**Prepared by the Public Safety Advisory Committee and Submitted to**


# Public Safety Advisory Committee

# Human Factors Report

**November 2013**

The FirstNet Board adopted a resolution on March 11, 2014 accepting the Public Safety Advisory Committee Human Factors Report.

**Public Safety Advisory Committee**
**Human Factors Report**

**Task Scope**: The Public Safety Advisory Committee (PSAC) was asked by FirstNet to analyze the long-range impacts of the nationwide public safety broadband network (NPSBN) on the way law enforcement, fire, and emergency medical services (EMS) operate and consider the impact it will have on their duties once the network is built and operating. It is important that the business and needs of first responders drive decision, not technology. This task looks to answer the questions:

- What are the human elements that FirstNet needs to consider when designing the network?
- What are the potential user issues that will arise when using the NPSBN?
- How will the NPSBN be used by first responders and how will it impact operations?

To determine the human factors[1] impact of the network, the PSAC Executive Committee (EC) defined the "human elements" of the system as users, operators[2], and maintainers[3]. Next, the PSAC EC identified categories to compartmentalize the various impacts, which are shown in the table below. Based on these categories, PSAC members were asked to brainstorm, list, and submit additional potential human impacts.

The design and deployment of FirstNet, including the subscriber units (portable radios to mobile computing technologies), have to be considered with great care so that it delivers both utility and usability. This is no casual communication; life and limb are often on the line. Thus, the goal here is not to drown the first responders with data because they have access to a fat pipe (broadband wireless network). In fact, for some mission critical use cases, (a data deluge) more data maybe worse than no data. Simply because, the constant data pings and voice chatter may distract the first responders from their primary task of saving lives. Remember High Velocity Human Factors![4] Under stress responders have limited cognitive resources and those resources are precious. They may need to put all their attention and cognitive effort in either focusing on the threat, saving lives, or putting out a raging fire. There is no mental bandwidth left to idly monitor the goings-on in their network or surf the data that is streaming through their device[5].

The PSAC EC compiled and reviewed the submitted PSAC member input and is providing this report to FirstNet for review. The PSAC EC is prepared to work with FirstNet to identify the highest priority categories and applicable human factors and, upon FirstNet's request, the PSAC will provide advice on how FirstNet plans to address these human factors.

---

[1] Human factors is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data, and other methods to design in order to optimize human well-being and overall system performance.

[2] Operator is responsible for the day-to-day operations of the network (e.g., FirstNet, commercial carrier)

[3] Maintainer would be the entities/divisions within the operator entity that are responsible for maintenance services for the operator. Personnel that keep the day-to-day infrastructure elements running.

[4] High Velocity Human Factors – application of human factors design of technology solutions when used in high stress, mission critical, life threatening situations or incidents.

[5] FirstNet Public Safety Wireless Broadband Network: User-Centered Design and Human Factors Driven Engineering of NextGen Public Safety Network – posted by Moin Rahman, 8/6/2013, http://hvhfsciences.blogspot.com/2013/08/firstnet-public-safety-wireless.html.

| Category | Human Element Group | | |
|---|---|---|---|
| | **Users** | **Operators** | **Maintainers** |
| **Device design/ ergonomics (detail public safety grade)** | • Devices shall provide usability and manipulation of controls through the use of only one hand<br>• Devices shall provide full usability, control, and manipulation of device controls, functions, and features while public safety personnel are wearing various type of personal protective equipment (PPE) (e.g., gloves [all types and thickness], protective/ballistic vest, protective padding and guards, visors, goggles, face shields, protective/ ballistic helmets, turnout gear, etc.)<br>• EMT/Paramedics need devices that support concurrent video, voice and telemetry transmissions for patient to ER Doctor teleconferences<br>• Devices shall support concurrent video, voice and sensor transmissions from information sources to user device(s)<br>• Devices shall be observable and useable in all environmental and lighting conditions. Devices shall support anti-glare surfaces, dimmable displays and alternative color backlighting for nighttime use, and incorporate displays sufficient for use in natural sunlight and darkened conditions. Device display transformation from normal light to high or low lighting ambient light conditions must be completed without user manipulation Need ruggedized devices that will withstand sustained use in harsh environments (e.g., resistant to extreme heat/cold (40F – 120F), drop, dust, water, etc.)<br>• Device hardware supports the collection and transmission of various biometric data from the user or others (collection via wireless technology and capable of resending the data collected)<br>• Device supports integrated security platform when coupled with proper application(s) can securely receive/transmit up to Top Secret (TS) classified materials (how do you confirm the user on the other end is TS cleared or is in a secure location?) | • Devices may be provisioned remotely by local and nationwide operational entities<br>• Device authorizations to information resources may be adjusted by competent authority "on the fly"<br>• Device hardware supports Band 14 LTE spectrum and multiple commercial LTE spectrum bands for interoperability<br>• Infrastructure will support, up to maximum available capacity, sufficient bandwidth availability for concurrent/multiple transmissions of biometric, video or large file data<br>• Infrastructure will support and accommodate differentiation of priority access of devices and applications accessed upon devices and will provide mechanisms to adjust day-to-day and ad hoc changes to priorities.<br>• Features and functionality of devices and uses thereof must be supported by effective Governance structures at the appropriate levels (e.g., national, state, county, and local) and as clear and logical SOPs and user guides<br>• Devices must support industry recognized standards based architecture/platform for greatest interoperability and marketability<br>• Infrastructure components will be hardened and solid in terms of a public safety grade of equipment incorporating survivability, reliability, security and velocity of all communications<br>• Infrastructure components such as, but not limited to, base stations and site controllers shall incorporate redundancy and no single points of failure<br>• Network design should be user centered to ensure deliver of useful, usable, and actionable information in real-time | • Devices may be provisioned remotely by local and nationwide operational entities<br>• Device authorizations to information resources may be adjusted by competent authority "on the fly"<br>• The fault management system(s) and console controls shall allow remote manipulation of devices to activate/deactivate, remove all data ("wipe device") from a device or components, and/or applications without user intervention<br>• Capable of remotely engaging device/software based on incident (emergency alert triggers video transmit back to center)<br>• Capable of purchasing/replacing device batteries |

