**This survey is voluntary and is NOT a required exercise. If you decide to take this survey, please turn it in at the SCCE/HCCA desk.**

**Please answer the below questions by circling the appropriate response. You may skip the questions that do not apply.**

-----------------------

1. In your experience, does the workforce have an adequate awareness and understanding of cybersecurity threats?

Yes

No

Not Sure

2. Do you have situational awareness of the organization's cybersecurity program?

Yes

No

Not Sure

3. Do you understand the organization's cybersecurity training in the context of your day-to-day use of information technology (e.g. software, systems, and network)?

Yes

No

Not Sure

4. Do the organization's vendors and clients have a comparable cybersecurity practice/program?

Yes

No

Not Sure

5. Is the organization's compliance team included in auditing/investigation of cybersecurity incidents that result in actual or suspected data, system, or network compromise?

Yes

No

Not Sure

6. Is cybersecurity included as an area within the organization's strategic plan?

Yes

No

Not Sure

7. Is compliance included as an area within the organization's strategic plan?

Yes

No

Not Sure

8. Has the organization experienced a cybersecurity incident within the past 12-months to include, but not limited to, virus, cyber attack, employee mistake, malicious insider threat, or mitigated information technology vulnerability?

Yes

No

Not Sure

9. Has the organization experienced an insider attack, or attempt, in the past 12-months?

Yes

No

Not Sure

10. Does the organization use a cybersecurity framework such as ISO/IEC 27001, NIST CSF, COBIT, ITIL, or an internally created framework/policy?

Yes

No

Not Sure

11. Are cybersecurity incidents studied/analyzed to help update cybersecurity practices?

Yes

No

Not Sure

12. Does the organization perform routine software updates to include virus software?

Yes

No

Not Sure

13. Does the organization employ a full time cybersecurity officer/team?

Yes

No

Not Sure

14. Is the organization focused on vulnerability mitigation (choose 1) or capability resiliency (choose 2)?

One

Two

15. Do vendors or other non-organization employees have unescorted physical access to company resources (e.g. facility, storage, diagnostic test/troubleshoot, email, inventory, database, system, or network)?

Yes

No

Not Sure

16. Do vendors or other non-organization employees have remote information technology access such as email, inventory/personnel/finance database, or other information technology account or network privileges?

Yes

No

Not Sure

17. Do employees have protected Internet access to company information technology resources?

Yes

No

Not Sure

18. Are client/customer personal mobile devices allowed in the workplace?

Yes

No

Not Sure

19. Does the organization have non-protected WiFi access that is provided for client/guest use?

Yes

No

Not Sure

20. Are employees allowed to download software from the Internet?

Yes

No

Not Sure

21. Are employees provided organization cybersecurity training to include social engineering, password strengths, and remote information technology procedures?

Yes

No

Not Sure

22. Does the organization have a capability/service resiliency plan that includes information technology assets?

Yes

No

Not Sure

23. Do you use firewall, intrusion detection system, and/or other preventive capabilities?

Yes

No

Not Sure

24. Do you believe that traditional cybersecurity techniques are adequate to protect the organization's information technology resources?

Yes

No

Not Sure

25. Do you have a monitoring strategy that includes the review of software, system, and network alerts and logs?

Yes

No

Not Sure

26. Is administrative and operational/client data seen on the same network?

Yes

No

Not Sure

27. Can external devices be connected to organization information technology devices such as a USB drive or laptop without requesting prior permission?

Yes

No

Not Sure

28. Does your organization have an auditing program that reviews user data searches against organization and client databases?

Yes

No

Not Sure

29. Have all default (factory set) passwords been changed on all information technology equipment including network, mobile, diagnostic/test, and desktop devices?

Yes

No

Not Sure

30. Is there an employee out-processing process that includes terminating information technology and physical (facility) access?

Yes

No

Not Sure

31. Is there a published password policy that requires specific password criteria such as the password including alphanumeric and special characters?

Yes

No

Not Sure

32. Are users required to change their passwords frequently using a strong password formula?

Yes

No

Not Sure

33. Is periodic cybersecurity testing conducted to include data, system, network, and physical security?

Yes

No

Not Sure

34. Is remote access used for administration of data, system, and/or network functions?

Yes

No

Not Sure

35. Is employee telework an option for performing assigned duties?

Yes

No

Not Sure

36. Is removable storage device connectivity restricted on information technology resources (e.g. desktop PC, servers, network devices)?

Yes

No

Not Sure

37. Are employee personal mobile devices allowed in the workplace?

Yes

No

Not Sure

38. If employee personal mobile devices are allowed in the workplace, is access to organization and/or client data authorized?

Yes

No

Not Sure

39. Is organization data encrypted in transit (e.g. network traffic)?

Yes

No

Not Sure

40. Is organization data encrypted when at rest (e.g. storage to include databases, files and folders)?

Yes

No

Not Sure

**COMMENTS:**