SECURING PUBLIC SAFETY

Your network is built with security at its core.

FIRSTNET
Built with AT&T

The mobile communications and security requirements of the U.S. public safety sector are as diverse as the agencies that constitute it.

Each type of agency—such as law enforcement, fire, or emergency medical services—has distinct communications demands (speeds, devices, coverage area, network interconnects, levels of encryption, and the like) and requires access to a variety of local, state, and/or federal databases. Each of these government databases, in turn, has its own security guidelines and regulations.

On top of these differences are agency variations in size, budget, and technical expertise, including different rates of smartphone and mobile data adoption. A large metropolitan police force may have many thousands of officers in the field, a multimillion-dollar IT and networking budget, and extensive in-house knowledge and skills. Its rural county counterpart, by comparison, may have a force of a dozen or fewer officers, a modest budget, and limited IT and security proficiency.

Regardless of their role, location, size, or budget, almost all public safety organizations share a common set of core security needs and objectives. They include:

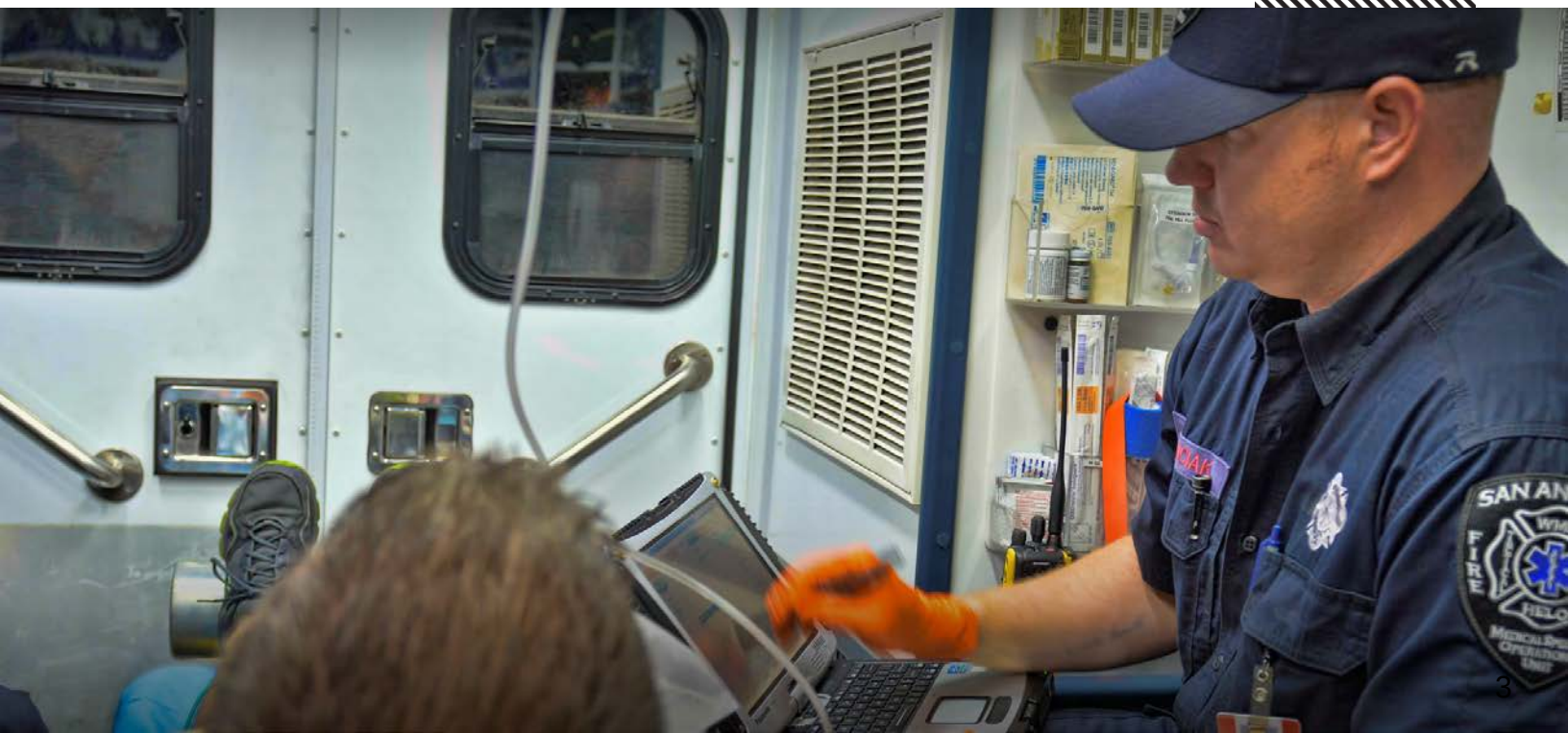
- *Ease of use:* First responders need to focus on their work, not on navigating onerous security passwords and procedures. They want a simple authentication and authorization process to access devices, applications, websites, and databases, and want to stay logged in even when moving across jurisdictions.
- *Authentication and access:* First responder agencies require trustworthy identity credential and access management (ICAM) solutions that are fast and simple for first responders but that also help ensure positive identification of both the devices and their users.

