



5G Security Overview

May 24, 2021

The call will begin shortly



5G Security Overview

May 24, 2021

Housekeeping

General:

- This call will be recorded.
- Slides and a recording will be distributed afterwards.
- Participants are muted upon entry.

Questions:

- Feel free to unmute yourself!
- Please submit questions into the chat box or question box
- “Raise your hand” and I will ask you to unmute
- Please chat or email ladams@nga.org with any technical questions



Agenda

I. 5G Security Overview

- Robert J. Zapotocky, Senior Principal Architect, AT&T Public Sector
- Nick Arconati, Director, Chief Security Office, AT&T
- Brian Daly, Assistant Vice President Standards and Industry Alliances, AT&T
- Patrick Robinson, Associate Director Public Sector Cyber Security, AT&T

II. Roundtable Discussion with AT&T

III. Audience Q&A





AT&T 5G Security Overview

Robert J Zapotocky | Senior Principal Architect, AT&T Public Sector

Nick Arconati | Director, Chief Security Office, AT&T

Brian Daly | Assistant Vice President Standards and Industry Alliances, AT&T

Patrick Robinson | Associate Director Public Sector Cyber Security, AT&T

May 24, 2021

5G Security Framework

Embedded Security Controls in 5G design instead of standalone technologies, coupled with insights and learnings from previous Wireless technologies



