Part B **Book 9 – Supplement**

Cybersecurity Basics for Courts

By the National Center for State Courts (NCSC), Joint Technology Committee (JTC)

1. Define a "cybersecurity incident":

_____
_____
_____

2. What are the three forms of cybersecurity incidents and the definition of each?

_____
_____
_____

3. According to the text, what is the "threat (or attack) surface," how should it be mapped out, and how often?

_____
_____
_____
_____

4. List at least one reason to include cybersecurity incidence response in Continuity of Operations Planning (COOP):

_____
_____
_____

5. At a minimum, who should be included in a court's "Cybersecurity Incident Response Team" and what should each of their roles entail?

_____
_____
_____
_____
_____
_____

6. What are the four basic task categories that should be executed during cybersecurity incident responses?

_____
_____
_____

7. When assessing the scope and impact of a cybersecurity incident, what five items should be identified?

_____
_____
_____

8. To appropriately document response efforts, what should be included in a response plan?

_____
_____
_____

9. When disseminating information, what should the response plan define for judges and court personnel?

_____
_____
_____

10. What key information should the spokesperson be prepared to communicate to potential victims and the public?

_____
_____
_____
_____
_____

11. When a court's system is breached, who should be considered as "potential victims" and why?

_____
_____
_____