PAPERWORK REDUCTION ACT STATEMENT

Cyber Resiliency 911 (CR911) Small Discussion Group Questions on Current Cyber Resiliency Measures for Emergency Communications Centers (ECCs)

Below is a list of open-ended questions that will be asked during a small group discussion that will take place in-person or by telephone through Teams.

Current State: ECC cyber resiliency and cybersecurity practices today

1. How do you identify or monitor to determine if you have a cybersecurity vulnerability? How do you mitigate or remediate an identified cybersecurity vulnerability? How do you prioritize to address or put resources towards mitigation and remediation?
   Partnered with CISA for monitoring? Using software or vendor to monitor? Use contractors/vendors? Skills in-house or outsourced?

2. How is information about cybersecurity threats shared with you today? Where do you get your cyber security alerts (internal govt vs media)?

3. Where do you go today to learn more about cybersecurity?

4. Can you tell us about the cyber policies you employ at your ECC? Does your center adhere to a cybersecurity framework (e.g., NIST)? *Physical Security/access control to IT rooms/center? Credentialing? Multi-factor authentication? Password hygiene? Network/vulnerability monitoring? Regular patch management? Data backups?*

5. What level of awareness is there in the average ECC on what is available related to cybersecurity preparedness, tools, training?

Funding

6. Do your state laws allow 911 funds to be used for IT/cybersecurity-related expenditures? If not, would that be helpful?

7. If the Federal government could apply funding to solutions that help reduce cybersecurity risks, where should it be directed? Are there priorities?

Cyber Planning, Training, Exercises

8. What role(s) does 911 play in your state or region's cybersecurity governance and preparedness?

9. Who is responsible for cybersecurity in your ECC? Would you recommend changing that? *(Devoted IT? ECC Manager? Managed Service Provider/Vendor?)*

10. Can you describe your state-level requirements for having a Cyber Incident Response Plan and any state-level policies regarding cyber response?

11. How does your ECC train personnel on cybersecurity in an NG911 environment? Which staff levels receive cybersecurity training?
(Director, Technical, Dispatch, Trainer, Call Taker) What type of training (e.g., awareness)?

12. How could CISA most effectively educate and possibly train the 911 community on the importance of cyber resiliency and security?

13. How could CISA most effectively educate/train the 911 community on response to cyber-attacks?

Cybersecurity Risk

14. What are your biggest cyber concerns? What keeps you up at night?

15. What do you think is your biggest target/most at risk? What do you perceive as the most significant consequences of a cyber incident? What do you assess is the probability/likelihood of an attack on your center in the next five years? *(Helps gauge urgency)*

16. What tools or products could help reduce your risk of a cyber incident or disruption?

17. If your vendor/managed service provider is part of your cybersecurity risk management approach or response plan, can you describe that relationship and how well it is working?

    a. How well do PSAPs understand their vendor's role in responding to and recovering from a cyber incident. What are the expectations of the vendor, especially if the cyber incident or compromise originates with the vendor's software/data? Are those expectations/ responsibilities of the vendor documented in your contract? Is your vendor included in cyber training/exercises/drills?

18. Have you conducted a cybersecurity assessment previously, and by whom (CISA, third-party vendor, etc.)? If so, were the cybersecurity assessments helpful? How could they be more helpful?

19. To what extent does your ECC outsource IT/cyber operations? Would additional guidance on best practices for communications with managed service providers/vendors and contract language be helpful?

Future State: How will you protect your ECC in the future?

20. How would you make your center more resilient from cyberattacks? Where could CISA offer assistance? What types of cyber services would benefit your center? What level of participation or engagement would you want from CISA (fed govt)?

21. What are three lessons learned that you would want every ECC Manager to know to enhance their cyber resilience?

22. What is the best forum/methodology for reaching individual ECCs and personnel? I.e., Regional? State by state?

Symposiums

23. What would attract you to a “conference” about 911 cybersecurity? What would you want to learn? What topics or content would be crucial to include?

24. What could be done to maximize attendance?
    a. Which organizations should CISA work closest with in order to reach the right audiences?

25. What could negatively impact attendance? How might state/local travel rules restrict attendance?

26. Who would be the ideal target audience? (Technologists? Decision makers? CTO, CIO, IT, ECC Director, ECC person with most cyber responsibility, experienced call taker?)