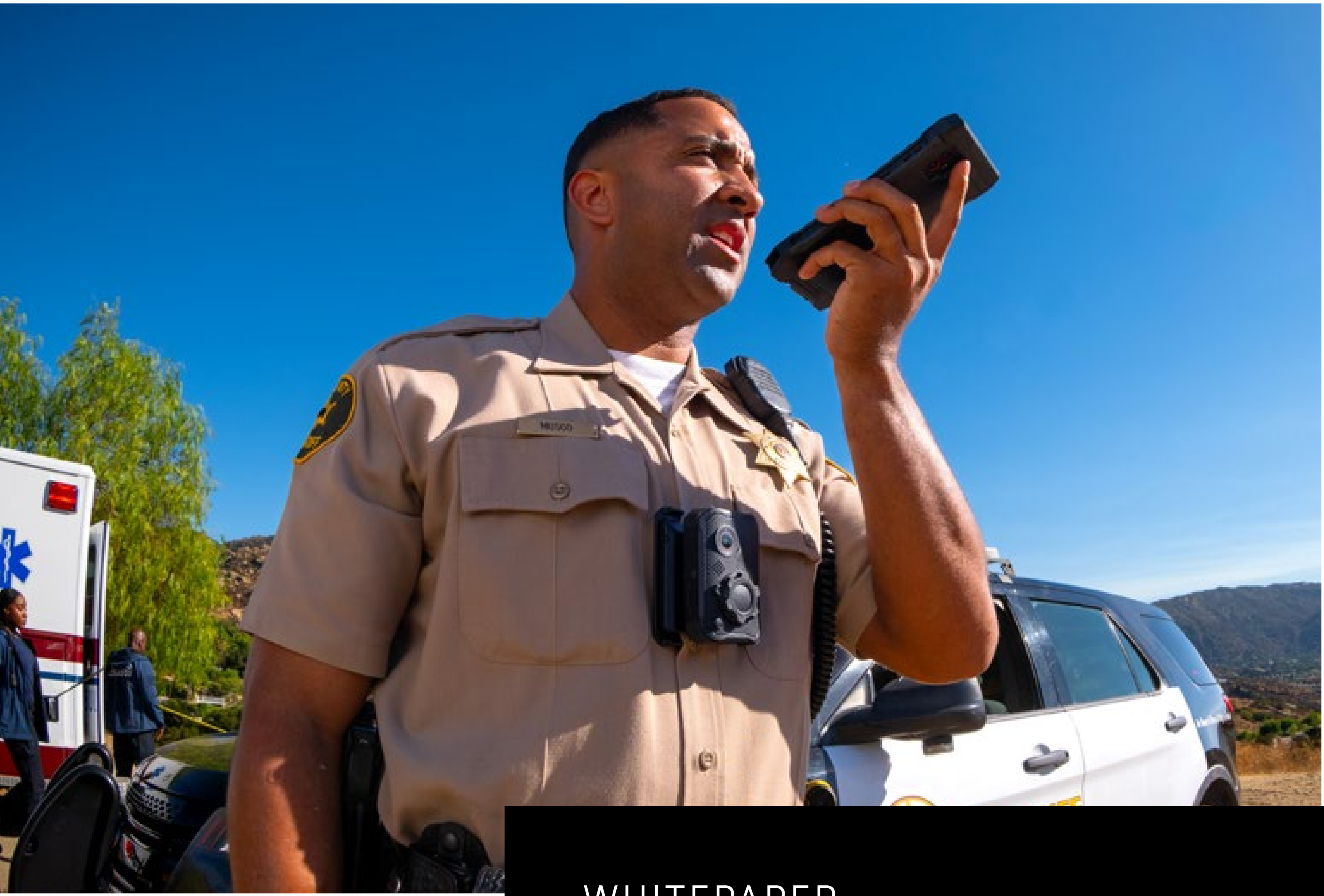
T-MOBILE FOR BUSINESS



WHITEPAPER

T-PRIORITY: DELIVERING PROTECTED NETWORK ACCESS AND CRITICAL COMMUNICATIONS

Securing reliable and prioritized connectivity for first responders.

Executive Summary.

In an emergency, there's no room for delay. With T-Priority, first responders stay connected and we're committed to keeping their critical operations secure, reliable, and built for the future.