IOT



RAN



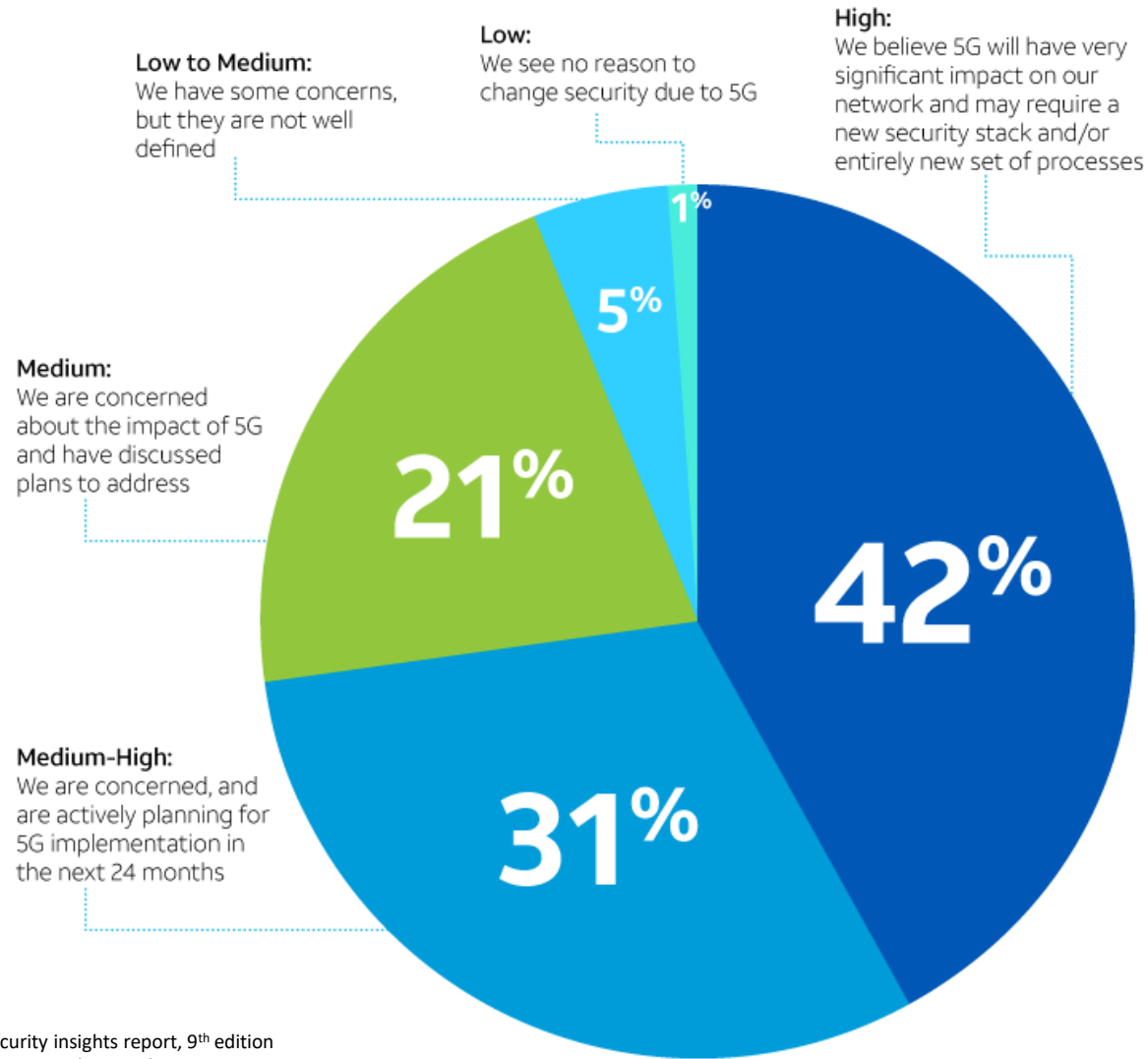
Mobile Edge



Smart Core



Enterprise 5G Security Posture Perception



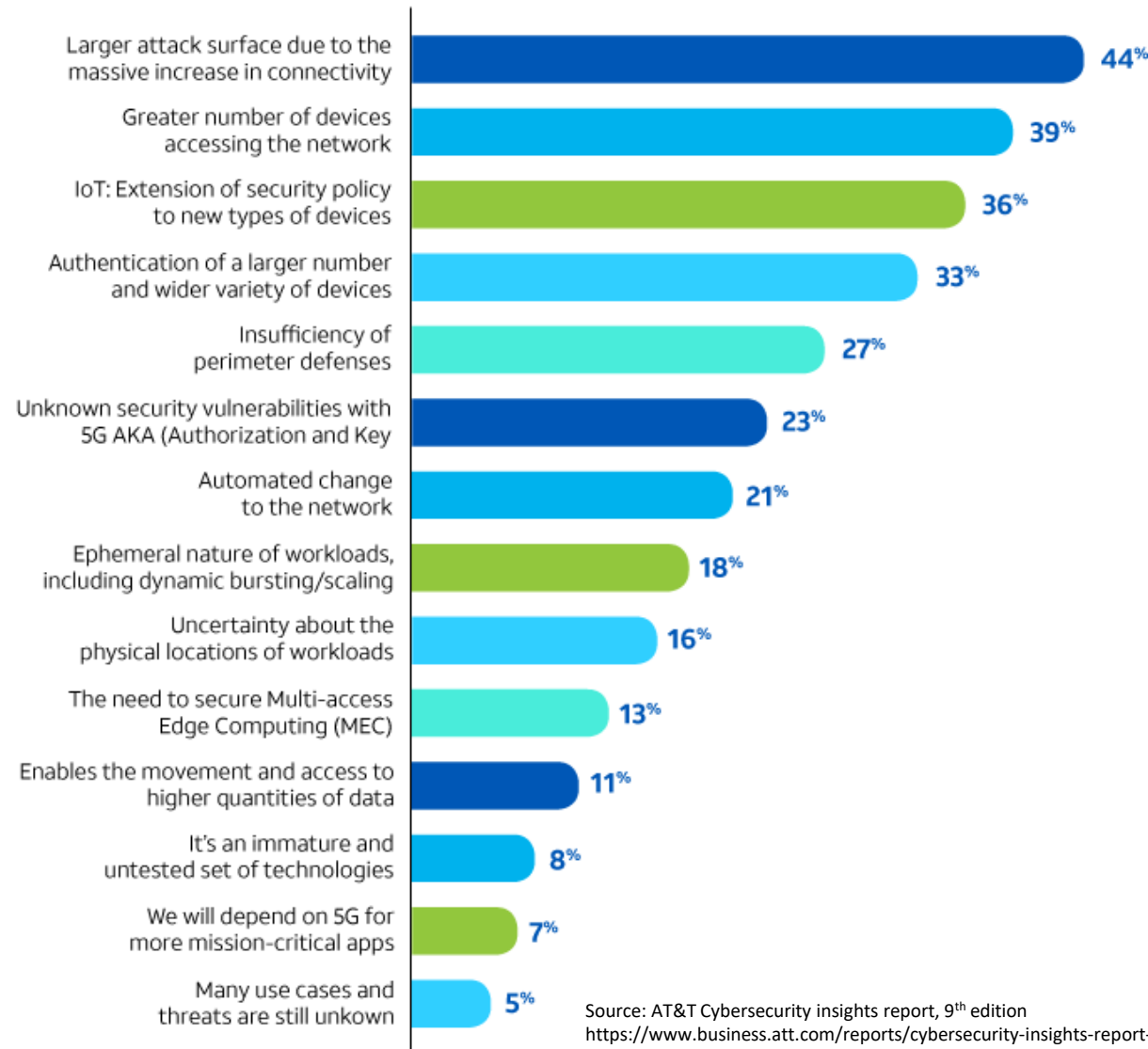
“How concerned are you about the effect of 5G on your security posture?”

