CATS + TORFP G20B5400007 10/16/2015

Questions and Responses:

1. How many hosts are located on the network(s) to be tested?
   Response: There are a maximum of 14 active devices with Internet-routable IP addresses in the Agency DMZ & 6 at the DR site.

2. What are the types of hosts?
   Response: A mixture of data security devices (e.g., firewalls, anti-malware/spam appliance, switch's) and Windows-based servers (e.g., mail/terminal/web servers.)

3. How many lines of code does each of the two applications have?
   Response: These numbers are more accurate and are different than what was communicated during the Pre-Proposal meeting on Oct. 9, 2015.

   The Employer Payroll Reporting application has approximately 5,000 LOC.

   The Secure Document Reprint application has approximately 1,100 LOC.

4. Is the agency open to sampling methodology for the lines of code which will be reviewed?
   Response: The Agency expects a full source code assessment to be conducted for each application.

5. Does the agency have any reporting or other deadlines which require the work being completed by a specific date?
   Response: None.

6. Has the agency performed this assessment before? If yes, when was the last assessment?
   Response: An assessment similar in scope was performed in the early summer of 2012.

7. How long does the agency anticipate this project lasting?
   Response: The Agency expects this project to last between 10-12 weeks from NTP to final submission of deliverables.

8. Our company is a MDOT Certified MBE/DBE and the solicitation is within our core service areas, however, the Minimum Qualifications are quite restrictive and tends to favor larger companies, which would thereby preclude many MBE / DBE firms like ours from biding this project. Therefore, regarding Section 2.1.1., would consider changing the language, "Only Master Contractor qualifications may be used to demonstrate meeting company minimum qualifications unless otherwise indicated" TO "The Master Contractor shall meet these qualifications or has fostered a relationship with a partner to meet these minimum qualifications unless otherwise indicated?
   Response: SRA has considered this request but it has determined that the minimum qualifications shall remain as originally stated in the TORFP.

9. Regarding Section 2.1.1.A, can our proposed team member whose resume meets each of these requirements be from either the sub-contractor or the master contractor?
   Response: SRA has considered this request but it has determined that the minimum qualifications shall remain as originally stated in the TORFP. Subcontracting is not permitted in this area.

10. Regarding Section 2.1.1.C, can our proposed team member whose resume meets each of these requirements be from either the sub-contractor or the master contractor?
    Response: SRA has considered this request but it has determined that the minimum qualifications shall remain as originally stated in the TORFP. Subcontracting is not permitted in this area.

11. Regarding Section 2.1.1.E, can demonstrated past performance requirement here be demonstrated both the sub-contractor and the prime cumulatively?
    Response: SRA has considered this request but it has determined that the minimum qualifications shall remain as originally stated in the TORFP. Subcontractors may not be used for past performance experience.

12. Please confirm that SRA requires a black-box external network test, that is an assessment from the Internet (with the perspective of an external attacker) with all currently existing layers of defenses in place, and
    confirm that no internal security testing is required.
    Response: Correct, a 'black-box' testing methodology is assumed and no external testing is involved in the PEN testing component of the TORFP.

13. Please confirm that any vulnerability scan will be unauthenticated (non-credentialed).
    Response: Scanning will not involve authentication.

14. How many hosts in each Internet facing computing environment are to be assessed as part of this engagement?
    Response: There are a total of 20 (max) Internet-facing devices to be tested.

15. Will SRA provide the vendor with the IP addresses of the target hosts or a range of IP addresses for discovery purposes?
    Response: The Agency will provide the range [block] of IP addresses to be tested.

16. Are the 2 Web applications to be tested protected by a Web application firewall (WAF)? If so, is it correct to assume that SRA requires the Web application security testing to also be conducted with all existing defenses in place?
    Response: There is no WAF technology protecting the applications under test.

17. Please confirm that the two Web applications are to be tested for common Web application vulnerabilities (i.e. based on OWASP Top 10)?
    Response: Yes, identifying common web vulnerabilities is within the scope of the application security assessment, which includes the functional areas identified in OWASPs list of 'Top-10'.

18. Is static analysis (security code reviews) within the scope of this engagement?
    Response: Yes, the benefits gleaned from a security code review are monumental and is within the scope of this engagement.

    a. If yes, how does SRA plan to provide the vendor with the source code of the 2 Web applications?
       Response: SRA can upload the source code to a secure data repository at the vendor's site or the vendor can conduct the code review on-site at SRA if a verifiable, secured remote data repository is not available for the review.
    b. Does SRA have software licenses for source code analyzers (i.e. Fortify) or is the vendor required to provide the tools and licenses?
       Response: No, the vendor is responsible for supplying the tools/analyzers necessary to conduct the code review.

19. Will SRA provide the vendor with security requirements tractability matrix (if one exists)?
    Response: SRA will not provide a requirements tractability matrix.

20. Have the applications been threat modeled? Has attach surface been analyzed? Is SRA willing to provide the vendor with relevant artifacts?
    Response: For the first two questions: if SRA's internal IT staff embraced the requisite knowledge to provide information at this level, SRA and not a vendor, would be conducting the security assessment. To answer the third question: Yes, SRA will provide documentation related to application design/architecture and any other artifacts it has available to assist in the security analysis.