When a wildfire races toward a densely populated area, emergency teams mobilize in seconds. Dispatchers deploy fire crews and track the real-time positions of emergency response personnel, while incident command teams coordinate containment efforts, relaying updates from the front lines.

In situations like this, first responders don't have time to wait for evacuation routes to update or drone footage to process. They need a secure network that can keep pace with the urgent demands of the situation.

During a crisis, networks get crowded quickly. As thousands of people make calls, stream video, and share updates at once, the network can become congested, slowing the very tools first responders need to coordinate and act fast. Such network surges can overwhelm security defenses, resulting in data breaches and system failures.

Whether it's paramedics sending electrocardiogram (ECG) data to a hospital through mobile devices or utility crews using drones to assess live hazards after a storm — first responders increasingly rely on connected technologies to carry out their life-saving work. However, without a network that can handle high-demand traffic — while maintaining speed, reliability, and security — congestion can stall recovery efforts.

That's why we created **T-Priority** — America's best and secure 5G network experience for first responders. T-Priority delivers the reliable connectivity emergency teams need with:

- Network slicing, providing dedicated prioritization for public safety.
- Priority access and preemption, moving critical communications to the front of the line.
- Ultra-fast 5G speeds and broad coverage, keeping teams connected in remote and high-traffic areas.
- Security and resilience, protecting sensitive emergency communications with advanced security measures.

T-Priority doesn't stop at connectivity—it's designed to address the security challenges of tomorrow. With advancements like satellite-based coverage and next-generation cybersecurity, we're helping first responders and critical service providers stay connected, no matter where they are or the threats they face.

In the sections that follow, we detail how T-Priority's cutting-edge connectivity overcomes legacy limitations and integrates advanced security measures to protect every critical communication channel.

Contents

T-Priority: Enhanced security and faster speeds.

When lives are on the line, secure and reliable communication isn't optional, it's essential. But during large-scale emergencies network congestion and evolving cyber threats can put the critical connections first responders rely on at risk.

Legacy networks weren't built to support the data-intensive tools today's first responders are using more and more. These outdated systems often struggle to keep up with the demands of real-time data sharing and high-bandwidth applications.

Older network architectures also lack the most advanced security features, making them more susceptible to cyberattacks, unauthorized access, and data breaches—risks that grow as more real-time data and high-bandwidth applications are added to the mix.

In contrast, T-Priority—built on our modern 5G Standalone (SA) core—delivers not only ultra-fast connectivity but also advanced security measures designed to defend critical communications from evolving cyber threats.

With features like end-to-end encryption, secure network slicing, and rapid threat detection, T-Priority helps keep critical communications safe so first responders can focus on saving lives instead of compromised systems and security breaches.

Unlock the power of our 5G network.

When a city goes dark in a power grid failure or a hurricane devastates a coastal region, the first responders and critical service teams jump into action. But overloaded networks can mean dropped calls, delayed emergency alerts, and lost connections—costing precious time.

That's where T-Priority comes in to prevent these failures.

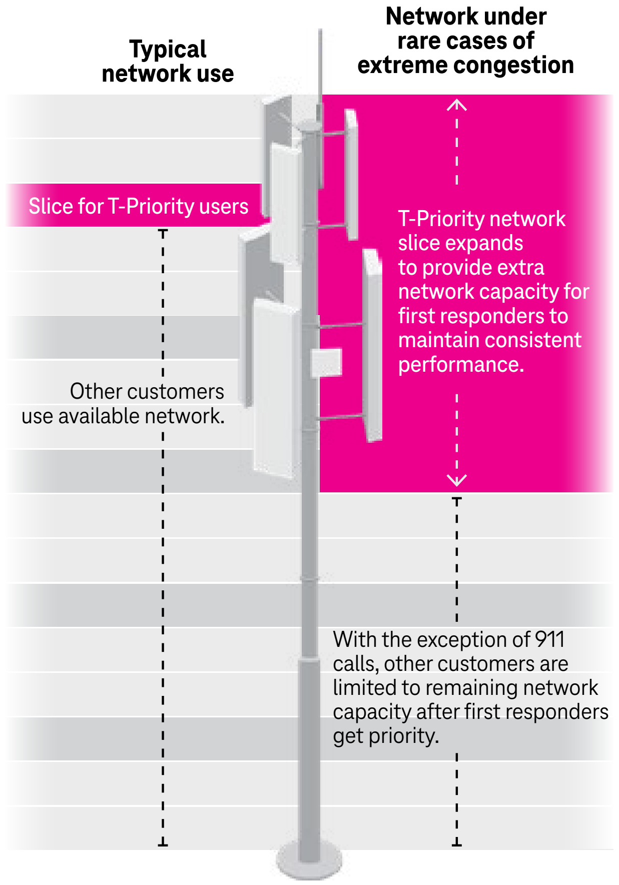
With a network slice purpose-built for public safety, first responders and critical service providers are given the highest priority across all 5G bands, even in extreme congestion. Unlike traditional networks, which share resources across all users, our 5G Standalone (5G SA) network architecture lets us dedicate customized network partitions to a specific use case. This is known as network slicing. Secure, isolated channels are created for sensitive information, and they dynamically expand to provide dedicated capacity for mission-critical needs.

