ARIZONA@WORK
Yuma County

Cybersecurity Assessment Questions and Answers

(The questions provided below were copied exactly as we received them)

Bidders submitted the following questions regarding the Cybersecurity Assessment RFP. The responses below are being provided for all potential bidders to ensure clarity on the scope of the RFP. More specific technical information, configurations, products, versions, IP ranges, and inventories will be shared only with the awarded vendor under appropriate confidentiality agreements, such as a non-disclosure agreement.

1. **Do they have current risk ratings for critical applications and systems**
   YPIC has internal views on risk and criticality for key applications and systems, but one of the goals of this engagement is to validate and improve that picture.

2. **What agencies use the YPIC Network, and how are they administratively/technically segmented**
   The YPIC network supports internal programs and partner agencies that participate in workforce and related services. Logical and administrative segmentation is in place, and part of this assessment will be to review that segmentation and provide recommendations.

3. **For the ITGC, have the controls been identified that will be assessed?**
   The RFP describes the general control areas that are in scope. The final list of IT general controls and the level of depth for each control area will be shared with the selected vendor during project planning.

4. **That is the OS of the systems being evaluated**
   The environment is primarily a Windows-based desktop and server environment, with some use of cloud and web-based applications. Any non-Windows or specialized systems will be documented and provided to the selected vendor as part of the detailed inventory.

5. **What hypervisors are being used**
   Virtualization is in use within the environment. Specific hypervisor products and versions will be shared with the selected vendor.

6. **What does YPIC use for backups?**
   YPIC uses standard backup solutions appropriate for a small to medium local environment. Details about backup platforms, schedules, and retention will be provided to the selected vendor.

7. **Is the wireless network a component of the assessment?**
   Yes. Wireless networks and their configuration are considered in scope for the assessment.

8. **Can you clarify the number of physical locations and endpoints involved in the assessment?**
   The assessment covers multiple physical locations used by YPIC and its programs, two sites in Yuma, Arizona, one in Somerton, and one in San Luis. For proposal purposes, vendors may assume a small to medium-sized local environment with about 180 devices in scope, including endpoints and servers. A detailed asset and site list will be provided to the selected vendor after award.

9. **Are there specific systems or applications (e.g., ERP or HRIS) that require deeper audit focus?**
   Certain systems that support financial, HR and case management functions are higher priority. The selected vendor will work with YPIC to identify which applications require deeper focus during detailed planning.

10. **Will [redacted] be granted administrative access for internal testing, or is it strictly black box?**
    The assessment is expected to include internal testing, and the selected vendor may be granted appropriate access where needed. The exact level of access, for example credentialed scans or admin access, will be defined during project planning to balance thoroughness and security.

11. **Are there any systems or networks excluded from penetration testing?**
    Some systems may have constraints or maintenance windows that limit active testing. For context, the RFP does not require a penetration test, so any testing limits will be reviewed with the selected vendor during planning.

12. **How many total IP's are in test?**
    Vendors may assume a small to medium environment consistent with the approximate device count provided above. The exact IP count and ranges will be provided to the selected vendor upon award.

13. **For the AI usage audit, are there known tools currently in use (e.g., ChatGPT, Gemini) that should be prioritized?**
    There may be use of common AI tools such as ChatGPT or Gemini.

14. **What level of detail is expected in the Zero Trust readiness roadmap?**
    The Zero Trust readiness roadmap should provide practical and prioritized recommendations, including near-term and longer-term steps mapped to recognized frameworks or principles. The goal is to give YPIC a clear, actionable path rather than high-level theory.

15. **Are there any compliance implications that the County is required to adhere to?**
    YPIC operates in a public sector and workforce development context and must align with applicable federal, state, and local requirements, along with funding and grant conditions. The selected vendor is expected to factor common public sector requirements and best practices into their recommendations.

16. **Is there a preferred framework to assess against? (NIST, CIS, ISO)**
    YPIC is open to common frameworks. Vendors should state which framework or frameworks they intend to use and how those will be applied in the assessment and reporting.