- 72.5% of the respondents rated their level of concern as high or medium-high
- Primary areas driving perception; 5G networks will bring new vulnerabilities and many organizations have not implemented or only partially implemented asset discovery and management and vulnerability assessment and remediation security programs.

Source: AT&T Cybersecurity insights report, 9th edition
<https://www.business.att.com/reports/cybersecurity-insights-report-ninth-edition.html>



Top 5G Security Areas of Concern



What are your top 3 security concerns regarding 5G?

- Increased attack surface due to massive increase in connectivity
- Greater number & variety of devices accessing the network
- Complexity of extending security policy to new types of non-traditional and IoT devices



The Foundation: 5G Development

Differences between 5G and LTE

Mobile Edge as a new network segment to enable next gen ultra-low latency and high bandwidth applications

Mobile Edge includes elements traditionally part of the RAN and mobile Core

Security controls are embedded in the network design to ensure highly secure implementation day-one compare to previous wireless technologies

Enhanced Security in 5G compare to LTE

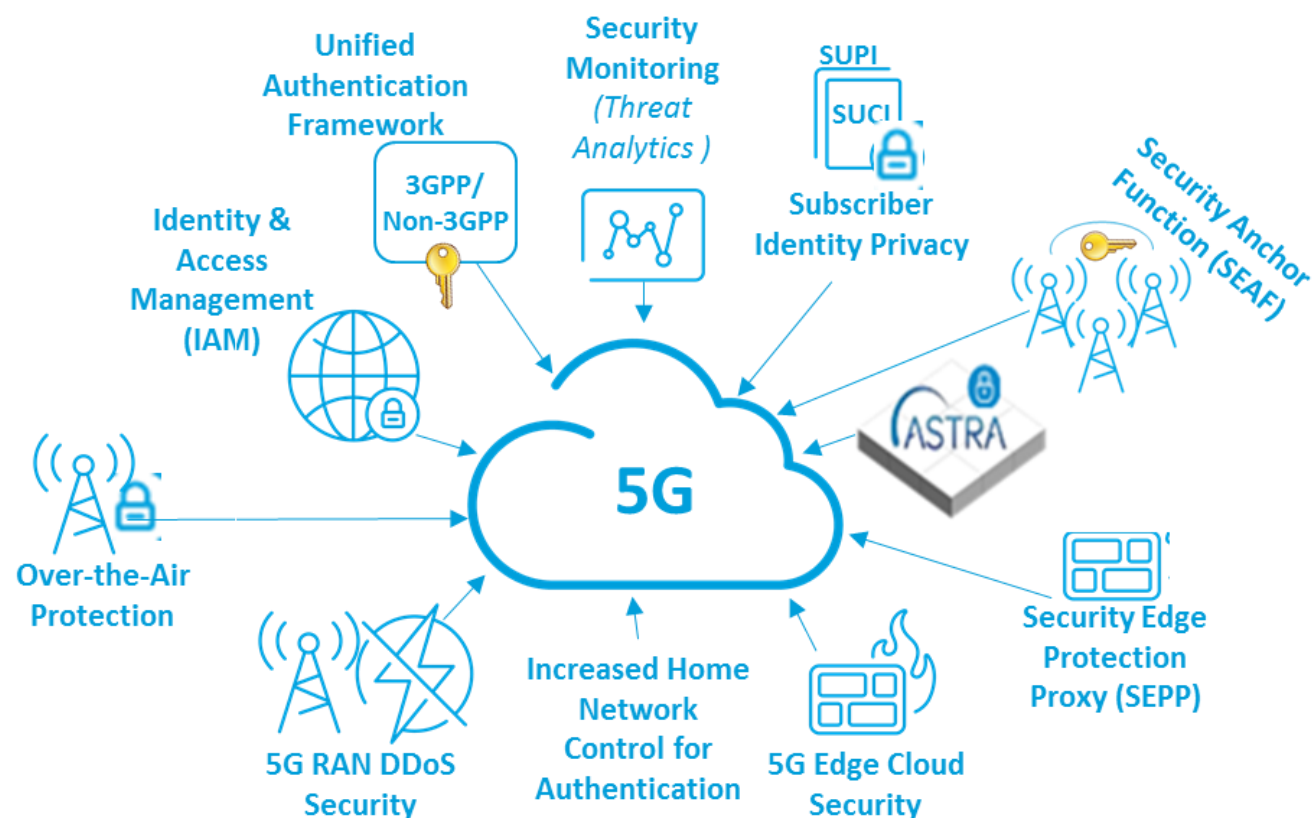
Distributed security with the ability to block malicious IoT traffic at the edge of the network