It's worth noting that we're the first and only U.S. network operator to deploy the nationwide 5G SA Core. T-Priority offers a dedicated 5G network slice to first responders and critical service teams responding to emergencies. Our unique 5G network slice delivers ultra-low latency, high capacity, and virtually seamless connectivity. Operating on a fully independent 5G network, T-Priority unlocks the full potential of the most advanced technologies.

While the network slice itself isn't inherently a security feature, it enhances network security by creating isolated environments with dedicated protections for different types of traffic. For example, public safety communications, IoT sensor data, and enterprise applications, for example, each have different security and performance needs. A network slice is configured to prioritize first responder communications with ultra-reliable, low-latency connectivity while keeping these communications separate from lower-priority data, like routine administrative traffic.

This isolation reduces the risk of unauthorized access, prevents congestion from impacting critical applications, and helps ensure sensitive data is handled with appropriate security measures.

How 5G SA works.


Typical network use
Network under rare cases of extreme congestion
Slice for T-Priority users
Other customers use available network.
T-Priority network slice expands to provide extra network capacity for first responders to maintain consistent performance.
With the exception of 911 calls, other customers are limited to remaining network capacity after first responders get priority.

Beyond wireless priority service.

To address the congestion issues that interfere with first responder work, the federal government established the Wireless Priority Service (WPS) program, prioritizing emergency calls on cellular networks. But during crises, today's first responders need more than just prioritized voice calls, which is why T-Priority goes further.

When wildfires tear through dry terrain, firefighters equipped with T-Priority can get the benefit of both mission-critical voice calls and drone footage to track the flames. Likewise, paramedics can have on voice and high-definition video calls to consult with emergency room teams during medical emergencies.

While our dedicated 5G slice plays a key role in making sure first responders and recovery teams can access the tools they need to save lives, so does network security. Without robust security measures in place, data breaches and system disruptions can jeopardize the safety of first responders and those they're trying to protect.

Unmatched network security in any emergency.

What sets our protections apart.

During a massive flood, the first responders will race to evacuate residents and coordinate rescues. But what if malicious actors were to intercept communications, distorting data, or even disabling key applications that response teams operate? With critical information delayed or corrupted and access to technological tools blocked, response and recovery efforts could be quickly thwarted.

We understand that security can never be an afterthought—with that in mind, we've built extensive security measures it into every layer of our network. With these robust protections in place, T-Priority helps keep first responders connected when whenever duty calls.

See for yourself how our security features stack up against what 4G/5G Non-Standalone (NSA) networks provide:

Security Feature	Description	4G/5G NSA	T-Priority
Robust authentication and authorization	**5G mutual authentication** between mobile devices and core network	Limited	✓
Custom security layers	Reducing denial-of-service (DoS) attacks and ensuring data isolation using **traffic segmentation and network slicing**	Limited	✓
Improved privacy protections	**Customer identifiers protected** with concealment and countermeasures over network, preventing location tracking	x	✓
External communication with 5G SA	**Secure APIs** ensure robust security for 5G services and applications	x	✓
Network slicing	**Customer data can be treated uniquely** depending on the type of traffic and customer's needs	x	✓
Encryption and Integrity Protection	Signaling traffic between mobile devices and core network encrypted	✓	✓
5G SIM Provisioning via Secure Wireless Updates	Subscriber identities are not transmitted in the clear during SIM updates	✓	✓

A closer look at inherent 5G security protection.

