RFP489

Atlanta Regional Commission

Network Security Audit and Vulnerability Assessment

Request for Proposals (RFP)

March 25, 2026

Proposals Due: Monday, April 27, 2026 by 5:00 p.m. EST

Introduction

The Atlanta Regional Commission (ARC) Office of Information Technology provides technology services to internal departments and partner agencies, with a focus on maintaining a secure, reliable, and highly available network infrastructure that protects the Agency's data assets.

ARC is seeking proposals from qualified, independent service providers with demonstrated experience in cybersecurity assessments to conduct a comprehensive Network Security Audit and Vulnerability Assessment in accordance with the specifications set forth in this document.

The engagement should assess the maturity of ARC's information security program and provide actionable, expert technical guidance to improve both security posture and operational efficiency. Required deliverables include:

- A findings document identifying all non-compliant network vulnerabilities.
- A risk analysis that prioritizes each identified risk or vulnerability (High / Medium / Low); and
- A security roadmap outlining technologies and best practices ARC should pursue to strengthen its security model.

Note: ARC is not seeking a Security Operations Center (SOC) team to assume ongoing security operations.

Proposal Submittal

Vendors with questions regarding this RFP must submit them by email to the contact listed below. All questions and official responses will be published to the ARC website per the schedule in the timeline table.

Milestone	Date / Deadline
RFP Release Date	March 25, 2026
Deadline for Questions	Monday, April 6, 2026 by 5:00 p.m. EST
ARC Responses to Questions Posted	Monday, April 13, 2026 by 5:00 p.m. EST
Proposals Due	Monday, April 27, 2026 by 5:00 p.m. EST

Proposals shall not exceed 15 pages (8.5 x 11 inches), printed double-sided, inclusive of resumes and firm experience. Cover pages, end sheets, budget exhibits, and introductory letters are excluded from the page count. Minimum font size is 12 points throughout.

If interviews are deemed necessary, a short list of service providers will be invited to participate in an evaluation committee interview, scheduled to take place in April. ARC will confirm interview

dates and times with selected firms. ARC reserves the right to award this contract based on initial proposals without formal interviews, and to award all or part of this project to one or more firms.

ARC further reserves the right to: select a proposal other than the lowest-cost submission; reject any or all proposals or portions thereof; waive or modify irregularities or inconsistencies in proposals; request modifications to proposals from any respondents during contract review and negotiation; and negotiate any aspect of proposals with one or more proposers simultaneously.

Proposal Format and Content

All proposals must include the following information:

1. Legal name of the firm.
2. Point of contact (name, title, phone number, mailing address, and email address) at the lead firm.
3. Qualifications and technical competence of the firm(s) in the required type of work.
4. Description of relevant project experience, including a minimum of three (3) client references for similar engagements completed within the past five (5) years, with current contact information.
5. Listing of key project personnel and their qualifications.
6. A detailed description of the proposed technical approach for accomplishing the Scope of Work.
7. A proposed cost breakdown in the format provided at Exhibit B-1.
8. Any other pertinent information.

The successful service provider should be prepared to begin work immediately upon contract execution. ARC reserves the right to award all or part of the available funds for this project.

Proposal Evaluation

Written proposals will be evaluated based on the following weighted criteria:

Evaluation Criterion	Weight
A. Technical approach to providing the requested services, including quality and thoroughness of sample reports	**35%**
B. Demonstrated qualifications and experience to perform the requested services	**30%**
C. Reasonableness of proposed fee and expenses	**20%**
D. Client references and letters of support	**10%**

Evaluation Criterion	Weight
E. Proposed Cost	**5%**

Service Provider Requirements

The service provider's proposal must include all of the following components:

Executive Summary

Provide an executive summary outlining the proposal, including: the proposed management philosophy; identification of the project team and each member's responsibilities; and a summary description of the services to be provided. Sample reports representative of the deliverables described in this RFP must be included.

