5G: A New Dimension of Opportunity and Risk

Agencies across the federal government are preparing for 5G connectivity. With the promise of super-fast speeds and stronger authentication mechanisms, 5G-powered networks present significant benefits and exciting new possibilities.

There are two main ways in which 5G will be deployed. Most of us associate it with the millions of next-generation mobile phones the public at large will use. However, agencies' internal network teams, contractors, or traditional service providers can adopt private subscriptions to 5G (comparable to traditional localized Wi-Fi networks) to run small cells where needed, such as on a military base, agency campus, or other limited area.

5G's smaller, more granular radio bands limit wavelength range more than earlier wireless generations, making it well-suited to serve dense populations in these kinds of locations. That includes not only people, but also the vastly growing internet of things (IoT)—connected devices with embedded sensors that will be increasingly integrated with agencies' information technology (IT) infrastructure. IoT devices will collect large amounts of data to be sent elsewhere for fast analysis and feedback. Applicable for particularly sensitive or urgent mission requirements, all of these devices will require secure, consistent, reliable network connectivity.

As we approach this new frontier, security for any new 5G network must be factored in from the start. 5G will require the same level of protection that we've seen for years across the physical network lifecycle. Augmenting those practices with modernized approaches like Zero Trust and artificial intelligence (AI)-based security automation will enable agencies to harness the power of 5G safely and for the long term.

New 5G Capabilities Power Growing Mission Demands

Regardless of their mission, agencies will have some common requirements in their 5G environments. These include:

- **Ubiquitous mobility:** The military continually requires strategic mobility, and the COVID-19 pandemic has forced more employees across the government to work remotely.
- **Enhanced simulation and training:** Advanced modeling and multiplatform virtual systems will enable warfighters and other personnel to access simulations in real time.
- **Improved inspection rates:** Agencies need to locate network equipment in the data center as well as see virtual circuit tracing, including tracking fiber cables through the conveyance system, rather than having to manually pull up cable.
- **Streamlining logistics:** The use of IoT devices and connected systems will make for a more efficient warehouse and global supply chain.
- **Better edge device connectivity:** This includes everything from satellites and vehicles to medical implants and thermometers.

5G delivers new and powerful capabilities for meeting these diverse needs. One is an architecture known as network slicing, which segments a network into independent, end-to-end, logical networks that can provide agreed levels of service quality. Network slicing is transparent to business users and comprises dedicated and/or shared resources (e.g., processing power, storage, bandwidth). It enables service providers to support different use cases, such as enhanced mobile broadband (eMBB), massive internet of things (mIoT), and ultra-reliable low-latency communication (URLLC). Network slicing also enables 5G core network services to be customized according to the functional and performance requirements for connected applications and devices. Ultimately, it allows for high-volume IoT connectivity and data processing tailored to specific agency mission requirements.

Exploring 5G Government Use Cases

5G will be applicable in myriad federal scenarios. Practically, this includes any situations in which multiple sensors and devices are collecting sensitive data and sending it elsewhere for use and analysis.

5G initiatives are already starting to move ahead at some specific agencies, and more will follow. The following are a few such initiatives currently in progress.

Department of Defense (DOD)—5G Tranche 1 and Tranche 2

Arguably the biggest opportunity for 5G will be in Defense, where highly advanced environments like warships and airplanes house complex systems driven by isolated networks. The DOD has already announced Tranche 1 and Tranche 2 of its larger 5G initiative. Per the DOD, these initial efforts are planned to accelerate adoption of 5G technology, enhance the effectiveness and lethality of US combat forces, and further the development and use of common 5G standards to ensure interoperability with military partners and allies. A total of 12 sites will serve as test locations for evaluating and applying a variety of 5G technologies.

Defense Advanced Research Projects Agency (DARPA)—Open, Programmable, Secure 5G (OPS-5G)

In January 2020, DARPA released a Broad Agency Announcement (BAA) for its new OPS-5G program. The goal is to pursue research that will lead to the development of a portable, standards-compliant network stack for 5G mobile—one that is open source and secure by design. It is an effort to address new security challenges posed by 5G and subsequent (e.g., 6G) mobile networks. For instance, the rapid increase in the scale of 5G networks, issues from unmanaged or forgotten IoT devices, and unwanted interactions between network slices create new security risks that this initiative is meant to assess.

Department of Homeland Security (DHS)—Secure and Resilient Mobile Network Infrastructure (SRMNI)

In April 2020, DHS released a BAA seeking development of new standards to improve the security and resilience of critical mobile communications networks. This research and development project seeks innovative approaches and

technologies to address weaknesses in legacy networks, build security into 5G networks, and provide federal enterprises with visibility into mobile network traffic that is accessing enterprise systems.

National Science Foundation (NSF)—Platforms for Advanced Wireless Research (PAWR)

In July 2015, the NSF began conducting fundamental research and releasing solicitations on novel communication technologies, networking and information architectures, and mobile applications that will enable advanced wireless capabilities. The research platforms are four city-scale test beds, enabling academic and industry researchers to experiment with approaches at scale over the next decade. PAWR is supported through public-private partnership to enable experimental exploration of new wireless devices, communication techniques, networks, systems, and services to revolutionize the nation's wireless ecosystem.

Department of Energy (DOE)—Secure Millimeter Wave Communication Network for Operating Drones

In December 2019, DOE released a BAA for development of a 5G wireless network using newly available millimeter wave frequency to operate unmanned aerial vehicles (UAVs) with machine-to-machine communications as well as provide an alternative to existing methods with improved RF coverage and resilience against cyberattacks at Idaho National Laboratory.