Robust authentication and authorization:

With mutual authentication in place, both devices and the network verify each other's identities. This deters intrusions, spoofing, and phishing. Additionally, encrypted identifiers protect sensitive data like phone numbers, device IDs, and subscription details from identity theft or malicious attacks.

Custom security layers:

Advanced techniques such as traffic segmentation and network slicing isolate data streams for T-Priority users. This approach strengthens defenses against denial-of-service (DoS) attacks and helps ensure critical communications for first responders and critical service organizations remain uninterrupted and secure.

Privacy protection:

We incorporate advanced privacy measures to protect sensitive customer information. What does this mean to you? Subscription concealment shields subscriber details from being intercepted by bad actors during transmission. At the same time, countermeasures against stingray devices defend against surveillance tools that imitate cell towers to intercept communications. In short, these measures keep your private data just that—private.

External communication with 5G SA:

Protecting exchanges between our network and third-party systems is essential for maintaining reliability. Secure APIs help ensure that 5G SA Core services and industry-specific applications are protected from unauthorized access and cyber threats. Furthermore, data integrity measures reduce vulnerabilities and help keep communications with outside networks secure and reliable.

Network slicing:

By segregating customer data and traffic based on specific needs, network slicing creates isolated environments for different types of services. This segmentation enhances security by ensuring that traffic from one customer or service remains separate from others, preventing potential breaches from spreading across the network.

Encryption and integrity protection:

T-Priority uses encryption to protect both signaling and wireless data traffic, adding a critical layer of security against interception. Encrypted signaling traffic helps secure communication between devices and the network, preventing eavesdropping and man-in-the-middle attacks where bad actors attempt to intercept or alter messages. At the same time, wireless data encryption helps protect user data from unauthorized access while in transit.

5G SIM provisioning via secure wireless updates:

We've eliminated the need for manual SIM cards configuration by are setting up and activating your SIM cards via wireless updates so there's no need for manual configuration. These updates follow strict security protocols that never allow a subscriber's identifying information to be transmitted in an unsecured format. Mandating the use of secure networks for wireless updates adds an extra layer of protection for customer data.

Enhanced network security differentiators.

Beyond the inherent security built into 5G, our cybersecurity team has developed additional security requirements for our infrastructure and device vendors. We've also mandated specific 5G security configurations and communication flows and further hardened our underlying IP networks.

Here are the security features you won't find together anywhere else:

Security Feature	Description
Industry security standards	**T-Mobile follows global security standards** (such as 3GPP, FCC, NIST, IETF, GSMA, ETSI) for security and reliability.
Zero-trust approach	**Strict access policies prevent unauthorized access;** measures to reduce impact of intrusions.
Advanced employee and contractor verification	**Employee identity verification** using CLEAR, FIDO2, and **AI-based** identity technologies.
Password-less	**T-Mobile adopted a password-less authentication approach** with the biggest deployment in the world (160K accounts).
Secure access service edge (SASE)	**Safeguards data traffic across devices** with an advanced, scalable, unified solution.

A closer look at how our network security stands out.

Compliance with industry security standards and frameworks: Global security frameworks like the 3rd Generation Partnership Project (3GPP)[1], Federal Communications Commission (FCC)[2], National Institute of Standards and Technology (NIST)[3], Internet Engineering Task Force (IETF)[4], Global Security Management Agency (GSMA)[5], and European Telecommunications Standards Institute (ETSI)[6] form the foundation of our safety and reliability practices. To begin with, T-Priority provides secure function separation which isolates the network functions to prevent breaches from lateral movement. Robust data protection helps shield against tampering, unauthorized access, and cyberattacks like denial-of-service (DoS). Rapid threat response quickly identifies and addresses risks before they affect the network's efficiency.

Zero-trust approach: Zero-trust security frameworks defend against ransomware, insider threats, and other cyberattacks. With this approach no entity within the network is automatically trusted, limiting attackers' ability to move laterally within the network. The zero-trust approach helps contain breaches and prevent unauthorized access from spreading to critical systems or sensitive data.

