# Overview of ITL's Public Safety Cybersecurity Efforts

**Nelson Hastings**

Electronics Engineer
National Institute of
Standards & Technology

**Sheila Frankel**

Computer Scientist (Security)
National Institute of
Standards & Technology

# Session Description

*This session will provide an overview of ITL's involvement with public safety communication research including a brief description of the joint NIST/NTIA Public Safety Communications Research (PSCR) program. The session will provide insight into ITL's approach toward cybersecurity research for public safety communication networks based on Long Term Evolution (LTE) technology, a brief description of current research, and participation in the LTE security standardization efforts.*

# Agenda

- Background
- Why is NIST involved?
- Public Safety Communications Research Program
- Cybersecurity Research Efforts
- Cybersecurity Standard Development Efforts

# Background

- Public Law 112-96 Middle Class Tax Relief and Job Creation Act of 2012
- Calls for the establishment of a nationwide, interoperable public safety network
- Initially funded by the auction of reallocated spectrum, then self funded after 2022

# Background

- Established the First Responder Network Authority (FirstNet)
  - Deploy and operate a Nationwide Public Safety Broadband Network (NPSBN)
  - Maintain and upgrade the network
  - Develop network infrastructure and device criteria
  - Represent the interest of public safety users before standards organizations

# Why is NIST involved?

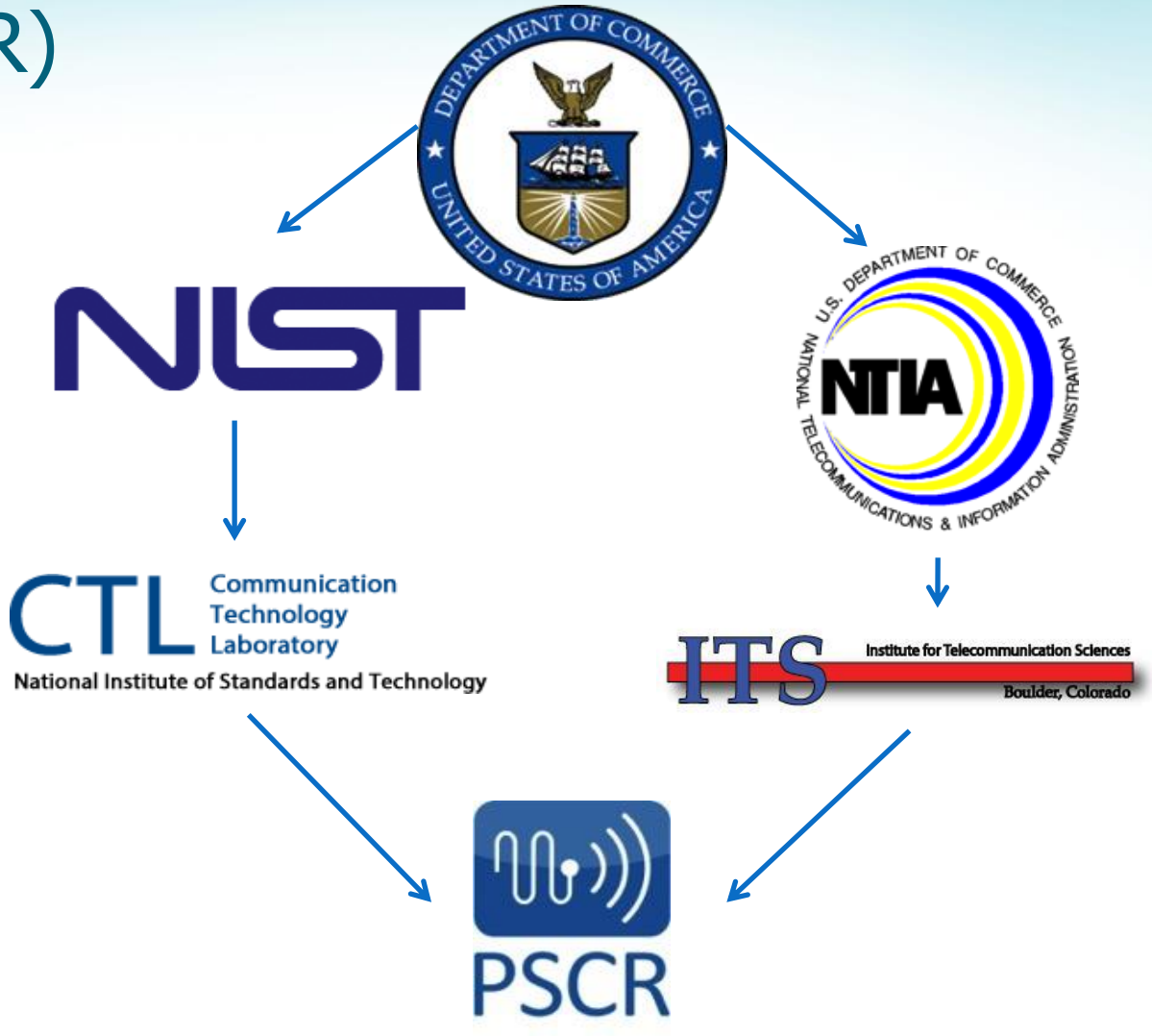
- Legislation calls on NIST to
  - Conduct research and assist with the development of standards, technologies, and applications to advance wireless public safety communications
  - Document public safety wireless communications technical requirements
  - Establish a research plan, and direct research, that addresses the wireless communications needs of public safety entities
  - Accelerate the development of mission critical voice, including device-to-device "talkaround" capability over broadband networks, public safety prioritization, authentication capabilities, and standard application programing interfaces for the nationwide public safety broadband network, if necessary and practical

