#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	The Association of Public-Safety Communications Officials-International, Inc. (APCO) is the nation's oldest and largest organization of public safety communications professionals. APCO is a non-profit association with over 25,000 members, primarily consisting of state and local government employees who manage and operate public safety communications systems—including Public Safety Answering Points (PSAPs), dispatch centers, emergency operations centers, radio networks, and information technology—for law enforcement, fire, emergency medical, and other public safety agencies. Considering the deployment of Next Generation (NG9-1-1) and the nationwide public safety broadband network, PSAPs serve an increasingly important role as the "nerve center" of emergency response. Further, the advent of IP-based communications to and from PSAPs increases their already-significant potential to become targets of cyber attacks. As a result, it is critical that cybersecurity for PSAPs and the entire 9-1-1 ecosystem be considered as part of the overall critical infrastructure approach.	
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	APCO responds as a subject matter expert, as well as with knowledge of multiple organizations, some of which are using the Framework.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	APCO recognizes that the Framework is highly applicable to PSAPs and other public safety entities, but as described more below, additional work is needed specific to public safety communications.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	APCO is currently developing education materials designed to familiarize the public safety community with the Framework and its applicability. Additionally, the Framework was used as the basis for certain recommendations and follow up work for the Federal Communications Commission's (FCC) Task Force on Optimal PSAP Architecture (TFOPA). APCO staff chaired TFOPA Working Group 1, which was tasked with developing recommendations on the "Optimal Cybersecurity Approach for PSAPs." As part of its report, the Working Group mapped various categories from the Framework to recommended implementation levels for the public safety communications ecosystem. TFOPA Working Group 1 mapped out the recommended level of operation that should be involved in each of the five key areas identified in the Framework, detailing both the recommended implementation level and high-level requirements to attain the stated goal. The TFOPA report also provides cybersecurity use cases that are specific to PSAPs. As noted in the report, additional study and a more detailed mapping of this approach should be considered.	The TFOPA Working Group 1 report is available at: https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_FINAL_Report-121015.pdf
5	What portions of the Framework are most useful?		
6	What portions of the Framework are least useful?		
7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	Use of the Framework has been limited, at least in part, by a general lack of awareness of cybersecurity issues in the public safety community. Additionally, PSAPs and other 9-1-1 stakeholders may lack the necessary resources to properly address cybersecurity challenges. In the FCC's recent annual report on 9-1-1 fee diversion among the states, only 9 states reported that they adhere to the Framework. It is important to note that the very nature of PSAP operations is highly localized and specific to the mission needs of client agencies and reponsders. As a result, while PSAPs certainly need to become much more cognizent of the risk, it takes additional effort to educate such a diverse population of users in order to create an enviroment of information sharing.	The FCC's Seventh Annual Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges is available at: https://transition.fcc.gov/pshs/911/Net%20911/NET911_Act_7thReport_to_Congress_123115.pdf .
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.		
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?		

#	Question Text	Response Text	References
10	Should the Framework be updated? Why or why not?	Yes. Future versions of the Framework would benefit from more specific input from the public safety community to ensure that public safety needs, roles, and responsibilites are considered. The advent of NG9-1-1 and FirstNet presents an excellent opportunity to begin the transition from individualized PSAPs to an enterprise-like approach of "connected PSAPs" via interconnected ESINets, comprising a true "network of networks." APCO is uniquely positioned to assist in gathering this input of the special considerations of PSAPs and public safety, and achieve a uniform awareness and acceptance of the Framework.	
11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.		
12	Are there additions, updates or changes to the Framework’s references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?		
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	As part of its recommendations, TFOPA Working Group 1 mapped certain functions from the Framework to the role of an Emergency Communications Cybersecurity Center (EC3) that would serve multiple PSAPs at the state or regional level. The intent behind EC3 is to create a centralized function and location for securing next generation networks and systems, providing intrusion detection and prevention services to multiple PSAPs and other emergency communications systems at the state or regional level. An EC3 would allow PSAPs to engage in improved information sharing, realize efficiencies from economies of scale, leverage existing systems and best practices, and otherwise take advantage of multiple resources.	The TFOPA Working Group 1 report is available at: https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_FINAL_Report-121015.pdf
14	Should developments made in the nine areas identified by NIST in its Framework-related “Roadmap” be used to inform any updates to the Framework? If so, how?		
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?		
16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?		
17	What, if anything, is inhibiting the sharing of best practices?	PSAPs, in general, lack the understanding and resources necessary to develop cybersecurity best practices and to share them with other PSAPs. This is not necessarily due to a lack of desire to share information, but the lack of effective mechanisms, information sharing processes, and a true understanding of cybersecurity as it relates to PSAPs and public safety.	
18	What steps could the U.S. government take to increase sharing of best practices?	Additional funding is essential, both for education and resources to assist PSAPs with developing cybersecurity best practices.	
19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?	Support for PSAPs, generally, and the EC3 concept described above would help increase the likelihood that organizations would share information. APCO and other organizations provide education and training opportunities for public safety professionals. Grant programs to make these opportunities more readily available would also increase the likelihood that organizations share information related to cybersecurity.	
20	What should be the private sector’s involvement in the future governance of the Framework?		
21	Should NIST consider transitioning some or even all of the Framework’s coordination to another organization?		

#	Question Text	Response Text	References
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?		
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?		
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?		
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?		