| Category | Human Element Group | | |
|---|---|---|---|
| | **Users** | **Operators** | **Maintainers** |
| | • Devices in all form factors shall support a secured common alerting protocol and two factor authentication for one-to-one and one-to-many communications<br>• Applicable devices should support the creation of ad hoc secured/non-secured WiFi personal area networks (PAN)<br>• Devices should support Bluetooth connectivity to allow connections to external speaker/microphone and data/information collection devices<br>• Device should activate, recognize and connect with other authorized equipment, devices, and information resources through simple, minimal and intuitive processes with relative ease, expediency, and minimal user intervention and manipulation Devices need to be highly portable/lightweight, and be of sizes which are not overly large and heavy to carry or overly small that would contribute to loss while operating in high velocity, time compressed, high stress environments<br>• Devices shall provide a satellite connectivity option for personnel who are primarily deployed and operating on foot in rural or urban environments<br>• Devices shall support visual indicators of connectivity to networks (i.e., NPSBN, Commercial LTE/4G/3G, WiFi, Bluetooth) with signal strength indications, as well as secure/encrypted mode indictors<br>• Devices incorporate power sources that provide a minimum of 12 hour duty cycles<br>• Device should be manufactured in a manner that it can be easily and effectively decontaminated from biological material.<br>• Devices for use in fire services must meet or exceed NFPA 1802 standards for operation in hazardous environments<br>• Device development shall be tiered to provide basic level devices that provide ability to connect current devices that only need air card connections, mid-level device that | | |

| Category | Human Element Group | | |
|---|---|---|---|
| | **Users** | **Operators** | **Maintainers** |
| | incorporate more features/functionalities and advanced devices that contain and support advanced features, functionality and connectivity.<br>• Vehicle mounted device with a wired Ethernet network connection vice the ability to establish an ad hoc WiFi personal area network (PAN) (Ad Hoc WiFi is already included)<br>• Multiple size/capability devices are needed, (i.e. Smartphone, small, medium, large tablets, and Laptop devices to allow user flexibility in different situations and/or environments<br>• Devices must support industry recognized standards based architecture/platform for greatest interoperability and marketability<br>• The device's human to machine interfaces (HMI) shall incorporate physical (knobs, buttons, keys) and graphical user-interfaces (information architectures and human-computer interaction design) that facilitate intuitive and useable interactions that augment the users senses (audible, visual, tactile) and deepen comprehension of what is occurring around the user | | |
| **Applications** | • Application design should incorporate algorithms, mechanisms to appropriately parse, display and deliver actionable and useful information or intelligence either on demand or via predictive analytics based upon situationally relevant information<br>• The application's human to machine interfaces (HMI) shall provide a graphical user-interfaces (information architectures and human-computer interaction design) that facilitate intuitive and useable interactions that augment the users senses (audible, visual, tactile) and deepen comprehension of what is occurring around the user<br>• All data, at rest or in transit, both on and off network, will be encrypted | • Infrastructure will support, up to maximum available capacity, sufficient bandwidth availability for concurrent/multiple transmissions of biometric, video or large file data<br>• Infrastructure supports ample bandwidth availability for the use of Video Analytics<br>• Over the air rekeying shall be provided. (This function/feature could be positioned at an operator or maintainer as one entity could provide both capabilities<br>• Infrastructure operators provide detailed notifications of downtime and maintenance periods<br>• Capable of supporting multiple vendor products | • Applications incorporate criterion that articulate suitability and authorization/certification for use upon the network specifying local, county, multi-county, regional, state, multi-state, nationwide access or use<br>• Data sources should incorporate criterion that articulate suitability and authorization for use upon the network specifying local, county, multi-county, regional, state, multi-state, nationwide access – supported by effective Governance structures which developed logical and effective policies<br>• Applications incorporate criterion that articulate and manage the application's status and provides detailed exception reporting to appropriate personnel |