DDoS detection and mitigation embedded in the edge of the network

Stronger encryption algorithms to enhance over-the-air interface

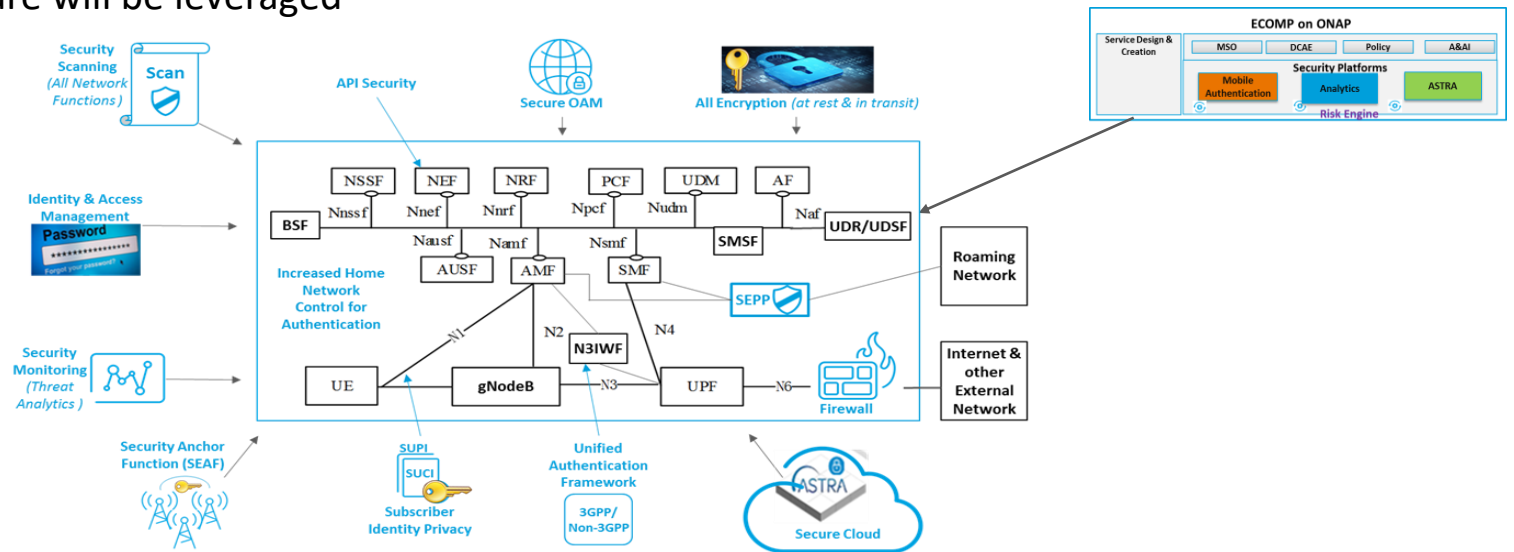
Enhanced subscriber privacy features and seamless authentications

Proxy capability to mitigate signaling attacks experienced with previous wireless technologies



❖ Software Defined Networking/Virtualization

- 5G will be built on a virtualized platform taking advantage of NFV, SDN and Containerization along with ECOMP-on-ONAP
- Closed-loop automation based on ECOMP-on-ONAP and virtualization's inherent elasticity feature will be leveraged



