overall use case.

Thus, you must specify the estimated timespan of patching services that you will need. You must also decide whether patches require an intermediary, such as a mobile service provider, that could delay delivery.

The vendor deliverables must include a security development life cycle, showing that you considered security from design to end of life for the technology. That consideration must include providing standard processes.

Including vulnerability-disclosure programs in the requirements enables a clear way for external researchers to make the vendor or servicer of the device aware of possible vulnerabilities. It also provides a means for the vendor to self-report vulnerabilities. Address fail-safe mechanisms in the requirements if they apply. They provide important backstops if a security incident occurs, as the system's design can prevent or reduce the severity of any unsafe consequences of its failure.

Next, you or your agency's requirements developer must document whether a Supply Chain Risk Management (SCRM) program is necessary. SCRM programs feature technologies used in sensitive areas or situations involving access to sensitive data.

Authentication

Authentication (you are who you say you are) and access (you are authorized to view or do something) are important aspects of keeping technology manageable and secure. Your requirements documentation must include integrating authentication and access into the user's infrastructure, management, and operational practices.

In addition to authenticating devices based on 3GPP protocols, you may want to authorize the devices to specific services. For example, a device will authenticate if the SIM is valid, but should that device be allowed access to specific services such as drone control? The private 5G network could also be configured to authorize access before it authorizes an application.

Encryption

Encryption is a common way of securing data. You can apply it at the device level for data "at rest" and "in transit" when data is being communicated over networks. Depending on the device's risk profile and the data's sensitivity, your agency's requirements developer may need to include encryption requirements.

Lastly, include an up-to-date device registry or log the requirements package. Such a resource must include devices' firmware and software, as well as their types and versions. This will help your agency rapidly and appropriately respond to a security incident. Procurements that feature devices, such as an IoT deployment, must include these. Specifications for devices must also include physical security controls per applicable policy.

Solicitation Development and Contract Award

Your agency's solicitation documents must include the requirements and source-selection criteria in the solicitation.

Solicitation

Your solicitation must include relevant security and privacy requirements according to NIST, CISA, and the agency's guidelines. The solicitation must also ensure the vendor is compliant with these requirements and outline the agency's approach to ensure they are evaluated as part of the selection process.

Your agency's contracting office may wish to apply your standard practices, such as using boilerplate language. If doing so changes the wording of the requirements or selection criteria, the developer must also approve the new language. Even small changes in requirements descriptions can have significant unintended consequences.

Use the categorization and terminologies developed by industry-recognized standards bodies, particularly those associated with cybersecurity and safety, as much as possible.

Explain your expectations to the vendor and make it easy for the vendor to respond correctly and completely. The procurement must at least identify the requirements for each of the following topics:

- Type and control of connectivity
- Third-party service and data management
- Patching
- General vendor cybersecurity practices
- Security of device and communications
- More considerations

If your agency does not require a specific category or topic, the Statement of Work (SOW) must state so clearly. The requirements language must clearly define whether a security practice or standard is a requirement or a suggestion. It should also define your agency's factors to evaluate offers.

The solicitation must establish deliverables the vendor must provide. These can be pre-award, post-award, or both. Agencies often ask vendors to deliver product specifications and documentation of the vendor's cybersecurity practices. The solicitation must only require a pre-award deliverable if the agency needs to evaluate whether an offeror can meet the minimum requirements.

Complex Acquisitions Evaluation Criteria

For complex acquisitions, structure the evaluation criteria so the agency can evaluate vendors based on their compliance with the specified security requirements in the solicitation.

Your agency can also evaluate contractors on whether they provide more protection beyond the minimum contract requirements. Include security as a separate evaluation factor or as part of a larger evaluation factor.

Evaluation Factors

Evaluation factors must assess the contractor on how they address questions related to the risk and mission impact of the acquired product or service.

Ask the vendor to describe aspects and answer the sample open-ended questions in this list:

- Describe the secure development life cycle used and document it in your processes.
- Describe the vulnerability reporting and response program being used.
- Describe the program using metrics, such as the time between a bug being reported and a fix/patch release.
- Describe patch and version updates of software libraries, open-source software, or copyrighted software in the public domain that your program uses.
- Describe your SCRM program. Does it meet the requirements of NIST SP 800-161?
- Do you have any alternate sources for critical components? If yes, please describe.
- Describe your quality standards for suppliers, such as their response to bugs and defects.
- Describe how you will comply with the security requirements of the solicitation. Do you provide protection beyond the minimum requirements of the contract?

