



**Public Safety Advisory Committee
Over the Horizon/Human Elements/Factors
Scoping and Data Gathering Template**

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 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 factors¹ impact of the network, the PSAC Executive Committee (EC) defined the “human element” of the system as users, operators², and maintainers³. Next, the PSAC EC identified categories to compartmentalize the various impacts, which are shown in the table below. Based on these categories, PSAC members are being asked to brainstorm and list potential human impacts. Examples are provided in *italics* for each category. Once PSAC members submit the initial list of impacts, the PSAC EC will compile and review the input and provide to FirstNet for review. The PSAC EC will then work with FirstNet to determine the highest priority categories and human factors/elements. Once the highest priority factors/elements are determined, the PSAC will develop recommendations or proposed processes outlining how these human elements should be addressed.

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.



Category	Human Element Group		
	Users	Operators	Maintainers
Device design/ergonomics (detail public safety grade)	<ul style="list-style-type: none"> • <i>Police officers need the ability to use device with one hand</i> • <i>Fire fighters need the ability to use devices while wearing heavy gloves</i> • <i>EMT/Paramedics need devices that support concurrent video, voice and telemetry transmissions for patient to ER Doc teleconferences</i> • <i>Need ruggedized devices – able to withstand harsh environments (e.g. resistant to heat/cold, drop, dust, water, etc.)</i> • <i>Device hardware supports the collection of various biometric data from the user or others</i> • <i>Device supports integrated security platform when coupled with proper application(s) can securely receive/transmit TS classified materials</i> • <i>Devices incorporate power sources that provide a minimum of 10 hours duty cycles</i> • <i>Devices in all form factors shall support a secured common alerting protocol for one-to-one and one-to-many communications</i> • <i>Applicable devices should support the creation of ad hoc secured/non-secured WiFi personal area networks</i> 	<ul style="list-style-type: none"> • <i>Devices may be provisioned remotely by local and nationwide operational entities</i> • <i>Device authorizations to information resources may be adjusted by competent authority “on the fly”</i> • <i>Device hardware supports Band 14 and commercial bands for interoperability</i> • <i>Infrastructure supports ample bandwidth availability for concurrent collection of various biometric data from the users or others</i> • <i>Infrastructure will support differentiation of priority access of devices and applications accessed upon devices</i> 	<ul style="list-style-type: none"> • <i>Devices may be provisioned remotely by local and nationwide operational entities</i> • <i>Device authorizations to information resources may be adjusted by competent authority “on the fly”</i> • <i>The fault management system(s) and console controls shall allow remote manipulation of devices to activate/deactivate the device or components, and/or applications without user intervention</i>



Category	Human Element Group		
	Users	Operators	Maintainers
Applications	<ul style="list-style-type: none"> • Applications support the collection, use, transmission, and receipt of multiple concurrent streams of biometric data • Applications support integrated security hardware platform that can securely receive/transmit TS classified materials • Applications incorporate Video Analytic capabilities • 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 • Applications allow devices to access and control switched video sources at or enroute to incident scenes • Applications will provide GPS and voice-enabled navigation systems providing turn-by-turn directions to locations 	<ul style="list-style-type: none"> • Infrastructure supports ample bandwidth availability for use, transmission, and receipt of multiple concurrent streams of biometric data • Infrastructure supports ample bandwidth availability for the use of Video Analytics • Infrastructure elements support the end-to-end provision of security elements supporting TS materials 	<ul style="list-style-type: none"> • 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. • 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.



Category	Human Element Group		
	Users	Operators	Maintainers
Policies and Procedures	<ul style="list-style-type: none"> • <i>Training and exercise doctrine is developed supporting various device form factors</i> • <i>Training and exercise doctrine is developed supporting various applicable applications and data sources</i> • <i>Differential operational documentation developed regarding the behavior of devices and applications on FirstNet vice Commercial Networks if applicable</i> 	<ul style="list-style-type: none"> • <i>Operating procedures and guidelines are developed for device, applications and access to various data sources</i> • <i>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</i> • <i>The network will incorporate and utilize standardized elements that dictate prioritization and Quality of Service (QoS) attributes</i> • <i>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</i> • <i>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</i> • <i>MOAs, MOUs, SLAs and/or contracts are developed between FirstNet and Local, State, Regional, Federal and Tribal governments for the use of their networks, elements thereof or data by FirstNet public safety users</i> 	<ul style="list-style-type: none"> • <i>Operating procedures and guidelines are maintained through a life-cycle process for applicable devices, applications and access to available data sources</i> • <i>The network must incorporate a comprehensive fault management system specifically focused for a high availability environment</i> • <i>Development of comprehensive doctrine for high availability environments</i> • <i>The network must take into off-network, peer-to-peer, and self-healing capabilities which are critically important</i>



Category	Human Element Group		
	Users	Operators	Maintainers
Access (security)	<ul style="list-style-type: none"> Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is provided 	<ul style="list-style-type: none"> Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is provided 	<ul style="list-style-type: none"> Ubiquitous end-to-end authenticity and confidentiality of information traversing the network is consistently maintained