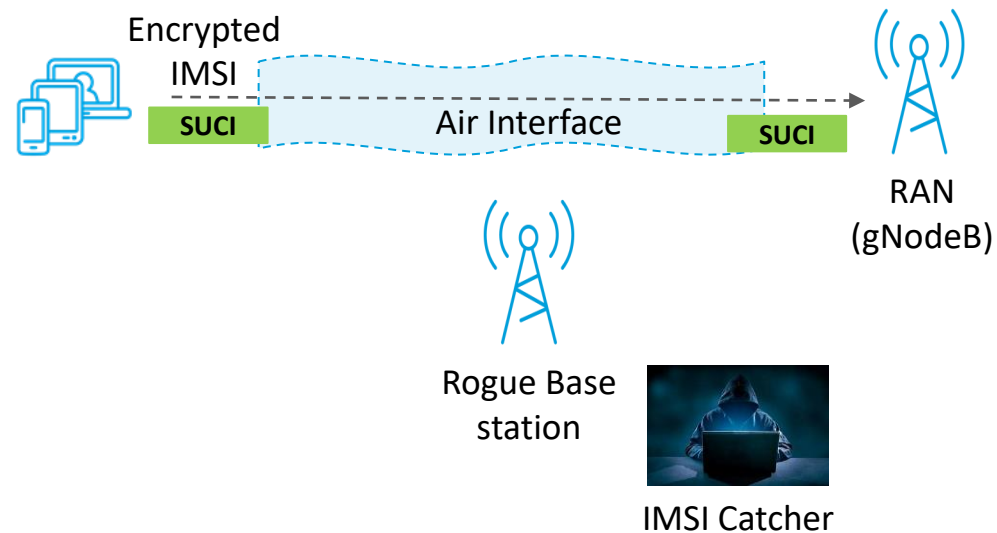
❖ Stronger 3GPP encryption for over-the-air encryption

- Provide confidentiality and integrity protection between the 5G mobile devices and the 5G network (*enforce 128-bit AES for over-the-air and 256-bit AES between network functions.*)

Security Advantages with 5G

❖ Subscriber Identity Privacy

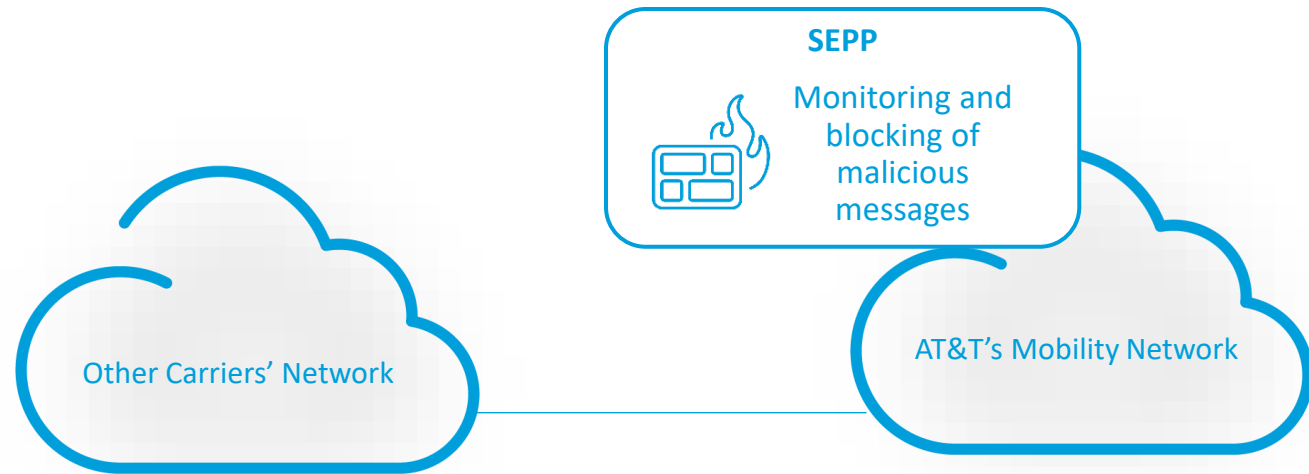
- Subscription Concealed Identifier (SUCI) to conceal(encrypt) and protect the 5G Subscription Permanent Identifier (SUPI / IMSI)
- Mitigates the risk of IMSI catchers currently present in previous wireless technology



