Standards and Requirements in 15 Minutes




Peter Reed

June 6, 2013

ADD PTCRB

PSCR
Public Safety Broadband
Stakeholder Conference

Standards and Requirements: early planning

- NPSTC and FCC Minimum Interop – completed
- Public Safety Grade Availability
  - TIA-222, rev g: Structural Standards for Communication Towers
  - TIA-942: Telecom Infrastructure Standard for Data Centers
- Standards groups
  - GSMA and ATIS
  - NFPA: In-building RF radiation, building safety rating
  - PTCRB
- PLMN ID and Numbering Plan
- Network Security Requirements
- Interfaces to external networks: potential third-party networks
  - Managed Trusted Internet Protocol Service (MTIPS)
  - Public Safety IP Network (PSInet)
  - National Transport Network
  - Nlets
  - Public Safety database access
- Local control

Public Safety Input To Date: More than 1,300 Requirements

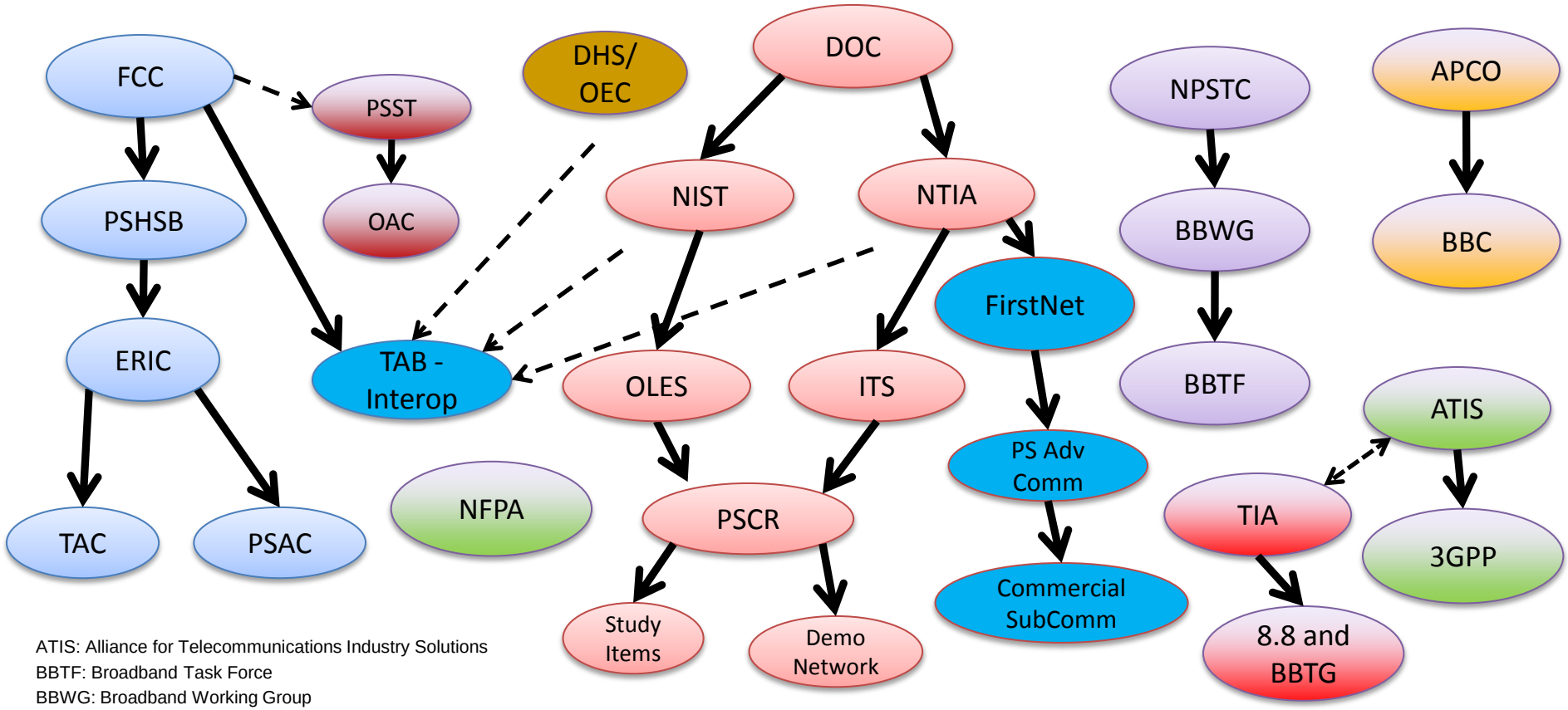
NPSTC Requirements	# of Req's
User Services	312
Network Services	209
Transport Requirements	154
System Design	66
User Equipment	60
Local Operations Support	157
Migration and Evolution	60
Governance	10
Policies and Procedures	94