# Public Safety Communications Research Program (PSCR)

Located at the
Department of Commerce
Boulder Labs in Colorado

The PSCR Program is a joint effort between:

NIST's
Communications Technology Laboratory (CTL)
and
NTIA's
Institute for Telecommunication Sciences
(ITS)



# PSCR Sponsors

- Department of Homeland Security's Office for Interoperability and Compatibility (DHS S&T OIC)
- Department of Homeland Security's Office of Emergency Communications (DHS NPPD OEC)
- First Responder Network Authority (FirstNet)
- National Institute of Standards and Technology (NIST)
- National Telecommunications and Information Administration (NTIA)

# PSCR Portfolio

| Broadband Standards and Technologies | Emerging Standards and Technologies |
|---|---|
| 700 MHz Demonstration Network | Bridging LMR & LTE |
| Requirements and Standards | Video Quality |
| Mission Critical Voice | Cybersecurity Research |
| Modeling and Simulation | R&D Technology Roadmapping |
| RF Propagation Studies | |
| Audio Quality | |

# NIST's Information Technology Laboratory Expertise

- The Computer Security Division (CSD)
  - Cybersecurity Risk Management
  - Cybersecurity Standards
  - Identity Management
  - Network Security
- The Software and System Division (SSD)
  - Software Assurance
- Information Access Division (IAD)
  - Human Factors
  - Usability

# Cybersecurity Research Efforts

- Investigating different identity management technologies for mobile device that could support public safety's requirements
  - NIST IR 8014 Considerations for Identity Management in Public Safety Mobile Networks (March 2015)
  - Developing document on authentication technologies and their ability to support different public safety disciplines
- Cybersecurity features (e.g. authenticating to a mobile device) should not interfere with public safety personnel performing their mission
  - Acquiring background knowledge from subject matter experts in fire, law enforcement, and EMS
  - Documenting current authentication challenges from public safety's perspective

# Cybersecurity Research Efforts

- Using the PSCR demonstration network, investigating the extent optional 3GPP capabilities to secure network interfaces are implemented in LTE equipment
  - Developed and executed a test plan to secure the interface between the base station and core network using IPSEC
    - Documenting results and updating test plan
  - Developing test plan to secure the interface between mobile devices and base stations
- Mobile applications provide the opportunity for software weaknesses and vulnerabilities to disrupt network operations and provide unauthorized access to information
  - Held two workshops in cooperation with APCO and FirstNet to identify and document public safety mobile application security requirements
  - NIST IR IR 8018 Public Safety Mobile Application Security Requirements Workshop Summary (January 2015)
  - Developing summary of workshop held in June 2015 and survey of mobile application vetting services

# Cybersecurity Research Efforts

- Mapping public safety network security requirements to existing threat mitigation security controls to determine if additional requirements should be considered
  - Using public safety requirements such as the NPSTC High-Level Launch Requirements
  - Mapping to existing security controls such as
    - NIST's Cybersecurity Framework (CSF)
    - NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

