



PSCR 2021

THE DIGITAL EXPERIENCE

#PSCR2021 • PSCR.GOV

NIST

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Guest speaker, Dean Prochaska from FirstNet Authority produced and presented slides 12 to 20 for publication in the National Institute of Standards and Technology's PSCR 2021 The Digital Experience. The contents of their presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government.

Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change

Posted with Permission.

Glossary

3G: 3rd Generation

3GPP: 3rd Generation Partnership Program

5G: 5th Generation

ICT: Internet Communications Technology

IPSec: Internet Protocol Security

LTE: Long Term Evolution

MC: Mission Critical

NR: New Radio

Oauth: Open Authorization

PS: Public Safety

TCP/IP: Transmission Control Protocol/Internet Protocol

TLS: Transport Layer Security

V2X: Vehicle to Everything

UE: User Equipment

VOLTE: Voice Over LTE

A STANDARDS UPDATE | 5G, MISSION CRITICAL SERVICES & SECURITY

Jeff Cichonski

Cybersecurity Engineer
NIST

Dean Prochaska

Senior Director Technology Standards
FirstNet

NIST

#PSCR2021





WHAT IS A STANDARD

Standards are quantifiable metrics to which parties adhere for purposes of allowing some common ground for interchange. A language is a standard for communication. The alphabet is a base standard for the exchange of information. Most of the standards in the realm of information & communication technology specify the nature of the agreement that will allow two things to interact.

FOUNDATIONAL STANDARDS ORGANIZATIONS



Internet Engineering Task Force

Internet Protocols

- TCP/IP, TLS, IPSEC



3rd Generation Partnership Program

Cellular Systems

- 3G, LTE, VOLTE, 5G



European Telecommunications Standards Institute

Virtualization Standards

ICT Standards



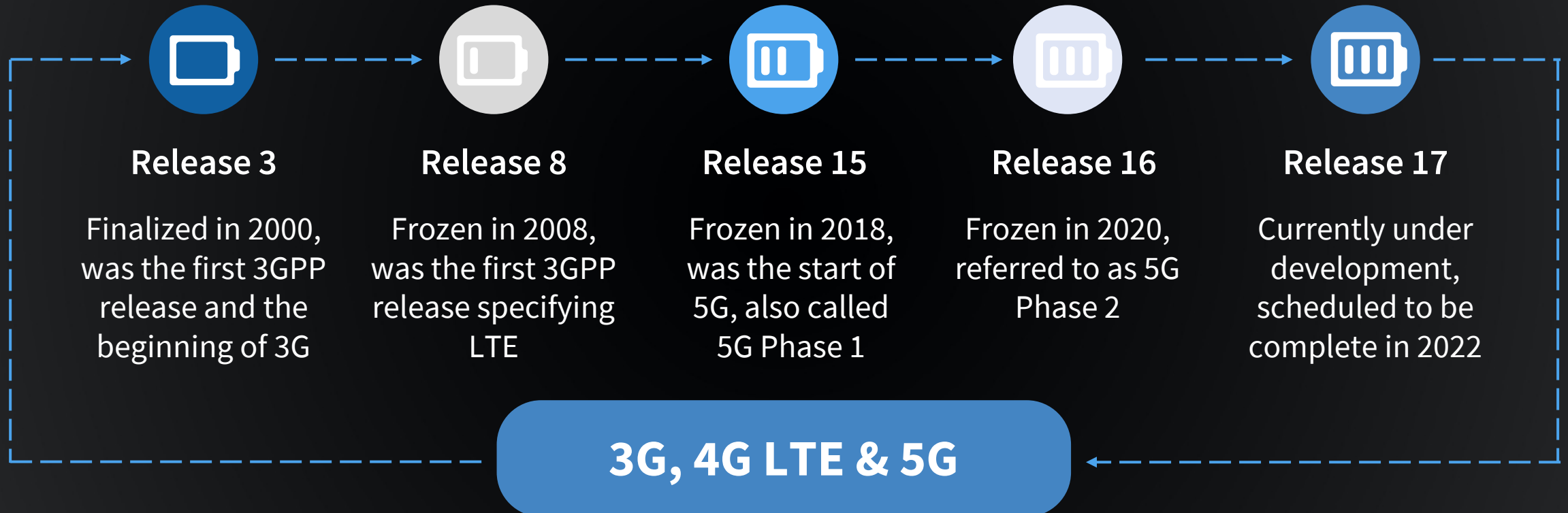
Institute of Electrical and Electronics Engineers

