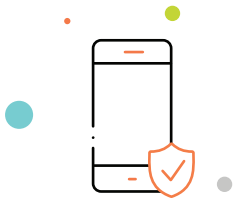
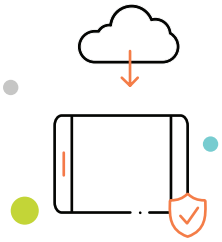
# Protecting America's 5G Networks

## 5G Security Highlights



**Enhanced Privacy Protections**



**Device-Specific Security Updates**

**Increased Network Virtualization**

The wireless industry has baked security into our networks since the beginning, and works diligently to continually update and build on our security capabilities with every generation of wireless. Today's 4G networks offer the most advanced security features to date, and 5G networks will further improve upon them. America's wireless industry is investing billions of dollars to build and secure 5G networks and help maintain our global wireless leadership.

### 5G More Secure than Any Prior Network Standard

The entire wireless industry continues to innovate and advance security—across networks, devices, operating systems and applications—as 5G networks are deployed.

#### Wireless Network Security

To maximize security, 5G has been designed from the ground up in the 3GPP standards process over years. 5G will continue to build on these security features by adding advanced encryption technologies built into mobile devices, among other innovations.

5G network defenses include the use of standards-based encryption algorithms, new and advanced authentication mechanisms, data encoding, anti-spamming software to protect against unwanted and illegal calls and messages, strict controls for physical and IT access, and customized security updates. Such network security protections will extend to the growing cellular-capable IoT market.

#### Wireless Device Protections

Mobile device manufacturers continue to innovate on a number of new and existing security mechanisms, including SIM card capabilities, the use of temporary identities, wireless account controls like passwords and multi-factor authentication, hardware-based cryptographic information—called roots-of-trust—which detects malware and authenticates the system software, device anti-theft tools, and integrated authentication systems that leverage 5G's speeds and encryption capabilities.

#### Mobile OS and Apps

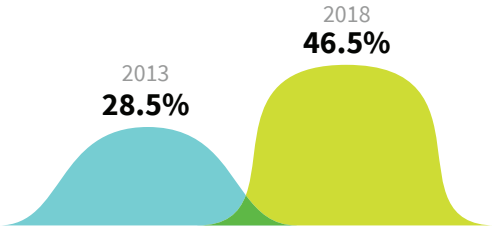
Mobile operating systems like Android and iOS work with app developers to improve security while screening for bad applications in order to prevent the spread of viruses and malware. OS providers and app developers will continue to advance software that protects wireless devices and consumers, including anti-malware and anti-virus software.

# 2018 U.S. 4G Infrastructure Market Share

**USA Shares**

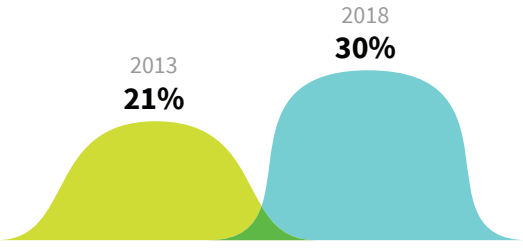
**77%** | Europe **18%** | Korea

**5%** | USA




**Asia Pacific**

China shares have seen a 63% increase since 2013.




**Europe/Middle East/Africa**

China shares have seen a 42% increase since 2013.

## Building America's Wireless Networks Securely

America's wireless industry builds our wireless networks with security top of mind. That means relying on network infrastructure from trusted partners and allies. In fact, China's 4G infrastructure market share in the U.S. is just one-fifth of one percent (~0.2%) as of 2018.

Many of our global peers are increasingly relying more on Chinese wireless infrastructure, which has led China to increase its market share of wireless infrastructure globally over 54 percent over the past five years.

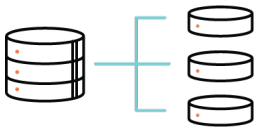
The key to strong network security is continued collaboration among industry stakeholders and between industry and government—led by the Department of Homeland Security. While many federal agencies have roles to play, the Department of Homeland Security is critical in convening industry and government stakeholders to work together toward a common cybersecurity framework. Our continued partnership is key to meeting the challenge of protecting our networks and our consumers against the dynamic global threat landscape.

# Securing 5G—Network Virtualization

America's wireless industry continually updates and enhances security capabilities with every generation of wireless. 5G networks will provide the most advanced security features to date, including more virtualized network functions to protect you and your wireless network in the face of cyber threats.

## Network Virtualization Benefits

5G networks will have more functions running virtually in the cloud than any generation before, making networks more resilient and customizable, which will improve your security and overall user experience.



**Decentralizing the Network**

**Customizing Security Functions**

**Leveraging Software**

### The Shift to Cloud Computing

Cloud computing refers to using a set of servers to remotely and virtually store your data, like photos or your address book, instead of relying on a physical device attached to the computing or network system, like a hard drive. Leveraging the cloud can increase a wireless network's flexibility, reliability, and security.

