Cyber Security Comments Template

Comments on the Appendix C-10 NPSBN Cyber Security

Association of Public-Safety Communications Officials (APCO) International
1426 Prince St
Alexandria, VA 22314

Contact:
Jeff Cohen, Chief Counsel
cohenj@apcointl.org
571-312-4400 ext. 7005

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
1	2	1 – “FirstNet intends to include a diverse multi-platform user equipment base, more than 60,000 public safety enterprise (PSE) networks, more than 6,800 public safety answering points,..”	FirstNet should provide more detail on how its cybersecurity strategy will involve and account for Public Safety Answering Points (PSAPs). The interfaces between FirstNet and both legacy and Next Generation 9-1-1 (NG9-1-1) PSAPs and Emergency Services Internet Protocol Networks (ESINets) need to be defined and protected. Specifically, there is a need to secure data both from the PSAP to FirstNet and vice-versa. In order to do this, a common cybersecurity core approach is necessary. The Cyber Security Incident Response and Security Operations Center referenced in Section 2.7 may not be the best approach. In general, FirstNet should consider a cooperative and consolidated model for cybersecurity. Such a combined approach could have economic and operational benefits. For example, FirstNet might consider the Emergency Communications Cybersecurity Center (EC3) concept being explored by the FCC’s Task Force on Optimal PSAP Architecture (TFOPA). EC3 will incorporate the concepts of Intrusion Detection and Prevention by leveraging a combination of passive sensor and active response capabilities. The model will reportedly mirror existing systems such as those provided by the Multi-State Information Sharing and		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
			Analysis Center (MS-ISAC) in cooperation with DHS and the interfaces between the MS-ISAC and DHS NCC, NCCIC, US-CERT, and SLTT entities. This proposed cybersecurity core is also inclusive of industry, specifically wireless and wireline carriers, as well as infrastructure providers. It provides for interfaces from OSPs as well as NG9-1-1 ESINets and PSAPs. Work from TFOPA as well as the Communications Security, Reliability, and Interoperability Council (CSRIC), along with standards work in this area from APCO, ATIS, NENA and others should be considered for inclusion in the FirstNet approach and design, especially with regard to integration with PSAPs.		
2	2	3 - "Security needs to be functionally and operationally focused in order to be effective and responsive. This can only be achieved if security is intrinsic to the design and implementation of every aspect of the network and data environment from inception. This is the goal and approach to be employed by FirstNet."	APCO agrees with this statement. Further, as referenced above, a combined and cooperative approach to cybersecurity for public safety may support FirstNet in achieving a functionally and operationally focused security.		
3	3	1 – "FirstNet's NPSBN cyber security efforts will be guided by three key principles: confidentiality, integrity, and availability."	APCO collaborated with the National Institute of Standard and Technology to host a workshop that brought together public safety professionals, app developers, and security experts. Using NIST's "Guide for Mapping Types of Information and Information Systems to Security Categories" as a starting point, participants began enumerating the public safety data types required for use by applications that serve the community. After categorizing these data types by their impact to confidentiality, integrity and availability, participants discussed appropriate safeguarding mechanisms available to public safety. One of the lessons learned from the workshop is that the "integrity" of public safety data is paramount. A NIST report is underway that will describe the lessons learned in greater detail. This may assist FirstNet in developing		

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
			its cybersecurity plan and identifying areas for additional research within the public safety community.		
4	3	2 – provisions of the Middle Class Tax Relief and Job Creation Act of 2012	FirstNet should also consider the implications of Section 6004, which describes national security restrictions on the use of certain funds made available by the Act.		
5	4	2.1(1) Public Safety Needs	APCO supports FirstNet's commitment to ensuring that protecting the network does not come at the expense of public safety users' ability to use the network. Some public safety needs, such as HIPAA and CJIS compliance, have already been addressed for NG9-1-1 design. FirstNet should leverage this work whenever feasible.		
6	9	2.2(4) Application Security	Application security is an absolute requirement, as apps are potentially the weakest link in this system next to the users themselves. The app store(s), APIs, and any cloud based services must comply with cyber requirements, and several partners may well be required to do so effectively.		
7	10	e. Application Security Certification	APCO agrees that FirstNet's application security certification should ensure speed, reliability and security, and that the process should allow PSEs to have a high degree of confidence when downloading or purchasing applications from the FirstNet app store. As described above, the research APCO has conducted into public safety app security indicates that integrity – the trustworthiness of the app and the data it uses – is paramount.		
8	11	2.7(5) - Strong Authentication/Identity Management	With regard to identity assurance, there should be multi-factor authentication required, which includes both user and device. BYOD must be accompanied by sufficient cyber requirements.		
9	11	2.2(7) – Provide Public Safety Enterprise Security	APCO is engaged in several outreach efforts related to cybersecurity and can serve as a continuing resource to FirstNet. Further, the FCC's TFOPA (mentioned above) is developing recommendations with a significant cybersecurity education requirement. FirstNet should consider leveraging this work, and CSRIC recommendations regarding cybersecurity, upon completion.		
10	13	2.4 - Cyber Security Guidance	In addition to the items listed, FirstNet should consider the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework, the TFOPA recommendations, and relevant recommendations from CSRIC.		
11	20	2.11 – Environmental and Physical Security	APCO has a pending ANSI standard on site hardening that will apply to physical security. FirstNet should consider this, as well as the APCO-NPSTC work on site security and site hardening which is contained in a May 2014 report on "Defining Public Safety Grade Systems and Facilities."		