802.11 - WiFi

3RD GENERATION PARTNERSHIP PROJECT (3GPP)



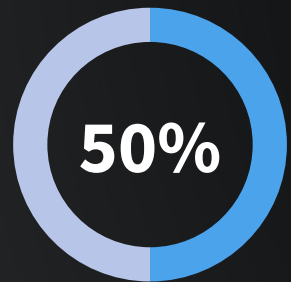
3GPP RELEASE TIMELINE



5G STANDARDS OBJECTIVES

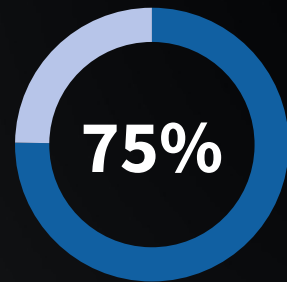
Three Core Tenants

Super fast speeds, ultra-reliable low latency, and massive number of connections



3GPP Release 16

2020

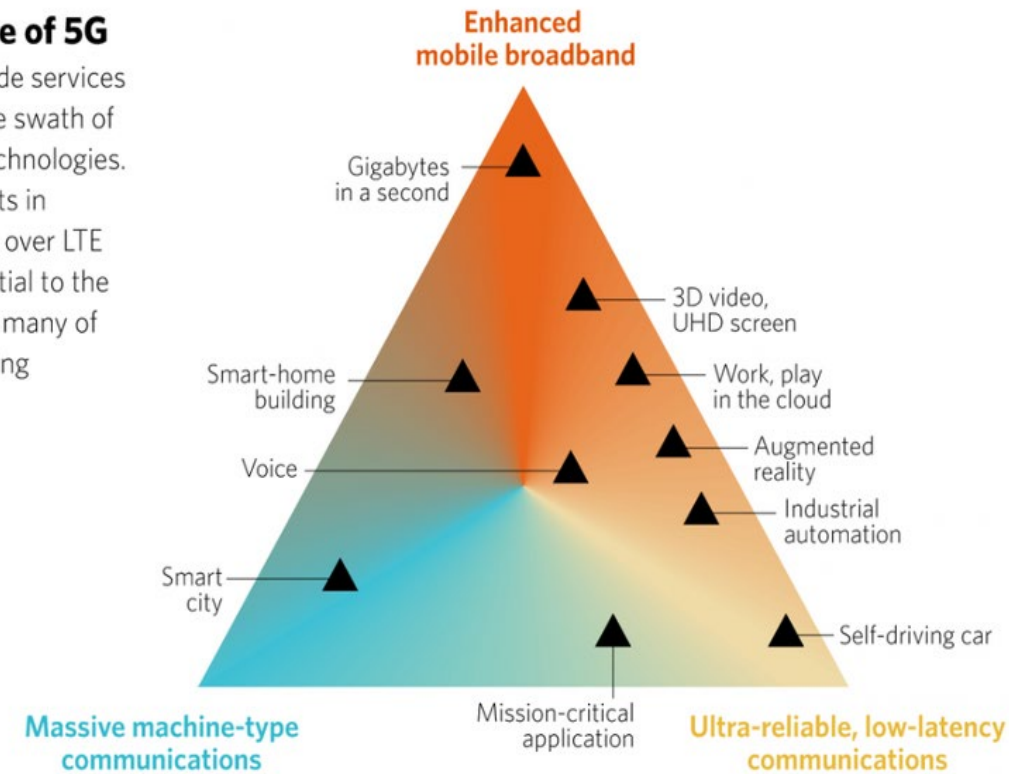


3GPP Release 17

2022

Future Use of 5G

5G will provide services across a wide swath of disruptive technologies. Improvements in performance over LTE will be essential to the future use of many of these emerging applications.



Copyright Stratfor 2018

SECURITY ENHANCEMENTS



Subscriber Privacy

System design changes that promote the protection of a subscriber's permanent identifier.



User Plane Integrity Protection

5G's new key hierarchy enables integrity protection to user plane traffic over the air.



New Authentication Methods

Provide additional flexibility for authenticating devices on a network while retaining robust security.



Network Exposure Function

Support for OAuth for secure exposure of network services to third-party applications over API.

A SECURE LOOK AHEAD

IMPORTANT SECURITY DISCUSSIONS HAPPENING NOW



256-Bit Cryptographic Algorithms

Evaluations and technical discussions are happening to identify and specify acceptable 256-bit algorithms to be used in future releases.