- *Mobile device security:* Different agencies and their first responders use different devices, with some agencies providing mobile equipment to their first responders, and others instituting bring-your-own-device (BYOD) policies. Any first responder network must be able to accommodate, and help secure, this wide range of devices and the data they store.

- *Encrypted data transmissions:* Sending highly sensitive information "in the clear" is risky from more than just a privacy and safety perspective; first responder agencies doing so can run afoul of various local, state, and federal regulations. Encrypted tools must be available at the appropriate level as transmitted data moves along its end-to-end path across the network.

- *Dynamic security:* The public safety network for agencies and first responders must provide security appropriate to the unique needs of this specialized user base. For example, if a threat management system identifies malware on a first responder's mobile device, the network should flag the problem for resolution. But it should not automatically block the device and its user—who could be in the middle of a crisis situation—from accessing the network and mission-critical applications.

FirstNet, conceived in the wake of the 9/11 terrorist attacks, has been designed and constructed to address these diverse security needs.



A Purpose-Built Ecosystem for Security and Compliance

Addressing the security needs of public safety organizations and their first responders is no trivial task; this challenge was clear before the creation of FirstNet. Until now, piecemeal solutions built on commercial public networks have required agencies or their contractors to manage a complex set of security requirements, compliance demands, security tools and services, and cyberthreats. Each of these elements is in a constant state of flux, which has made it difficult for even the most sophisticated agencies to stay both secure and compliant. Another critical factor: In today's market, it is extremely challenging to attract and retain cybersecurity talent.

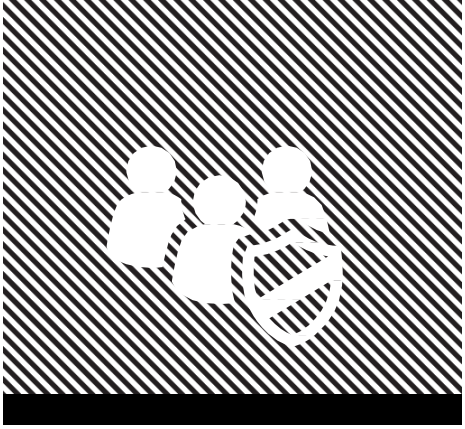
Recognizing these challenges, FirstNet delivers a comprehensive ecosystem solution that takes on much of the security burden for these agencies. The highly available, redundant, physically separate, dedicated core was designed to comply with many standard security regulations and needs, and it will continue to evolve to take advantage of new technologies and address emerging requirements.

FirstNet consists of a series of Radio Access Networks (RANs) that provide wireless communications to first responders in the field. The RANs, in turn, connect to the FirstNet core, a physically separate and isolated nationwide core. The core is highly resilient and serves to connect first responders with one another, with their own and other public safety agencies, and with those that support them.

Integral to FirstNet's capabilities is a dedicated Security Operations Center (SOC) as well as a security engineering organization, both staffed by FirstNet security experts. The SOC monitors and manages FirstNet traffic 24x7 and employs many of the security systems and procedures that

▼ FirstNet Security Operations Center

A team of cybersecurity professionals at Network Operations and the dedicated Security Operations Centers (NOC/SOC) employ state-of-the-art tools to constantly scan the network to help detect and prevent intrusions and to address and resolve vulnerabilities.



