ARC Network Security Audit and Vulnerability Assessment RFP

April 5, 2021

Atlanta Regional Commission

Introduction

Atlanta Regional Commission(ARC) Information Technology Group provides technology services to internal Centers\Groups and partner agencies with a focus on providing a secure, protected network infrastructure dedicated to the protection, reliability, and availability of the Agency's data. We are looking for a service provider to help determine the maturity of the Agency's information security program, while providing expert technical insight that will assist us in improving efficiency and security in the future.

Atlanta Regional Commission is soliciting proposals from qualified independent service providers with security assessment experience sufficient to perform a Network Security Audit and Vulnerability Assessment in accordance with the specifications outlined in this document. Deliverables from the assessment must include a findings document to include any non-compliant network vulnerabilities; a risk analysis listing the priority of each risk or vulnerability identified (i.e. high/med/low) and a roadmap document outlining technologies and best practices that the Agency should focus on to improve its security model. ARC is not looking for a SOC's Team to take over security operations.

RFP Submission

All quotes may be submitted via electronic and/or print formats. Please include the original Scope of Work document, a Statement of Work as described below, the pricing breakdown worksheet, and a signed signature page.

ARC must receive updated and new proposals by May 5th, 2021, at 5:00pm. No proposal after the 5th will be accepted.

Email submission: it-rfq@atlantaregional.org (please include "IT Security RFP" in subject line)

Hard copy submission: Atlanta Regional Commission
229 Peachtree St
Suite 100
Atlanta, GA 30303

Proposal evaluation will focus initially on the written proposals. Should it be determined that interviews are required, a "short-list" of firms will be selected from the proposals received. ARC offices are currently closed. Any interview, if necessary, would take place in a virtual environment. ARC reserves the right to award this contract based on initial proposals received without formal interviews. ARC also reserves the right to negotiate the final scope and budget with the selected firm. ARC reserves the right to reject any or all proposals, to request additional information from all proposers, and to waive any informalities during the RFP process. ARC may make such investigations as deemed necessary to ensure that the companies have the requisite experience, skills, and resources to serve the needs of the agency throughout the term of the contract including contacting all listed references. In all cases, the needs and requirements of ARC will be considered first.

Vendor Requirements

The service provider must submit an executive summary, which outlines its proposal, including the proposed general management philosophy. The executive summary should include an identification of the proposed project team, the responsibilities of the project team, and a summary description of the services proposed. The vendor should also provide sample reports similar to the ones to be delivered (see list of deliverables below).

The service provider must submit a Statement of Work and proposed timeline, which describes tasks associated with the services including the vendor and Agency's responsibilities along with the deliverables for each task of the project. Any Agency responsibilities identified should indicate the required skills needed.
The service provider must have Computer Information Security Audit (CISA) certified security experts (or equivalent certifications) with an onsite presence.

The service provider must provide three former customers as references for which similar services were performed (preferably local government). With each reference, please include a 1-2 paragraph summary of the work scope, deliverables and key outcomes.

CONFLICT OF INTEREST AND CONFIDENTIALITY

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 the 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 the 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.

Scope of Work

The vendor will perform a Network Security Audit and Vulnerability Assessment review that will address the following areas of the Agency's infrastructure **(Please note the actions listed below is indicative but not exhaustive list. Vendor may propose additional services to be executed to achieve the stated objectives):**

1. Edge Security
    a. Perform ping sweep and port scan of external IP addresses
    b. Perform vulnerability scan of all external IP addresses
    c. Review ingress and egress firewall policies
    d. Review network address translation rules for publishing internal systems
    e. Verify firewall inspection layer - application layer / stateful inspection
    f. Determine if reverse proxy is in place for inspecting encrypted traffic and pre- authentication
    g. Determine if any unified threat management is configured for the edge security
    h. Review current auditing policies and practice for edge security devices
2. Network Security
    a. Review switch configurations to determine if network segmentation configured between networks
    b. Determine if any internal firewalls are in place between workstations and servers
    c. Determine if encryption is configured to protect internal communications
    d. Review wireless security settings to validate security measures in place
    e. Validate port security and whether or not network ports are active by default and if port security enforces based on MAC address
    f. Determine if any network intrusion detection or prevention systems are providing network scanning
3. Systems Security

a. Perform ping sweep and port scan of internal IP addresses
b. Review all servers and workstations(see appendix) in the environment to determine if the following configurations have been made or security measures are in place
    i. Have any unnecessary services been disabled?
    ii. Is an existing patch management solution in place to ensure the latest operating system security updates are installed?
    iii. Review the auditing policies and procedures in place for each system
    iv. Does each system have an updated Endpoint protection application installedto provide for:
        1. Anti-malware
        2. Host IDS/IPS
    v. Are host based firewalls enforced and centrally managed on each endpoint?
    vi. Is the local Administrators group membership restricted to privileged accounts?
    vii. Are local Administrator and Guest user accounts renamed or disabled?
    viii. File shares
        1. Are default file shares still enabled?
        2. What share permissions are configured

4. Access Management
    a. Review the methods of authentication currently in place
    b. Review domain group membership for high privilege groups
    c. Determine policy for using separate accounts for user level access and privileged access
    d. Review the current password policy enforced on the domain
    e. Perform password auditing for existing user passwords on the domain
    f. Review remote access methods and security

Deliverables

- A findings document Assessment document that details and demonstrates all threats and vulnerabilities that are identified. A risk and severity level will be assigned for threats and vulnerabilities identified.