Examples of 5G-Specific Requirements

5G-specific requirements will vary, depending upon the implementation. Consider factors such as whether it is a private deployment or uses a public wireless network and the data's sensitivity. Further, some requirements apply only to one aspect of the architecture, while others apply end-to-end.

Significant Aspects of the Architecture

User Equipment

User Equipment (UE) stores subscriber data and profiles. UE includes a subscriber's mobile device, a modem, or endpoints associated with IoT devices.

Radio Access Network

Radio Access Network (RAN) has evolved. Today, RANs can support multiple-input, multiple-output (MIMO) antennas, wide-spectrum bandwidths, multi-band carrier aggregation, and more.

This evolution of RAN for 5G will significantly impact wireless technologies. It can enable Mobile Edge Computing (also called Multi-Access Edge Computing) and network slicing. These RANs of the future will also contribute to the lower latency that makes 5G so powerful.

Cellular networks traditionally have closed architectures, with proprietary network hardware tailored specifically for its operators.

O-RAN is a new approach that can add flexibility, interoperability, and market competition through standardized interfaces and multi-vendor infrastructures. Although O-RAN is not the only approach for 5G, federal agencies anticipate being able to manage private O-RAN 5G networks for secure enterprise use.

DOD has already demonstrated this approach in its smart warehousing, AR/VR, and spectrum sharing use cases.

The O-RAN Alliance, a consortium of industry and academic institutions, is developing O-RAN specifications as part of its vision for enabling next-generation cellular networks. They embrace and promote the functional split approach advanced by 3GPP to achieve this goal.

Base-station functionalities are virtualized as network functions in the functional split approach and divided across multiple network nodes. For example, nodes can be designated as Central Unit (CU), Distributed Unit (DU), and Radio Unit (RU):

- CUs implement functionalities at the higher layers of the protocol stack operating over larger timescales
- DUs handle time-critical operations at the lower layer
- RUs manage radio frequency (RF) components and lower physical (PHY) layer parts

This approach allows diverse networking processes at different points of the network.

Another core innovation is the RAN Intelligent Controller (RIC). RIC is a new architectural component that provides a centralized network abstraction, allowing operators to implement and deploy custom control plane functions.

5G Core

5G Core, defined by 3GPP, uses cloud-aligned, service-based architecture across all 5G functions and interactions. These include authentication, security, session management, and end-device traffic aggregation.

Services

Services include those for management, orchestration, and business applications relying on the 5G system.

Technical Requirement Considerations

Radio Performance

- Baseline radio performance
  - Coverage area: rooms, common areas, indoor/outdoor, enterprise reach across multiple regions
- Radio performance under varying challenging transportation conditions, including speed conditions, line of sight, and non-line of sight – consider conditions when access to positioning, navigation, or timing capabilities is unavailable.
- Performance of the technology at channel capacity, including the performance of congestion control mechanisms
- Performance of the technology when operating with coexisting technologies, adjacent channel technologies, and other potential sources of interference
- Sensitivity testing of the technology in the presence of interference from co-channel, adjacent channel, or radio interference
- Antennae testing results to understand placement and directionality issues

Communications Performance

- Performance requirements demanded by applications using the 5G service
- Performance of 5G when participating in a broader edge-computing environment and/or when integrated with artificial intelligence/machine-learning processing
- Demonstrations and/or published testing results of the new 5G communications technologies and their safety and effectiveness in supporting priority use cases

Active commercial uses are driving the growing demands on the wireless spectrum, such as providing mobile broadband wireless services.

Effective Spectrum Utilization and Coexistence Spectrum Utilization

Spectrum Utilization

Innovations to improve spectrum utilization efficiency within frequency bands that are pre-allocated for wireless communications and networking are in progress. These types of use cases may include but are not limited to:

- Massive MIMO antenna arrays
- Advanced signal processing for communications and networking
- Novel and efficient error-control coding
- Joint source-channel coding
- Passive and active intelligent surfaces
- New transceiver designs

All involve balancing the trade-off among capacity, complexity, and cloud-based radio signal processing.

Spectrum Coexistence

Active commercial uses are driving the growing demands on the wireless spectrum, such as providing mobile broadband wireless services.

However, critical non-commercial systems will also share the same or adjacent spectrum bands, whether active or passive:

- Active: weather radar and GPS
- Passive: radio astronomy, atmospheric and geospatial sciences, and climatological observations

The current means of spectrum sharing are limited to sensing and database management around mostly active users.