FCC Minimum Interopability Specifications	# of Req's
Requirements (Must)	46
Considerations (Should)	55
Interfaces (Architectural)	11
Recommended Interfaces Requirements	9

FirstNet will:

- Build on the foundation of early work done by public safety groups
- Seek vendors who will meet or exceed these requirements
- Broaden the requirements to increase flexibility and decrease costs

Regulatory/Standards Influencers



ATIS: Alliance for Telecommunications Industry Solutions
BBTF: Broadband Task Force
BBWG: Broadband Working Group
DOC: Department of Commerce
DHS/OEC: Department of Homeland Security / Office of Emergency Communications
ERIC: Emergency Response Interoperability Center
FCC: Federal Communications Commission
GSMA: GSM Association
ITS: Institute for Telecommunications Sciences
NFPA: National Fire Protection Association
NIST: National Institute of Standards and Technology

NPSTC: National Public Safety Telecommunications Council
NTIA: National Telecommunications and Information Administration
OLES: Office of Law Enforcement Standards
PSAC: Public Safety Advisory Committee
PSCR: Public Safety Communications Research
PSHSB: Public Safety Homeland Security Bureau
PSST/OAC: Public Safety Spectrum Trust / Operational Advisor Committee
TAC: Technical Advisory Committee
3GPP: 3rd Generation Partnership Project

Telecom Infrastructure Standard for Data Centers: TIA-942

Tier 3 – Concurrently Maintainable: 99.982% Availability

Typical Commercial Data Center

- Enables planned activity without disrupting operation, unplanned events can cause disruption
- Multiple power and cooling paths but only one active, includes redundant components (N+1)
- Reliability of parallel data centers: 99.99999% availability (7 9's)

Tier 4 – Fault Tolerant: 99.995% Availability

Special construction

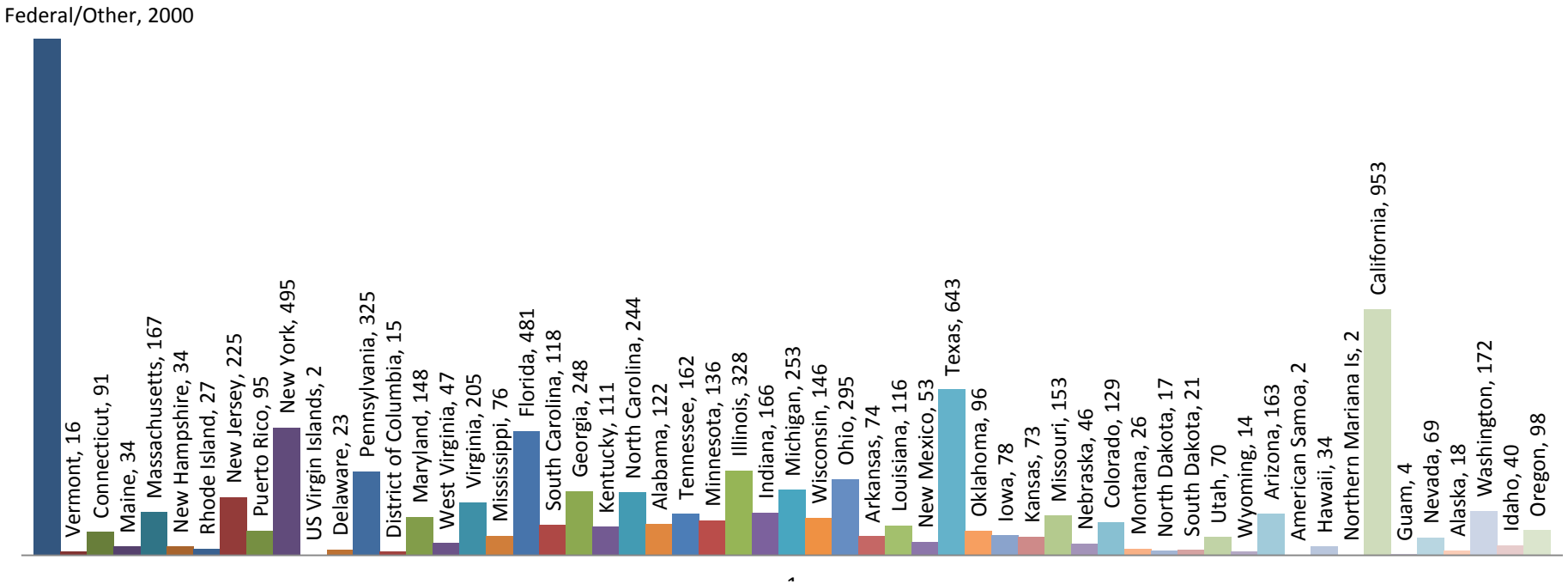
- Planned activity does not disrupt critical elements. Can sustain at least one worse-case unplanned event with no critical load impact.
- Multiple active power and cooling distribution paths. Two UPS with redundant components.
- Reliability of parallel data centers: 99.999999% availability (8 9's)