- A risk analysis listing of recommendations based on risk severity, probability, cost, and scope of work. This should also include recommendations that address policy or procedural vulnerabilities.

- A Security Roadmap that lists the technology recommendations for the next 3-5 years and includes a strategic direction in support of the Agency's security infrastructure.

- Estimated length of project should be no more than 60 days.

Pricing

Pricing MUST include all aspects of the Project. Service providers should provide a summary sheet including approximate hours per task, based on the requirements and terms set forth in the Scope of Work. Pricing must be all-inclusive and cover every aspect of the Project.

Evaluation Criteria

The following are evaluation criteria. While negotiations may be held,vendors are advised to submit their most competitive Cost and Technical Responses.

A.	Technical approach to provide the requested services, including the quality/thoroughness of example reports	35%
B.	Demonstration of expert qualifications and experience to perform requested services	30%
C.	Reasonableness of fee and expenses	25%
D.	References of the firm/organization, letters of support	10%

Appendix

Network Resources

VMWare Cluster physical servers (6), virtual (35), SANS (2)

Domains Controllers (4)

Physical Servers (7)

External IPs (21)

Firewall (1)-Managed by ISP

Routers (1)-Managed by ISP

Layer 2 Switches (10)

Endusers (220)

Email on prem (Exchange)

Office365

IIS and Apache in use

RFP Questions Addendum

- What kind of firewall is being used and the model and how many lines are the firewall policies both external and internal? **Fortinet 200D, 2 lines**
- How many NAT translation rules are there? **17**
- How many edge security devices are there and what model? **1 router 1 firewall**
- How many network switches are there and what model? **11 Cisco 3850(Infrastructure), 4 Meraki MS350(Wireless), 9 Cisco SG300(VO/IP)**
- What kind of wireless controller and access points are there? How many SSIDs are there? **Cloud based controller**, **Meraki MS53 AP, 2 SSID's**
- What kind of Network Intrusion Detection or Prevention Systems are there and how many? **No true IDS, use firewall and Sophos Anti-Virus**
- Would we expect these to be a mix of 220 workstations and/or laptops? **90% laptops**
- Would ARC accept a sample-based assessment of the 220 workstations if they configured consistently through a configuration management tool or domain policies? **Yes**
- Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? If so - can you please provide incumbent contract number, dollar value and period of performance? **No**
- Specify the VLAN details how many is included in the Scope? **2**
- Is there any External Interface need to Pentest? If yes then please specify details? **No**
- Are any vendor products installed for Governance, Risk, and Compliance (GRC) tracking? **No**
- Are any vendor products installed for Security Incident & Event Management (SIEM)? If yes, please provide currently used SIEM product name. **Solarwinds-server is shutdown**
- How many Active Directory Environment domain is included in Penetration testing? **1**
- We may use sampling for configuration review based on number and function of the system (Web server, file server, app server, database, firewall (int/ext), VPN, Load Balancer etc). **Ok**
- Do you want this as a red team exercise to test the SOC/NOC's response where they will get to see the results and update their Knowledge Base (KB) afterward or Blue team where we work with the SOC/NOC and share our attacks so they can update their KB during the testing? **No**
- How many physical locations are included in Pen testing? **1**
- Is "web application" security testing in scope? If yes, please provide number of applications, External facing (internet accessible) or Internal facing? **IIS with 20 to 30 bindings**, **1 internal.** How Many Web Application is in Scope for Pen testing? **All**
- Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities? **We manage**
- The scope seems to focus on both verification as well as vulnerability discovery, as well as a maturity determination around efficiency and security that, in our experience, best requires more than just the technical testing and determinations.

    - We read this to ask for a technical roadmap, but shouldn't it be a strategic roadmap, with maturity elements to be met, that allows ARC to choose the correct technology when you need it? **Will review at time of determination**
    - Can we propose additional steps like interviews and artifact analysis to support this strategic deliverable? **Will review at time of determination**
- What if any framework / certification do you have now (ISO 27001, NIST 800-53, Etc.)?
    - What are the main cyber requirements of the groups/agencies that ARC supports (CMMC, ISO 27k, etc.)? **None**
- What regulations govern ARC or the groups/agencies that ARC supports, relative to cybersecurity? **HIPPA**
- The overall network / user base seems small – seems to be a lot of servers for the # of people.
    - Does ARC host / operate servers or services for any of the groups / agencies which you support? **External groups\agencies-No**
    - If yes, are there requirements that could affect this engagement?
- What are the approximate number of internal IP's? **subnet is 255.255.192.0 or /18**
- In reference to the RFP Scope of Work Section 3.b.i, how are unnecessary services identified/determined? **Internal customer discussion**
- In reference to the RFP Scope of Work Section 3.b.iii, does the auditing review include written policies and procedures? **Yes** Is this an audit of performance / adherence? **both**
- In reference to the RFP Scope of Work Section 3.b.viii, does "File shares" include O365? **No**
- Vendor Requirements, page 3, 2nd paragraph. You request certifications with "an onsite presence" - what do you mean by "an onsite presence"? **Company representative onsite**
- What, in total, of the infrastructure does the ISP manage? **Firewall and Router**
- Is IP-managed infrastructure on-premise or off? **On**
- Will we be granted access to test ISP-managed resources? **No-we can request logs**
- Do you anticipate us performing a firewall rules review? **If ISP provides configuration**
- How many security/auditing policies exist? **We'll request answer form ISP**
- How many wireless access points exist? **22**
- Can all wireless testing be performed from a centralized location? **Yes**