Department of Veterans Affairs (VA)—5G-Enabled Hospital

In February 2020, the VA Palo Alto Health Care System became the first 5G-enabled hospital in the VA system and was among the first in the country. Presenting opportunities for dramatic advances in healthcare, the 5G implementation enables telemedicine, connected health, smart medical devices, augmented reality, AI-assisted electronic health records, and more in ways—and at a speed—never before possible.

Looking to the Future of 5G in Government

Beyond known solicitations, many other use cases are likely to develop in the coming months. Other agencies are researching opportunities in spectrum management and monitoring, cybersecurity standards, storage, and edge capabilities to enable future 5G projects.

For example, the National Institutes of Health (NIH) may pursue connected health facilities, using smart devices in a hospital setting to collect health data and send it to a central repository for use by medical professionals.

The Department of Justice (DOJ) may apply the use of connected UAVs and satellites to recognize and capture images of wanted criminals or suspicious objects in crowded environments, and then send that data to a remote command post for analysis and action.

Possible applications of 5G for the Department of Transportation's Federal Aviation Administration (FAA) are nearly endless. As just a few examples, 5G can be used to establish reliable high-bandwidth connections to track aircraft; improve connectivity between unmanned flights and control towers; or connect onboard systems that allow real-time decision-making rather than relaying data back to a command post and waiting for a response.

Of course, the Department of Agriculture (USDA) has been using connected devices since before the concept of IoT was formalized. The USDA has long kept sensors in soil throughout the country to measure factors that impact crop-raising, such as ground acidity, humidity and precipitation levels, and wind speed and direction. 5G connectivity will enable the USDA to improve both edge device connectivity and the speed at which data collected in the field is processed.

Many more agency applications for 5G will likely evolve as the technology moves into more widespread adoption.

5G's Escalated Security Demands

The many use cases for 5G hold great promise, but they also carry an exponentially increased level of risk. Far more capability will be vested in technology than ever, over open radio waves rather than closed networks. Purpose-built IoT devices designed solely for data collection lack strong security, leaving their inevitable vulnerabilities ripe for exploit. There is a quickly emerging need for cybersecurity solutions that address 5G implementations driving large numbers of devices that collect and distribute sensitive data.

One of the biggest areas of risk is at the user level. Many users will likely carry mobile devices beyond the boundaries of private 5G networks. They may connect a device to other open 5G networks or private Wi-Fi. They may download unsanctioned applications to a device or unintentionally connect it to malicious websites. Because user behavior cannot be fully controlled, security must be transferred to the devices and, perhaps most importantly, to the 5G network infrastructure itself.

The physical infrastructure of the network packet core is frequently the target of attacks. Protecting 5G will require the same level of strict controls and protections as those applied to physical networks. This requires several proven practices. It starts with imposing accountability, enabled through granular logging and deep visibility into encrypted tunnel traffic that is analyzed for threats.

Next is segmenting 5G networks for Zero Trust access, an architectural security strategy rooted in the principle, "never trust, always verify." As with traditional network access controls, 5G users should only be able to access what they need to perform their day-to-day job functions. Because new connected devices will rely on analytics from the applications they work with, all network traffic will need to be segmented and prioritized to make sure the highest performance traffic has the necessary quality of service (QoS), latency, and network performance. Also, as is done with physical networks, 5G will require determination of the subscriber ID and application of granular controls to verify how and from where a user or device is attempting to gain network access.

Each type of device will need to be dynamically protected based on known vulnerabilities. 5G networks will see sensors that still run on legacy operating systems for years to come. Exposing such devices to 5G's power will necessitate deeper visibility and controls, which will be best achieved by automating mechanisms to find device vulnerabilities and, when vulnerabilities are identified, classify the controls needed to protect the devices as quickly as possible.

Thorough network protections will be imperative to monitor the critical infrastructure and high-risk devices agencies will be putting into the 5G environment. As 5G scales to connect exponentially more devices, human operators that run today's security operations centers (SOCs) won't be able to keep up. Automation will be the only option with the speed and efficiency to isolate and counter threats as quickly as they will be found.

Palo Alto Networks: First in 5G-Native Security

Palo Alto Networks offers the industry's first 5G-native security solution, providing the most granular security for highly distributed, cloud native 5G networks. This includes containerized 5G security, real-time correlation of threats to 5G identifiers, and 5G network slice security.

Our 5G security solution is supported on physical appliances in our PA-7000 Series and PA-5200 Series Next-Generation Firewalls (NGFWs), our VM-Series Virtual NGFWs for virtualized 5G deployments, and our CN-Series Containerized NGFWs. This means that agencies already using our NGFWs can continue using the same platform to secure service provider 5G infrastructure or enterprise 5G networks.

Context-Driven Security at Scale

Agencies can now gain visibility and control across all layers (signaling, data, control, and application) and at all key locations of 5G networks, enjoying comprehensive protection for 5G infrastructure. The Palo Alto Networks platform is available in all form factors—physical, virtual, and container—to provide consistent security enforcement across cloud native 5G core and distributed edge clouds.

Security Automation

A tightly integrated 5G security platform leveraging automation, native Kubernetes® orchestration, and integration with open APIs offers operational simplicity. Automated cloud-delivered threat intelligence powered by machine learning enables agency IT teams to defend against adversaries operating at 5G speeds, preventing known and unknown threats in real time across 5G networks on a global scale.

Accelerating IT Modernization

Agencies across the government will increasingly rely on private 5G networks to drive modernization and digital transformation. With Palo Alto Networks, any agency can deploy a strong security posture that extends Zero Trust security into 5G. By providing granular visibility into 5G traffic with automated, real-time security enforcement at both the subscriber and device levels, Palo Alto Networks empowers agencies to accelerate 5G digital transformation with confidence.

To learn more about Palo Alto Networks 5G security, please visit our 5G Security page.

For more information about how Palo Alto Networks supports the US federal government, please visit our US Federal page.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com