TORFP G20B9400004 - External Network, Internal Wireless Network, and Application Security Testing

Questions and Answers

1. For the penetration test requirement in section 2.1.2.1, do any of the IP addresses host web applications in addition to the agency's public website? If so, is authenticated testing required or black box only?
   Yes. Web application security assessment should include authenticated testing.

2. For the penetration test requirement in section 2.1.2.1 and the application testing in section 2.1.2.2, is a retest of the findings desired once you have had an opportunity to remediate the findings in the original test?
   Not a requirement.

3. For the application assessment requirement in section 2.1.2.2, is a source code review desired in addition to the dynamic application scanning/testing? If so, what language(s) and how many lines of code are to be reviewed for each application?
   A static code review is expected. All apps developed on the Microsoft platform (.NET); C#.NET, VB.NET, Angular with Typescript. Employer Payroll: approximately 5,150 lines, Secure Reprints: approximately 1,100 lines, File Upload: approximately 1,300 lines.

4. For the application assessment requirement in section 2.1.2.2, can testing be performed remotely or will testers need to be on-site?
   Remote testing only for web application testing.

5. For the applications that require credentialed scanning as set forth in 2.1.2.2, how many user roles should be included in testing?
   1-3 roles.

6. For the wireless testing requirement in 2.1.2.3, does each of the 8 VLANs have its own wireless SSID? If not, how many SSIDs are to be included in the assessment?
   2 SSID's.

7. For the wireless testing requirement in 2.1.2.3, is a wireless site survey and rogue access point detection desired? If so, please list the physical address of the facility to be assessed, the approximate size or square footage, and the business use (i.e. data center, offices, etc).
   A wireless site survey is desired which should include rogue AP detection. WiFi spans 4 floors in the 120 E. Baltimore St. Suntrust Building.

8. Will all details on sites and testing/targets at the beginning of the test? Not during the course of the test?
   Details relevant to the testing will be discussed prior to the testing timeframe.

9. Will the Contractor be notified / be able to ask questions about infrastructure details?
   Yes.

10. Is this a clear box test?
    Not entirely. The RFP was crafted with the intention of providing some level of detail of the network UT, but not to the level a white box test demands.

11. For the 3 web applications described on 2.1.2.2 (page2), there is a mention of 4 unique URLs. How do these 4 URLs map to the 3 web applications?
The 4th URL is the SRA public website.

12. Will the web application testing be done on non-production systems as well as production systems? Testing on non-production systems allows for more in-depth testing as we can inject more data into the system.
All testing will be performed on production systems.

13. How many and what levels of access will be tested for each of the 3 web applications described on 2.1.2.2 (page2)?
The web apps vary in design complexity (1 w/a single page (SPA), the other 2 having between 2-4 pages. That stated, authentication credentials will be provided to assess security from 1 up to 4 levels deep into the web apps.

14. How many IP addresses are on the internal WLAN/Wifi across the 8 VLANS as described in section 2.1.2.3 (page 2)?
1024 max IP addresses available on the Wireless (WiFi) network.

15. Are all IPs on the WLAN accessible from the Baltimore MD site?
Yes.

16. In 2.3.4 (Application Testing) a code review is mentioned. Will Contractor have access to all backend code for all of the web applications?
Yes.

17. Is static analysis and code review the intention of this requirement?
A static code review is a minimum requirement.

18. Referring to section 2.1.2.1, are any of the penetration targets hosted in the cloud and if so with which cloud provider?
No cloud hosting used.

19. Referring to section 2.1.2.1, What is the security classification of the penetration testing targets?
“Moderate’ as defined in the TORFP (sections 2.1.2.2, 2.4.4.3/.5)

20. Referring to section 2.1.2.1 and 2.1.2.2, How many subnets are in scope?
PEN/Application – 3, WiFi (section 2.1.2.3) – 8.
(Verified - 3 subnets (Balt. DMZ, DR & Public Website for sections 2.1.2.1 & 2.1.2.2).

