

Definitions - Acronyms

(All references are FirstNet related) [Definitions](#)

[A](#) • [B](#) • [C](#) • [D](#) • [E](#) • [F](#) • [G](#) • [H](#) • [I](#) • [J](#) • [K](#) • [L](#) • [M](#) • [N](#) • [O](#) • [P](#) • [Q](#) • [R](#) • [S](#) • [T](#) • [U](#) •

[V](#)

•

[W](#)

•

[X](#)

• [Y](#) • [Z](#)

[Acronyms](#)

Definitions

3GPP - The 3rd Generation Partnership Project (3GPP) is a collaboration among telecommunications associations known as the Organizational Partners. The initial scope of 3GPP was to make a globally applicable third-generation (3G) mobile phone system specification based on evolved Global System for Mobile Communications (GSM) specifications within the scope of the International Mobile Telecommunications-2000 project of the International Telecommunication Union. The scope was later enlarged to include the development and maintenance of:

- GSM and related 2G and 2.5G standards, including GPRS and EDGE
- UMTS and related 3G standards including HSPA
- Long Term Evolution and related 4G standards
- An evolved IMS developed in an access-independent manner

ABAC - Attribute-based access control defines an access control paradigm whereby access rights are granted to users through the use of policies that combine attributes together. The policies can use any type of attributes (e.g., user attributes, resource attributes, environment attributes).

Aggregation Network - A regional network that aggregates backhaul traffic toward regional data centers and national transmission networks.

AppContainer - The virtual machine construct also referred to as a sandbox, which creates an isolated security boundary around the application to keep its operation isolated from other applications and the operation system.

Application components - consisting of the overlay software and testing necessary for the use of the network features.

Application Ecosystem Security - The policies, technology, and controls to protect data applications within the applications store, the development environment, and the distribution system from the store to the various user equipment types.

Application Security Certification - The process whereby applications are vetted to ensure compliance with security controls. Applications must be compliant during development and tested in actual operation before being authorized for use on the NPSBN.

Attenuation - The gradual loss in intensity of any kind of flux through a medium.

Availability - The third leg of the Confidentiality, Integrity, and Availability triad of information systems security. Availability refers to the availability of information resources. It is critical to ensure the highest levels of availability in all contexts of the FirstNet environment.

Backhaul network - Network that consists of the network required to connect the RAN sites to the core network.

Band 14 - The spectrum licensed to the First Responder Network Authority (FirstNet) to create a nationwide public-safety wireless broadband network. It represents 20 MHz of highly desirable spectrum in the 700 MHz band that provides good propagation in urban and rural areas and decent penetration into buildings.

Blacklist - An electronic list that indicates devices or applications that are blocked from

operating on a network, including blocked websites that may not be accessed.

Bring Your Own Stuff (*also referred to as **Bring Your Own Technology***) - The policy of permitting employees to bring personally owned mobile devices (i.e. laptops, tablets, smartphones, and wearables) to their workplace and to use those devices to access privileged company information and applications. The phenomenon is commonly referred to as information technology consumerization.

Broadband (*per [Reference.com](#)*) (*also referred to **Wideband***) - Term used to refer to the amount of bandwidth used to transfer information, expressed in terms of band size (e.g. Kilohertz, kHz, megahertz, MHz, and gigahertz, GHz). Broadband internet connections can accommodate bandwidth greater than 50 megabytes per second.

Broadband Conferences (*per NTIA*) - Third-party conferences where stakeholders and staff attend using SLIGP grant funds for eligible expenses (PSCR, IWCE, etc.)

Capital Expenditure (CAPEX) - Funds used by a company to acquire or upgrade physical assets such as property, industrial buildings or equipment.

Centralized Security Log Management - The policies and technology to store, search, and analyze security logs from host devices, including firewalls, intrusion detection systems, routers, and gateways, across an enterprise to evaluate trends and conduct forensics.

Cloud Security - A broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Confidentiality - The first leg of the Confidentiality, Integrity, and Availability triad of information systems security. It is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people while making sure that the right people can get it. Access must be restricted to those authorized to view the data in question. It is common for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less

stringent measures can then be implemented according to those categories.