17. **Is the 3-4 week timeline flexible based on scope complexity?**
    The timeframe in the RFP reflects the desired project window. Some flexibility may be possible based on complexity and scheduling. Vendors should propose realistic timelines tied to the scope they are proposing.

18. **Are interim deliverables (e.g., weekly status reports) expected?**
Yes. YPIC expects at least brief status updates during the engagement so that any issues or adjustments can be addressed early. Vendors may suggest their standard cadence for status reporting.

19. **Is the 35,000 budget firm, or is there flexibility based on scope?**
The budget in the RFP reflects the current expectation for the defined scope. Vendors may describe any assumptions behind their pricing and may propose optional services separately if those would exceed the base budget.

20. **Should the fixed fee proposal include optional services or just core deliverables?**
The fixed fee proposal should clearly cover the core deliverables described in the RFP. Optional services, such as extended monitoring or additional testing, should be listed and priced separately so they can be considered as add-ons.

21. **Are subcontractors allowed for specialized testing (e.g., social engineering), and what documentation is required?**
Subcontractors may be used for specialized tasks subject to YPIC review and approval. Vendors should disclose any planned use of subcontractors in their proposal and be prepared to provide information on qualifications, roles and how confidentiality and data protection will be handled.

22. **What format should the data destruction certification take?**
A written certification on company letterhead, signed by an authorized representative, confirming that confidential data collected during the engagement has been securely destroyed in accordance with agreed-upon methods, will be sufficient. Vendors may include their standard data destruction language for review.

23. **Is there a preferred method for securely transferring sensitive findings?**
YPIC can support several secure transfer options. Encrypted email is available. Encrypted USB flash drives may also be used and delivered in person. If the awarded vendor prefers a secure file transfer platform, YPIC is open to reviewing it during project planning to make sure it meets security requirements.

24. **Will oral presentations be required for shortlisted vendors?**
Oral presentations are not planned at this stage. If that changes, YPIC will notify shortlisted vendors.

25. **Is there a weighting preference among technical expertise vs. cost?**
The selection process will consider the vendor's experience, methodology, understanding of the scope, and overall value.

26. **Is there an expectation for ongoing advisory or remediation support after the final report?**
The primary focus of this RFP is the assessment and the final report with recommendations. Vendors may describe their capability and pricing for ongoing advisory or remediation support as optional services, which YPIC may consider separately.

27. **How many users, endpoints, and servers are expected to be in scope for testing during the assessment?**
For proposal purposes, vendors may assume a small to medium-sized local environment with several dozen internal users and approximately 180 devices in total, including endpoints and servers. A detailed inventory and exact counts will be provided to the awarded vendor under appropriate confidentiality agreements.

28. **Does YCWDB authorize limited physical social-engineering testing (e.g., badge testing or controlled access attempts)?**
Physical social engineering activities, such as badge testing or controlled access attempts, are not required under the current RFP. Vendors may describe such services as optional items if they choose to, but proposals should focus on the technical cybersecurity and hardware/software assessment described in the RFP.

29. **If yes, how many locations would require on-site presence?**
Not applicable at this time. Any optional services would be discussed with the awarded vendor and scoped separately if needed.

30. **Aside from Microsoft 365, are there additional cloud platforms, SaaS applications, or third-party systems that should be included in the assessment scope?**
The scope of this RFP is defined by the systems and services described in the solicitation, with a primary focus on the existing on-premises and networked environment. For proposal purposes, vendors should base their approach on those in scope systems. If any additional cloud or SaaS platforms are to be included, they will be discussed and confirmed with the awarded vendor during project planning so that assessment boundaries are clear.

31. **Does the Board require a formal remediation retest as part of the not-to-exceed $35,000 budget?**
The primary focus of the RFP is the initial assessment, findings, and recommendations within the not to exceed 35,000 dollars. A formal remediation retest is not specifically required. Vendors may outline their standard approach for validating remediation or may propose an optional retest as a separately priced item.