### Cloud-Powered 5G Network Virtualization

With 5G's ability to rapidly process enormous amounts of data these networks will harness the power of the cloud in ways that weren't possible for previous generations of wireless. Specifically, wireless providers are moving more of their core network functions—such as billing, authentication, network management, etc.—from physical network locations to the cloud, an action referred to as network virtualization. Network virtualization will reduce outages and improve security.

### Safer and More Resilient Virtualized 5G Networks

The virtualization of 5G wireless networks improves your security because it decentralizes the network, encourages security customization, and leverages the power of software to deploy new features.

**Decentralizing the Network.** Limiting the amount of physical hardware needed to run the network and dispersing network functions to multiple locations removes obvious targets for a cyberattack.

If a network outage or cyberattack does occur, network virtualization makes it much easier to limit the impact by isolating a specific area from the rest of the network with just a few clicks. These updates can be made without impacting your service since the virtual nature of the cloud allows wireless providers to efficiently create redundancies, making it easy to turn on network functions in another part of the cloud or relocate them in minutes.

**Customizing Security Functions.** Security can be easily customized for different parts of a virtual network to match the needs of a specific function. This allows for more efficient and effective security protocols to be deployed to different network elements as needed.

**Leveraging Software.** A software-based network means system security updates and tools that analyze data for vulnerabilities and malware can be deployed quickly. Software can help continually authorize your device, enhancing your data security.

# Securing 5G—
# Home Network Control

America's wireless industry continually updates and enhances security capabilities with every generation of wireless. 5G networks will provide the most advanced security features to date, including new protections when you're on Wi-Fi networks or roaming, thanks to what's known as home network control.

## Five Key 5G Network Defenses

Today's mobile networks offer a series of defenses that 5G networks will build on and enhance, including:

- Authentication standards to validate and authorize a user
- Data ciphering or coding to keep data free from corruption or modification while in transit
- Investments in network resiliency, including the creation of redundancies for network functions and the deployment of back-up power
- Anti-spamming software
- Strict access controls—to both hardware and software—that limit who can access the network and monitor network resources.

## Home Network Control

With 5G, wireless providers will extend the security protections you have when you're using their network to other networks you may use, including Wi-FI or while roaming.

### Extending Security Protections to Other Wireless Networks

Wireless providers recognize that you connect your devices to many wireless networks regularly. Compared to your wireless provider's network, these other networks—such as Wi-Fi, Bluetooth, or a 3G network overseas—may be less secure or may not have the most advanced security protections.

With 5G, wireless providers will extend your network's security protections to the other networks you access on your mobile device. This feature is called "home network control," and is a key part of new 5G network standards developed to make your wireless experience more secure.

### Making Your Mobile Experience Safer

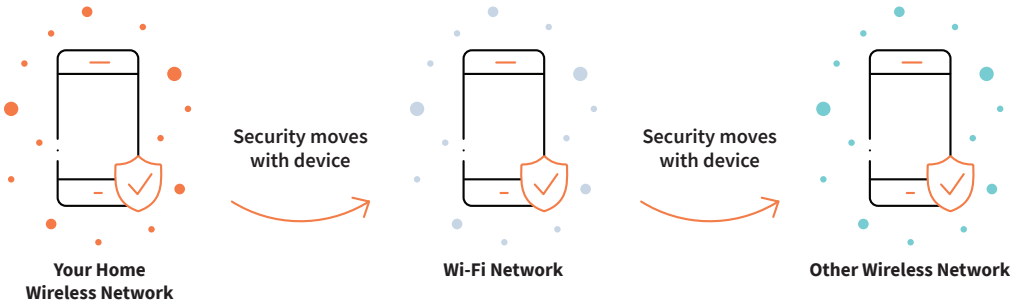
Home network control works by keeping the line of communication open between your device and your 5G network—your "home wireless" network, even when you are using another wireless network.

With your 5G network, if you're at a café and connect to their public Wi-Fi network, your home wireless network will stay active, allowing you to continually leverage 5G's advanced security protections—including those listed here—even while you are connected to the Wi-Fi network.

To enable this innovative security protection, your wireless provider will leverage the same technology that enables you to travel from one cell site to another to authenticate your device in order to provide you with your home network security features, even when you are using other, potentially less secure wireless networks.

