COMMENTS on the Appendix C-10 NPSBN Cyber Security

Jackie Mines, Director, Emergency Communication Networks
jackie.mines@state.mn.us
(651) 201-7550

Ref. No. D15PS00295

COMMENTS OF THE STATE OF MINNESOTA

THE STATE OF MINNESOTA PROVIDES THESE COMMENTS IN RESPONSE TO FIRSTNET'S SPECIAL NOTICE ISSUED ON OCTOBER 5, 2015.

Introduction:

This document serves as the State of Minnesota's response to the Special Notice, reference number D15PS00295, issued on October 5, 2015. The State appreciates the creative time and effort expended in preparing the cyber security document. Security is a fundamental concern and challenge for public safety nationwide. The State will continue to offer our support to FirstNet to assist in attracting the best partner for a secure broadband network solution in Minnesota. This initial cyber security document as written provides a general best in class lifecycle description of cyber and physical security. The document as written solicits recommended approaches from the bidder allowing for very different solutions to a complex challenge. The State understands the fine balance between being too restrictive with requirements, hence boxing the types of responses, versus being too prescriptive allowing for solutions that fall short of the expectation. It is our opinion that the NPSBN cyber security document does not go far enough in establishing the expected policies, procedures and guidelines for cyber and physical security resulting in limited minimum requirements. This approach is likely to result in very different, non-comparable, applications of cyber security practices.

Consistent with the State of Minnesota's response to the special notice issued on April 27, 2015, proposals from bidders must be comparable, which necessitates a statement of minimum requirements, priorities, expectations and goals for cyber security. The current draft frequently uses the word "should" when stating FirstNet security requirements. In drafting Request for Proposal language, requirements are typically stated in a "shall" be provided terminology. In the absence of using "shall" or 'must", which are infrequently offered within the notice, FirstNet, public safety and the bidder are unclear on the required solution. There are certainly good reasons and opportunities to open the solution proposal to the bidder, expanding upon the options over and above the minimum; however, we encourage FirstNet to work with NIST and public safety to define our collective requirements wherever possible, and to turn as many of the "should" requirements to "shall", prior to releasing the RFP. The alternative solutions provided by vendors will need to be vetted and demonstrate an ability to keep pace with advancements of the cyber security landscape.

Within the State of Minnesota's comments, there are recommendations for additional requirements, representing minimum achievements in an effort to establish state priorities. The comments provided are not meant to be all inclusive, but are examples of needed minimum thresholds for the successful bidder. The

limited time for review has required prioritization of comments. The State would like to have further opportunities to review and comment on this and future draft RFPs sections, and encourages FirstNet to establish working groups inclusive of experts from public safety, government information technology, the commercial industry, academia, the State of Minnesota, and the consulting community to guide the development of meaningful requirements. Such a working group should be established immediately on cyber security.

Comments

The State of Minnesota's comments to Appendix C-10 NPSBN Cyber Security document are organized into:

- General Comments
- Specific Comments – Included within template supplied by FirstNet

General Comments:

Overarching themes and highlights from Minnesota's comments on the NPSBN approach:

- The State of Minnesota recommends that all "over the top" application ecosystem requirements be separated from the RFP to be issued at the end of this year. Public Safety's expectation is that all "over the top" applications be delivered by commercial stores already available to android and IOS platforms. Any applications critical to Public Safety (PS), like push to talk, will need to be tightly woven into LTE or the network and can be side loaded by the PS device administrator.
    - It is recommended that FirstNet remove the requirement for an "over the top" application ecosystem and utilize commercial delivery software solutions such as the App store, Play Store or AppComm (APCO).
    - FirstNet should avoid any device level or OS-level requirements that would add a layer of difficulty to commercial providers thereby limiting the device choices for public safety users.
- Public Safety Entities (PSE) and individual users of the NPSBN have the expectation for neutral transport; these users have the right to privacy including privacy from FirstNet. PSE shall have commitments from FirstNet that they are being offered neutral transport where their traffic will not be inspected, altered, decrypted or intercepted in anyway.
- From the state and user point of view, there is no expectation that the NPSBN will become a PSEN (Public Safety Enterprise Network). In fact, interoperable communication is not achieved simply by deploying the NPSBN. As an example, within the State there are different security needs across agencies so it is unlikely that sharing can be accomplished across the nation just by using the NPSBN as an enterprise network. Agencies will continue to use VPN technologies leaving the same challenges for sharing.
- As a standard expectation, PSEs will treat the NPSBN as an untrusted network and utilize VPN technology to access their own internal agency networks.
- Within the Cyber Security architecture, FirstNet does not address DiffServ anywhere. Traffic should be assumed to be encrypted at the point of origin and encrypted until it reaches the destination point. FirstNet and the vendor of the NPSBN will not have visibility or access into the contents of each packet. FirstNet will have access to the packet header for the purposes of routing packets. To prioritize traffic, FirstNet must establish a standardized DiffServ framework across the NPSBN.

