# Request for Proposals
# RFP489 - Network Security Audit and Vulnerability Assessment
# Questions and Answers

*The following questions have been consolidated from multiple vendor submissions. Duplicate and substantially similar questions have been merged into single items. Responses are provided below each question in italics.*

## Technical Scope

1. Can ARC confirm the exact active IP counts (internal and external) for scoping purposes? Appendix A indicates fewer than 500 internal IPs and fewer than 20 external IPs.

   *ARC is a hybrid work environment and may experience fluctuations in the number of internal IP addresses in use based on the presence of staff, visitors, and device usage. The selected vendor should anticipate the potential for scanning up to the provided range in the RFP.*

2. Is exploit testing / active exploitation included in the external network vulnerability assessment, or is the scope limited to identification and documentation of vulnerabilities?

   *The primary goal is the improvement of the agency's security posture through identification of potential vulnerabilities. Active exploitation should only be considered where there is no known impact(s) to the stability or availability of the systems under review.*

3. Can all internal network testing be conducted from a single network location, or will access to multiple VLANs or segments require separate connection points?

   *All scanning will be available from a single point of access.*

4. The network includes 10 physical servers, 47 virtual servers, and 6 VMware cluster hosts. Does the systems security review cover all 63 server instances, or is sample-based testing acceptable for virtual environments? Will the assessment cover all 47 virtual servers, or only a defined subset based on criticality?

   *The assessment should include all areas of the environment as listed in Appendix A of the RFP.*

5. How many unique operating systems and versions are deployed across servers and workstations?

   *The environment consist of a mix of Windows Server versions ranging from 2016 through 2025 and various Linux distros.*

6. The environment includes three IIS web servers and three Apache web servers with 25–40 bindings. Are these web servers in scope for web application security testing (e.g., OWASP-based), or is the scope limited to network and infrastructure-level vulnerability scanning?

*OWASP based testing of web applications is welcomed in addition to infrastructure scanning.*

7. Will ARC provide vendor access and administrative credentials for the AWS Elastic Disaster Recovery environment, or will the vendor work through ARC IT staff? Has AWS Elastic Disaster Recovery already been implemented and configured, or is the selected vendor expected to support initial setup and replication configuration?

   *An existing Elastic Disaster Recovery instance is implemented and configured. The vendor should expect to work through ARC IT staff.*

8. Is there an IDS/IPS, UTM, or WAF/reverse proxy solution deployed? If so, which products?

   *All IDS, IPS, and WAF functions are managed through the Versa UTM appliance currently deployed, as noted in Appendix A of the RFP.*

9. Are mobile devices (iOS/Android) or BYOD endpoints included in the systems security assessment scope?

   *No mobile devices are in scope for this assessment.*

10. How many distinct internal firewall appliances or virtual instances are currently deployed? Does the environment include additional internal firewalls or security appliances beyond the ISP-managed Versa Appliance listed in Appendix A?

    *All segmentation is managed through the Versa appliance as listed in Appendix A. No other appliances or instances are present.*

11. Does the assessment scope include the Microsoft 365 cloud tenant configuration (e.g., conditional access, MFA enforcement, admin role review) or only on-premises/hybrid components?

    *All Microsoft 365 configurations, policies, and MFA enforcement conditions are within scope for this assessment.*

12. Is the SIEM (Graylog/ManageEngine) and EDR (Arctic Wolf Aurora) configuration review within scope, or is the assessment limited to the underlying infrastructure those tools monitor? Will the vendor be granted read-only access to these tools as well as firewall configs (Versa)?

    *The review of these systems is within scope. The vendor should expect to work with IT staff to obtain access.*

13. Beyond AWS for Disaster Recovery, are other critical SaaS or cloud environments (e.g., Azure, Microsoft 365, Salesforce) included in the security audit scope?

    *No other cloud or SaaS environments beyond those listed in Appendix A are currently in scope.*

14. Is wireless network testing in scope? If so, how many SSIDs, wireless locations, or physical sites need to be included?

    *ARC has one office included in this assessment. The vendor should anticipate testing the agency's three SSID's.*

15. Are there persistent connections to third-party or vendor-managed systems (e.g., HVAC, IT service providers) in scope? If so, please list them.

    *There is one persistent connection to assist with management of door access systems and cameras. No other vendor connections are present.*

16. How many remote access services are in scope (e.g., VPN, GoTo My PC, LogMeIn)? How many employees use remote access?

    *All agency staff have access to VPN services.*

17. How many domains and distinct authentication methods are currently in use? Is a review of identity and access controls (e.g., Active Directory/Entra ID, MFA, privileged access) included in scope?

    *Active Directory, Entra ID, MFA. All methods are in scope for review.*

18. Please list all internal network segments in scope (e.g., management, production, development, DMZ).

    *Production, Guest, Audio-Visual, Telephone*

19. Regarding switch configuration analysis for the ten identified devices: will the Commission provide configuration dump files for offline analysis, or will the vendor be granted direct access to administrative portals?

