State of Texas – Cyber Security Comments

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
1	8 – 9	2.2.3. Devices	**Include Removable Media** – It is recommended that guidelines be added to this section to address removable media. It is unclear whether or not removable media will be allowed to connect to devices that are connected to NPSBN, and if so, whether or not removable device security will be applied (e.g. port/device controls, media encryption, etc.). Removable media is a common entry point for malware and also a common vehicle for data leakage.		
2	8 – 9, 20	2.2.3. Devices, 2.12 Info Sec & Data Sensitivity	**Accessibility of External Content, Messaging** – It is recommended that guidelines be added to clarify the extent to which external file sharing, content collaboration and personal email/messaging platforms will be accessible from the NPSBN network. Is DLP the only intended control to prevent data leakage through these platforms, or is web filtering going to be implemented to remove access altogether? This is especially important to clarify, since "Bring Your Own Stuff" is in scope.		
3	9	2.2.3.g	**Reconsider Wide Open, "Bring Your Own Stuff" Approach** – This open-ended requirement is an example of a perhaps off-hand thought which might have some unforeseen consequences. From a bidders perspective this could be interpreted to mean at worst, that ANY device, without preconditions must be fully secured, or at best any device will need to be considered and put through a rigorous process. Especially because this service will require a specialized Band 14 capability, it seems this is a great example of a later roadmap milestone, which could be traded off in early phases. Otherwise, it may inject an unacceptable amount of cost, complexity and delay to the initial rollout. Please clarify this requirement.		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
4	11	2.2.5. Strong Auth./ Identity Management	**Add IdM Lifecyle, Access Management Governance** – This document provides guidance on strong authentication in several places, but does not appear to address identity management lifecycle requirements or access governance requirements. It is recommended that guidelines are added to clarify requirements for: • Access provisioning/provisioning processes, including removal of access immediately upon a user's termination or departure from his/her role. • Documented access approval processes • Access reviews and certification processes (clean-up of accounts) • Processes for managing and maintaining granular user permissions and entitlements to applications and resources, beyond the access to the NPSBN network itself • Signed user acknowledgement/agreements		
5	11	2.2.5.	**Strong Authentication/Identity Management** – This section requires more clarity and detail. For example: ➢ "ICAM" – Identity, Credentialing and Access management is an umbrella term for a variety of critically important management functions ➢ These seem to be shortchanged in this section ➢ All of these functions are critical to achieving many, if not most, of the Cyber Security objectives outlined in Appendix C-10 ➢ These requirements should be articulated as decomposed IdM functions. A good reference is the "*National ICAM Summit Report*".		
6	4	2.1.1.j	**Adjust Key Concept (Privacy)** – The State strongly disagrees with what sounds like a general opinion, perhaps leftover from a consumer cellular or personal privacy policy, which is not the Use Case of primary concern. Although laws protect employee's personal information, this aspect is not		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
			applicable in many if not most PS Use Cases, particularly situations where public safety must record information for evidentiary purposes. Please rewrite to clarify need to protect personal privacy while enabling an accurate capture of the very different privacy situations and policies associated with live public safety operations.		
7	4, 5	2.2.1.i	**AES-128 vs AES-256** – Seems to be a conflict of requirements here. Both the FCC document and the 3GPP documents call for AES-128 (the AES algorithm with 128 bit key). The US Federal Government has recommended AES-256 for a number of years for Federal Law enforcement traffic and for State and Local traffic. (see https://www.nsa.gov/ia/programs/suiteb_cryptography/) Please clarify how requirements will be modified to accommodate Federal users that require AES-256 traffic encryption The P25 Standard requires AES-256 encryption for secure traffic, voice and data, which means the vast majority of existing state and local users are currently operating using AES-256.		
8	4	2.1.1.l	**"Multi-Layer Security," Clarify Wording** – Please reword to state that PSE jurisdiction may be more restrictive but must meet predetermined security levels and protocols. Network would not function if everyone is using different protocols and security policies.		