21. Referring to section 2.1.2.1, During penetration testing, are there specific things that are not allowed such as denial of service, fully exploring vulnerabilities, data exfiltration, etc.?
As defined in the TORFP, testing is to be “non-intrusive” and not impact production business processes.

22. Referring to section 2.3.1, What risk scoring mechanism (CVSS, NIST 800-30, etc.) should we apply for vulnerabilities that are discovered?
CVSS or NIST, CVSS preferred

23. Are we giving the remediation/mitigation to fix the findings?
Yes (see sections 2.4.4.3/2.4.4.5 – "and recommendations to remediate risk….").
If so, will that result in another contract vehicle being awarded to do the remediation/mitigation? No

24. Do they need us to do a SAR/RAR and show how the findings categorized as "critical" or "high" can be compromised?
Not required

25. Does an incumbent exist on this RFQ? If yes, could you please provide the incumbent details? Is Incumbent allowed to bid on this TORFP?
This is a new solicitation, no incumbent.

26. What is the estimated annual budget of the contract?
Not available

27. What is the expected start date for the contract?
April, 2019 or sooner

28. Please specify the working place.
Read the RFP, please.

29. Is it required that the Certificate of Insurance submitted with the proposal or after reward? You must submit what Insurance you have and if you are awarded the Contract, you must submit what is requested in the RFP.

30. Who were the previous similar three (3) PEN TESTING contracts awarded to and for what contract value?
a. G20B9200020 - Hewlett Packard Co. (2012) $59,208.00
b. G20B5400007 – Janus Software, Inc. (2016) $39,985.00
c. G20B8400006 – This was cancelled in 2018 and re-bid as G20B9400004

31. Section 3.9.2, point A (page number 21 of the TORFP) – TO Contractor shall have successfully completed at least 2 PEN tests within the last 3 years.
Question – Does this mean that the Prime Contractor needs to have this experience or does this requirement extend to the entire team that the prime puts together?
Section 1 – Minimum Qualifications (pg. 1): "At least one team member (the individual performing the work) shall have experience in conducting web application security risk assessments, with at least two (2) application security risk assessments performed within the past three (3) years."

32. Will the Companies that have already executed similar projects for SRA in the past be allowed to bid on this TORFP?
Yes, this is a new solicitation, no incumbent.

TORFP G20B9400004 – Additional Questions and Answers (cont.) 01.24.19

1. **Page 2, Section 2.1.2.1. Are the 16 IP addresses each unique to an individual infrastructure component supporting the applications? Or are the 16 addresses just potentially shared external addresses exposed to the internet?**
   Addresses are unique.

2. **Page 2, Section 2.1.2.2. Are the applications hosted solely within the DMZ, i.e., do all of the components of the application and all of the supporting infrastructure reside within the DMZ?**
   In the DMZ.

3. **Page 2, Section 2.1.2.3. Is the reference to *access points* intended to include both 1) examination of the configuration of the legitimate access points and 2) *war-walking* to identify potential inappropriately added access points? If the Agency's intent includes *war-walking*, does this include *war-walking* of the Agency's data center?**
   War-walking is considered in scope and would typically be included in a security practitioners' WLAN assessment.

4. **Page 2, Section 2.1.2.3. The paragraph states "…encompassing areas such as…" in introducing a list of topics to be addressed in the WLAN assessment activity – does the Agency have particular additional areas in mind in addition to the specified list? Is the Agency looking to bidders to suggest other topics for inclusion in the WLAN assessment?**
   The wording is such that it grants the vendor the liberty to bring their expertise "to the table" to illustrate their own unique approach in assessing the Agency's WLAN.

5. **Page 2, Section 2.1.2.3. Is there a need for inspection of WLAN components in the remote disaster recovery location? If so, would that include *war-walking* of the remote disaster recovery location?**
   No, the RFP specifically states that the WLAN assessment is restricted to the Baltimore, MD headquarters site.