Statement of Work and Proposed Timeline

Provide a detailed Statement of Work describing all tasks associated with the engagement, including the respective responsibilities of the vendor and ARC, along with deliverables for each task. Where ARC responsibilities are identified, the required skills or resources should be noted.

Certifications

The service provider must have at least one (1) Certified Information Systems Auditor (CISA) or equivalent certification holder assigned to the project. Equivalent certifications include, but are not limited to, CISSP, CISM, CEH, or OSCP. Please identify all relevant certifications held by proposed team members.

Client References

Provide three (3) former clients as references for which similar services were performed, with preference given to engagements with local government entities. For each reference, include a one-to-two paragraph summary describing the scope of work, key deliverables, and notable outcomes.

Conflict of Interest and Confidentiality

ARC is subject to the Georgia Open Records Act. All submitted proposals become public records upon request. Any information containing trade secrets or proprietary data, as defined under

Georgia state law, must be clearly marked as "Confidential" on the specific pages or sections containing such information. Marking an entire proposal as confidential will not be honored.

Respondents must disclose any potential conflicts of interest that may arise from the provision of services described in this RFP. Required disclosures must include: (1) the name(s) of the individual(s) with whom a conflict exists; (2) all relevant facts pertaining to the potential conflict; and (3) a description of internal controls proposed to mitigate the conflict. ARC's Staff Legal Counsel will determine whether any disclosed conflict presents an organizational conflict of interest that would preclude award.

Conflicts of interest are governed by the ARC Standards of Ethical Conduct, available on the ARC website.

Exhibit A — Scope of Work

The selected vendor will perform a comprehensive Network Security Audit and Vulnerability Assessment addressing the following areas of ARC's infrastructure. The actions listed below are indicative but not exhaustive; vendors may propose additional services to achieve the stated objectives.

1. Edge Security

- Conduct ping sweep and port scan of all external IP addresses.
- Perform vulnerability scan of all external IP addresses.
- Review ingress and egress firewall policies.
- Review network address translation (NAT) rules for published internal systems.
- Verify firewall inspection capabilities (application-layer and stateful inspection).
- Determine whether a reverse proxy is in place for inspection of encrypted traffic and pre-authentication enforcement.
- Determine whether unified threat management (UTM) is configured for edge security.
- Review current auditing policies and practices for edge security devices.

2. Network Security

- Review switch configurations to determine whether network segmentation is in place between network segments.
- Determine whether internal firewalls are deployed between workstations and servers.
- Determine whether encryption is configured to protect internal communications.
- Review wireless security settings to validate applicable security controls.
- Validate port security settings, including whether network ports are active by default and whether port security is enforced based on MAC address.
- Determine whether network intrusion detection or prevention systems (IDS/IPS) are providing active network scanning.

3. Systems Security

- Conduct ping sweep and port scan of all internal IP addresses.
- Review all servers and workstations (see Appendix A) to assess whether the following configurations or security controls are in place:
  - Unnecessary services have been disabled.
  - A patch management solution is in place to ensure current operating system security updates are applied.
  - Auditing policies and procedures are defined and implemented for each system.
  - Each system has an up-to-date endpoint protection solution providing anti-malware and host-based IDS/IPS capabilities.
  - Host-based firewalls are enforced and centrally managed on all endpoints.
  - Membership in the local Administrators group is restricted to privileged accounts.
  - Local Administrator and Guest accounts are renamed or disabled.
  - Default file shares are disabled or appropriately secured, and share permissions are reviewed.

4. Access Management

- Review all authentication methods currently in use.
- Review domain group membership for high-privilege groups.
- Assess the policy for separating standard user accounts from privileged access accounts.
- Review the password policy enforced on the domain.
- Conduct password auditing for existing domain user accounts.
- Review remote access methods and associated security controls.