Experienced Engineering & Security Support

FirstNet's team of security professionals maintain certifications and credentials such as:

- Certified Information System Services Professionals (CISSP)
- Certificate of Cloud Security Knowledge (CCSK)
- Certified Information Systems Auditors (CISA)
- Certified Information Security Management (CISM)
- Certified in Risk and Information Systems Controls (CRISC)
- Certified Ethical Hacker (CEH)
- Global Information Assurance Certification (GIAC)
- RSA Certified Security Professional (CSP)
- Microsoft Certified Professional (MCP)Cisco Qualified Professional.
- Cisco Qualified Professional

AT&T has honed over decades of operating its highly secure global networks. The engineering unit focuses solely on the security needs of FirstNet but collaborates closely with the thousands of other engineers working throughout AT&T.

Although the FirstNet platform provides much of the security functionality that public safety agencies require, it is also easily augmented with the value-added tools and services required to meet any agency's unique security and operational demands. Ultimately, there is no one-size-fits- all security solution that meets each and every agency's needs, but FirstNet provides the most comprehensive security foundation on which to construct solutions fine-tuned to any agency-specific requirements.

For example, FirstNet provides end-to-end virtual private network solutions that are compliant with the Federal Information Processing Standard (FIPS) Publication 140-2 as well as radio, transport, and network core encryption, plus sophisticated physical and logical security protocols. Although the system wasn't designed to meet all the elements of the FBI's Criminal Justice Information Services Security Policy (CSP), FirstNet will provide avenues for individual criminal justice agencies or each state's Criminal Justice Information Services (CJIS) System Agency to meet its own CSP compliance requirements.

FirstNet includes several elements that collectively help provide comprehensive security from the mobile device and its applications to the network and the data that traverses it.

Simplifying the Security Experience for First Responders

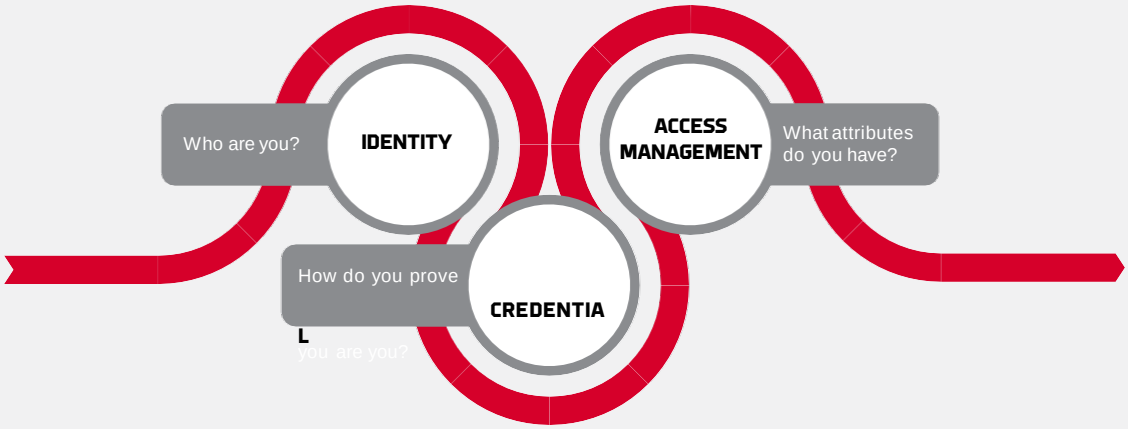
First responders working a crime scene, fire, or natural disaster don't want to repeatedly enter complex passwords just to get and maintain network and application access. They need fast and reliable ways to authenticate their identities so they can focus on performing the jobs they've been trained to do. FirstNet is designed to help them do their jobs better without being distracted or restricted by heavy-handed, recurring security procedures.

For starters, FirstNet offers public safety organizations and their workers a sophisticated but easy-to-use identity credential and access management (ICAM) system. Each mobile device has a SIM card that points the device to the FirstNet platform. Once workers use the ICAM system to log in, FirstNet's single sign-on (SSO) capability enables them to access network resources and other secured destinations without having to continually enter additional passwords.