Configuration Management - The systems engineering process concerned with ensuring all components in the network environment are maintained in a consistent fashion to ensure standardization and currency. Changes to the components and system are carefully managed and controlled to minimize or prevent disruption as well as facilitate ongoing operations.

Core Network - Network consisting of national and regional data centers that provides connectivity between the radio access network and the public Internet or the public switched network, or both.

Covered Leasing Agreement (CLA) (*Act, Sec.6208 (2)(B)*) - A written agreement resulting from a public-private arrangement to construct, manage, and operate the nationwide public safety broadband network between the First Responder Network Authority and secondary user to permit (i) access to network capacity on a secondary basis for non-public safety services; and (ii) the spectrum allocated to such entity to be used for commercial transmissions along the dark fiber of the long-haul network of such entity.

Cyber Security Systems Engineering Plan - A documented process that ensures the sustainability of an organizations's cyber security environment. It includes ongoing monitoring, testing, procurement, and validation of existing processes, technology, and policies as well as the requirement for periodic review and updates to ensure hardware, software, processes, and policy continue to be effective in preventing, countering, and surviving cyber threats to the operation of the organization's mission.

Cyber Supply Chain Security - The methods and processes to ensure hardware and software components comprising the NPSBN are acquired from trusted providers and manufacturers to mitigate the risk of malware and other potential vulnerabilities being introduced into the system from within the system itself.

Diameter Routing Agents (DRA) - A functional element in an LTE network that provides real-time routing capabilities to ensure that messages are routed among the correct elements in a network.

Digital Signature - A mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Domain Name System (DNS) - A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

Downlink - The throughput from the base station to the user handset or computer.

Economic distress - (*F.S. 288.0656 (c)*) Conditions affecting the fiscal and economic viability of a rural community, including such factors as low per capita income, low per capita taxable values, high unemployment, high underemployment, low weekly earned wages compared to the state average, low housing values compared to the state average, high percentages of the population receiving public assistance, high poverty levels compared to the state average, and a lack of year-round stable employment opportunities.

Embedded Application - A program that is implemented within a device at a level closer to the physical hardware to ensure optimal performance, reliability, and security. In a smartphone, the phone application would be an example of an embedded application.

Equipment Identity Register - A database that contains a record of all the mobile stations that are allowed in a network as well as a database of all equipment that is banned (e.g., because it is lost or stolen).

Extended Primary User Group - The extended primary user group consists of other PSE users—beyond law enforcement, fire, and emergency medical services.

FirstNet Cloud Environments (cloud computing) - A model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources.

Federal Information Security Management Act (FISMA) - The United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.

Governance Meeting Metric (*per NTIA*) - Includes any official sub-committees or working groups (Technical Committee, Executive Committee, etc.)

Heterogeneous Networks - Mobile experts define a Heterogeneous Network or HetNet as a network with complex interoperation between macrocell, small cell, and in some cases WiFi network elements used together to provide a mosaic of coverage with handoff capability between network elements.

Identity, Credential, and Access Management (ICAM) - A process and set of technologies to permit authentication to be accomplished by a consistent set of criteria agreed to by all parties participating in the transaction. This authentication methodology permits the creation and use of roles in addition to the more traditional user ID in order to assign rights, privileges, and access on a contextual basis, as needed.

Initial Operating Capability (IOC) - The state achieved when a capability is available in its minimum usefully deployable form.

Integrity - The second leg of the Confidentiality, Integrity, and Availability triad of information systems security. It involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

Interoperability – News and information related to the technology and governance that enable disparate voice and data systems to communicate with each other during multijurisdictional

events.

Jail Break - The act of overriding software limitations on a mobile operating system.

Messaging Services - Messaging services include common wireless services like short messaging service, multimedia messaging services, instant messaging, and email.

Mission Critical Push to Talk (MCPTT) - A work standard for LTE that will permit high-priority voice communications in a manner similar to that employed by land mobile radios today.

Mobile Application Management (MAM) - Describes software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business settings on both company-provided and “bring your own” mobile devices.

