Retirement Systems of Alabama
RFP #19000000008
Security and Penetration Testing Services

1. Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? Yes
2. If so - can you please provide incumbent contract number, dollar value and period of performance? RSA policy is that a written public records request be submitted to the Legal Department for review for compliance with contract language and state law prior to such information being released.
3. Are you satisfied with incumbent performance? We are selecting not to answer this question in an effort to ensure a fair RFP process.
4. Please provide Incumbent support staff (quantity) for each requirement and also provide how many were onsite and offsite? We are asking proposers to independently create a solution for these services; therefore, we feel it is not in RSA's best interest to disclose this information at this time.
5. Please provide Yearly hours of services provided by incumbent? We are asking proposers to independently create a solution for these services; therefore, we feel it is not in RSA's best interest to disclose this information at this time.

6. Does this opportunity contain local preference? If yes, please provide the details. RSA does have the discretion to take location of service providers into consideration; however, there is no statutory requirement for local preference.
7. What is the budget of this opportunity? Is Budget approved? There is not a specific budgeted amount set for these future services at this time.
8. How many sample job description and/or resume, we have to provide? There is not a stated minimum; we ask that you use your discretion in determining what to provide.
9. Can you allow the offeror use the past performances of teaming partners as valid past performance references? Please use your discretion; however, we do ask that such information be fully disclosed.
10. Can you please provide current number of users and infrastructure details? (VMWare, MAN, # of Servers, # of Workstations) RSA will not disclose that information in public documentation. In the event proposer is awarded the contract and the information becomes necessary, we will disclose under confidentiality agreement.
11. Approximately how many live hosts, # of internal and external IPs are in scope for the Network Vulnerability Assessment? Approximately 30 hosts outside. Internal will be scoped by project.
12. Are any cloud providers used? Do you manage your own datacenter, or do you utilize any 3rd-party/colocation facilities? Cloud and/or colocation providers are not used at this time but may be used in the future.

13. Are any vendor products installed for Governance, Risk, and Compliance (GRC) tracking? Vulnerability Management Software is utilized.
14. How often are information security policies updated? When it was updated last time? Security policies are reviewed and updated at minimum yearly, with the last update occurring in May 2019.
15. What is the number of wireless controllers supporting the organization wireless networks? We are unable to disclose this answer publically.
16. Are IoT devices included as "assets" on the network? No
17. Are any vendor products installed for Security Incident & Event Management (SIEM)? If yes, please provide currently used SIEM product name. We are unable to disclose this answer publically.

18. For each application being assessed, which application server or middleware is used? We are unable to disclose this answer publically.
19. How many and what OS and applications, databases etc.? Windows and SQL are used primarily.
20. How many applications are being assessed and, of those, how many are internet facing versus internally hosted? 2 primary applications. Others will be defined by quote.
21. How many applications are in scope for the application security assessment? Two primary applications.
22. Approximately how many web service methods are supported? We support standard asp web service calls.
23. On p 13 for the initial scope and deliverables, it refers to providing a daily report of each ongoing test to the security manager. Is this a written or verbal report? If written, is there a specific format? Is an email update acceptable or are you looking for a true formal report? Email is acceptable, with high risk findings being reported immediately.
24. Under additional service rates, for the application code piece and the data base code piece, we need to know what type of code so they can write these pieces and price them. Majority is .net and C#.
25. Is the Dexter datacenter in the scope of this project? No
26. Are 3rd party connections in scope of this project? Not at this time, may be defined by quote later.
27. Could darkweb analysis be added as a separate service option? Yes
28. The minimum experience for the responsible person has several items listed such as .Net, SQL, and Word Press which are programming specific applications. Must the responsible persons be actual programmers or is extensive knowledge in security application testing sufficient? Security application testing is sufficient, but for code review in future projects a programmer with expertise in security would be preferred.
29. The web-application testing is listed as blackbox, will you be providing the authentication credentials after the initial testing? If so, how many sets of credentials will be tested? Correct. At least two sets of credentials will be tested.
30. Does RSA currently utilize any specific software packages for both application and database code reviews? If so, what are they? If not, is it acceptable to utilize software

for code reviews? Qualys network and web application packages as well as Visual Studio Code Review. Other open source applications as needed.

31. Does RSA hold credit card information? No
32. Does RSA have internal PCI network zones? If so, how many zones? One, however we do not store or process card holder information.
33. What is the current RSA PCI merchant level? RSA does not process card transactions, the web sessions are sent to a clearing house directly. We do not store cardholder information.
34. In section L. Engagement Requirements there is no mention of “Quarterly PCI Scans”, however in section M. there is a list of “additional services…..needed in the future” and “PCI Quarterly Scans” is listed. This would seem to indicate that PCI Quarterly scans are not needed in the current engagement but may be required quarterly, which is confusing as this is a 2 year contract. Can you clarify whether and how frequently PCI Scans will be needed, and if any special PCI qualifications will be required for those conducting PCI scans? This is a 5 year contract. Scans will be conducted as required or based upon change in business process, which may require a quarterly scan.