TORFP G20B9400007 - External Network, Internal Wireless Network, and Application Security Testing
Questions and Answers

1. Is it required to have the onsite personnel to perform pen testing or can it be done from an offsite location?
   Only WiFi testing requires personnel onsite.

2. Can the work be done during off hours from an offsite location?
   Yes.

3. What level of clearance is required for the personnel?
   As defined in the TORFP, personnel must pass a security background check (Refer to section "3.7.2 Security Clearance / Criminal Background Checks").

4. For the following referenced procurement, G20B9400007 - External Network, Internal Wireless Network, and Application Security Testing, will the State allow the experience of a named, sub-contractor (on the proposed team) to be substituted for Master Contractor experience?

   Additional Comment: To be a PRIME CONTRACTOR, the Subcontractor must be a Master Contractor in the CATS Plus Contract. Also See Section 6.2 - Evaluation Criteria and -

   The Master Contractor must fulfill the TORFP experience requirements:
   3.9.2 Offeror Experience (pg. 21)
   The following experience is expected and will be evaluated as part of the TO Technical Proposal (see the Offeror experience, capability and references evaluation factor from **Section 6.2**):
   A. TO Contractor shall have successfully completed at least two (2) PEN tests within the last three (3) years.
   B. **The Master Contractor must demonstrate in its TO Proposal that it has previously performed PEN testing and security vulnerability assessments on all of:**
      1) Internet-facing systems,
      2) Network perimeter security devices and equipment, as described in this TORFP,
      3) Internal WLAN devices, including wireless access points, and
      4) Hardware devices to include all of (but not limited to) firewalls, routers, Windows-based servers, and comparable network infrastructure devices.

5. Pen test in 2.1.2.1 and application test in 2.1.2.2: Are all systems hosted in the two Internet facing compartments?
   Yes, PEN: Baltimore & DR / App testing: Baltimore Only

6. Wireless testing in 2.1.2.3: How many SSIDs are included in the testing and how many IP addresses across the 8VLANs?
   2 SSID's & 8 x (x.x.x.x/16) networks.

7. Application assessment in 2.1.2.2: Three applications are listed but 4 URLs are referenced, what is the purpose of the fourth URL?
   The public website URL.

8. For the three applications in 2.1.2.2, please provide a description of their complexity.
   Low/Moderate complexity – mostly are SPA (single-page application) designs.

9. Applications in 2.1.2.2: Which applications/URLs require credentialed scanning?
   2 (File Upload & Employer Payroll Reporting).

10. For the applications requiring credentialed scanning, how many user roles should be included in the testing?
    1-2 roles.

11. Pen test in section 2.1.2.1 and application testing in 2.1.2.2: Can testing be performed remotely or will testers be required to be on-site?
    Remotely

12. Application assessments in section 2.1.2.2 with code review: What language(s) and how many lines of code are to be reviewed for each application?
    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.

13. Background check in 3.7.2: Can an active SECRET or Top-Secret clearance be substituted in place of the criminal background check?
    Yes.

14. Will any testing be done in a non-production environment?
    No

15. Section 2.1.2.1 – Will the PEN test be conducted on the external network on a total of 20 IP addresses?
    Yes

16. Section 2.1.2.2 – Application PEN Test will be conducted on 3 applications with 4 different URLs. Will all the applications have a code review performed?
    Yes

17. Are all the applications on .NET framework?
    Yes

18. Section 2.1.2.3 – Are there only 8 different SSIDs?
    2 SSID's, 8 VLAN's

19. How many different physical locations will need to be considered for performing a wireless PEN Test?
    1 physical location

20. Section 4.5 Oral Presentation – Can this be done remotely via video conferencing or is physical presence mandatory?
    Remote conference can be arranged.

21. How many web applications are being assessed?
    3, +1 public website

22. How many login systems are being assessed?
    2

23. How many static pages are being assessed? (approximate)
    3-5.

24. How many dynamic pages are being assessed? (approximate)
    2-3

25. Will the source code be made readily available?
    Yes

26. Will there be any kind of documentation provided?
    No

27. Does the client want fuzzing performed against this application?
    If available

28. Does the client want role-based testing performed against this application?
    Yes

29. Does the client want credentialed scans of web applications performed?
    Yes

30. What programming languages are being used?
    .NET

31. What CI systems are in use?
    TFS coupled with manual processes

32. What development methodologies are in place?
    Agile

33. How many scrum teams are there? (if using Agile)
    1

34. How frequently are releases performed?
    <2 per year

35. Will we be involved on every release to evaluate risk of changes prior to implementation?
    No

36. What code repositories are in use?
    TFS

37. What targets are in play? (x86, x64, ARM, Motorola, Other, etc.)
    x86