Exploring new spectrum use and sharing paradigms for bidirectional sharing with passive uses remains largely unexplored.

Proposals that use specific frequency bands must demonstrate awareness of incumbent passive and active uses and must address coexistence issues with these uses.

Secured and Verifiable Spectrum Use Through RF/Analog/Mixed-Signal Techniques

Security and verifiability protect storage and information flow and ensure trust in any coexistence scheme.

While more wireless devices share the electromagnetic spectrum, you must ensure the security of wireless communications and sensing. These security approaches could include a combination of RF, analog, mixed-signal, protocol, and algorithmic techniques. They may also include innovative, low-cost security techniques for unlicensed band applications.

System Architectures, Designs, and Algorithms

Future communication systems must operate in more-challenging scenarios with more-stringent performance requirements. Scenarios of this type may feature:

- Higher carrier frequencies
- Higher spectrum utilization efficiency
- Low or intermittently available power
- Coexistence with other active and passive radio systems
- Lower latencies
- High user density
- Environments where conditions change rapidly

Other considerations may include but are not limited to:

- System design and algorithms that can better cope with uncertainties such as carrier frequency offset and phase noises at higher carrier frequencies
- Reconfigurable surfaces that can adaptively change the electromagnetic wave propagation environment and associated design, control, and optimization algorithms
- System designs and innovative solutions for rural wireless broadband access
- Distributed wireless communication and scheduling algorithms
- Designs for machine learning applications

Federal agencies have already invested heavily into Wi-Fi in building solutions and wireless carrier services. 5G and Wi-Fi, including Wi-Fi 6, can complement each other for many scenarios and use cases:

- Use different spectrums
- Provide different quality of service (QoS)
- Employ different authentication and security
- Present different total cost of ownership

Program offices and contracting activities must look for new approaches for communication systems, including advanced 5G features, to use to assess the acquisition risk. As new technologies and approaches arise, agencies need to judge whether they are good fits for their needs.

Agencies should not risk vendor lock-in, in which only one vendor on the market produces a particular proprietary solution incompatible with other vendors' solutions.

National Institute of Standards and Technology (NIST) Publications

The following table lists NIST publications related to 5G security, Supply Chain Risk Management, and the security of mobile applications.

Series and Number	Title	Status	Released
SP 800-161 Rev. 1	Cyber Supply Chain Risk Management Practices for Systems and Organizations (**https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final**)	Final	5/05/2022
SP 1800-33B	5G Cybersecurity (**https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf**)	Preliminary Draft	4/25/2022
SP 800-218	Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (**https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf**)	Final	2/03/2022
SP 800-163 Rev. 1	Vetting the Security of Mobile Applications (**https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf**)	Final	4/19/2019
SP 800-161 Rev. 1 (Draft)	Cyber Supply Chain Risk Management Practices for Systems and Organizations (**https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/archive/2020-02-04**)	Draft	4/29/2021
NISTIR 8276	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry (**https://csrc.nist.gov/publications/detail/nistir/8276/final**)	Final	2/11/2021
NISTIR 8272	Impact Analysis Tool for Interdependent Cyber Supply Chain Risks (**https://csrc.nist.gov/publications/detail/nistir/8272/archive/2020-08-25**)	Withdrawn	8/25/2020
NISTIR 8179	Criticality Analysis Process Model: Prioritizing Systems and Components (**https://csrc.nist.gov/publications/detail/nistir/8179/final)**	Final	4/09/2018
ITL Bulletin	Increasing Visibility and Control of Your ICT Supply Chains (**https://csrc.nist.gov/publications/detail/itl-bulletin/2015/06/increasing-visibility-and-control-of-your-ict-supply-chain/final**)	Final	6/15/2015
White Paper	Final Report: Leveraging the Cyber Risk Portal as A Teaching and Education Tool (**https://csrc.nist.gov/publications/detail/white-paper/2015/06/10/leveraging-cyber-risk-portal-as-a-teaching-and-education-tool/final**)	Final	6/10/2015
NISTIR 8041	Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium (**https://csrc.nist.gov/publications/detail/nistir/8041/final**)	Final	4/10/2015
SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations (**https://csrc.nist.gov/publications/detail/sp/800-161/archive/2015-04-08**)	Final	4/08/2015

Acquisition Types and FAR Considerations

Agencies can procure 5G technology through Other Transaction Authorities (OTAs), commercial contracts (FAR Part 12), or non-commercial negotiated acquisitions (FAR Part 15), depending on their specific requirements.