| Category | Human Element Group | | |
|---|---|---|---|
| | **Users** | **Operators** | **Maintainers** |
| | • Applications support integrated security hardware platform that can securely receive/transmit TS classified materials<br>• Applications incorporate Video Analytic capabilities<br>• Applications and supporting systems shall incorporate mechanisms/capabilities to citizen alerts and warnings (social media) of public safety activities in specific areas. (Automated Location based alerting)<br>• Applications integrate with and expand capabilities of connections to National Crime Information Center (NCIC), National Law Enforcement Telecommunications System (NLETS), State, Regional and local Criminal Justice Information Systems<br>• Applications allow devices to access and control switched video sources at or en route to incident scenes<br>• Applications will provide GPS and voice-enabled navigation systems providing turn-by-turn directions to locations<br>• Application design allows for concurrent users<br>• Applications contain onboard training tutorials or manuals and/or context sensitive help or connectivity links to training/help documents<br>• Agencies should have sufficient authority level to determine which Apps are loaded or available to a specific device (or groups of devices) from approved App Store(s). The assigned device authority level should be determined locally, but based on a larger scale criteria<br>• Applications to provide the capability of using the network as a radio system bridge to allow interoperability of disparate radio systems. This is the same concept as Radio over IP<br>• Applications to allow use of various GIS formats, (e.g. ESRI, ARC, Intergraph, etc.,) that are in use in public safety systems<br>• Applications that allow use of multiple CAD information for building plans | • Appears to call for a vetting/certification program for operators and products that would be used on/in the network<br>• Operators will provide a network that possesses the highest possible resistance to physical attack, virtual hacking, and peak demand failure due to overload from a natural and/or manmade disaster | • Manipulation/programming/setup to meet differing user needs/qualifications<br>• Maintainers will maintain the network to possesses the highest possible resistance to physical attack, virtual hacking, and peak demand failure due to overload from a natural and/or manmade disaster |

| Category | Human Element Group | | |
|---|---|---|---|
| | **Users** | **Operators** | **Maintainers** |
| | • Applications integrate with and expand capabilities of connections to National, State, Regional and Local law Enforcement, Fire and EMS Information and reporting systems | | |
| **Policies and Procedures** | • Standardized training and exercise doctrine is developed supporting various device form factors and offered at local, State and national levels<br>• Sufficiency and application of Training and Exercise doctrine is tracked and reported through States OEC Statewide Communication Interoperability Plan (SCIP)<br>• Differential operational documentation developed regarding the behavior of devices and applications on FirstNet vice Commercial Networks if applicable<br>• There will be a system in which users can share "lessons learned" after deployment to not only assist in training, but possibly drive changes to policies and procedures<br>• Common language used globally for cross discipline/jurisdiction applications<br>• Effective Governance structures at local, State and Federal levels shall drive creation of clear, logical and accepted SOPs<br>• Must develop and implement a policy and procedure to adjust priority for users and applications based on local criteria<br>• Must develop a training/testing methodology for ensuring continued proficiency | • Operating procedures and guidelines are developed for device, applications and access to various data sources<br>• FirstNet and operators must define the required availability of the network in terms of availability = (total time – down time) / total time based upon the defined public safety need<br>• The network will incorporate and utilize standardized elements that dictate prioritization and Quality of Service (QoS) attributes<br>• Redundancy/Resiliency and high availability elements of the network must incorporate accepted practices of elimination of single points of failure, graceful and reliable failover between primary and secondary/backup elements or components and the prompt notification of failures<br>• MOAs, MOUs, SLAs and/or contracts are developed between FirstNet and Commercial Carriers regarding the use of commercial networks or elements thereof by public safety users<br>• Operators will create as part of the fault management system a notification system for all users that advises of planned and unplanned outage notifications and scheduling for updates, minimizing impacts to users<br>• Effective Governance structures at local, State and Federal levels shall drive creation of clear, logical and accepted SOPs<br>• Must develop and implement a process for local maintainers and/or users to adjust priority levels for users and applications | • Operating procedures and guidelines are maintained through a life-cycle process for applicable devices, applications and access to available data sources<br>• The network must incorporate a comprehensive fault management system specifically focused for a high availability environment<br>• Development of comprehensive doctrine for high availability environments<br>• The network must take into account off-network, peer-to-peer, and self-healing capabilities<br>• Key to clear, logical and adhered to SOPs are effective Governance structures at the national, state, and local levels<br>• Must develop and implement a process for handling priority change requests<br>• Must develop a training/testing methodology for ensuring continued proficiency |

| Category | Human Element Group | | |
|---|---|---|---|
| | **Users** | **Operators** | **Maintainers** |
| **Access (security)** | • Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is provided<br>• Shared password and login credentials between applications | • Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is provided<br>• Shared password and login credentials between applications | • Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is consistently maintained<br>• Shared password and login credentials between applications |