The FirstNet ICAM system can also accommodate the various identification systems supported by different devices. Supported processes include biometric or other multifactor authentication (some of which is dependent on the security features of each mobile device), one-touch mobile SSO, and federated SSO. Using the latter capability, public safety agencies can federate their identity provider to the ICAM system, allowing users to log in with their existing credentials and gain access to authorized applications, portals, and resources. The FirstNet ICAM solution uses the attribute-based access control framework to standardize attributes to individual users so they can access different resources.

A related security challenge common among first responders is the need to move across different wireless networks without losing connectivity or having to re-authenticate themselves. To address this requirement, many public safety agencies have deployed NetMotion®, a mobile virtual private network (VPN) solution that provides a wide range of security and operational capabilities. NetMotion's capabilities—which are fully compatible with FirstNet—include the ability for mobile users to maintain session continuity and user authentication credentials throughout their travels.

FirstNet Identity Credential Access Management (ICAM)



ICAM is the front-end application through which FirstNet users can create and manage digital identities and credentials. Users can log onto FirstNet directly utilizing FirstNet-issued credentials, or have the flexibility to federate with existing credentials.

First responders will be "identity proofed" by their local agencies through ICAM and, if approved, the system will issue credentials that verify their identity and allow access to the services and applications they need. Key benefits include:

- *One touch mobile Single Sign-On*
- *Federated Single Sign-On*
- *Biometric or other multifactor authentication*
- *End-user authentication with advanced encryption*
- *Identity management*

Securing Mobile Device Data and Network Access

No one doubts that first responders can benefit greatly by having simple and non-disruptive security processes. But their agencies—and others with whom the first responders communicate—need robust, end-to-end security controls in place. Those controls start with the mobile device, the data it stores, and the network access it provides.

Although FirstNet's ICAM functionality can provide a first step in helping to secure device and network access, most midsize or large public safety organizations have already deployed enterprise mobility management (EMM) systems to provide additional security controls. At present, three EMM systems—MobileIron, VMware® AirWatch, and IBM MaaS360 with Watson™—are approved to work with FirstNet. These EMMs help agencies and departments of all sizes see, secure, and manage their mobile endpoints, meet compliance requirements, and remotely respond to security alerts.

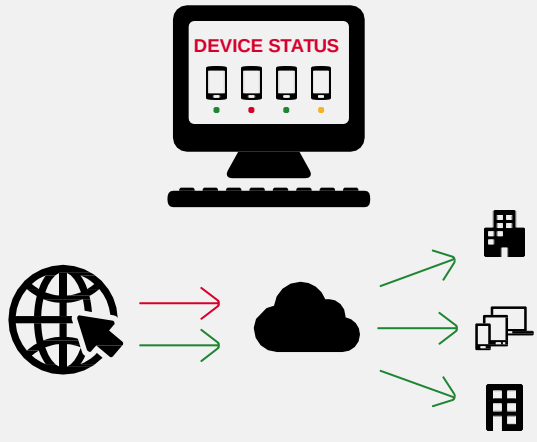
Among the many capabilities an EMM system provides is the ability of an agency to place the device in "supervised mode," locking the device into a desired configuration. This enables administrators to restrict which apps are available and what websites and databases can be accessed, make over-the-air changes or updates, or even make changes to the appearance of the device, all without requiring user intervention. An EMM system can also be set up to force devices to use a VPN or an SSL-encrypted link in order to communicate with other networks.

An EMM system is required if an agency wants to give users the ability to authenticate themselves on different devices. For example, a fire chief could use another firefighter's device with his own credentials to access FirstNet, with different permissions and capabilities. EMM capabilities also come into play in BYOD scenarios in which first responders have personal

Protection for FirstNet Mobile Devices

Prevent
Manage a diverse set of devices and help provide employees with highly secure access to approved applications.

Detect
Provide highly secure access to content and help block malware and viruses from reaching your assets.



data and apps as well as work-related content and software on their smartphones or tablets. Various "container" solutions exist to keep the personal and professional environments of the devices separate. However, enforcing the necessary security and privacy controls on the professional container side requires an EMM solution to play an oversight role.

Even if they've deployed an EMM solution, public safety agencies may want to bring in additional device-centric security controls. One common concern is the risk of so-called "man in the middle" Wi-Fi® network-based breaches, where a first responder's device is spoofed by a rogue Wi-Fi network designed to look like a legitimate and secured network. If a device logs into the masquerading Wi-Fi network, all of the transmissions to and from the device become susceptible to theft, exposure, or corruption, and malicious code and malware—such as a keylogger—can be loaded onto an unsuspecting first responder's device.