    *Files for these devices will be provided by IT staff.*

20. Regarding firewall policy review: will the selected vendor be provided with configuration export files or direct read-only access to the administrative interface for the ISP-managed Versa Appliance and any other in-scope firewall appliances?

    *As noted in Appendix A, the Versa is owned and managed by ARC's ISP. Any review of the device configuration will require coordination with IT staff and the ISP's security team.*

21. Will ARC provide a complete and validated asset inventory (IP ranges, hostnames, system classifications) to ensure full coverage of all in-scope assets?

    *IT Staff will provide a list of the environment inventory. However, as a best practice of assessment, the vendor should expect to scan and identify devices not included in the provided inventory.*

22. Please clarify ARC's expectation for "password auditing for existing domain user accounts", including whether this should be performed through password policy review only, Active Directory configuration review, hash-based analysis under ARC control, another approved method.

    *The vendor should review password policy and Active Directory configuration analysis.*

## Compliance Depth

23. Please confirm that the compliance frameworks adopted by ARC are HIPAA, ISO 27001, and NIST SP 800-53. Are there any other formally adopted security control frameworks?

Have any prior gap assessments been completed against these frameworks? Is ARC seeking a gap analysis against one specific framework or a general best-practices audit referencing all three? Is formal control mapping required?

*ARC conducts a risk assessment on an annual basis to score the security posture of the agency against an evolving threat landscape. All previous assessments have been inclusive of the three frameworks listed.*

24. Which departments or programs at ARC handle Protected Health Information (PHI), how many locations or systems are involved, and is a formal HIPAA risk analysis a required deliverable under this engagement?

    *ARC's department of Aging and Independence Services interacts with PHI housed through the State of Georgia and agency partners.*

25. How many documented IT security policies, procedures, standards, and guidelines are currently in place?

    *The selected vendor will be provided access to existing policies during the assessment period.*

26. Are there specific regulatory or compliance requirements beyond the listed frameworks that ARC must align with (e.g., CJIS, CIS)?

    *Currently, there are no specific regulatory requirements.*

27. Are audit artifacts or prior assessment reports available to align with? Has a similar comprehensive security audit been conducted within the last 24 months, and will those findings be shared with the winning bidder?

    *ARC conducts a risk assessment on an annual basis. The vendor should expect to assess the environment without review of previous reports.*

28. Does your cyber insurance policy have any recommended exercises for you to achieve?

    *There are no currently recommended exercises.*

## Operational Logistics

29. When is the anticipated contract start date? Are there preferred milestones within the 30-day assessment window?

    *Start date is contingent upon award and acceptance of contract by both parties. ARC has no preferred milestones during the 30-day period. However, the vendor should expect to provide weekly feedback to IT staff on current activities and findings.*

30. Are there any blackout periods or operational constraints that would prevent testing during certain windows (e.g., budget cycles, major events, peak service periods)? Are there defined scanning windows or after-hours-only requirements?

    *There are currently no known blackout periods or operational constraints. Vendor will be advised if constraints arise during the assessment.*

31. Is attendance at the pre-proposal conference mandatory, and will a virtual attendance option be available?

    *This RFP has no pre-proposal activities. Potential vendors should submit their proposals directly through ARC's procurement portal for review.*

32. The three tabletop exercises include one executive-level and two IT staff exercises. Will these be conducted in person at ARC's Atlanta facility or virtually? Who are the intended participants for the executive-level session (e.g., board members, department heads, senior IT leadership)?

    *The executive-level exercise is to be conducted in-person with attendees consisting of ARC's executive leadership team, lead IT staff, and other select staff as required. The IT staff exercises may be conducted virtually and will be limited to the IT team.*

33. Do the tabletop exercises have expected time durations?

    *The vendor should anticipate an approximate duration of 90-120 minutes for the executive session and 60-90 minutes for the IT staff sessions.*

34. Are the two IT staff tabletop exercises using the same playbook or different ones? What type of DR/BCP and cybersecurity IR scenarios are desired (e.g., ransomware, natural disaster, insider threat)?

    *The scenario type and development are at the discretion of the vendor. Each exercise should represent realistic opportunities for staff development and incident preparedness against the current threat landscape.*

35. The security roadmap is described as covering 24–36 months. Is ARC looking for high-level strategic direction or a granular project-by-project plan with estimated budget cycles? Are there existing technology plans or strategic IT initiatives the roadmap should align with?

    *The security roadmap should provide a high-level strategic and actionable plan for improving cybersecurity over the set timeline, bridging the gap between current state and desired future state.*

36. In 2025, ARC issued a similar RFP. Was that assessment conducted or cancelled? Is there an incumbent service provider, and if so, what is the firm's name and contract duration?

    *The assessment was conducted and contract concluded.*

## Resource Constraints & Access

37. Who will serve as ARC's primary point of contact, and what is the anticipated availability of IT staff for interviews, walkthroughs, and testing coordination? Will ARC provide designated SMEs for structured sessions, or should the vendor assume ad-hoc coordination?