# Standards: 3GPP LTE

- **Motivation**: FirstNet, the nationwide dedicated Public Safety Broadband Network that is currently under development, will be a 3GPP (Third Generation Partnership Project) LTE (Long Term Evolution) network. However, public safety has special requirements, not met by commercial broadband networks.
- **Goal**: Work on the development of the 3GPP LTE standards to ensure that they fulfill, as much as possible, the demanding requrements of public safety practitioners for security, scalability, availability, and reliability.
  - Represent public safety and FirstNet in 3GPP's security working groups (SA3 and SA3-LI)
  - Ensure that features critical to public safety align with US public safety's requirements

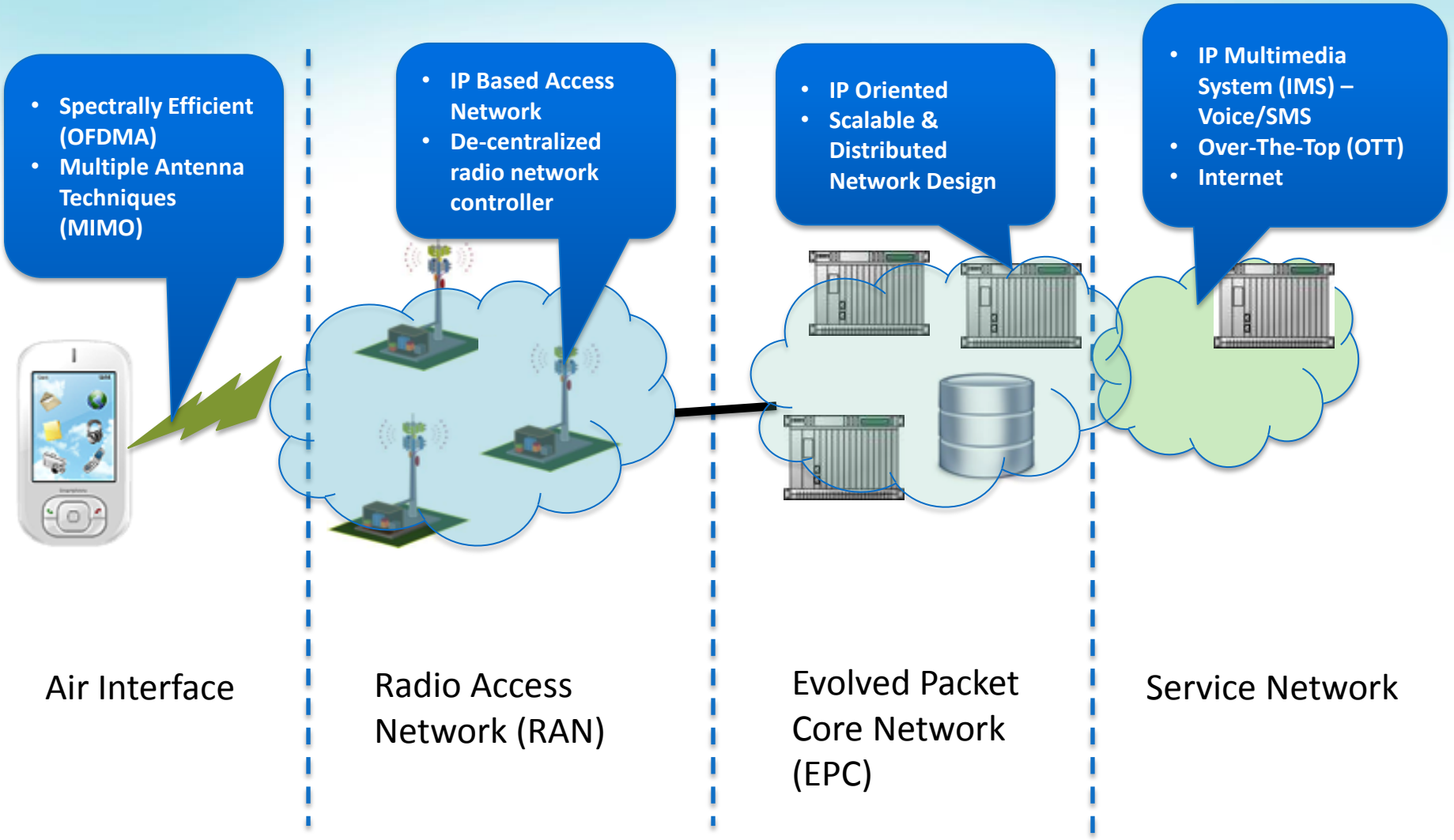
# Standards: 3GPP LTE (cont'd)