OTAs are acquisition transactions (other than a contract, grant, or cooperative agreement) for prototype projects that generally are not subject to the federal laws and regulations governing procurement contracts. As such, they are not required to comply with the Federal Acquisition Regulation (FAR), its supplements, or laws limited in applicability to procurement contracts. Specific agencies have limitations on OTA scope. Those typically limit OTAs to research and development, prototype development, and limited-production projects.

The authority to enter OTAs is specified by law for the following 11 agencies:

- **Advanced Research Projects Agency–Energy (ARPA-E)**
- **U.S. Department of Defense (DOD)**
- **U.S. Department of Energy (DOE)**
- **U.S. Department of Health and Human Services (HHS)**
- **U.S. Department of Homeland Security (DHS)**
- **U.S. Department of Transportation (DOT)**
- **Domestic Nuclear Detection Office (DNDO)**
- **Federal Aviation Administration (FAA)**
- **National Aeronautics and Space Administration (NASA)**
- **National Institutes of Health (NIH)**
- **Transportation Security Administration (TSA)**

For most production uses of 5G technology, you must follow more-traditional FAR-based contracting. Commercially available 5G must consider security and prohibited sources. Several FAR considerations for 5G technology are detailed on pages 22, 23, and 24.

Cybersecurity Executive Order 14028

On May 12, 2021, President Biden issued the executive order (EO) on improving the nation's cybersecurity. The scope of the EO spans information technology (IT) and operational technology (OT) systems, no matter the type of operating environment: on premises, off premises, or hybrid.

It also calls for agencies to adopt Zero Trust cybersecurity principles. Through a series of EO-related memoranda, the Office of Management and Budget (OMB) directed agencies to better secure federal systems and achieve an optimal Zero Trust environment.

The EO also directs NIST to define critical software.

It assigns the CISA the responsibility of creating a list of software categories that meet the definition of critical software. For example, Mobile Device Management (MDM) solutions meets the definition of "EO Critical Software" as detailed in OMB M-21-30.

Among other important issues, Section 2(a) of EO 14028 required a review of contract requirements and language for contracting with IT and OT service providers. It also detailed recommendations for such requirements and language updates to the FAR Council and other appropriate agencies. As of July 12, 2021, the DHS Chief Procurement Officer submitted draft clause language and a business case to the FAR Council, pursuant to EO Subsection 2(i).

Trade Agreements Act (TAA) Compliance and Exceptions

One thing you need to consider for all 5G acquisitions is whether to include equipment or supplies. If 5G acquisition includes equipment, the contract must include the TAA clause (FAR 52.225-5 Trade Agreements). TAA requires that products originate from the United States or another approved country.

The TAA does not apply to the following:

- Acquisitions set-aside for small businesses
- Acquisitions of arms, ammunition, or war materials, or purchases indispensable for national security or for national-defense purposes
- Acquisitions of end products for resale
- Acquisitions from Federal Prison Industries, Inc. or non-profit agencies employing people who are blind or severely disabled
- Other acquisitions not using full and open competition
- Certain services are listed in FAR 25.401(b)

If the equipment is necessary for the services provided, an agency may use the equipment as a service at no additional cost to the government.

For example, the wireless-carrier services under the Multiple Award Schedule (MAS) permit devices to be managed and used as a service at no cost. Vendors must self-certify for TAA compliance with all offerings available on their MAS contract.

However, there are no devices available for purchase under SIN 517312 wireless services. The service provider retains asset ownership of the device. The service they provide may include the following:

- Asset issuance
- Endpoint performance management
- Service plan management
- Mobility management software
- Support services

This could constitute a full solution that minimizes earlier device-centric costs and streamlines operations.

Section 889 and Prohibited Sources

Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232) includes two prohibitions regarding certain telecommunications and video surveillance equipment and services (telecommunications). Section 889 was implemented in two phases and incorporated into FAR 4.2102.

As of August 13, 2019, the government may not obtain (through a contract or other instrument) certain telecommunications equipment or services produced by the following companies or their subsidiaries and affiliates:

- Dahua Technology Company
- Hangzhou Hikvision Digital Technology Company
- Huawei Technologies Company
- Hytera Communications Corporation
- ZTE Corporation

As of August 13, 2020, the government may not contract with an entity that uses telecommunications equipment or services, as a substantial or essential component of any system, or as critical technology as part of any system, produced by any of the Chinese companies listed on this page.