    *Curt Davis is the project manager for the risk assessment. IT staff will be available for all activities as required. ARC will schedule weekly check-ins and facilitate scheduling of staff based on need and vendor activity.*

38. Will ARC provide documentation such as network diagrams, firewall rule exports, and Active Directory reports, or will the vendor be expected to gather this information independently? Will existing DR plans, BIA documents, and prior assessment reports be provided?

    *ARC will provide all current environment documentation on commencement of assessment.*

39. How many full-time IT staff are employed by ARC, and how many are dedicated to cybersecurity functions?

    *ARC's IT team consists of 8 members with one lead position holding the primary oversight for cybersecurity. All staff are responsible for security awareness and management.*

40. Will ARC provide secure VPN access for remote scanning or must all internal assessments be conducted on-site?

    *Provisions for access will be arranged with selected vendor, including VPN if required*.

41. Can any portion of the assessment, analysis, or report development be performed by personnel located outside the United States?

    *Due to security requirements, ARC strongly encourages the use of onshore personnel.*

42. Would you allow an end-point vulnerability scanning agent on-device?

    *ARC's preference is agentless analysis and discovery.*

43. Is the environment managed withing Microsoft365 Intune?

    *The environment is integrated with Microsoft365 and Intune management suite.*

44. Has a formal Business Impact Analysis been previously completed, or will the vendor develop BIA documentation as part of the DR engagement? Is there a current Incident Response Plan with a clearly marked last update and approval date?

    *Vendor should anticipate developing BIA documentation as part of the DR engagement. ARC will provide all available incident response documentation.*

45. Are the two DR drills expected to be full production failover tests with live workloads switched to AWS, or simulation-based exercises without production impact? What is the scope of systems included (all workloads vs. a subset)?

    *DR drills should demonstrate the capability of production failover of the systems currently included in the EDR instance. The current EDR instance consists of a subset of the environment.*

46. Approximately how many personnel are expected to participate across the three tabletop exercises?

    *The executive tabletop session may include up to 20 participants. The IT team exercises will include up to 8 staff.*

47. Are rescans expected after remediation? If yes, what is the expected timeline? Are false positive validations required? Is this a continuous scanning engagement or a baseline scan plus revalidation cycle?

    *Rescans to demonstrate remediation of any findings are requested within 60 days of final report. The engagement is a baseline review followed by rescan validation. Vendor should confirm any findings are not false positives.*

## Reporting Expectations

48. Do the required sample reports count toward the 15-page proposal limit, or may they be submitted as a separate appendix?

    *Sample reports may be submitted as an appendix outside the stated page count.*

49. The RFP references '30-Day Vulnerability Risk Assessments.' Does this require continuous monitoring and repeated rescanning, or a single assessment completed within 30 calendar days? Is reporting expected periodically during the engagement or as a consolidated deliverable at the end?

    *The vendor shall complete a single assessment during the engagement within 30 calendar days.*

50. What is the expected level of detail in deliverables? Is executive vs. technical separation expected? Are there any preferred report formats, templates, or risk scoring models ARC requires?

    *The deliverables should include both an executive summary of findings and a technical detail with recommended remediation actions. ARC prefers risk scoring models based CISA's CVE 1-10 scale.*

## Commercial & Administrative

51. Is this contract intended to be awarded to a single vendor or multiple vendors? Is there a preference for local vendors?

    *The contract award is intended to a single vendor. No preference is given for local vendor.*

52. In the interest of efficiency, would a comprehensive reference list be an acceptable alternative to formal letters of recommendation?

    *Formal letters of recommendation are preferred as this format is in line with our review process. All references should be available for confirmation by ARC staff of vendor's previous work.*

53. What is the intended pricing structure for this engagement (e.g., fixed-price or time-and-materials)?

    *Method of pricing is at the discretion of the vendor but under no circumstances should the engagement exceed the allowed budget.*

54. Does the $45,000 maximum contract value include all travel and incidental expenses, or are those reimbursed separately?

    *The selected vendor shall not exceed $45,000 in total for assessment activities including travel and incidentals.*

55. Are there specific DBE/MBE/WBE participation percentage goals or Good Faith Effort requirements associated with this contract?

    *Please reference the following URL for information on ARC's DBE goals in compliance with 49 CFR Part 26. https://procurement.atlantaregional.org/disadvantaged-business-enterprise/*

56. What was the annual spend on this project in the previous year? What is the annual budget for this engagement? What challenges is ARC trying to address with the new contract?

    *The previous contract award totaled $40,000. As noted in the RFP, the allowable budget for this engagement is $45,000. The purpose of this engagement is to assess and further develop the agency's security posture and incident preparedness.*

57. Could ARC share an anticipated contract award timeline to assist with resource planning?

    *Award date is contingent upon review of all submitted proposals and fulfillment of ARCs procurement requirements. However, vendor should anticipate work will commence within 60 days of proposal acceptance.*