9	5	2.1.1.m	**Correct Cyber Security Scope Statement** – Please remove the reference to "inability to access the data when it is needed (availability)". This is inaccurate, since data protection has nothing to do with "A" in the CIA triad. Please rework and reorganize this information for accuracy and clarity.		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
10	5	2.1.2	**Dedicated Cyber Security Program Statement Correction: Remove "ALL"** – Because it is impossible for a program to consider an unqualified description "all source threats," this language is not practical in a requirements context. Also most of wording should be done before a "national, state, or local emergency" rather than using phrase "in the midst" in the requirements.		
11	5	2.2	**Cyber Security Architecture Would Benefit From Adding an Illustration** – Since the purpose of this document is to convey needs as precisely as possible, the specification misses an opportunity to clarify the environment by inserting an illustration which explains the "architecture." Indeed, it could be argued that just as an architect designing a building must deliver an illustration, the same could be argued here. A number of the illustration in the Draft RFP could be repurposed and it is strongly urged that these be modified and articulate the functional elements described in this section.		
12	6	2.2.2.g	**Protection Between Users: Add More Content on IoT and M2M** - Document seems to focus on human users using SmartPhones and requires more content around the plethora of Internet of Things (IoT) or Machine to Machine (M2M) devices such as CAMERAS, microphones, sensors, signage and vehicles. Each of these device types potentially create use cases and particular issues which need to be considered. Please add clarity and detail on this topic. Change "End Users" to more expansive term to reflect this, such as "all users and devices" or PS LTE "Units."		
13	6	2.2.2.i	**Rogue or Stolen Devices: Need "Kill Switch" with Reactivation** – Public Safety users are currently accustomed to the capability of instantly "bricking" an active, rogue device. More importantly if recovered, the device can be		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
			reactivated instantly. This Selective Radio Inhibit/Re-Inhibit has been a functioning baseline feature in trunked radio systems for over 20 years and is one of many examples of PS security functionality which exceeds and eludes today's commercial cellular networks. Being able to reactivate recovered devices results in enormous costs savings to PS agencies.		
14	6	2.2.2.i	**Rogue or Stolen Devices: Adjust Last Sentence** – Reconsider last sentence to allow for some situations where this might be required as absolute statements can create project risk and misinterpretations. For instance, a migration might have to be done in order for the network to remain up and functional for other public safety practitioners.		
15	7	2.2.2.p	**Mobile VPNs: Wording Correction** – Please remove the word "core" from the last sentence.		
16	7	2.2.2.s.ii	**Security Hardening: Add and Clarify** – Mention reuse of NPSTC/APCO Site Hardening work to prevent replication of effort (s.ii) Please add description and definition and perhaps examples of "security hardening tool portfolio."		
17	8	2.2.2.u	**Cyber Supply Chain Security: Adjust Language** – As with similar comments, it is impossible for any solution provider to assert something like "NO vulnerabilities, exploits, or threat vectors have been introduced PRIOR to NPSBN," emphasis added. Perhaps use the DISA Vulnerability (Categories I, II, or III) scale to clarify. Also add clarification on treatment of legacy systems that may have vulnerabilities.		
18	8	2.2.2.y	**Virtualization Security: Request Clarification** – Please strengthen phrase from *"requires additional focus"* to a phrase such as *"specifies the controls which need to be put in place."*		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
19	5	2.2	**Add: Security During Emergency Deployment** – The document needs to account for the needs to very quickly deploy devices and deployable sites in disaster situations. These scenarios typically create particularly complex security challenges. Please add content and detail to address the secure, emergency deployment of FirstNet resources including deployables.		
20	5	2.2	**Add: Securing of Evidentiary Logging Subsystems** – Another critical difference from commercial deployments is the need for evidentiary logging of officer voice, video and data. Familiar to citizens as the "911 tapes" the underlying logging subsystems are extremely complex and specialized in order to meet stringent evidentiary standards. It is critically important the data from FN First Responders can be used and accessed reliably by court systems. The current challenge is to expand current voice-based storage to enabling logging of much larger amounts of *video* data for evidentiary purposes. Please add a category to capture this aspect.		
21	5	2.2	**Add: Secure Group-Based Communications –** The FirstNet vision includes mission critical group-based voice and data communications, which means security measures need to be extended to include those additional architectural demands and critical Use Cases. Please add clarity and some detail to this aspect.		