Mobile Device Management (MDM) - An industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices.

Narrowband ([per Reference.com](#)) - Bandwidth used to transfer information that uses a smaller bandwidth range than wideband (broadband) communications. The connections provide data at a slower rate. An example of this is dial-up Internet connections in which data is transferred at less than 56 kilobytes per second.

Next Generation 911 (NG911) - An Internet Protocol (IP)-based system that allows digital information (e.g., voice, photos, videos, text messages) to flow seamlessly from the public, through the 911 network, and on to emergency responders.

Operational Expenditure (or Operational Expense) (OPEX) - The ongoing cost for running a product, business, or system.

Patch Management - The systems engineering process to control what patches should be applied to which systems at a specified time in the enterprise. It includes the testing processes and methodologies to preclude inadvertently breaking systems as a result of applying patches.

Primary User Group - The primary user group consists of law enforcement, fire, and emergency medical services users.

PSAP connectivity - consisting of the network required to connect the broadband network to local Public Safety Answering Points (PSAP's)

Public Switched Telephone System (PSTN) - The aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication.

Radio access network (RAN) - Network that consists of all cell site equipment, antennas, and backhaul equipment, based on commercial standards, that are required to enable wireless communications with devices using the public safety broadband spectrum; and shall be maintained, and operated taking into account the plans developed in the State, local, and tribal planning and implementation grant program under section 6302(a).

(§6202(b)(2))

(Also known as BAN)

Range - The maximum range possible to receive data at 25% of the typical rate.

Risk - The likelihood of a threat or vulnerability to occur or be exploited and the impact such an event would entail to the organization. Risks can be accepted, mitigated, or transferred.

Rogue Application - A program or other code that does not conform to normal security and application constraints on a device or system; it typically takes the form of a virus or other malware.

Rooted - The act of overriding software limitations on a mobile operating system.

Rural community (*F.S. 288.0656 (e)*) -

1. A county with a population of 75,000 or fewer.
2. A county with a population of 125,000 or fewer which is contiguous to a county with a population of 75,000 or fewer.
3. A municipality within a county described in 1. or 2.
4. An unincorporated federal enterprise community or an incorporated rural city with a population of 25,000 or fewer and an employment base focused on traditional agricultural or resource-based industries, located in a county not defined as rural, which has at least three or more of the economic distress factors defined above and verified by the department.

S1 - The reference point between the eNodeB and the Evolved Packet Core elements: Mobility Management Entity and Serving Gateway.

S6a - Enables the transfer of subscription and authentication data for authenticating/authorizing user access between the Mobility Management Entity and the Home Subscriber Server.

S8 - A reference point between two roaming networks providing user and control plane messaging between the home and visited networks.

Security Information and Event Management (SIEM) - A term for software products and services combining security information management and security event management. SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.

Security Operations Center (SOC) - The people, processes, and technologies involved in providing situational awareness through the detection, containment, and remediation of information technology threats. A SOC manages incidents for the enterprise, ensuring they are

properly identified, analyzed, communicated, actioned/defended, investigated, and reported. The SOC also monitors applications to identify a possible cyberattack or intrusion (event) and determine if it is a real, malicious threat (incident) and if it could have a business impact.

SGi - The reference point between the Packet Data Network Gateway and the packet data network. Typically the packet data network may connect to services like messaging, private networks or the Internet.

Signaling Storm - A scenario where the signaling traffic within a network has increased, due to some incident or occurrence, beyond the network's ability to handle the signaling traffic.

Stakeholders (*per NTIA*) - State, Local, Tribal, and Regional Governments and Public Safety agencies (Law Enforcement, EMS, Fire Fighters, etc.)

Threat - An event that has an impact on the organization but generally cannot be controlled (e.g., terrorist attack, earthquake). The risk or risks associated with threats can be mitigated or otherwise addressed.

Uplink - The throughput from the user handset or computer to the base station.

User logging - The process and tools to track activity on the network to ensure that users are able to access those resources they require and that unauthorized users are not able to access data or other resources.

Value-Added Services - Services beyond telephony like Short Messaging Service or Multi-Media Messaging Service.