21. Will SRA share its policies, standards, and procedures regarding "malware protection" with the vendor?
    Response: SRA's baseline data security malware protection standards are derived from the policies and recommendations established by the MD Department of Information Technology (DoIT - http://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf) in combination with guidance from the National Institute of Standards and Technology [i.e., NIST Special Publication 800-83] and the data security industry's "due care" practices regarding malware protection.

22. Can you please clarify the requirements on page 3; item C, Question number 3 concerning the requirement for Employment References for our Full Time employees? We are unsure of what information to put here as our employees have been with the company for a minimum of 5 years.
    Response: The language in question is State-provided language in the TORFP template. We believe that it accommodates that Offerors on proposal opportunities may at times submit resumes of individuals who do not work for, not have ever worked for, the Offeror. The intent is to provide some means of verifying the background credentials and experience of the individuals. For the current TORFP, if the proposed personnel is currently an employee of the Offeror or its subcontractor for at least 1 years' duration, employment references will not be required.

23. Can the pen testing and security assessment work be performed in the evenings? Are there are a core set of hours that must be met?
Response: PEN testing cannot be conducted during regular business hours (M-F 8am to 5 pm). Testing can be performed anytime outside of this window with exception of the night of the Agency's generation of monthly benefits checks/payments (on or around the 15th).

24. Can the work be performed off site?
Response: It is assumed that the PEN testing & the application security assessment will be performed off-site via the Internet.

25. How long do you anticipate each stage to take to complete?
Response: The Agency expects this project to last between 10-12 weeks from NTP to final submission of deliverables.

26. The second stage/group 2 deliverable does not reference a "thorough security assessment" as outlined in the scope of work. Where does this work fall from a deliverable perspective?
Response: This work would fall under deliverable 3.8.4.5 - Analysis, Conclusions, and Recommendations from the Secure Internet Application Test.

27. Can this contract be performed on a time and material basis, similar to how we perform these services for DC Government?
Response: No. The contract is fixed-price.

28. Do you anticipate having additional cyber requests that must be met in conjunction or in addition to what's laid out in the SOW?
Response: No.

29. How many IP addresses are on the DMZ and Disaster Recovery networks to be pen-tested?
Response: The subnet mask for each network is 255.255.255.240, therefore, there are 16 potential IP addresses available within each respective network (32 IP's total).

30. Of these addresses, how many are live (have a running host/device assigned to it)?
Response: Refer to Q1. Each active device (20 max) is assigned an IP address.

31. If there are web application in the DMZ and Disaster Recovery, is a detailed penetration test of these web applications to be undertaken?
Response: The web applications are hosted on SRA's public web server, and therefore, will be "live" and testable during the penetration test.

32. Do the two web applications specified in section 3.3.B reside in one of the two networks to be pen-tested?
Response: Yes, both of the applications are hosted in SRA's DMZ.

33. If so, are they in scope for the pen-test?
Response: This appears to be the same as Q31.

34. For any web application that is to be tested, please specify the number of dynamic pages (pages that take input from the user, or display input based on data coming from either the user or a database) and how many roles (e.g. regular user, administrator) the applications have. Detailed information is preferred, but rough estimates are acceptable if no detailed data is available.
    Response: The Employer Payroll Reporting application has approximately 5,000 LOC and does include authorization security roles.
    The Secure Document Reprint application has approximately 1,100 LOC and does not utilize security roles.

35. Do these applications have any special functions or requirements that might add additional complexity? Examples of these functions are file upload, payment, any special data processing and application development environments.
    Response: The applications are designed to perform data upload and data reporting functions.

36. Are the two web applications listed in section 3.6.1.2 to be tested live (either in a production or testing environment), or to be assessed only by performing a source code audit?
    Response: The web applications will be tested in 'production mode' and not in a test environment.

37. If they are to be tested in a live environment, please detail the application's parameters as requested in questions 34 and 35.
    Response: Refer to responses given in Q's 34 & 35.

38. Are the tests to be conducted over the Internet, or is it necessary to conduct them in person at a MRSA facility?
    Response: All testing to be conducted from the Internet with the exception of the application code review which must be done locally (at the vendor or SRA site).

39. Regarding the first stage of the project (PEN Test), how many servers are included in each location?
    Response: A black-box testing methodology is assumed for the PEN test. Out of the 20 devices being tested, approximately 50% are servers.

40. Regarding the second stage of the project (Application Test), what is the size of the two applications (i.e., number of pages, etc.)?
    Response: Duplicate of Q34.

41. On page 36, at the top of page it states: "5) Draft Risk Assessment: Identification and prioritization of risks inherent in meeting the requirements in Section 3 - Scope of Work. Includes a description of strategies to mitigate risks. If the Risk Assessment appears as a deliverable in Section 3 - Scope of Work, that version will be a final version. Any subsequent versions should be approved through a formal configuration or change management process." What do they mean? Is this our plan to mitigate risk to the project or is it something else?
    Response: Please see the transcript of the Pre-Proposal Conference on Oct 9, 2015.