The prohibition applies "regardless of whether that use is in performance of a federal contract" or the use is only for non-federal customers.

Section 889 Part B applies to every sector, no matter what the company makes or sells. All contractor systems are required to be checked for prohibited telecommunications equipment and services.

Section 889 Parts A and B are included in the following FAR clauses and provisions:

- A representation provision (FAR 52.204-24)
- A System for Award Management (SAM) representation provision (FAR 52.204-26)
- A reporting clause (FAR 52.204-25)

All contractor systems are required to be checked for prohibited telecommunications equipment and services.

Security and Supply Chain Risk Management

As the federal government continues to move closer to proactive threat management, federal agencies must use risk management to achieve their objectives.

Effective risk management requires knowing the organization's assets – tangible and intangible (e.g., data) – to manage risks properly.

NIST develops standards and guidance to manage information security risks to an organization's assets, mission, systems, and personnel. The following NIST publications show the foundational approaches to risk management:

- Cybersecurity Framework
- Developing Cyber Resilient Systems: A Systems Security Engineering Approach Guide for Conducting Risk Assessments
- Managing Information Security Risk: Organization, Mission, and Information System View
- Risk Management Framework
- Security and Privacy Controls for Information Systems and Organizations

Supply Chain Risk Management (SCRM) is particularly important for 5G technology. SCRM is the process of assessing and mitigating the activities of foreign intelligence entities and other adversaries who attempt to compromise government and industrial supply chains.

These adversaries exploit supply chain vulnerabilities to

- Steal intellectual property
- Corrupt software
- Monitor critical infrastructure
- Carry out other malicious activities

They infiltrate trusted suppliers and vendors to target equipment, systems, and information that the government, businesses, and individuals use daily. In cases where the adversary plays a key role in the manufacturing process, no active infiltration is necessary – the equipment is compromised from the start.

Therefore, the government prohibits certain sources outlined in Section 889.

You need to develop an SCRM plan for 5G technology as an important element of your acquisition life cycle. Make it align with the overall agency business strategy.

Consider whether to implement standards for supply chain more stringent than the applicable NIST standards made obligatory by OMB and CISA. The standards must, at a minimum, contain those baseline standards and be consistent with agency policies and guidelines.

Suggested SCRM practices include but are not limited to:

- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- Defense IT Standards for Business Systems of the DOD Supply Chain

Available Acquisition Vehicles

5G technology can be acquired in several ways, including separate contracts for the technology or orders under existing indefinite-delivery/indefinite-quantity (IDIQ) contracts.

In 2020, the Federal Mobility Group (FMG) published guidance, Mobility Categories and Acquisition Options, for using existing IDIQ contracts for wireless communications services. IDIQ acquisition vehicles give federal agencies an expedited way to contract for goods and services. By pre-vetting contractors during the award of the IDIQ vehicle, the government saves time in contracting for goods or services.

An IDIQ contract provides an indefinite quantity of services for a fixed time. Under the IDIQ contract, the government places delivery orders (for supplies) or task orders (for services) against a basic contract for individual requirements. The IDIQ does not specify exact quantities of products or services being procured other than the minimum or maximum quantities.

Best-in-Class

OMB designates Best-in-Class (BIC) as a preferred governmentwide solution. This signals to acquisition experts that the contract is pre-vetted, mature, and market-proven. The following IDIQ contracts for wireless services allow for secure 5G services within their scope:

- GSA Enterprise Infrastructure Solutions (EIS)
- GSA Multiple Award Schedule (MAS) Wireless Mobility Solutions SIN 517312
- GSA 2nd Generation IT Blanket Purchase Agreements (2GIT; equipment-only requirements)
- NASA Solutions for Enterprise-Wide Procurement (SEWP)
- NITAAC Chief Information Officer – Commodities and Solutions (CIO-CS)

Among these sourcing options, you may choose one or more to best meet your needs. These contracts provide a framework regarding which technology solutions are readily available to government buyers. How you conduct your acquisition will vary when considering terms, technical considerations, or vehicle limitations in scope.

Additional Resources from CISA and NSA

- NSA and CISA Publish Third Installment of 5G Cybersecurity Guidance: **https://www.cisa.gov/news/2021/12/02/nsa-and-cisa-publish-third-installment-5g-cybersecurity-guidance**
- 5G Resource Library: **https://www.cisa.gov/5g-library**

www.gsa.gov
March 2023
05-23-00283

Access publications via
www.gsa.gov/cmls.