22	10	2.2.4 (b.iii)	**Application Security: Clarify Requirements Conflict** – This bullet mentions API threat due to "…unencrypted data" while 2.12.1 page 20 states, "… all data in transit… will be encrypted…" Please clarify or add detail to ensure this cannot be interpreted as conflicting requirements.		
23	10	2.2.4.c	**Application Audit: Add Detail** – Please add additional		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
			detail which specifies how often audit logs must be reviewed by trained Application Auditing personnel.		
24	10	2.2.4.d	**Application Security: Reword** – Please change "should avoid" to "shall not use" in last sentence		
25	10	2.2.4.i.i	**Validate the Application Network: Add Internal-Facing Devices**		
26	13	2.4.2.d	**Application Domain Security: Delete Phrase** – Remove "over the application layer" phrase, as this makes it sound like we are referring to just Layer 7 of the OSI model.		
27	15	2.5.7.b	**3GPP Specs: Clarify Spec for IPv4 OR IPv6** – Please specify IPV4 or IPV6. Ensure if IPV4 is chosen the network is configured to easily change to IPV6 if needed.		
28	16	2.7.1.e	**Incident Response: Clarify Need/Term** – Please clarify the need and use case for this requirement. It was not clear what logs would be useful or what we what would be revealed by examining "System Logs".		
29	17	2.8.2	**Monitoring and Mitigation: Add Service** – Please add management of Security Patches to list of services in bullet 2.: *"(e) Security Patch Management"*		
30	1	Paragraph 1	**Security of CLA Operator** - The scope of the NPSBN is not clarified with respect to the spectrum lessees operating on the NPSBN under a Covered Leasing Agreement (CLA). Please add clarification on which Cyber Security requirements those entities will be required to meet in order to not expose the NPSBN.		
31	4	Key Concepts	**Key Concepts should include mention of defining Disaster Response Use Cases.** The need for security to		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
			support but not inhibit operations of Public Safety Entities during severe weather events or major events. Please add a clarification on this point.		
32	3	Paragraph 1	**Reduce Delay, Reduce Risk to Bidders** - *"A cyber security solution that establishes a secure network at the cost of delays or needless hindrances is not workable…"* This is the essential dilemma in security; this comment extends to the implications of the Cyber Security requirements on the acquisition process. The approach taken with the Appendix C-10, presents requirements which may explode the costs and schedule of the program because: ➢ It is a "flat, wish list", just a first step in a true Cyber Security solution planning process. ➢ A solution set of this complexity should be framed in terms of a roadmap. This enables the solution to evolve with a changing security environment. Like interoperability, security is an ongoing process. ➢ Without prioritization (beyond "should") and guidance on PHASING, Bidders have no choice but to assume most if not all of these requirements are mandatory which could result in unnecessarily inflating both the price and the schedule ➢ Just decomposing and estimating them could take many calendar months, and staff years of effort to determine, only the most serious bidders will attempt it ➢ We believe the "open-endedness" could deter potential bidders from participation. These requirements could be interpreted to mean the system would never be accepted, and/or almost arbitrary acceptance criteria. ➢ This spec, to its credit, requests solutions which have never been fully instantiated in the federal IT domain. The document misses the opportunity to create potential areas of trade-offs and key areas of Public Safety *advantage*.		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
			While many of the requirements are common practice, some truly represent a "paradigm shift." While that sounds great in the prose, it screams huge risk to a potential bidder. The concern about the approach to these requirements is that the lack of planning and management on the front end will cost months if not years of delay and hundreds of millions of dollars in unnecessary costs on the "back end."		
33	3	Second paragraph, first bullet	**All Requirements Must (SHALL) be Met, Should? -** Any cyber security solution adopted by FirstNet must also comply with the provisions of the Middle Class Tax Relief and Job Creation Act of 2012 (Act): ***"Specifically, Section 6206(b)(2)(A) of the Act requires FirstNet to "ensure the safety, security, and resiliency of the network, including requirements for protecting and monitoring the network to protect against cyberattack."*** Is it FirstNet's position that the 21 pages after page 3 of the Cyber Security document describe the mandatory and normative requirements of the requested Cyber Security Solution, such that ALL of the requirements need to be met to comply with the RFP? This seems unclear and the assumptions on this point would drive fundamental pricing factors for final bidders.		