TORFP G20B8400006 – External Network, Internal Wireless Network, and Application Security Testing

Questions and Answers:

1. What are compliance requirements for the scope of work stated in RFP - is it HIPAA, PCI-DSS, FISMA, etc?

   There are no specific compliance requirements for the Agency related to the TORFP, other than a policy-level requirement to periodically conduct this testing. The Agency generally operates within the State of Maryland IT Security policies, which are found on the web site for the Department of Information Technology (DoIT).

2. Are the contractor services required throughout the contract period or only for specific duration of times per contract year?

   The TORFP spells out the timing requirements for given defined deliverables. The Agency anticipates a gap of time between completion of the initial scope of work and commencement of any subsequent optional Work Order, for testing the fourth application referenced in the TORFP (see the transcript of the pre-proposal conference for more information).

3. Can the services be provided from contractor facility or it has to be onsite?

   The Agency expects that external penetration testing of the primary networks would be conducted from externally, that is, off-site (whether from the contractor's facility or another off-site location). Testing of the Agency's wireless network will have to be conducted from within the network (preferably from onsite rather than through a secure remote connection). Briefings and presentations are expected to be delivered on-site. Otherwise, scoped work (results compilation, production of deliverable reports, etc.) can be physically conducted remotely.

4. Is there a security policy document that you can share?

   The State's IT Security Policy is found on the DoIT web site. Agency-specific IT security policies do not impact the TORFP's scope of work beyond State-level policies.

5. Are there any current incumbents and if so when did the government exercise all options? When is the contract expiring?

   There are no current active incumbents. Prior testing contracts have all expired.

6. In general what is the FISMA level of the MSRS systems - HIGH, MODERATE or LOW?

   This Agency's operation is considered a MODERATE risk environment per NIST guidelines.

7. Are there any external audit findings for the systems in scope stated in the TORFP?

   No.

8. What is the size of the Penetration Testing project?

   The Agency believes it is incumbent on the bidder to tell us this information, based on information provided in the TORFP, responses to questions posed at the pre-proposal conference and/or submitted before the question submission deadline, and the bidder's professional judgment.

9. How may VLANS/Subnets/Devices/Access Gateways/Endpoints will need to be tested on fixed network and wireless network?"

   Network: approximately 20 endpoint (2 subnets – Baltimore & DR Site)
   Wireless: 8AP's (access points) & 8 VLAN's

10. 2 External facing systems – How many servers and URLs?

    Approximately 20 endpoints. 4 URL's (this includes the public webserver).

11. Was any penetration testing/assessment performed before? If so, when was the last penetration testing completed?

    Several times. The last such test was completed in late 2015.

12. Should the penetration testing for external facing systems be conducted with or without credentials?

    More thorough testing of the web applications is possible using an authenticated account. One will be provided.

13. Would we be permitted to do a credential scan?

    Yes

14. Has your organization ever been compromised (internally or externally)?

    Not that we are aware of.

15. What service(s) does SRA expose to the internet? (Examples: Web, Database, FTP, SSH, etc.)

    Standard Internet-hosted business services Web (HTTP/HTTPS), SQL, FTP, SSH, SMTP, etc.

16. What service(s) does SRA expose to the DMZ?

    Same as those listed in Question 15

17. What type of authentication does SRA use for web services? (Examples: PubCookie, Windows Integrated, htaccess, etc.)

    Windows authentications (LDAP) & SQL authentication.

18. What platform does SRA use for web services? (Examples: PHP, Perl, Ruby, ASP .NET, etc.)

    All built on the Microsoft .NET platform

19. Does your organization desire penetration testing without knowledge ("black box") or with knowledge ("white box")?

    IT will be a blend of both worlds. We will provide limited scoping to include the Internet-facing IP addresses and the URL's.

20. Are there any physical locations that are expected to be included in the scope of work for security review?

    See the TORFP

21. How many stakeholders (e.g., department heads, subject-matter experts) are to be interviewed as part of this assessment?