32. **Is an in-person executive presentation required, or will a virtual briefing satisfy the reporting and closeout requirements?**
A virtual briefing presentation that allows for discussion will satisfy this requirement. Vendors may propose an in-person presentation as an optional item if they believe it adds value.

Questions on Existing Users

33. **How many internal users currently access the YPIC network?**
Approximately 80 internal users.

34. **How many remote users and third-party partners are connected to the network?**
A small number of remote users access systems as needed.

35. **Are there any shared accounts or privileged access users that need to be reviewed?**
Yes. Privileged access will be included in the assessment review.

Questions on Existing Technologies

36. **What are the current hardware and software platforms in use across YCWDB and partner agencies?**
The environment is primarily a standard Windows-based desktop environment with common productivity, line-of-business, and web applications, plus some locally hosted systems and cloud services.

37. **Which antivirus/malware solutions and firewalls are currently deployed?**
YPIC uses commercial, industry-standard endpoint protection and network firewall solutions.

38. Are there any existing endpoint protection or EDR solutions in place?
Yes. Endpoint protection is in place today.

Questions on Tools / Technologies Requested

39. Are there any preferred tools or technologies for risk assessment, vulnerability scanning, and Zero Trust evaluation?
YPIC does not require specific commercial tools for assessments. Vendors may propose the tools and methodologies they believe are most appropriate and can be clearly documented in the deliverables.

40. Do you have any existing AI-based phishing simulation tools or plans to implement them?
YPIC does not currently have a specific AI-based phishing simulation platform in place today.

41. Are there any restrictions on using third-party cloud-based security tools?
Cloud-based security tools are acceptable as long as they comply with applicable federal, state, and local requirements, contractual obligations, and YPIC policies. Any proposed tools must clearly describe data residency, logging, retention, and access controls.

Monitoring vs Incident Handling

42. Is the expectation limited to assessment and reporting, or do you require ongoing monitoring services?
The current RFP is focused on assessments, findings, and recommendations.

43. For incident handling, do you expect the vendor to provide breach response services beyond assessment (e.g., forensic analysis, containment)?
The primary expectation is assessment and advisory support.

24x7 Monitoring Support

44. Do you require 24x7 monitoring support or only periodic assessments during the engagement?
The RFP scope is for periodic assessments and related activities.

Tool Licensing

45. Are you expecting the vendor to provide only tool licensing or full implementation and configuration services?
YPIC expects the vendor to provide assessment services and recommendations. If specific tools are proposed, vendors should indicate whether licensing, implementation, and configuration services are included or optional.

Post-Installation Support

46. After installation/configuration, what level of support do you expect from the vendor (e.g., break-fix, advisory, managed services)?
The baseline expectation is advisory support related to the assessment and its recommendations. Additional support models may be proposed as optional services.

47. Do you require post-breach professional services such as legal counsel and insurance coordination?
No.

Microsoft Licensing

48. What type of Microsoft license is currently being used (e.g., G3, G5, G5 Security)?
YPIC uses standard Microsoft licensing appropriate for a local government / non-profit environment.

49. Are there any plans to upgrade or change Microsoft licensing tiers in the foreseeable future?
Potential changes to licensing may be considered as part of the recommendations that emerge from this assessment.

Asset Inventory

50. Can you provide a complete list and count of all assets (hardware, software, endpoints, servers) that fall under the scope of this assessment?
Asset inventory information will be provided to the selected vendor after award under appropriate confidentiality protections. For proposal purposes, vendors may assume a small to medium-sized local environment with around 180 devices.

51. How many agencies use the YCWDB Network?
The network supports internal programs and partner agencies involved in workforce development and related services. The selected vendor will receive additional context on participating agencies and how they are supported during project planning.

52. Which compliance frameworks are they legally obligated to meet? (PCI vs HIPAA etc)
YPIC operates in a public sector and workforce development context and must align with applicable federal, state, and local requirements, along with funding and grant conditions. The selected vendor is expected to factor common public sector requirements and best practices into their recommendations.