Advanced verification and password-less authentication: We use Fast Identity Online 2 (FIDO 2)-based authentication for all individuals accessing our systems, including full-time employees and contractors. This method eliminates the need for traditional passwords, offering a more secure and convenient alternative than ever before. Additionally, we use AI-powered technology from the CLEAR AI platform, which achieves stringent identity validation, delivering fast and reliable verification. Notably, this represents the largest global deployment of its kind, underscoring our commitment to both robust security and seamless user experiences.

Secure access service edge (SASE): By combining several security features such as threat protection, secure access, and data encryption, SASE protects remote workers and devices, including IoT devices, routers, and fixed wireless connections. This approach is scalable and simplifies security management.

A closer look at how our network security stands out, cont.

Comprehensive device security: Devices connected to our network adhere to rigorous security standards designed to minimize risks from threats like malware, tampering, and unauthorized access. Protections are built into every step, from secure boot processes that validate system integrity during startup, to encryption that protects sensitive data. Regular software updates further safeguard devices against cyber threats.

Data encryption: User data exchanged between devices and our network is fully encrypted, keeping communications private and secure. Protecting wireless transmissions from interception or leakage keeps your communications intact, giving you peace of mind with every connection.

Enhanced physical security: Physical security plays a vital role in the T-Priority infrastructure, with stringent measures to protect cell sites, data centers, and offices from tampering or breaches. These facilities undergo regular security testing and monitoring to uphold best practices, minimize vulnerabilities, and strengthen the network's overall resilience.

Internet routing protection: Border Gateway Protocol (BGP) routes are signed cryptographically to prevent hijacking attempts. We're the only nationwide operator implementing Resource Public Key Infrastructure (RPKI) for 100% of its traffic, a cutting-edge framework that helps ensure your data takes the correct path to its destination securely and reliably.

Global signaling protection: We follow GSMA interconnect security standards to defend against interception and impersonation by malicious actors. This is done through comprehensive message filtering, which checks key signaling details such as IP addresses, application identifiers, command codes, and locations. These protections help maintain the integrity of communications across networks, even when users connect across different regions or through international systems.

Position, navigation, and timing resiliency: Position Navigation and Timing (PNT) provides precise time synchronization across cellular networks, which is essential for coordinating data transmission, minimizing interference, and making the best use of the available spectrum. With PNT redundancy, multiple independent systems back up timing sources at key locations, such as cell sites and mobile switching offices (MSOs). These backups allow the network to maintain continuous, reliable performance, even if one timing source is disrupted.

Supporting first responders with comprehensive solutions.

Cutting-edge security forms the backbone of T-Priority, but it's only one aspect of the comprehensive support we provide to first responders and critical service teams responding to emergencies. Our mission is to equip emergency teams with the tools, connectivity, and resources they need to perform their duties.

Frontline response.

When disaster strikes or critical events unfold, our Emergency Response Team (ERT) is on the front lines, ensuring that first responders and critical service providers have the reliable connectivity they need to secure public safety.

Equipped with heavy-duty SatCOLTs (Satellite on Light Trucks) and SatCOWs (Satellite Cells on Wheels) and other advanced technologies, the ERT is ready to deliver swift, reliable connectivity where it's needed most. Whether responding to hurricanes, wildfires, or tornadoes, the ERT provides a lifeline of communication even in the most challenging conditions.

Our partnerships with government, emergency services, utilities, and other providers keep critical communications running 24/7. It's all part of keeping communities safe.

The ERT doesn't just restore communication networks. The team can provide free Wi-Fi, device charging stations, and unlimited talk, text, and data to affected customers. These services create vital connections for families, businesses, and first responders, keeping people informed and empowered during uncertain times.

When devastating wildfires swept across the Hawaiian island of Maui in August 2023, causing massive loss of life, local fiber was destroyed, and commercial power was lost. As part of the emergency response, we brought in portable cell equipment, generators, VSATs, and microwave equipment to restore sites, including the FEMA center in Kaanapali. We supplied first responders with activated phones and WPS. And T-Mobile Community Support provided device charging, portable battery packs, and connected devices to local residents.

From generators and mobile satellite cell vehicles to VSATs (very small aperture terminals) and microwave equipment, the ERT brings a versatile toolkit to every mission. These resources help the team to adapt quickly, deploying connectivity solutions where they are needed most—even in remote or severely impacted areas.