UE to Network Relay Security

SA3 is designing security and privacy functionality to support proximity services UE to Network Relay.



Network Slicing Security

Security considerations for network slicing are currently under discussion and development.

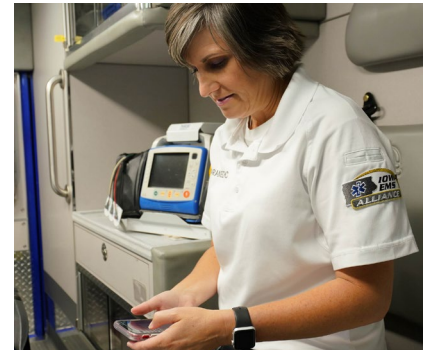


FirstNet Authority Standards Update

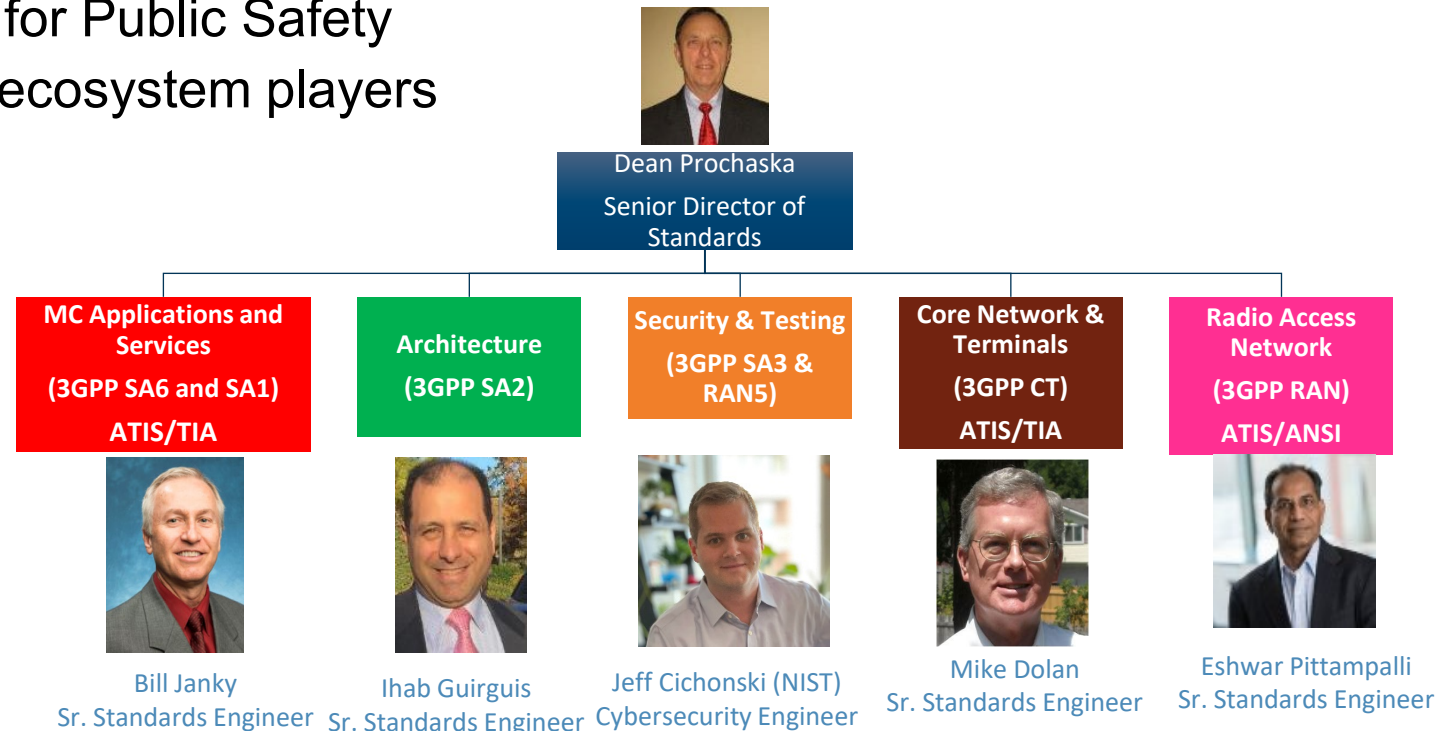
PSCR Stakeholder Conference 2021

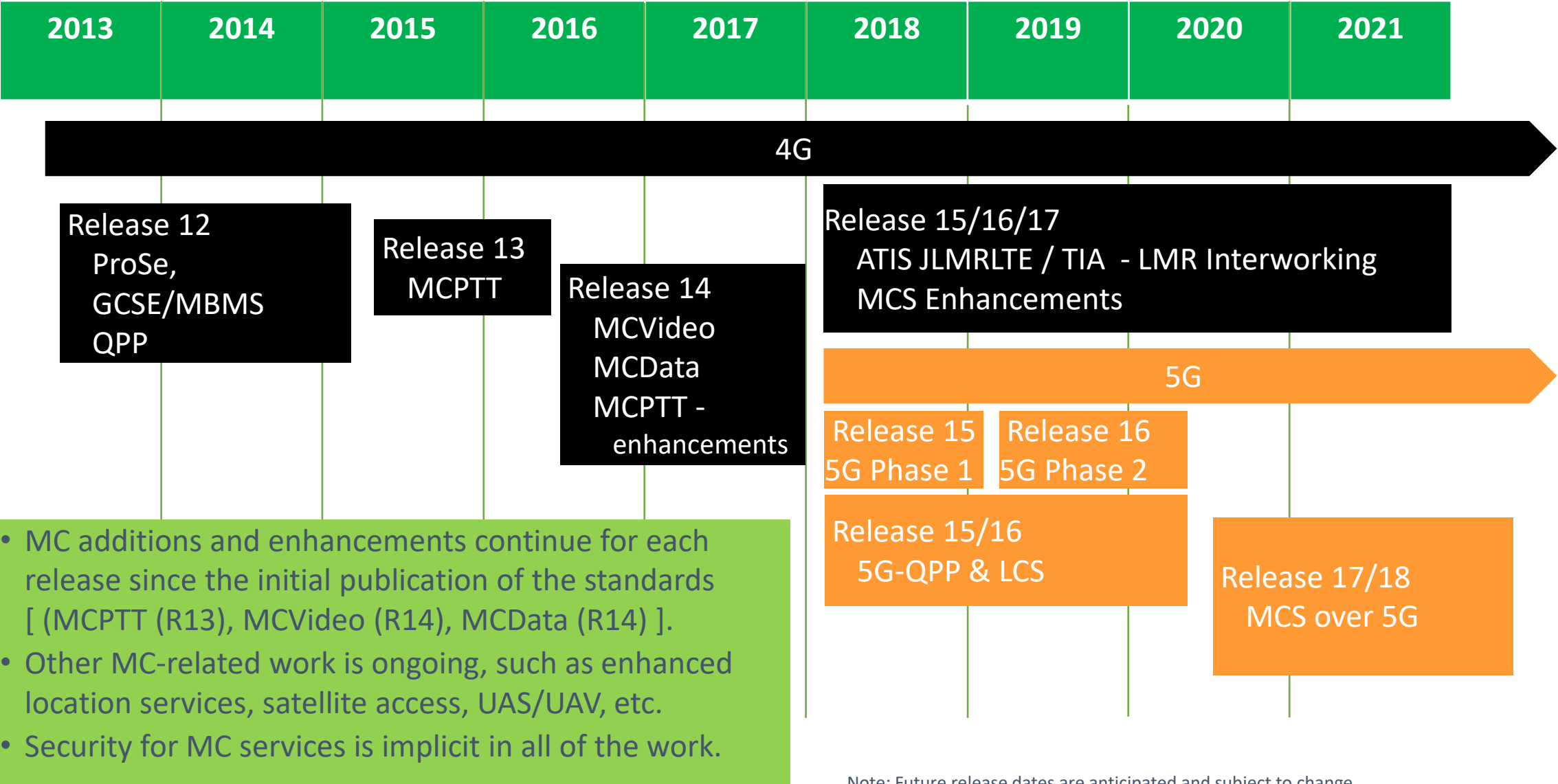
Dean Prochaska

Senior Director Technology Standards



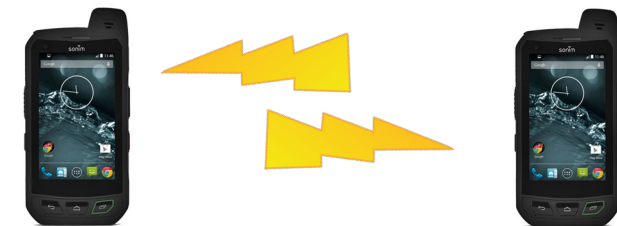
- ❖ Leads Public Safety contributions
 - Build consensus via collaboration
 - Co-signs important contributions with Public Safety members from around the world
- ❖ Most public safety representatives in 3GPP Working Groups
 - Participates in CT (Core and Terminal) working groups, and most SA (System Architecture) and RAN (Radio Access Network) working groups