Public Land Mobile Network ID (PLMN ID)

- FirstNet PLMN ID is 313-100
  - Ninety-nine more held on reserve at ATIS, can be obtained later
    - "313" is a Globally unique country code.
  - Thank-you: DHS OEC, PSCR, and contractors SAIC & Dr. Devasirvatham
  - DHS OEC to continue support until FirstNet has automated process
- Defines FirstNet uniquely across all States, territories, tribal areas.
- IMSI: PLMN ID + Mobile Subscriber Identity (MSIN)

MSIN Allocation by Block

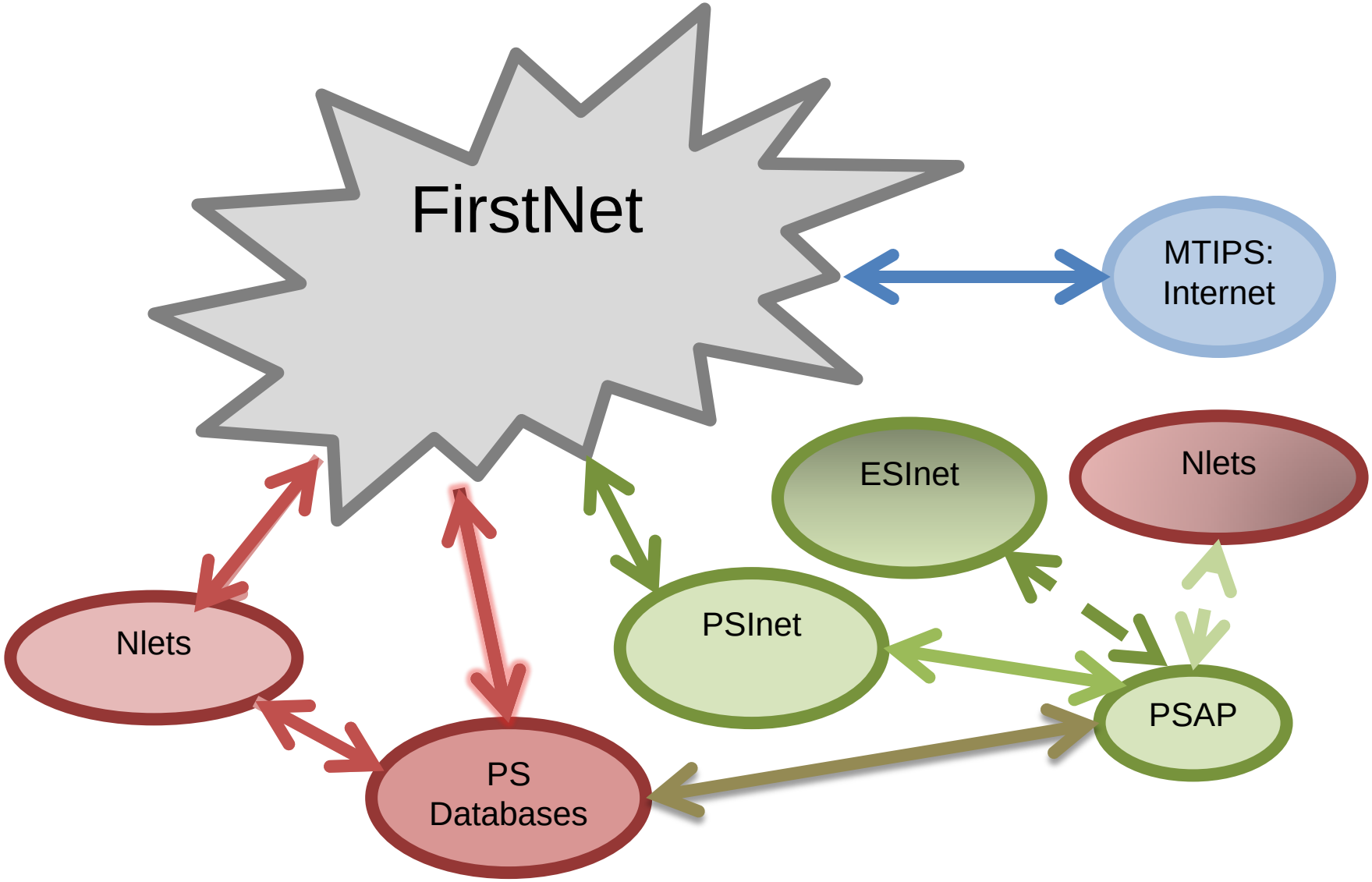
100M Identifiers (2000Blocks) allocated to Federal/Other
400M Identifiers (8000 Blocks) allocated to States and Territories
500M Identifiers (10000 Blocks) reserved for future growth (Not Shown)