5. Disaster Recovery

- Plan and facilitate three (3) tabletop exercises (TTX) covering disaster scenarios within the context of the Cyber Response Team (CRT):
  - One (1) executive level exercise, Two (2) IT staff exercises
  - Develop a Tabletop Exercise Briefing Book for each exercise.
  - Prepare a detailed exercise script specifying how each exercise will be conducted, including injects, roles, and facilitation guidance.
- Conduct a minimum of two (2) full Disaster Recovery (DR) drills using AWS Elastic Disaster Recovery, evaluating and documenting:
  - Business Impact Analysis (BIA)
  - Time to recovery (TTR)
  - Recovery point objectives (RPO)
  - Disaster recovery site configurations

- Data backup integrity and procedures
- Testing and validation results
- Incident response plan effectiveness

Deliverables

1. Findings and Assessment Report — A comprehensive document detailing all identified threats and vulnerabilities, with an assigned risk and severity level for each finding.
2. Risk Analysis — A prioritized list of recommendations based on risk severity, probability, cost, and scope, including recommendations addressing policy and procedural gaps.
3. Security Roadmap — A 24–36 month technology roadmap with a strategic direction supporting ARC's security infrastructure goals.
4. Executive Presentation — A presentation of findings and recommendations delivered to the ARC executive team.
5. 30-Day Vulnerability Risk Assessments — Ongoing vulnerability risk assessments for the 30-day assessment period.
6. Two (2) Full DR Drills — Using AWS Elastic Disaster Recovery, with full documentation as outlined in Scope of Work Section 5.
7. Three (3) Tabletop Exercises — Conducted with the Cyber Response Team (CRT) per Scope of Work Section 5.

Estimated Project Duration: The vulnerability assessment and risk assessment activities should be completed within 30 days. Disaster recovery drills and tabletop exercises should be completed by the end of the calendar year.

Exhibit B — Compensation and Method of Payment

Maximum Contract Value: In no event shall total compensation and reimbursements paid to the Consultant under this contract exceed $45,000.00. A budget breakdown must be submitted using the format provided in Exhibit B-1.

Method of Payment

Progress Payments: The Consultant shall submit monthly invoices documenting work performed during the invoice period. ARC will pay or reject properly submitted invoices within 45 days of receipt. ARC may, at its reasonable discretion, disallow any work not properly documented in the required monthly progress report.

Final Payment: Final payment will be made only upon ARC's determination that all contractual requirements have been fulfilled. The Consultant's final invoice and final narrative progress report must be received by ARC no later than fifteen (15) days after the project completion date

specified in the contract. ARC may disallow all or part of a final invoice received after this deadline.

Invoice Submission: Invoices must be submitted by the 10th day of each month and directed to:

Curt Davis | 229 Peachtree St NE, Suite 100, Atlanta, Georgia 30303 | cdavis@atlantaregional.org

Each invoice must include: a description of work completed; percentage of work completed; amount previously billed; a unique invoice number; the performance period; and a valid payment address. Subcontractor payments must be itemized on invoices, including notation of DBE/MBE/WBE status where applicable.

Exhibit B-1 — Proposed Cost Breakdown

Service Area	Proposed Amount
Edge Security	$
Network Security	$
Systems Security	$
Access Management	$
Disaster Recovery	$
TOTAL (Not to Exceed $45,000)	$

Appendix A — Network Resources

The following table summarizes ARC's current network environment. This information is provided to assist vendors in scoping their proposals.

Resource	Quantity	Description / Device
ISP-Managed Router	1	—
Layer 2 Switches	10	Cisco 3850, Meraki MS350, Cisco SG300
VLANs	3	—
Internal IP Addresses	<500	—
External IP Addresses	<20	—
Physical Servers	10	—
VMware Cluster Physical Servers	6	—
Virtual Servers	47	—
SANs	2	—
Domain Controllers	4	—
Access Points	22	Meraki MR Series
End User Devices	240	Windows and macOS
ISP-Managed Firewall	1	Versa Appliance
SIEM	1	Graylog and ManageEngine
EDR	—	Arctic Wolf Aurora
Web Servers (IIS)	3	20–30 bindings
Web Servers (Apache)	3	5-10 bindings
Email	—	Microsoft365 hybrid

Compliance Frameworks

- HIPAA
- ISO 27001
- NIST SP 800-53

Required Forms

The following forms must be completed, signed, and included with the submitted proposal:

- Georgia Security and Immigration Compliance Act Affidavit (Contractor Affidavit)
- Contractor/Vendor Information Form
- Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion — Lower Tier Covered Transactions and Lobbying

Blank copies of each form are attached to this RFP.