- ❖ Introduce new service requirements for Public Safety
 - Collaboration with 3GPP wireless ecosystem players
- ❖ Designated as the 3GPP lead for Plugtest issue resolution
- ❖ Partner with over ten global PS entities (e.g., UK Home Office, S. Korea, Germany, Finland, the Netherlands, French Ministry of the Interior, etc.)



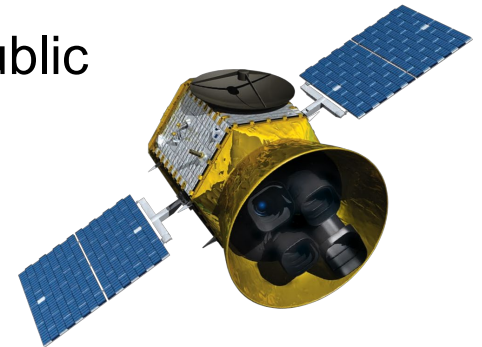


Note: Future release dates are anticipated and subject to change.

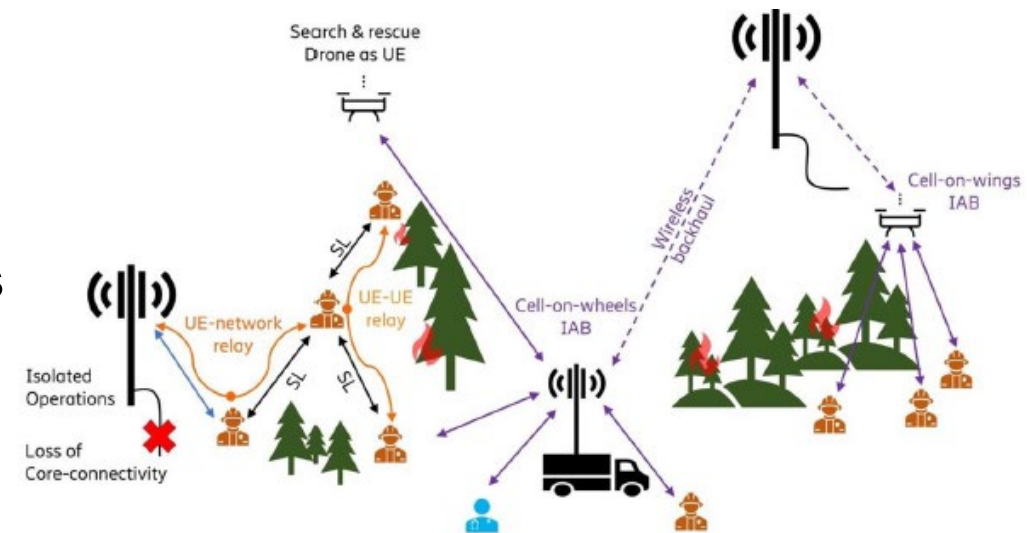
- ❖ 5G NR Proximity Services Direct Communications
 - Provides off-network coverage
 - Relay coverage extension
 - V2X used as a basis to take advantage of economies of scale
- ❖ 5G NR Multicast Broadcast
 - Supports broadcast and multicast modes in 5G NR
- ❖ Dynamic Spectrum Sharing (DSS) Enhancements
 - DSS provides a migration path from LTE to NR by allowing LTE and NR to share the same carrier at the same time
- ❖ Release 18 study for a vehicle mounted relay (VMR)
 - Supports coverage extension



- ❖ NR positioning enhancements
 - Enhanced positioning accuracy requirements for general commercial and Industrial Internet of Things (IIoT) use cases:
 - For commercial : sub-meter level position accuracy (< 1 m) and for factory floor, IIoT: position accuracy < 0.2 m
 - Some of the solutions developed for commercial could be used for public safety as long as the requirements can be met
- ❖ RAN enhancements to improve device battery life
 - Reduce UE paging reception
- ❖ Support for Non-Terrestrial Networks (i.e., satellite)
 - Provides connectivity in low / no cellular coverage for industries such as transportation, solar, oil and gas, utilities, farming, environmental monitoring and mining