Security Advantages with 5G

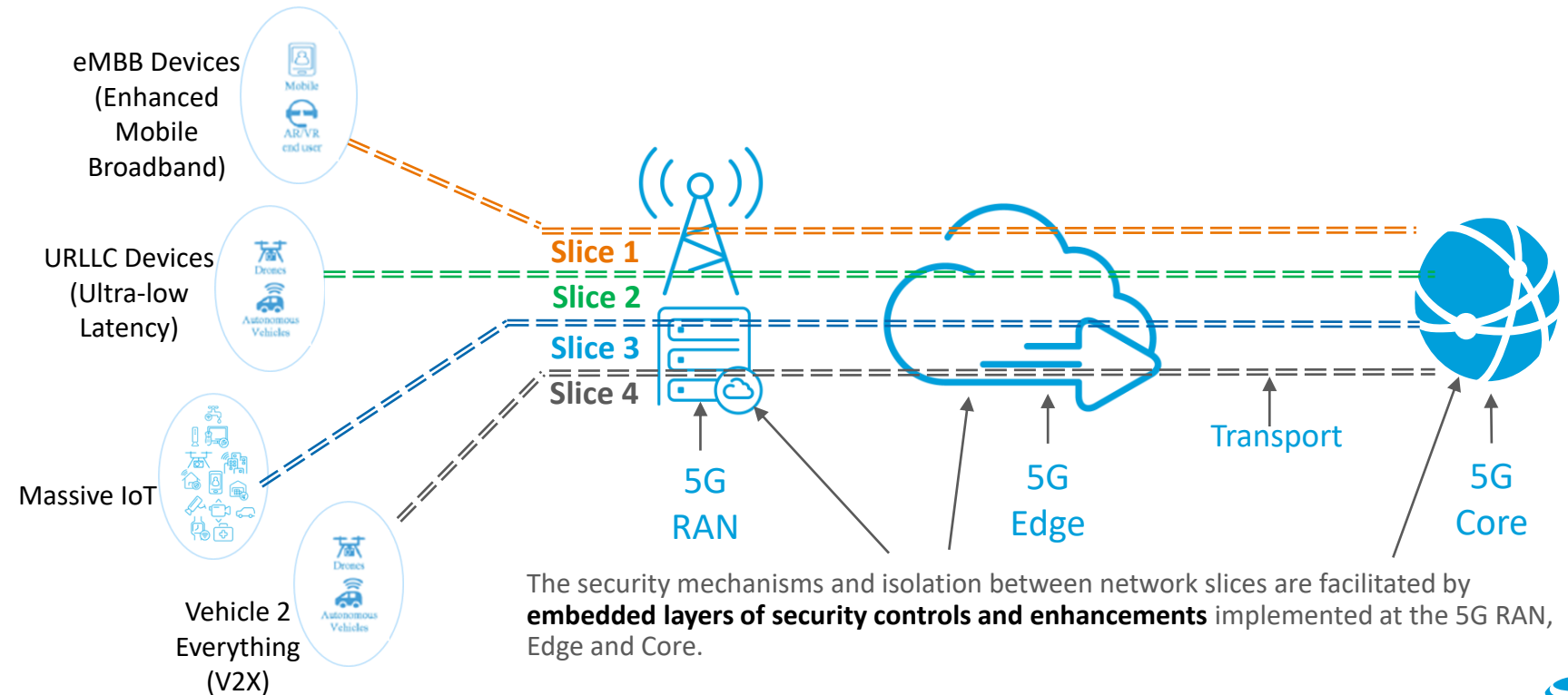
❖ Roaming or network-to-network protection

- 5G's new Security Edge Protection Proxy (SEPP) element at the operators roaming border
- Embedded security control to mitigate the risk of signaling attacks



Security Advantages with 5G

- ❖ **Network Slicing** is an infrastructure segmentation capability for network resources. The network resources can be physical or virtual, dedicated to a given slice or shared between slices. Slicing allows for isolation and segmentation of the mobility network traffic for security and privacy purposes.





New Attack Vectors in 5G

❖ 5G Edge attacks from 3rd party applications & new external connections

- 5G Edge can be located on enterprise premise to facilitate Ultra-low latency services. Direct connections to the Internet streamline connectivity which no longer need to pass through the mobility core.
 - Security controls need to mitigate risk of data exfiltration/leakage and malware via unauthorized access and connections; including the risk of insider abuse of enterprise or carrier personnel.
- **Mitigations:** Virtual firewall, host/network IDS/IPS, malware protection, encryption, RBAC, MFA, security monitoring and scanning