### Protecting You throughout the Mobile Ecosystem

5G networks' use of home network control will help provide protection to your devices, data, and even wireless networks themselves, no matter where or how you are connecting your mobile device—raising the level of security for the entire mobile ecosystem.




ctia™

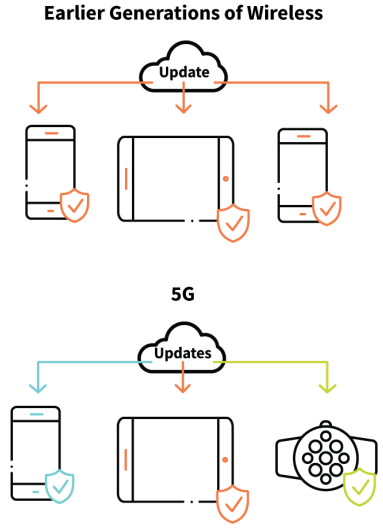
# Securing 5G—Enhancing Device Security

## Cybersecurity certification

In 2018, CTIA launched a first-of-its-kind IoT Cybersecurity Certification Program. Designed for devices that connect to cellular and/or Wi-Fi networks, the program allows manufacturers to choose one of three levels of certification, depending on the sophistication of the device and needs of the marketplace.

## Providing native support for plug-in security

5G networks will allow providers to send customized security updates to specific device types, enhancing your security no matter what device you're using.




America's wireless industry continually updates and enhances security capabilities with every generation of wireless. 5G networks will provide the most advanced security features to date—including key new protections for the growing range of devices that connect to wireless networks.

### Keeping the Wireless Devices of Today & Tomorrow Secure

The wireless industry builds in a number of security mechanisms that protect your devices from cyber threats, including:

- **SIM cards.** Securely store and authenticate your phone's identifying information.
- **Device access control.** Protect access to your device using PINs and passwords.
- **Roots-of-trust.** Pieces of hardware that cannot be modified and are therefore key for authentication.
- **Anti-theft tools.** Allow you to remotely locate, lock, and erase your devices.

As in every new generation of wireless, these features will continue to evolve with the changing cybersecurity landscape and accommodate the rise of new Internet of Things devices—from smartwatches to drones to agricultural sensors—that you will be able to connect to 5G networks.

### Enabling Device-Specific Updates

To address specific security needs of IoT devices, in 5G, wireless providers are updating the system for sending security patches and updates out to devices on a network.

Currently updates are sent to all devices, no matter what type of device they are. With 5G, providers will leverage advanced authentication systems to better identify the different devices—smartphones, sensors, appliances, etc.—on 5G networks and send tailored security updates to your different device types. This is known as providing native support for plug-in security.

These security updates are customized to your device type. In addition, 5G's low latency and fast speeds will allow providers to push these security updates quickly, with little to no disruption to your service. Device-specific updates enable your 5G-powered devices to run more efficiently, avoiding updates and data that aren't relevant and could slow down your device and wireless experience.

# Securing 5G—IMSI Encryption

## IMSI Encryption

5G networks will offer IMSI encryption to keep your identifying information secure when it travels over the airwaves from place to place on the network, which is typically when it is most vulnerable.

America's wireless industry continually updates and enhances security capabilities with every generation of wireless. 5G networks will provide the most advanced security features to date, including encryption of your device's IMSI number, a key identifier for your mobile device that authenticates you on wireless networks.

### The Importance of IMSI

In your phone, there's a SIM card, a small chip that stores the phone's information for your provider. The SIM card contains a unique user identifier called an International Mobile Subscriber Identity (IMSI).

The IMSI is comprised of your country code, wireless provider code, and phone number—and is key for identifying devices on a wireless network. When a wireless provider needs to know who and/or where you are—to authenticate you to access the wireless network, collect billing and use services, or allow you to roam on another network—your IMSI is used.

Today, given the sensitivity of this type of identifying information, your IMSI is turned into a randomly assigned identifier once you authenticate on the network or when you switch provider base stations. The identifier is then changed at random intervals to keep your IMSI shielded within the network.

"At each generation of wireless, operators and standards bodies learn from the past to innovate and advance security. IMSI encryption is one example of how security has evolved for 5G."

**JOHN MARINHO**
VP, TECHNOLOGY AND CYBERSECURITY
CTIA

### Encrypting IMSIs with 5G

With 5G, wireless providers will encrypt your IMSI under new 5G network standards developed to make your wireless experience more secure. Encrypting your IMSI means that the IMSI numbers are turned into a code that cannot be accessed without a virtual key.

5G networks will use a key embedded in the SIM card to encrypt an individual's IMSI before that information is sent to the network to protect it. These encrypted codes are random and change every time IMSI information is sent. When the wireless network receives the encrypted message, it pings a second key in the SIM card to read the IMSI.

### Safeguarding Sensitive Data

5G's IMSI encryption will keep your unique network identifier safe from cyber criminals while it travels around its 5G wireless network since they will be unable to read the code while it travels or access a key to unlock the code. Encryption protects information about who and where you are and how you use your wireless network, improving both your personal security and making the network safer by removing a target of cyber criminals.