    None. This is not an assessment. It is testing, and the only interviews per se are conversations with Agency IT staff to enable work to progress.

22. File Upload application - how many servers and instances of this application are currently running in production and DR?

    1 server/1 instance. None at the DR site.

23. Employer Payroll Reporting application – how many servers and instances of this application are currently running in production and DR?

    1 server/1 instance. None at the DR site.

24. Secure Document Reprint feature how many servers and instances of this application are currently running in production and DR?

    1 server/1 instance. None at the DR site.

25. Has any system security assessment (of the targeted systems, as specified in the solicitation) been completed before? If yes, what is their system categorization (High, Moderate or Low)? If no, is there any System Security Plan, Organization Policies, Disaster recovery documentation, Privacy Impact Analysis (PIA)?

    The Agency is categorized as a MODERATE risk environment per NIST standards. That applies to all Agency applications and technology. The Agency has a DR plan and other documentation; however, the Agency does not believe these are relevant to the Scope of Work of this TORFP.

26. How many of the following types of servers are currently part of SRA's infrastructure:

    a. Microsoft Server (2008/2012/2016) including Microsoft terminal services/remote desktop,
    b. Microsoft SQL Server (2008/2012/2014),
    c. Microsoft Internet Information Server (IIS),
    d. Routers and switches,
    e. Wireless access points, and
    f. UNIX-OS based firewalls.

    Numbers will not be provided for these. This is a copy and paste from the TORFP.

27. Are there any mobile devices?

    Yes. This TORFP does not involve testing any of them. Applications are not specific to mobile devices.

28. **Policy & Procedure Review:** please describe the objectives and requirements of this component.

    The Agency does not understand this question relative to the Scope of Work of this TORFP. This is not an assessment or security review; rather, it is technical testing of several specific technical components.

29. **Organizational Assessment:** please describe the objectives and requirements of this component.
    (Same as 28 above)

30. Can the entire network be accessed and assessed from one centrally managed physical location?
    Yes.

31. Are any code reviews part of the scope of work?
    Yes.

32. If the vendor is an MBE, can they be considered to cover 15% (or a lesser portion) of the required 30% MBE participation goal?
    If the Vendor is an MBE, they can only account for 50% of the MBE Goal. This TORFP has a 30% MBE Goal, so the Vendor can cover 15%.

33. Clarification needed: According to **Paragraph 5.3.5 (A)**, it appears that the respondents of this solicitation must include, at a minimum, 2 copies of the "TO Technical Proposal" consisting of (i) Microsoft Word format, version 2007 or greater; and (b) in searchable Adobe PDF format. In addition, an "optional" third redacted copy is also needed (to be submitted) with confidential and/or proprietary information removed, if and where applicable. Please confirm.
    Only one copy is emailed in a Word document; a Searchable Adobe PDF format and an "**optional**" Redacted Version with confidential and/or proprietary info removed. If your file is too large, that is when we ask that you send the information in two emails as directed on page 31 of RFP.

34. Same question (as above) for the "TO Financial Proposal".
    Only a Word document is to be emailed for the Financial. This document is already established as a confidential item. If the Financial Proposal was more than one page in length, that is when you would need to send a searchable Adobe PDF format copy. The Financial Proposal for this TORFP is only on one page.

35. In **Paragraph 2.1.2.3**, does "internal Wireless Local Area Network (WLAN/WiFi) infrastructure" refer to a WiFi or network infrastructure or both?
    Strictly the WiFi network

36. In Section 2.3.1 under penetration testing, there is mention of routers, switches and firewalls. Are these part of the applications or the infrastructure system?
    These devices are more relevant to the PEN testing (DMZ/external network) and not the web application assessment phase of the TORFP.

37. In Table 2: TORFP ATTACHMENTS AND APPENDICES (on pg.38), for attachment B, it states to submit "Before TO Proposal." Is that correct? Shouldn't it be submitted along with the TO Proposal?
    Please submit the TO Financial Proposal "**With** the TO Proposal"

38. Section 2.1.2.1

- How large are the environments to be tested in terms of public facing IP addresses?