PROPOSAL SUBMISSION THROUGH WEBSITE

Electronic Submission Requirements

All proposals must be submitted electronically through the Atlanta Regional Commission (ARC) procurement website. Proposal submitted by any other method (including email, mail, fax, or hand delivery) may not be accepted unless specified in the solicitation document.

Respondents must register and complete the application on the ARC procurement website to access the solicitation and submit a proposal. It is the responsibility of the respondent to ensure successful registration and timely submission.

Proposals must be received no later than **5:00 PM EST, Monday, April 27, 2026**. The procurement system will automatically record the date and submission. Late proposals will not be accepted under any circumstances.

The Respondent(s) is solely responsible for:

- Uploading all required documents;
- Verifying that files are complete, readable, and properly labeled; and
- Ensuring submission is finalized prior to the deadline.
- Only one proposal containing all required information may be uploaded per responder (the system will only submit the latest uploaded).

ARC is not responsible for technical difficulties, internet outages, user errors, or system delays experienced by the respondent. Respondents are strongly encouraged to submit proposals well in advance of the deadline.

Upon successful submission, the system will provide email confirmation. This confirmation serves as proof of receipt.

QUESTIONS AND ANSWERS (Q&A)

Questions Regarding Solicitation

All questions concerning this RFP must be submitted electronically through the procurement website by **5:00 PM EST, Monday, April 6, 2026**. Questions submitted after this deadline or through any other means will not be considered.

To ensure fairness and transparency, respondents are prohibited from contacting ARC staff, board members, or consultants regarding this solicitation outside of the formal Q & A process.

RESPONSE TO QUESTIONS

Official responses to all timely submitted questions will be posted on the procurement website as a written addendum by **5:00 PM EST, Monday, April 13.** Only written responses issued through the website shall be considered official and binding.

It is the responsibility of each respondent to regularly check the procurement website for addenda, clarifications, and updates. Failure to review posted addenda shall not relieve a respondent from compliance with any requirements of the RFP.

RESTRICTION OF COMMUNICATION

From the date of the advertisement of the solicitation through contract award and selection is announced, respondents are not allowed to communicate about this solicitation or scope with any staff of ARC, except for submission of questions as instructed in the RFP or as provided by any existing work agreement(s). In the case of violation of this provision, ARC reserves the right to reject the submittal of the offending respondent.

CONFIDENTIALITY AND CONFLICT OF INTEREST

ARC is subject to the Georgia Open Records law. All proposals submitted will become public records to be provided upon request. Any information containing trade secrets or proprietary information, as defined by state law, must be marked as confidential to prevent disclosure. Confidential markings must be limited to protected information. Entire proposals marked confidential will not be honored. Additionally, conflicts of interest are governed by the ARC Standards of Ethical Conduct available here: Standards of Ethical Conduct. Respondents must disclose any potential conflicts of interest that may arise from the provision of services described herein. Such disclosure should include the name of individual(s) with whom there is a conflict, any relevant facts to the potential conflict, and a description of the internal controls proposed to mitigate any such conflict.

ARC's Staff Legal Counsel will determine whether such disclosure presents a potential organizational conflict of interest that should preclude award to the respondent.

CONTRACTOR/VENDOR INFORMATION

Legal name & address of entity: _____

_____

_____

_____

If different from above-
Legal name of Payee: _____
Payment Address: _____

_____

_____

(If additional addresses are needed, identify each and its purpose on the reverse of this page.)