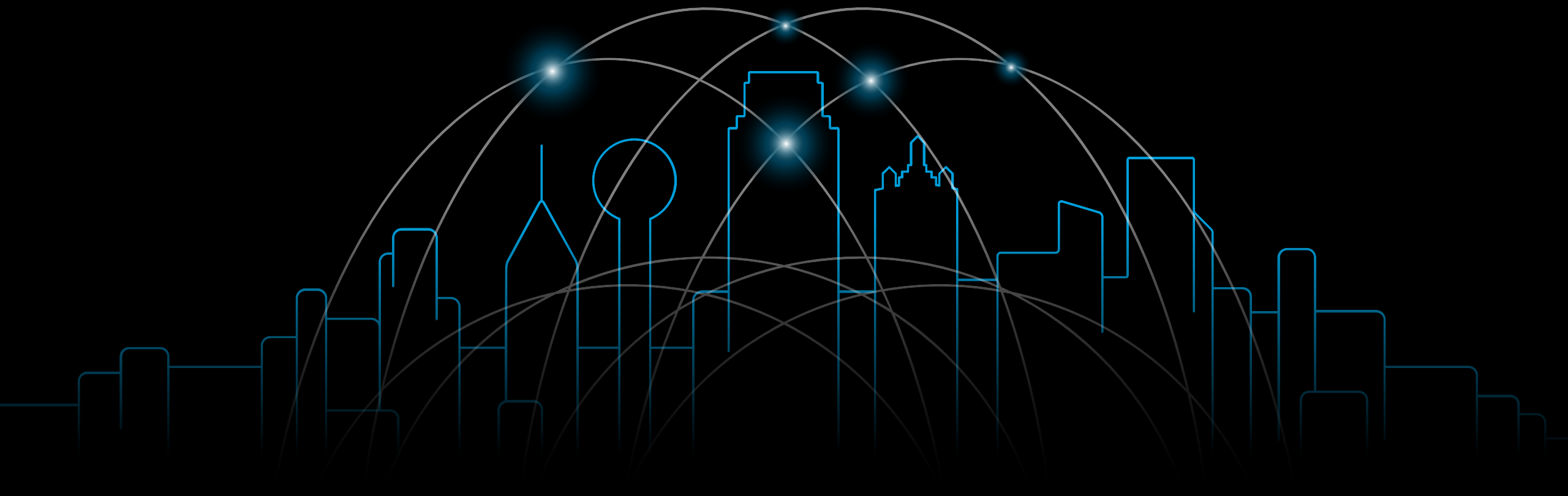
❖ DDoS attacks against the 5G RAN via Massive IoT

- 5G will facilitate billions of Things connecting to the 5G RAN
- Many of these Things will have Zero Day vulnerabilities which can be exploited and potentially used to execute DDoS attacks against the 5G RAN and services
- **Mitigations:** Embedded network controls, network slicing, and O-RAN via RIC



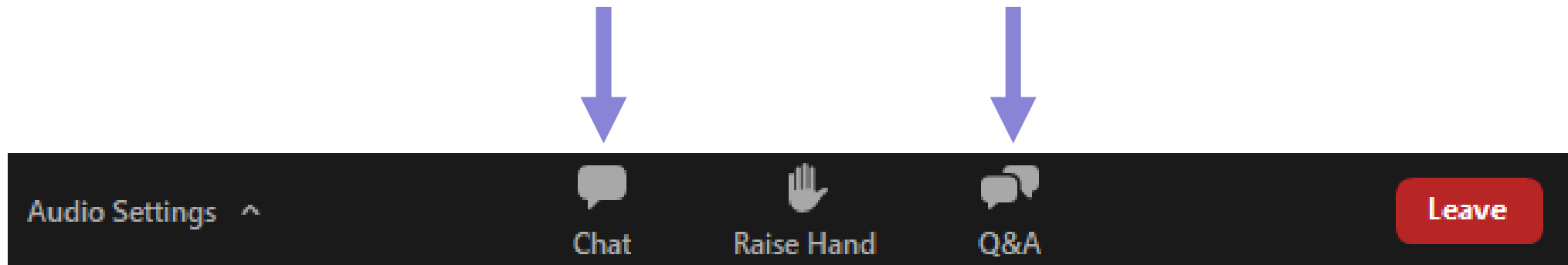


AT&T Public Sector



Audience Q & A

- Please submit questions into the chat box
- Unmute yourself
- Please chat or email Ladams@nga.org with any technical questions



Contact

John Guerriero

Cybersecurity Program

Jguerriero@nga.org

Lacy Adams

Policy Coordinator

Cybersecurity Program

Ladams@nga.org