- **Strategy**
  - Push as much of this work into 3GPP as possible, making standards based solutions globally available for all public safety operators given operating needs
  - Public safety vs. commercial: prevent development of separate solutions, maximizing use of commercial products
  - Expand this work into commercial areas (social network, gaming, etc.) as much as possible to grow market opportunity
  - Global: coordinate with global public safety community (critical to drive unified standards solution)
- **Risks**
  - Some commercial operators are expressing interest in public safety; some are disinterested from a commercial perspective
  - Proprietary app development, increasing procurement and operations costs, and maintenance of multiple app management systems (e.g. group management)

# Standards: 3GPP LTE (cont'd)

- **Process**
  - Each individual feature is developed over several LTE releases
  - Initial deployment: minimal solution
  - Later releases: added enhancements

# Standards: LTE Network Architecture



# Standards: 3GPP Structure

## Technical Specifications Group (TSG) Structure

| TSG GERAN | TSG RAN | TSG SA | TSG CT |
|---|---|---|---|
| **GSM EDGE Radio Access Network** | **Radio Access Network** | **Service & Systems Aspects** | **Core Network & Terminals** |
| GERAN WG1<br>Radio Aspects | RAN WG1<br>RL 1 Spec | SA WG1<br>Services | CT WG1<br>MM/CC/SM (lu) |
| GERAN WG2<br>Protocol Aspects | RAN WG2<br>RL 2 Spec<br>RL 3 RR Spec | SA WG2<br>Architecture | CT WG3<br>Interworking w/ Ext networks |
| GERAN WG3<br>Terminal Testing | RAN WG3<br>Lub, lur, lu specs<br>UTRAN O&M Reqs | SA WG3<br>Security | CT WG4<br>MAP/GTP/BCH/SS |
| | RAN WG4<br>Radio Perf<br>Protocol Aspects | SA WG4<br>Codec | CT WG6<br>Smart Card App Aspects |
| | RAN WG5<br>Mobile Terminal Conformance Testing | SA WG5<br>Telecom Mgt | |
| | | SA WG6<br>Mission Critical Applications | |

# Standards: Proximity-based Services

- Proximity Services (ProSe)
  - The equivalent of direct mode or talk around in Land Mobile Radio terminology.
  - Enables critical communications without network coverage
  - Components:
    - Discovery: ability to discover other devices in physical proximity
    - Communications: ability to directly communicate with 1 or more devices in physical proximity without infrastructure
    - Relays: device-to-device and device-to-network
  - Other beneficial results (also applicable to commercial applications)
    - Reduce network load
    - Increase capacity in given bandwidth

# Standards: Group Communications

- Group Communications System Enablers (GCSE)
  - Making the 3GPP ecosystem more group aware, allowing more efficient group and broadcast communications by forcing 3GPP RAN and EPC to track group membership in addition to device location and facilitate group communications setup
  - Most public safety communications are group based
  - Features:
    - Dynamic groups involving mobile users and dispatchers
    - Support for large groups (perhaps up to 5000)
    - Dynamic membership
  - Complication:
    - Some vendors are trying to limit level of group awareness in 3GPP

# Standards: Mission Critical Push to Talk

- Mission Critical Push to Talk (MCPTT)
  - A group communication service with fast setup times, ability to handle large groups, strong security and priority handling
  - Requirements (more stringent than those for regular communications):
    - Direct mode
    - Priority control
    - Floor control
    - Individual and group calls
    - Interworking with other voice systems (e.g. PSTN, LMR)
    - Imminent Peril and Emergency calls and alerts
  - Future developments
    - Mission Critical Data (MCData)
    - Mission Critical Video (MCVideo)

# Standards: Isolated E-UTRAN Operation for Public Safety

- Isolated E-UTRAN Operation for Public Safety (IOPS)
  - Locally routed communication for devices with no network connection or experiencing temporary or intermittent loss of network connectivity
  - Challenges
    - Special credentials for user and device authentication without access to the centralized database
    - Pre-configuration of known local devices vs. inclusion of non-local devices

# Questions?