Legal entity status (please mark all that apply):

☐ **Corporation/C-Corp LLC/S-Corp LLC**

☐ **Partnership/LLC Partnership/LLP**

☐ **Non-Profit: 501(c)(3)/501(c)(4)**

☐ **Individual/Sole-Proprietor/Single Member LLC**

☐ **Government: Federal/State/Local/Authority**

☐ **Other: (describe)**_____

_____

(Federal) Employer Identification Number: _____
OR
Social Security Number (for an individual): _____

Is this contractor/vendor an attorney/law firm? YES☐ NO☐

Is this contractor/vendor debarred, suspended, ineligible or excluded from participation in federally funded projects? YES☐ NO☐

E-verify Status: ☐ **Registered: E-verify Number**_____
☐ **Not Registered**

Is this contractor/vendor a:

Disadvantaged Business Enterprise under 49 CFR Part 26? YES☐ NO☐
Minority or Women Business Enterprise under 49 CFR Part 23? YES☐ NO☐

Attach a copy of current certification(s).

Is this contractor/vendor a Non-federal entity that expends $750,000 or more in a year in Federal awards? YES☐ NO☐
If so, attach a copy of most recent single or program-specific audit conducted in accordance with the provisions of OMB Circular A-133.

Certified true and correct:

Name: _____ **Signature:** _____

Title: _____ **Date:** _____

GEORGIA SECURITY AND IMMIGRATION COMPLIANCE ACT AFFIDAVIT
CONTRACTOR AFFIDAVIT

By executing this affidavit, the undersigned person or entity verifies its compliance with O.C.G.A. §13-10-91, stating affirmatively that the individual, firm or entity which is engaged in the physical performance of services under a contract with the Atlanta Regional Commission has registered with and is participating in a federal work authorization program, in accordance with the applicability provisions and deadlines established in O.C.G.A. 13-10-91.

The undersigned person or entity further agrees that it will continue to use the federal work authorization program throughout the contract period, and it will contract for the physical performance of services in satisfaction of such contract only with subcontractros who present an addidavit to the undersigned with the information required by O.C.G.A. 13-10-91(b).

The undersigned person or entity further agrees to maintain records of such compliance and provide a copy of each such verification to the Atlanta Regional Commission within five (5) business days after any subcontracter is retained ot perform such service.

_____ _____

EEV / E-Verify™ Company Identification Number Date of Authorization

_____

Company Name

_____

Signature of Authorized Officer or Agent

_____

Title of Authorized Officer or Agent

_____

Printed Name of Authorized Officer or Agent

SUBSCRIBED AND SWORN
BEFORE ME ON THIS THE

____ DAY OF _____, 20__

_____ [NOTARY SEAL]

Notary Public

My Commission Expires:

CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS AND LOBBYING

1. DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION- LOWER TIER COVERED TRANSACTIONS

The prospective lower tier participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 45 CFR Part 76, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

The terms "covered transaction", "debarred", "suspended", "ineligible", "lower-tier covered transaction", "participant", "person", "primary covered transaction", "principal", "proposal", and "voluntarily excluded", as used in this clause have the meaning set forth in the Definitions and Coverage sections of rules implementing Executive Order 12549.

The prospective lower tier participant certifies that, by submission of this proposal, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

Where the prospective lower tier participant is unable to certify to any of its statements in this certification, such prospective participant shall attach an explanation to this proposal.

---

2. LOBBYING

As required by **Section 1352, Title 31 of the U.S. Code** (as implemented at 45 CFR Part 93), the applicant certifies that to the best of his or her knowledge and belief that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

Statement for Loan Guarantees and Loan Insurance

The undersigned states, to the best of his or her knowledge and belief, that:

If any funds have been paid or will be paid to any persons for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this commitment providing for the United States to insure or guarantee a loan, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

Submission of this statement is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required statement shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

As the duly authorized representative of the applicant, I hereby certify that the applicant will comply with the above applicable certification(s).

NAME OF APPLICANT	AWARD NUMBER and/or PROJECT NAME
PRINTED NAME OF AUTHORIZED REPRESENTATIVE	TITLE OF AUTHORIZED REPRESENTATIVE
SIGNATURE OF AUTHORIZED REPRESENTATIVE	DATE