

## State Capability Assessment Project



### Draft Questions

#### CYBERSECURITY

<b>Capability Description:</b>	Protect against damage to, the unauthorized use of, and/or the exploitation of (and, if needed, the restoration of) electronic communications systems and services (and the information contained therein).
<b>Mission Area:</b>	Protection
<b>Resources Used to Develop Questions:</b>	<ul style="list-style-type: none"> <li>• Comprehensive Preparedness Guide 201</li> <li>• Emergency Management Standard by EMAP</li> <li>• <i>Please note: No compatible TCL capabilities</i></li> </ul>

#### PLANNING

1. Does your jurisdiction have plans that address cybersecurity? *Answer: radio button, yes/in progress/no*
2. If your jurisdiction has plans that address cybersecurity, do they: *Answer: multi-answer*
  - a. Include a hazard and threat analysis for cyber events? [CPG]
  - b. Address cybersecurity of public infrastructure?
  - c. Address cybersecurity of private infrastructure?
  - d. Address cybersecurity of critical infrastructure?
  - e. Address cybersecurity of schools?
  - f. Address business continuity?
  - g. Address disaster recovery?
  - h. Address availability requirements?
  - i. Include deterrence strategies?
  - j. Include surveillance/detection strategies?
  - k. Include and assessment of supply chain risk of cyber attack?
  - l. Address intra- and inter-jurisdictional maintenance of situational awareness of cyber security, threats, and attacks?
  - m. Include notifying the Fusion Center?
3. **Based on your responses to the questions above, how would you rate your overall cybersecurity capability as it relates to planning?** *Answer: dropdown, 1 - 10*

#### ORGANIZATION

4. Have you identified primary and supporting agencies responsible for coordinating cybersecurity efforts? *Answer: radio button, yes/in progress/no*
5. Do you have a mechanism in place to engage local partners in planning for cybersecurity? *Answer: radio button, yes/in progress/no*
6. Are mutual aid agreements in place to acquire additional resources to aid in cybersecurity efforts? *Answer: radio button, yes/in progress/no*
7. Are contracts with private vendors in place to acquire additional resources to aid in cybersecurity efforts? *Answer: radio button, yes/in progress/no*
8. Do you have procedures, protocol, or methods in place for: *Answer: multi-answer*
  - a. Maintaining cyber security within your jurisdiction?
  - b. Protecting hardware from theft?
  - c. Protecting software from theft?
9. **Based on your responses to the questions above, how would you rate your overall cybersecurity capability as it relates to organization? *Answer: dropdown, 1 - 10***

## EQUIPMENT

10. Do you have adequate equipment and supplies to implement cybersecurity actions for your jurisdiction? *Answer: radio button, yes/in progress/no*
11. If not, which of the following equipment and/or associated resources are you most in need of to support cybersecurity actions? *Answer: multi-answer*
  - a. Planning resources
  - b. Qualified personnel
  - c. Information management tools
  - d. Other (note in gaps)
12. **Based on your responses to the questions above, how would you rate your overall cybersecurity capability as it relates to equipment? *Answer: dropdown, 1 - 10***

## TRAINING

13. Have you identified staff and key partners responsible for implementing cybersecurity actions? *Answer: radio button, yes/in progress/no*
14. Have identified staff been trained on cybersecurity actions? *Answer: radio button, within the past year/within the past 2 years/within the past 5 years/no*
15. If you have offered cybersecurity training, have private sector partners been included? *Answer: radio button, yes/no/Not applicable*
16. **Based on your responses to the questions above, how would you rate your overall cybersecurity capability as it relates to training? *Answer: dropdown, 1 - 10***

**EXERCISES**

17. Has your emergency management organization conducted a disaster mitigation exercise that incorporates elements of cybersecurity? *Answer: radio button, yes/in progress/no*
18. If your emergency management organization has conducted a disaster mitigation exercise that incorporated elements of cybersecurity, when? *Answer: radio button, within the past year/within the past 2 years/within the past 5 years/no*
19. If your emergency management organization has conducted a disaster mitigation exercise that incorporated elements of cybersecurity, which of the following elements were included?  
*Answer: multi-answer*
  - a. Disaster recovery
  - b. Cyber attack
  - c. Critical infrastructure
20. Has exercising of the cybersecurity capability led to identification of corrective actions in regard to this capability? Please identify in the gaps section of this question. [EMAP] *Answer: radio button, yes/in progress/no/not applicable*
21. **Based on your responses to the questions above, how would you rate your overall cybersecurity capability as it relates to exercises? *Answer: dropdown, 1 - 10***

**GLOBAL**

22. **Based on your responses to the questions above, how would you rate your overall cybersecurity capability? *Answer: dropdown, 1 - 10***
23. **Based on your responses to the questions above, what priority (high, medium, low) would you assign to the cybersecurity capability for your jurisdiction? *Answer: radio button, H, M, L***
24. **Please identify which hazard/threat would most likely tax your ability to perform the cybersecurity capability? *Answer: dropdown, hazards***
25. **Have you identified any planning barriers or do you have any additional notes or comments regarding the cybersecurity capability? *Answer: Text***