Virtualization Security - The policies, technology, and controls to protect data and applications by running them in a software-defined portion of memory as a self-contained machine that can be logically and functionally isolated from the primary device hardware and operating system to prevent attacks against or from the items running in the virtual machine.

Voice over IP (VoIP) - A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks, such as the Internet.

Vulnerability - A weakness that allows an attacker to reduce a system’s security and potentially compromise data and access.

Whitelist - An electronic list maintained to indicate either devices or applications that are permitted to operate on a network, including allowed websites that may be accessed.

X2 - A reference point between eNodeBs for signaling and handover of user traffic between eNodeBs.

Acronyms

- [A](#) • [B](#) • [C](#) • [D](#) • [E](#) • [F](#) • [G](#) • [H](#) • [I](#) • [J](#) • [K](#) • [L](#) • [M](#) • [N](#) • [O](#) • [P](#) • [Q](#) • [R](#) • [S](#) • [T](#)
- [U](#)
- [V](#)
- [W](#)
- [X](#) • [Y](#) • [Z](#)

Acronym	Definition
3GPP	Third Generation Partnership Program
ABAC	Attribute-based access control
AFCEA	Armed Forces Communications and Electronics Association
APA	Administrative Procedure Act
APCO	Association of Public-Safety Communications Officials
APCO 25	Project 25
AQD	Acquisition Services Directorate
ARP	Allocation and Retention Priority
AVL	Automatic Vehicle Locator
AWS	Advanced Wireless Services
BAN	Broadband Access Network (Same as RAN)
BTOP	Broadband Technology Opportunities Program
BYOD	Bring Your Own Device
CAD	Computer Aided Dispatch
CAPEX	Capital Expenditure
CASM	Communications Asset Survey and Mapping

CDMA	Code Division Multiple Access
CIO	Chief Information Officer
CJIS	Criminal Justice Information Services
CLA	Covered Leasing Agreement
COLT	Cell (Tower) on Light Trucks
COW	Cell (Tower) On Wheels
DACA	Deployable Aerial Communications Architecture
DAS	Distributed Antenna Systems
DEM	Department of Emergency Management
DHS	Department of Homeland Security
Diff Serve	Differentiated Service
DISA	Defense Information Systems Agency
DMR	Digital Mobile Radio
DMS	Department of Management Services
DNS	Domain Name System
DoC	Department of Commerce
DoD	Department of Defense
DoI	Department of Interior
DRA	Diameter Routing Agent
DSOC	Domestic Security Oversight Council
ECPC	Emergency Communications Preparedness Center
EDGE	Enhanced Data rates for GSM Evolution
eNB	Evolved NodeB or E-UTRAN Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Access Network
FAR	Federal Acquisition Regulation
FAR Part 12	Acquisition of Commercial Items
FAR Part 15	Contracting by Negotiation
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FEMA	Federal Emergency Management Agency
FFO	Federal Funding Opportunity
FHA	Florida Hospital Association
FICEMS	Federal Interagency Committee on EMS
FIN	Florida's Interoperability Network
FirstNet	First Responders Network Authority
FISMA	Federal Information Security Management Act
FLEX	Florida Law Enforcement Exchange
FSLTT	Federal, State, Local, Tribal & Territorial
GAO	Government Accountability Office
GIS	Geographic Information System
GPRS	General Packet Radio Services
GPS	Global Positioning System
GSM	Global System for Mobile Communications ()