- In the State of Minnesota's comments on the NPSBN approach, there was a reference to a concept of "commercial grade or commercial" service that was used to describe services provided by top tier wireless carriers. The expectation of the PS community is that security is equivalent to industry leading commercial carriers. This special notice does not develop the standard or specification that would define the current benchmark of commercial grade security.
- The State of Minnesota's minimum expectation is that the vendor shall provide security that is equivalent to industry leading commercial carriers. It would be important to quantify this benchmark as a reference while defining the NPSBN requirements that are over and above the commercial grade security that is available today.
- The State of Minnesota's concern is that onerous security measures will degrade the system quality. PS has the obligation to secure their data independently and with FirstNet's security document there is a risk that quality of network service or access to network service might be impacted.
- The Security approach outlined would represent a "state of the art" security architecture, lifecycle, risk management, incident response and security operations center, continuous monitoring and mitigation, testing and certification, network management as well as environmental and physical security approach. This approach may prevent viable bidders from participation on the RFP. The state requires commercial equivalent security for the protection of the network.

Specific Comments: Starting on Next Page

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
1	4	2.1 1k "Authentication methodologies on the network and for devices should allow public safety easy access, but provide a high level of security. The solution should include a federated identity, credential, and access management (ICAM) solution in concert with appropriate multifactor approaches to authentication."	A framework needs to be established for PS agencies to participate in the identity management framework and to be included in the framework discussion in systematic ongoing process over time.		
2	5	2.2 2. Within the cyber security architecture, the objective is stated: "to implement industry best practices for wireless carriers, information technology, and critical infrastructure in order to provide cyber security protection for the NPSBN."	• The expectation from Public Safety is that the NPSBN will be protected against attack by any means, be it cyber, internet or physical attack, and the PSE will follow all security policies implemented by FirstNet. • FirstNet shall define the NPSBN information security policies to ensure the confidentiality, integrity and availability of data that is in transit or at rest for NPSBN applications and services. Furthermore, the security policy needs to address monitoring, logging and data retention for the applications and services riding on the NPSBN (2.2, 2. d.).		
3	8	2.2 3a Within the Cyber security architecture section pertaining to "secure operating system architecture" for devices:	Public Safety has expressed a need for devices with the apple iOS or android iOS as a basic premise for adoption of the NPSBN. Current commercial operating system (OS) characteristics offer the same sandbox and AppContainer as described. Requirements should not be written in a way that requires a FirstNet bidder to establish a proprietary approach as this would lead to higher device costs and a potential barrier for PS.		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
4	9	2.2 3a vi Within the Cyber security architecture section pertaining to "secure operating system architecture" for devices, part vi. "FirstNet and its selected contractors will work with Device Manufactures…"	Although FirstNet and the selected contractors will work with Device Manufacturers on OS updates related to security issues and local control Mobile Device Management solutions, there shall be a forum which solicits input and involves Public Safety.		
5	9	2.2 3b Under the cybersecurity architecture devices, the section relating to "authentication of the users and applications"	The expectation from Public Safety is that there should be no limitation to prevent multiple users from sharing devices with proper authentication and credentials. The authentication of PS agency use is the individual agency responsibility, and FirtsNet will not apply additional layers of user authentication for devices accessing the NPSBN.		
6	9	2.2 3b iv. Under the cybersecurity architecture devices, the section relating to "authentication of the users and applications" part iv. "Device-specific biometric authentication should be integrated for supplemental authentication of certified application access".	Public safety users and application users shall have the ability to set passwords and other security features for their devices.		
7	9	2.2 3c Under the cybersecurity architecture devices, the section relating to "Embedded Applications"	Public safety does not recommend requiring devices to have pre-installed mission critical applications as this may add complexity and reduce the selection of devices available to the public safety community. The Public Safety device administrators can side load mission critical applications at the time of activation on the network.		
8	9	2.2 3f	• The PSE device administrator and/or IT administrator requires the ability to implement, manage and enforce security		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
		Under the cybersecurity architecture devices, the section relating to device security solutions:	features for the device as well as applications. Examples include passwords, encryption, firewalls, anti-virus, VPN connections, authentication and strength of authentication. Where appropriate these policies can be enforced remotely by the administrators. This enforcement of security policies will also require the ability to remove applications and/or deactivate device applications. • PS has the obligation to secure its data independently using encryption and utilizing Public Safety's VPN. FirstNet shall not perform content inspection or filtering as users have the right to the privacy of their data.		