Coverage without limits.

Our satellite messaging service, T-Mobile Starlink, is a groundbreaking advancement in mobile connectivity. Integrating SpaceX's direct-to-cell satellite technology into our network will help eliminate dead zones and extend coverage to areas unreachable by traditional cell towers.

The integration of Direct-to-Cell with SpaceX also supports Wireless Emergency Alert features, including WEA 2.0 and WEA 3.0, which allow for longer messages, up to 360 characters, and device-based geo-fencing capabilities. These enhancements are designed to improve the delivery of critical communications during emergencies.

While this feature has not yet been commercially launched, we have already tested its capabilities in critical, high-stakes situations:

Post-hurricane relief efforts:

During Hurricane Helene, the FCC granted us and SpaceX temporary emergency capabilities to provide our Direct-to-Cell satellite service in affected areas. This service enabled the broadcast of emergency alerts and supported basic SMS texting capabilities on our network in North Carolina, where a significant portion of cell sites were knocked out of commission. The service also provided vital connectivity to first responders and the community, playing a critical role in rescue and recovery efforts.

LA wildfires response:

In the wake of the LA wildfires, we opened our T-Mobile Starlink Direct-to-Cellular service in partnership with SpaceX to help restore connectivity in areas affected by the fires. The service allowed residents to send text messages to first responders and family members, providing crucial updates on their statuses and whereabouts. We also deployed community support vehicles to provide charging and Wi-Fi connectivity and distributed power packs and connectivity devices to those in need.

By bridging connectivity gaps, this technology helps relay critical information to those who need it most, redefining what connectivity can look like during emergencies.

Mission critical communications.

Our Mission-Critical Push-to-Talk (MCPTT) delivers high-priority, low-latency voice services tailored to public safety and enterprise needs. Powered by our strong LTE and 5G networks, MCPTT helps ensure that first responders, emergency teams, and critical businesses stay connected.

This service is fully integrated into T-Priority and based on globally recognized 3GPP (Third Generation Partnership Project) standards. These standards outline the technical specifications that help deliver reliable, high-priority connectivity and seamless interoperability across networks—essential for mission-critical applications in both public safety and enterprise settings.

Our MCPTT makes real-time communication smooth and effortless for large teams, providing fast, clear, and reliable message delivery. When paired with Land Mobile Radio (LMR) systems, MCPTT extends the reach of traditional radio communication over cellular networks, creating a more unified and reliable way for teams to communicate across different devices and platforms.

Next gen 911 support & integration.

We're committed to enhancing public safety by supporting and integrating with Next Generation 9–1–1 (NG911) services[7]—a cutting-edge IP-based system designed to transform emergency communication. This advanced system integrates hardware, software, data, and operational policies and procedures to modernize and streamline the way emergency calls are handled.

NG911 provides:

- **Standardized interfaces for emergency communications:**
  Helps ensure seamless connectivity between emergency call and messaging services to public safety systems.
- **Support for all types of emergency calls:**
  Handles not just voice calls but also data and multimedia messages, enabling better situational awareness during emergencies.
- **Enhanced data utilization:**
  Acquires and integrates additional data—such as location, medical history, and real-time video—helpful for call routing and decision-making.
- **Accurate call routing and delivery:**
  Directs emergency calls, messages, and data to the appropriate public safety answering points (911 call centers) or emergency entities for prompt response.
- **Advanced incident response coordination:**
  Facilitates data and video communication to aid first responders in managing coordinated responses during complex incidents.
- **Broadband services for first responders:**
  Ensures high-speed, reliable broadband connectivity for PSAPs and other emergency teams.

Keeping enterprises and government agencies connected and protected.