HIPAA	Health Insurance Portability and Accountability Act of 1996
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
IACP	International Association of Chiefs of Police
IAFC	International Association of Fire Chiefs
IBC	Interior Business Center
IBW	In-building Wireless
ICAM	Identity, Credential, and Access Management
ICTAP	Interoperable Communications Technical Assistance Program
IDIQ	Indefinite Delivery, Indefinite Quality
IMSI	International Mobile Subscriber Identity
I/O	Interoperability
IOC	Initial Operational Capability
IoE	Internet of Everything
ISO/IEC	International Organization for Standardization/International Electrotechnical
IT	Information Technology
ITA	International Trade Administration
ITIL	Information Technology Infrastructure Library
IVR	In-vehicle router
IWCE	International Wireless Communications Expo
LMR	Land Mobile Radio
LTE	Long Term Evolution
MACINAC	The Mid-Atlantic Consortium for Interoperable Nationwide Advanced Communications
MAM	Mobile application management
MCCA	Major Cities Chiefs Association
MCPTT	Mission Critical Push to Talk
MCU	Mobile Communications Unit (Deployables)
MCV	Mission Critical Voice
MDM	Mobile device management
MDST	Mobile Data Survey Tool
Metro Chiefs	Metropolitan Fire Chiefs Association
MFN	MyFloridaNet
MMI	Man-Machine Interface
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MVNO	Mobile Virtual Network Operator
NACo	National Association of Counties
NASCIO	National Association of State Chief Information Officers
NAEMSO	National Association of State EMS Officials
NASNA	National Association of State 911 Administrators
NCSWIC	National Council of Statewide Interoperable Coordination
NEMIS	National EMS Information System
NEMSMA	National EMS Management Association
NG911	Next Generation 911
NGA	National Governors Association
NHTSA	National Highway Traffic Safety Administration

NIST	National Institute of Standards and Technology
NLC	National League of Cities
NOC	Network Operations Center
NPSBN	Nationwide Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
NSA	National Sheriffs' Association
NTIA	National Telecommunications and Information Administration
OAC	Operator Advisory Committee
OEC	Office of Emergency Communications
OFDMA	Orthogonal Frequency-Division Multiple Access
OPEX	Operational Expenditure (or Expense)
OPSC	Office of Public Safety Communications
P25	Project 25
PCI	Payment Card Industry
PCII	Protected Critical Infrastructure Information
PEIS	Programmatic Environmental Impact Statement
PMI	Project Management Institute
PPP	Public Private Partnerships
PSAC	Public Safety Advisory Committee
PSAP	Public Safety Answering Points
PSBN	Public Safety Broadband Network
PSCR	Public Safety Communications Research
PSE	Public Safety Entity
PSEN	Public Safety Enterprise Network
PSIC	Public Safety Interoperable Communications
PSST	Public Safety Spectrum Trust
PSTN	Public Switched Telephone System
PTO	Patent and Trademark Office
PUC	Public Utility Commissions
QCI	Quality Class Indicator
QPP	Quality of Service, Priority, and Preemption
RAN	Radio Access Network
RDSTF	Regional Domestic Security Task Force
RECCWG4	Regional Emergency Communications Coordination Working Group - Region 4
RFC	Request for comment
RFI	Request for information
RFP	Request for Proposal
RFQ	Request for Quote
RMTR	Recommended Minimum Technical Requirements
RUS	U.S. Department of Agriculture's Rural Utilities Service
SBDD	State Broadband Data and Development
SBI	State Broadband Initiative
SCADA	System control and data acquisition
SCIP	Statewide Communications Interoperability Plan
SDP	Service Delivery Platform
SHSGP	State Homeland Security Grant Program

SIEM	Security information and event management
SLA	Service Level Agreement
SLERS	Statewide Law Enforcement Radio System
SLIGP	State and Local Implementation Grant Program
SMS	Short Messaging Service
SOC	Security Operations Center
SOF	State of Florida
SOO	Statement of objectives
SOP	Standard Operational Procedure
SOR	Statement of Requirements
SOW	System on Wheels
SPOC	State's Single Point of Contact
SWIC	Statewide Interoperability Coordinator
SWG-ICC	State Working Group - Interoperable Communications Committee
TAB	Technical Advisory Board
TDMA	Time Division Multiple Access
TETRA	Terrestrial Trunked Radio (fka Trans-European Trunked Radio)
TIA	Telecommunications Industry Association
TICP	Tactical Interoperable Communication Plan
TTI	Transmission Time Interval
UASI	Urban Areas Security Initiative
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Terrestrial System
USB	Universal Serial Bus
USCM	US Conference of Mayors
VoIP	Voice over Internet Protocol
VNS	Vehicular network system
WCS	Wireless Communication Service

[Back To Top](#)