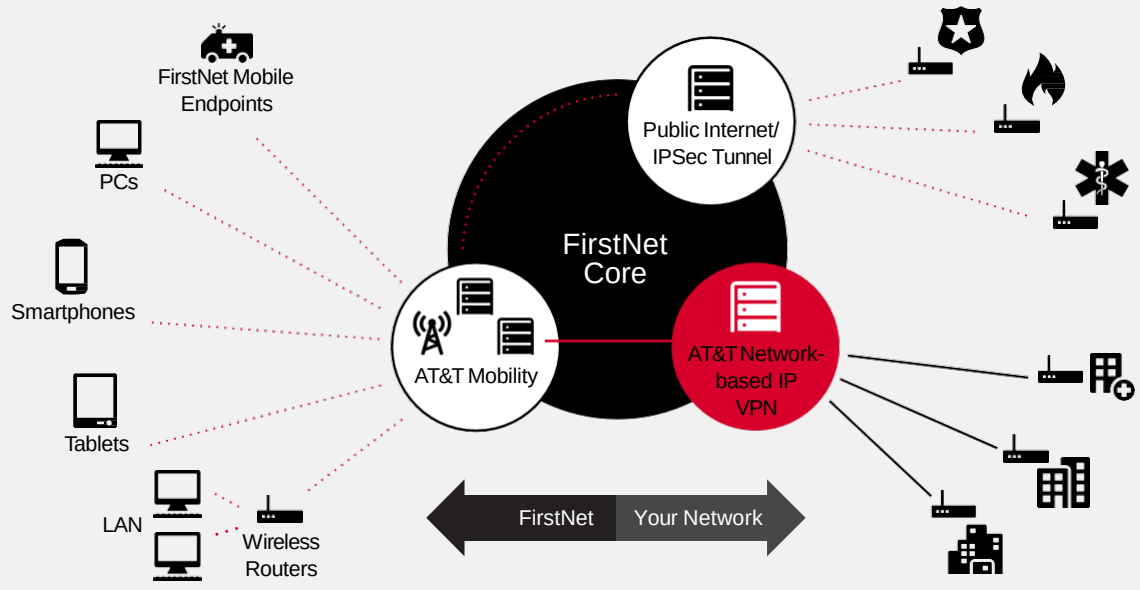
Device-centric security tools, referred to collectively as mobile threat defense, work in conjunction with the EMM solution to identify fake networks and alert users and administrators to the threat—enabling it to be blocked and remediated. Beyond countering rogue Wi-Fi networks, these mobile threat defense solutions can identify malware as well as application and operating system vulnerabilities that can also undermine mobile device and data security.

Securing Communications

Once their users are equipped with highly secure and easy-to-manage mobile devices, public safety organizations also need confidence that

▼ *Allows FirstNet customers to securely and reliably extend their WAN infrastructure to mobile end points by providing standards-based connectivity options between the enterprise and FirstNet networks.*

FirstNet Private Mobile Connection



transmissions to and from those devices are protected. FirstNet is designed with end-to-end encryption tools to support public safety users transmitting encrypted data securely across Long-Term Evolution (LTE)– enabled devices. For first responder scenarios and applications that require even greater transmission security, agencies may elect to deploy various types of VPNs. The NetMotion VPN, for example, meets the requirements of FIPS 140-2 and the Advanced Encryption Standard established by the National Institute of Standards and Technology.

Other VPN solutions focus on safe data transmissions between the FirstNet core and other destinations, including restricted government databases. Private Mobile Connection, for example, is a highly secure private connection that enables organizations to extend their agency network all the way out to mobile devices. Agencies can establish custom Access Point Names to more safely access the agencies' enterprise networks or any mobile network.

Using Private Mobile Connection, a public safety agency can also use a mobile device's IP address to control which databases the device can access. Additionally, the agency may require the device to be routed through the agency's infrastructure before reaching Internet-based sites and resources, thereby limiting that access to only approved destinations.