- ❖ Isolated Operation for Public Safety (IOPS)
 - Provide communication between MC UEs when a cell, or group of cells, is disconnected from the core
- ❖ Gateway UE
 - A device to connect multiple 3GPP or non-3GPP devices to the 4G/5G network via non-3GPP access methods (e.g. Ethernet, Bluetooth)
- ❖ MCX Enhancements
 - Enhanced location services, addition of some MCPTT features to MCData/MCVideo, e.g., functional alias, and other enhancements
- ❖ MC services over 5G
 - General agreement on a phased approach to bringing MC services onto 5G
 - First phase will include on-network, unicast services
 - Next phases will include off-network and multicast-broadcast (dependent on development in other working groups)



❖ Standards Organizations

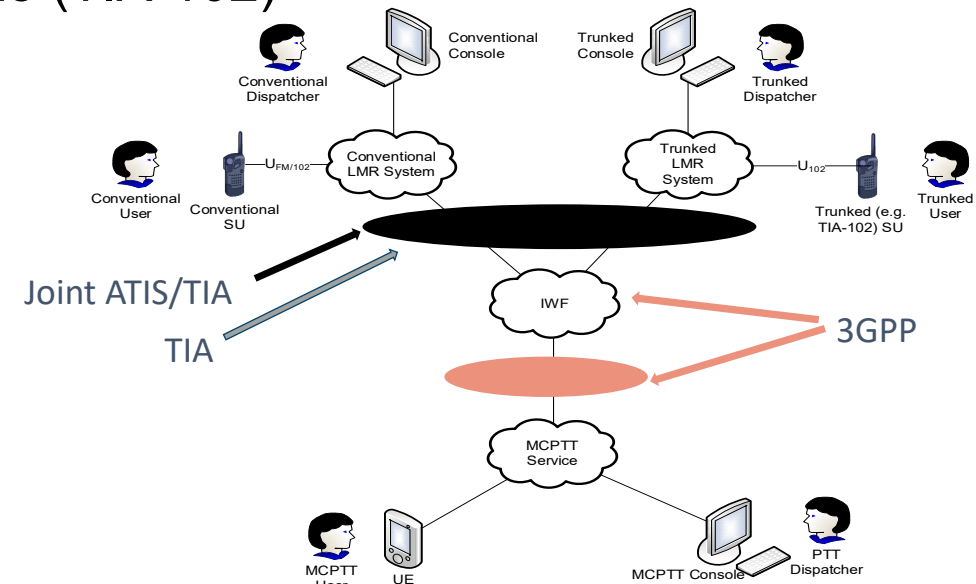
- ATIS/TIA joint committee, JLMRLTE, is developing the Stage 2 architecture
- TIA TR-8 is defining the Stage 3 protocols

❖ JLMRLTE

- Work has been unofficially organized in phases with architecture hand-off to TIA at phase completion
- Phases 1, 2 and 3 are complete (all common P25 trunking features); phase 4 in progress
- Phase 4 will focus on conventional operation, both P25 (TIA-102) and analog FM (TIA-603) conventional interworking

❖ TIA

- Completed Stage 3 and voted to publish addenda supporting phases 1, 2, and 3 (TIA-102.BACA-B-3 and TIA-102.BACD-B-3)
- ATIS/TIA development will continue through 2021
- Complete Phase 4



❖ Interworking features/functions are supported in phases 1, 2, and 3

Addressing

- TIA-102 trunking unit and group addressing
- TIA-102 conventional unit and group addressing
- 3GPP MC unit and group addressing
- TIA-603 analog conventional group system addressing

Mobility Management

- Registration/De-registration
- Affiliation
- De-affiliation
- Supplementary services registration

Security Services

- Encryption overview
- Key management including details for end-to-end encryption

Supplementary Services

- Emergency Alarm and Emergency Alarm cancel (P25 trunked and conventional)

Voice Services

- TIA-102 Trunking
 - Group call – non-emergency and emergency, and call continuation
 - Broadcast Group Call
 - Announcement group call
 - System group call
 - Individual Voice Call – Non-Emergency – with and without availability check
- TIA-102 Conventional
 - Digital conventional group transmission – non-emergency
 - Digital conventional group call – call continuation
 - Digital conventional group transmission – emergency
- Audio takeover
- Group emergency cancel

Thank you!

For questions contact:

dean.prochaska@firstnet.gov