6. **Page 2, Section 2.1.2.3. Section 2.2 references a "small remote office in Annapolis" – does this office also have a WLAN? If so, is this WLAN covered by the testing at the Baltimore HQ office? Or does the Annapolis office location require a separate WLAN assessment? Would Annapolis office require a *war-walking* exercise of its own?**
   Refer to response in Question #5.

7. **Page 2, Section 2.1.2.3. Does either location include a wired LAN running in parallel to, or instead of a WLAN?**
   Yes, Baltimore office hosts the WLAN, which includes a wired LAN.

8. **Page 2, Section 2.1.3. Does the Agency have an intended target timeframe/window for start of the assessment?**

   April 2019

9. **Pages 3-4, Section 2.3.1. In the discussion of external PEN testing the Section introduces a list of testing goals with the phrase "shall include at a minimum" – does the Agency have particular additional goals in mind in addition to the specified list? Is the Agency looking to bidders to suggest other goals for inclusion in the PEN testing?**

   Refer to response in Question #4.

10. **Page 4, Section 2.3.2 Application Testing, Bullet A. How many lines of code will need to be code reviewed?**

    Answered in a previous question asked by another vendor in prior Q&A document.

11. **Page 4, Section 2.3.2. In the discussion of application-level security assessment, the Section introduces a list of target functional areas with the phrase "shall include, at a minimum, the following functional areas" Does the Agency have particular additional functional areas in mind in addition to the specified list? Is the Agency looking to bidders to suggest other additional functional areas for inclusion in the assessment?**

    This question is similar to one asked during the pre-proposal bid conference. The Agency includes a baseline of parameters to examine. The vendor is expected (as the experts in this discipline) to include other areas in addition to those listed.

12. **Page 6, Section 2.4.2, Deliverable Acceptance, Bullet C. In what period of time must the TO Manager issue to the TO Contractor the notice of acceptance so that invoicing may be performed?**

    Five business days.

13. **How many pages are in each of the targeted web applications that need to be assessed?**

    Most of the applications are SPA (single page applications).

14. **Page 10, Section 2.5, Optional Work. Are you expecting us to attempt to price anything in this Optional Future Work item?**

    Not at this time.

15. **Section 1.1 - For A, we understand that one team member must possess either a CISSP or a CEH certification. For B and C, can this experience be met be a team member other than the certified individual listed in A?**

    Yes

16. Section 2.1.2.3 - How many endpoints and users comprise the 8 VLANs, 8 Aps, and 1 Controller?
    Varies on any given day. A rough estimate is in the 10-25 range. The WiFi is basically a complementary service and not a primary communications resource for day-to-day essential business functions (with the monthly Board of Trustee's (BOT) meeting being one exception).

17. Section 2.2 - How are the identified 210~ users spread between the main building in Baltimore and the DR site?
    All 210 located in Baltimore. DR is as it's defined, only used in a disaster scenario.

18. Section 2.3.1 - Do user's mobile devices count as "in scope" for the Wireless Penetration testing?
    No. Testing is localized to the WiFi infrastructure itself and not the endpoints.

19. Section 3.5.1.D/E - Is the SRA asking the vendor to perform DR testing as a project task? The only reference to Disaster Recovery is related to the PEN testing at the disaster recovery location in Annapolis, MD.
    No requirement for DR testing. Only assess the internet-facing 1)devices located at the DR site.

20. Will the State provide licenses for the tools to be used for the code review and/or scanning, or should vendors include the cost of those licenses in our price proposal?
    SRA relies on the vendor to provide all the tools/software licenses needed to perform the code review.

21. Does SRA have a preference for the tools that they would like to have used for the code review and/or scanning, or does SRA want the vendor to recommend tools?
    SRA has seen a number of code review tools used in the past and they are all different. SRA will leave it up to the vendor to take the lead and map out how they will perform this task within the TORFP.