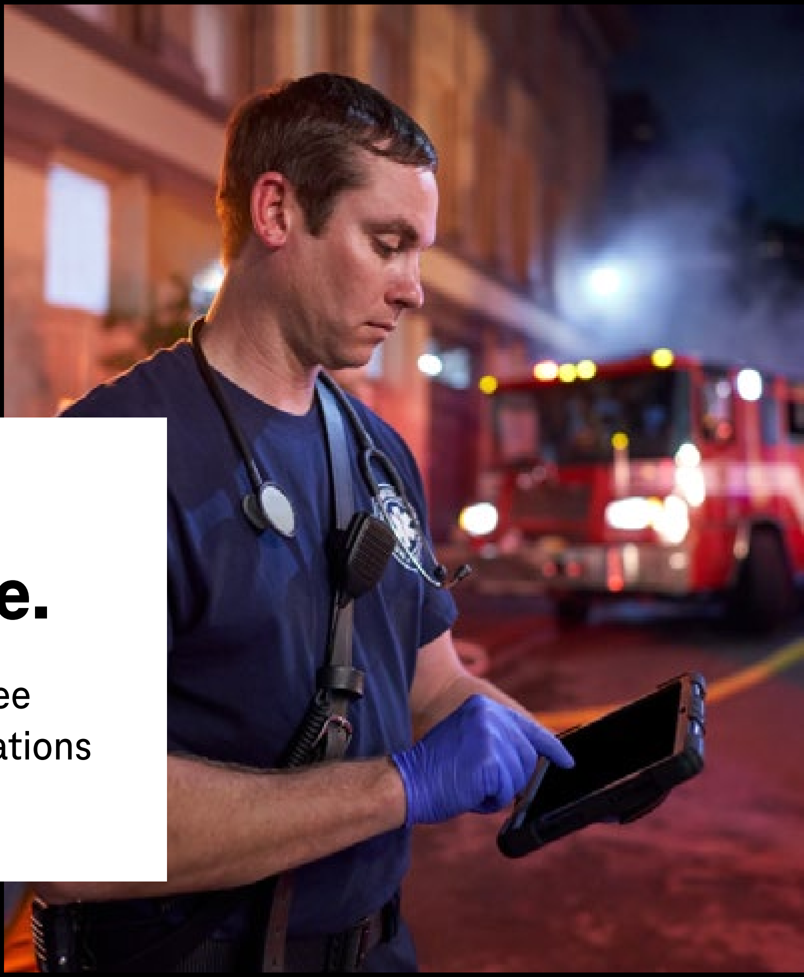
Our 5G network stands out as the most awarded in the U.S., delivering the fastest download speeds and the most extensive 5G network coverage in high-traffic areas like Freemont Street in the Las Vegas Strip or Times Square in New York City.

For three consecutive years, we've won all five overall network experience categories in Opensignal's January 2025 Mobile Network Experience Report. These categories include 5G download speeds, 5G coverage experience, 5G availability, consistent quality experience, and reliability experience.

From dedicated network slices and priority access to advanced encryption and real-time threat detection, every feature of T-Priority is designed to keep critical communications secure and resilient.

Our 5G SA Core is built for the future—delivering the reliability, scalability, and advanced security that modern enterprises and government agencies demand. With built-in protections against evolving cyber threats, it forms the foundation you need for secure, high-performance connectivity.
Whether it's private 5G networks tailored to your operations, fixed wireless solutions for flexible connectivity, or satellite coverage that extends beyond traditional reach, we provide secure, next-generation solutions that keep your organization online and protected.

You're not just choosing a network—you're choosing a partner dedicated to empowering your mission with security and innovation.



This is enhanced security with T-Mobile.

Explore solutions at **T-Priority.com** to see how we protect your critical communications and deliver reliable connectivity.

Citations

[1] 3GPP: https://www.3gpp.org

[2] FCC: https://www.fcc.gov/csricreports

[3] NIST: https://www.nccoe.nist.gov/5g-Cybersecuritysecurity

[4] NSA: https://www.nsa.gov/About/Cybersecuritysecurity-Collaboration-Center/Enduring-Security-Framework/

[5] GSMA: https://www.gsma.com/

[6] ETSI: https://www.etsi.org/

[7] Next Generation 9–1–1: https://uscode.house.gov/view.xhtml?path=&req=%28title%3A47+section%3A942+edition%3Aprelim%29&f=&fq=&num=0&hl=false&edition=prelim

For qualifying organizations on eligible rate plans. WPS enrollment with USDHS required. Features available on our network; not available while roaming. Some T-Priority features only available in areas of Ultra Capacity 5G coverage with capable device and 5G Standalone settings; see T-Mobile.com/5Glayers. Coverage not available in some areas and may be impacted by emergencies; check your response area.