9	9	2.2 4 This section itemizes requirements for application security.	• As stated in the general comments, the State of Minnesota recommends that all "over the top" application ecosystem requirements be separated and removed from the RFP to be issued at the end of this year. Public Safety's expectation is that all "over the top" applications be delivered by commercial stores already available to android and IOS platforms. • Public Safety requires flexibility for buying apps and although closed ecosystems are typical with the Apple store, the Google play store does not offer similar protections. The suggested compromise is to utilize commercial app stores but utilize a certification process. Further, it is suggested that NIST / PSCR (Public Safety Communications Research) could act as a clearing house for application certification. • Public Safety Agencies are ultimately responsible for the security of their data and will work to restrict apps that are not approved. This would continue to be a local level decision. • The application landscape is further complicated by BYOD with users that will need to download personal apps as well as apps necessary for public safety. The security of the network and data will also have to be protected from the use of personal apps on BYOD. • Public Safety Agencies will consider NOT moving to the NPSBN if they can't continue to run and use their current Apps. • Public Safety Agencies will want to understand what types of Apps are being used and there needs to be some control over the types of Apps used. At the local level, oversight and decisions about what Apps are supported and used will be required.		
10	10	2.2 4f	• Requiring application developers to register and establishing a certification and audit process will be a barrier for application		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
		This item within the application security section addresses the need for "application developer certification"	development, but this strategy must be balanced with a need for a minimum requirement for developers. Recognize that application security cannot be so onerous as to result in a network that is too expensive to operate, or to diminish creative application development. A compromise must be found such that not just anyone can publish an App that creates a risk to the security of the NPSBN versus potential diminished availability. • Ultimately Public Safety is responsible for the integrity of their data and will be responsible for the "non-FirstNet" applications used such that all federal, state and local security requirements are achieved.		
11	10	2.2 4i This section addresses the need to "validate the application network elements and the associated software/hardware be continuously monitored"	• It is important to again reiterate that the State of Minnesota recommends that FirstNet remove the need for an application ecosystem from the NPSBN vendor requirements. By removing this need, the commercial application ecosystems will fulfill the need of Public Safety. • Public Safety has the responsibility for delivering mission critical applications through a variety of methods including standard device images, side loading, through purpose-build enterprise application management systems and through the Apple App store and the Google Play Store. • In order for Public Safety to better understand and respond to the concept of a FirstNet App Store, FirstNet should provide details regarding the FirstNet App Store and the proposed apps that FirstNet speculates will be utilized.		
12	13	2.4 "Cyber Security Guidance"	This section of the document represents a nice reference of all the security guidance; however there are no requirements for the bidder to address in this section. • Bidders shall be required to explain the guidelines that will be used to maintain security on the network. The vendor must state which of these standards will be used to comply with physical and cybersecurity requirements to protect the network.		
13	16	2.7 Opening Paragraph: "…the government will require the contractor to dispatch staff within a time period to be established, but potentially	Cyber security incident response of one business day is too long as most commercial technical response times range from two to four hours. FirstNet should require the vendor to provide their expectation for getting a contractor on site and responding immediately to the potential threat.		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
		in as little time as one business day."			
14	16	2.7 1. "FirstNet envisions that incident response management will be performed by a cyber security incident response team, which should perform the following activities at a minimum:"	The expectation of Public Safety is that FirstNet shall define policies that enable the NPSBN to respond immediately to security threats without incurring a service outage.		
15	17	2.8 Cyber security continuous monitoring and mitigation methodology	Vendors should be required to provide details of their plan, tools, protocols and guidelines for maintaining security on the network.		
16	18	2.9 Cyber Security Testing and Certification Plan	• The vendor should provide specific and measurable methods for the security testing and certification plan including requirements for periodic testing of approaches, processes, operational management and cyber security testing by a third party. • The vendor should explain how it expects implementation of its plan for continuous monitoring, testing and certification to impact system performance or features of the network.		
17	19	2.10 4. The cyber security network management and configuration management policies section includes item 4 related to patch management.	FirstNet shall define policies, tools and processes that mitigate the risk of introducing security updates that compromise existing security measures.		
18	20	2.11 "Environmental and physical security is critical to security planning for any information systems."	FirstNet must request the bidder to explain all security protocols to be used in securing the RAN and Core network assets. How will the bidder deny unauthorized physical access to facilities, equipment and resources?		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
19	20	2.12 Within the information security and data sensitivity section	There is no mention of policies related to end of life user equipment (UE). • FirstNet shall provide guidelines and a process for safe disposal of end of life user equipment (UE) to protect against unauthorized access to the NPSBN.		