Network Security Requirements

- Assigning Impact Levels and Security Categorization
  - NIST SP 800-60: two impact studies:
    1. Nationwide Public Safety Broadband Network Cyber Infrastructure Risk Assessment (CIRA) - DHS
    2. NPSTC BBWG Security Task Group (STG)
- Next steps FIPS 200 / NIST SP 800-53
  - Most likely, MOD/High Appendix F "Security control catalog"
- All third-party networks are in a separate security zones.
- US-CERT and DHS security consultants

Some third-party networks



FirstNet's Core Network CoS Marking

QCI	DSCP (name/value)	Notes
-	CS6 (48)	Network routing protocols
1, 5, 7	EF (46)	MC voice, IMS signaling
2,3	AF41(34)	Conversational video (GBR), robotics?
4	AF31(26)	Video (GBR)
6	AF21(18)	Video (non-GBR)
8, 9	BE (00)	TCP apps

- Differentiated Services (DSCP): Field in IPv4 & IPv6 to identify quality of service (QoS).

* Base requirements: NPSTC QoS definition document

Preemption Needs of PS community

Application	Default preemption		Responder emergency		ICS in use		Immediate peril		
Mission critical voice	y	n	y	n	y	n	y	n	Must <u>always</u> be available
Mission critical data (CAD)	n	y	y	n	n	y	y	n	
Low priority voice	n	y	y	n	n	y	y	n	
Video	n	y	y	n	n	y	y	n	
File transfer	n	y	y	n	n	y	y	n	

Cell Legend:

Can preempt (y / n)	Can be preempted (y / n)

Interface to third-party networks: COS Marking

QCI	DSCP	Notes
1, 7, 5	EF (46)	MC voice
2,3	AF41(34)	Conversational video (GBR), command/control
4, 6	AF31(26), AF33(30)	Video (GBR), Video (non-GBR)
8, 9	BE (00)	TCP apps and all other undifferentiated applications

* Four class of service (CoS) most common commercial design.

Managed Trusted Internet Protocol Service (MTIPS): Internet Access

- Protected by best-in-class intrusion detection and prevention systems
  - Current and future standards compliance to strict IETF, NIST, and other industry requirements
  - Best-in-class systems, 3rd generation
  - Monitored by specialized security operations centers
    - Requires specialized trained engineers
  - Available through AT&T, Verizon, Sprint, CenturyLink
    - FirstNet could build own MTIPS facilities

Local Control: Governance

- Network design and delivery
  - SLAs with local entities that contain guarantees and penalties
  - An unbiased process for dispute resolution must be in place (e.g., Neutral 3rd party arbitration)
- Cell site selection
  - Location and coverage rules
- Network topology
  - Must support interconnection to existing PS data and application services
  - Must reuse existing local entity IP networks
  - Must provide flexibility to reuse existing backhaul facilities