53. How many publicly facing IP addresses do you have?
For proposal purposes, vendors may assume a small to medium-sized local environment with about 180 devices in scope, including endpoints and servers. A detailed asset and site list will be provided to the selected vendor after award.

54. How many web applications are being hosted in that space?
There is a limited number of internally accessible web applications that support workforce and related services. A detailed list of in-scope web applications will be provided to the selected vendor after award so that testing can be planned appropriately.

55. **Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?**
Standard security controls, such as commercial firewalls and related protections, are in place today, appropriate for a small to medium local environment. Details on specific products, configurations, and monitoring will be shared with the awarded vendor during planning.

56. **How many internal IP addresses are in your network?**
Vendors may assume a small to medium internal environment aligned with the previously noted device count. The exact number of internal IP addresses, address ranges and segmentation details will be provided to the selected vendor under appropriate confidentiality protections.

57. **Is there any network segmentation in place?**
Logical and administrative segmentation is in place, and part of this assessment will be to review that segmentation and provide recommendations. Specific network diagrams and segmentation details will be provided to the selected vendor during project planning.

58. **Are you using cloud hosting? If so, which provider(s) and what are the current number of resources in those cloud environments?**
The scope of this RFP is defined by the systems and services described in the solicitation, with a primary focus on the existing on-premises and networked environment. For proposal purposes, vendors should base their approach on those in scope systems. If any additional cloud hosting is to be included, they will be discussed and confirmed with the awarded vendor during project planning so that assessment boundaries are clear.

59. **Do you currently have a device inventory of all authorized devices on your network?**
Asset and device inventory information is maintained and will be provided to the selected vendor after award under appropriate confidentiality protections. For proposal purposes, vendors may assume a small to medium-sized local environment with around 180 devices in scope.

60. **Do remote users connect via VPN? If so, which VPN service?**
Remote access methods are in scope for this assessment, and the selected vendor will work with YPIC to confirm the appropriate assumptions about remote connectivity, including any VPN technologies, during project planning. Specific products and configurations will be shared with the awarded vendor under confidentiality.

61. **Should on-premises social engineering also include testing physical access controls (badge systems, door locks, cameras) or exclusively personnel and associated policies?**
The current RFP does not require physical social engineering activities. The primary

focus is on technical cybersecurity and the hardware/software assessment. Vendors may describe social engineering or physical testing services as optional items if they choose to, clearly separated from the core scope.

62. **How many locations are in scope for on-premises social engineering?**
Because physical social engineering activities are not a required part of the RFP, there is no defined count of locations for this type of testing. If any optional services are considered with the awarded vendor, they would focus on the primary program and administrative locations and would be scoped separately.

63. **Are mobile/byod devices separated to a specific subnet?**
Network architecture, including treatment of mobile and BYOD devices, will be reviewed as part of the assessment. Detailed network design information, including any segmentation related to these devices, will be shared with the selected vendor under appropriate confidentiality protections.

64. **Would you like testing of wireless network controls? If so, how many SSIDs are in scope?**
Yes. Wireless networks and their configuration are considered in scope for the assessment. For proposal purposes, vendors may assume a small number of SSIDs associated with internal and guest access. A detailed list of wireless networks and SSIDs in scope will be provided to the selected vendor after award.

65. **Do you currently have an inventory of sanctioned software that may be used by employees and/or a list of explicitly banned software?**
Software use is governed by internal policies, and inventory information for sanctioned and restricted software can be provided to the selected vendor as part of the assessment planning process. One of the engagement goals is to validate and, where helpful, improve the current picture of software governance.

66. **How many unique email addresses will be tested as part of phishing simulations?**
Any phishing simulations conducted as part of this engagement are expected to focus on a representative group of users rather than a specific fixed count. The exact scope, including the number and type of email addresses to be included, will be defined with the selected vendor during project planning, taking into account risk, business operations, and the overall engagement timeline.