Strong Security Support

FirstNet staff interacts with and participates in several U.S. and international security organizations, including:

- Computer Emergency Response Team/Coordination Center (CERT/CC)
- Forum of Incident Response and Security Teams (FIRST)
- U.S. Department of Homeland Security's National Security Telecommunications Advisory Committee (NSTAC) and National Coordinating Center (NCC) for Telecommunications
- U.K. Centre for the Protection of National Infrastructure (CPNI) National Security Information Exchange (NSIE)
- Australian National Information Exchange (NIE) and National Security Information Exchange (NSIE)
- Various Information Sharing and Analysis Centers (ISACs), including Information Technology-ISAC and Communications-ISAC
- US InfraGard
- Security activities within the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE)
- Cloud Security Alliance
- IoT Cybersecurity Alliance
- Open Daylight

Securing Public Safety Applications

FirstNet has established programs and controls minimizing the risk that any applications residing on the network will become vulnerable. In the fall of 2017, FirstNet launched a developer program designed to foster the creation of innovative and highly secure public safety solutions. The program includes a specialized portal from which developers can access resources for building, testing, deploying, and maintaining highly secure public safety applications. Developers can submit their applications for evaluation, certification, and inclusion in the FirstNet App Catalog.

As part of the application evaluation process, FirstNet assesses not only an app's security but also its robustness and relevance to the public safety community. That assessment includes an evaluation of the application's performance, its service-level agreements (SLAs), and any potential source code vulnerabilities. Applications posted to the FirstNet App Catalog will carry either "Certified" or "Reviewed" labels, reflecting the applications' uptime availability, resilience, and scalability for multiple users.

Applications will also be subject to ongoing assessment. For example, if the FirstNet security team identifies a vulnerability in an existing application, the developer will be required to quickly address the problem and deliver an update.

FirstNet App Lifecycle

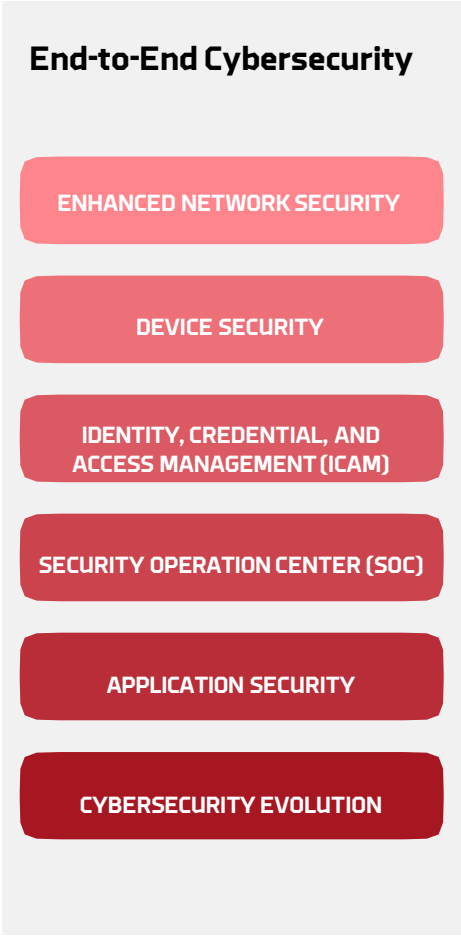
A Shared Focus on Security

As part of its contract with FirstNet, AT&T isn't just building out public safety's FirstNet national core and state-based RANs; it is also applying its extensive expertise and advanced security systems to help protect the network's users, data, and applications.

AT&T's broad and deep experience in highly secure network solutions is one of the major reasons why it became the go-to partner when the First Responder Network Authority sought to establish a strong public/private partnership delivering on its charter.

On an average day, AT&T routinely scrutinizes more than 200 petabytes of data across hundreds of billions of traffic flows on its global networks. Traffic on FirstNet will likely never approach those volumes, of course. Even so, the FirstNet Security Operations Center will apply the same sophisticated monitoring and threat intelligence tools that AT&T uses commercially to help secure this critical nationwide public safety broadband network platform.

AT&T also brings to the FirstNet ecosystem its many security relationships, including leading EMM and mobile threat defense vendors and providers of advanced solutions such as NetMotion. AT&T will continue to work to extend the FirstNet core capabilities in ways that can meet public safety agencies' security needs.



To learn more about how FirstNet can help you and your first responders perform their essential roles both effectively and securely, go to

www.FirstNet.com

FIRSTNET™