* Base requirements: NPSTC Local Control document

Local control: User and device management

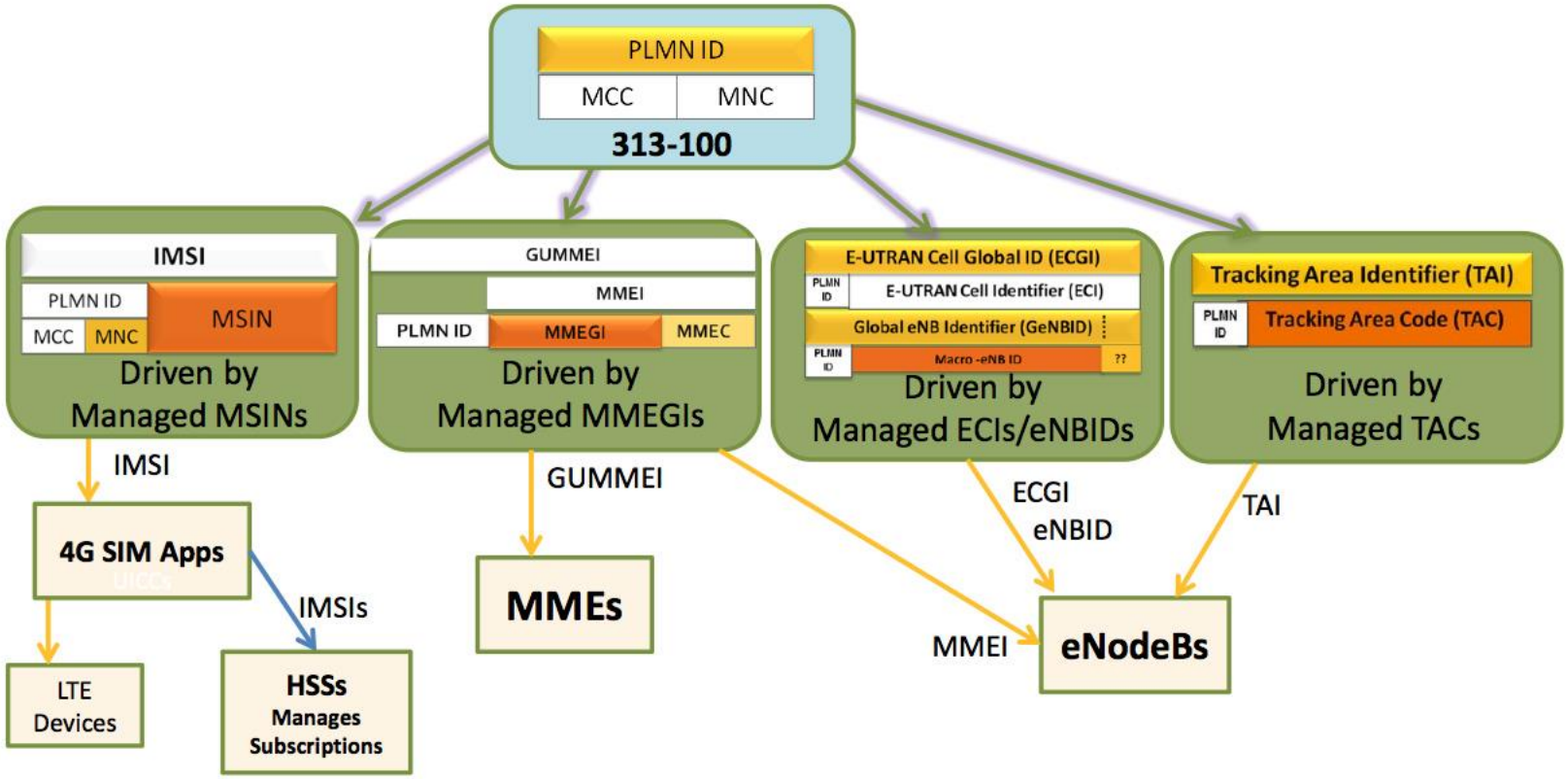
- Subscription management
  - Local entities must have ability to change, add or delete device subscription of all users in their span of control
    - control of change event timing (i.e. so they don't occur when the bars are closing)
- Device Procurement
  - Local entity to choose any LTE device from NTIA list
  - Local entity may bring their own device
- Device inventory controlled by local entity

Local Control: Network operations and maintenance

- Network monitoring
  - Ability to view local network status – e.g., network faults
  - Notification of local maintenance plans
  - Ability to view local network utilization and congestion
- Control of scheduling for network maintenance
- Local entity must have autonomy to invoke dynamic QoS policies
  - Pre-configure templates to account for different user/device priority and preemption requirements of public safety

APPENDIX

Identifiers in an LTE Network



NPSTC User Requirements Analysis

Technical Requirements	*Launch SoR*
User Services	80
Network Services	55
Transport	43
System Design	40
User Equipment	9
Local Operations Support	42
Migration and Evolution	10
Administrative Requirements	
Governance	2
Policies and Procedures	39

FCC Interop Minimum Requirements

Requirements by Category	*Desirable Considerations*
Network Architecture Evolution (12)	IMS
Handover/Mobility (6)	VoLTE
Prioritization/QOS (8)	eMBMS
User Equipment (5)	NG911 Interworking
Testing (6)	Roaming continuity
Security (9)	UICC Extensions