MORE POWER TECHNOLOGY GROUP

C H E C K L I S T

Public-Sector Security Visibility Checklist

21 questions for a first review of your technology visibility and responsibilities.

Complete this with whoever handles your technology. Mark **Yes** when you can support the answer, **No** when the arrangement is missing, and **Not sure** when it needs checking. Allow about 20 minutes for a first pass, then follow up on missing information. Do not enter passwords or sensitive system details.

Organization _____ **Completed with** _____ **Date** _____

1. DO YOU KNOW WHAT YOU HAVE?

Include remote work and equipment bought or replaced outside the usual IT process.

Question	Yes	No	Not sure
1. Do you have a current inventory of devices connected to your network or used to access your data?	☐	☐	☐
2. Has someone reviewed that inventory within the last 12 months and checked subsequent changes?	☐	☐	☐
3. Do you know which work devices leave the building or are used remotely?	☐	☐	☐
4. Would your IT contact know if a department bought and connected a new device?	☐	☐	☐

2. DO YOU KNOW WHAT IS PROTECTED?

Check current status, not just the original deployment. Record any unsupported devices or exceptions.

Question	Yes	No	Not sure
5. Is endpoint security installed on the workstations and servers that require it?	☐	☐	☐
6. Do you know the actual coverage percentage and how it was calculated?	☐	☐	☐
7. Does someone verify that security agents are running, current, and reporting?	☐	☐	☐
8. Do you know which devices, if any, lack endpoint protection?	☐	☐	☐

3. DO YOU KNOW WHAT IS HAPPENING?

Device, email, and account activity may come from different sources. Confirm which are included.

Question	Yes	No	Not sure
9. Are security events being logged on the systems and services you rely on?	☐	☐	☐
10. Do you know how long those logs remain available?	☐	☐	☐
11. Does someone review security alerts on an agreed schedule?	☐	☐	☐
12. Would a sign-in from an unexpected country be identified and reviewed?	☐	☐	☐

4. DO YOU KNOW WHO OWNS THE NEXT ACTION?

A named owner needs time, authority, and support. Alert review and incident response are different responsibilities.

Question	Yes	No	Not sure
13. Is there a named person or provider contact for alert review, with backup coverage?	☐	☐	☐
14. Is alert review a documented job or service responsibility?	☐	☐	☐
15. Do you know what your monitoring provider is contracted to do when a problem is found?	☐	☐	☐
16. Have you reviewed the exclusions in your monitoring or IT agreement?	☐	☐	☐

5. PUBLIC-SECTOR PLANNING AND READINESS

Use your agency's requirements and calendar. A public-safety question may not apply to every agency.

Question	Yes	No	Not sure
17. Do you know your next budget or procurement decision date?	☐	☐	☐
18. Have you confirmed your incident-reporting obligations, contacts, and deadlines?	☐	☐	☐
19. Have you named both a lead and a backup lead for cybersecurity incident response?	☐	☐	☐
20. For public safety: do you know which systems process or access criminal justice information?	☐	☐	☐
21. Have you used any free state cybersecurity assessment resources available to your agency?	☐	☐	☐

Question 20 only: ☐ Not applicable. Agency-confirmed reason

REVIEW YOUR ANSWERS

Count: Yes _____ **No** _____ **Not sure** _____ **Not applicable** _____

Total: 21.

Use Not applicable only for question 20 when your agency confirms that criminal justice information is outside its scope. Record the reason. The other answers identify topics for review; they are not a maturity score or a comparison with other agencies. A No on question 21 may simply mean a resource was unavailable or unnecessary.

Regardless of the total: follow up on any **No** or **Not sure** in section 4. Confirm who reviews a finding, who approves action, and who performs the work. A high count of Yes answers does not close an ownership gap.

For question 18: Oregon's Security Operations Center publishes guidance to report cybersecurity incidents within 24 hours of discovery. Confirm the applicable process with your agency's responsible official; Washington agencies should confirm their own requirements. [1]

CHOOSE THE NEXT USEFUL RESOURCE

For service responsibilities, read IT Monitoring vs. Managed IT Services. For vendor review, use How to Evaluate a Monitoring Provider for a Public Agency and the Government Sentry Brief. Budget timing questions belong with your finance or procurement lead.

For a second opinion on monitoring fit, schedule a review with More Power Technology Group.

Next action _____ **Owner** _____ **Review date** _____

REFERENCE

Oregon Security Operations Center. Published incident-reporting guidance. This checklist does not determine legal obligations or certify compliance.