  Approximately 20 IP addresses

- Will all testing be inbound from the Internet only, or is internal testing of the environments required?

  Inbound Only

- If internal testing is required, how large are the environments in terms of IP addresses?

  N/A

- Is evasive testing (designed to avoid detection) required, or will the blue team be fully informed and involved?

  Evasive Testing is not a requirement.

39. Section 2.1.2.2

- Should the Web applications be tested as an authenticated user?

  Yes

- If so, how many different user roles should be tested?

  1-2 Roles

- Does SRA have a dev environment to allow for testing of the web applications, or will they be tested live?

  Tested live

- Do any of the applications incorporate SSO technology?

  No SSO

40. Section 2.1.2.3

- Is configuration review of the wireless platform available?

  Yes

- Should policy review be performed to determine incident response capabilities? If so, how many individuals are on the security team?

  IR policy review is not a requirement.

- What brand is the wireless platform, and are the access points centrally controlled?

  The specific brand will not be disclosed at this time. (it is a mainstream brand). AP's are centrally managed.

- How many wireless controllers exist in the network?

  1 controller and 8 AP's.

41. Section 2.1.3

- What is the NTP date?

  The expectation is 2-3 months after proposal submission deadline (August 15th).

42. Section 2.3.1

- Will up to date and accurate network diagrams be provided to allow for architecture review?

  Yes

- Are both sites identically configured or will a separate review be required?

  The DR Site is not a hardware/software mirror-image of the production environment and small-in-scale. It will require a separate review.

- How many network devices are in the architecture, and what makes and models?

  Refer to Question No 38 (Section 2.1.2.1). Make/models not disclosed at this time.

- Is review of firewall rules required? If so, what make and model are the firewalls in each location?

  No firewall rules review needed. No make/model will be disclosed.

43. Section 2.3.2.A

- What language are the applications written in?

  All apps developed on the Microsoft platform (.NET); C#.NET, VB.NET, Angular with Typescript.

- Approximately how many lines of code are in each application?

  Employer Payroll: approximately 5,150 lines, Secure Reprints: approximately 1,100 lines, File Upload: approximately 1,300 lines.

- What is the repository for the applications?

  Microsoft Team Foundation Server 2018.

- Is a single scan of the codebase all that is required or is SRA interested in more continuous scanning?

  SRA is interested in the most thorough code review possible and will rate the proposals with that expectation in mind. If the Offeror offers differing levels of service, then the Agency wishes the Offeror to decide on a baseline level of service appropriate to the Scope of Work in the TORFP, include that level of service in the proposal response, and separately describe any further enhanced levels of service available in the Technical Proposal (only).

44. Section 2.3.2.G

- What logging analysis is required?

  To determine that logging is properly tuned/configured to capture network attack attempts and malware infiltration.

- How are the systems logging? To what system?

  Logs are ported to a SIEM via Syslog and local server agents.

45. Does each county have one physical location where the Risk Assessment will take place?

  The Agency does not understand the reference to "county" in the question.

46. Does each county have its own network?

  The Agency does not understand the reference to "county" in the question.

47. How many total IP's are in scope per location? (Internal and External).

  Internal: 8 External: approx. 20.

48. How many systems per county are in scope?
    The Agency does not understand the reference to "county" in the question.

49. What is the anticipated start date?
    2 months after TORFP submission deadline (8/15/18).

50. When will the previous Risk Assessments be provided to the winning organization?
    Previous Risk Assessments will not be provided.

51. Is there a current inventory of assets?
    Will not be made available.

52. Is there a current hardware and software inventory for each county? Will it be shared with winner?
    The Agency does not understand the reference to "county" in the question. Inventories will not be shared.

53. Is the pricing to be inclusive of all three years or priced per year?
    Please read the Financial Proposal Sheet (Attachment B). All pricing is inclusive for First Stage and for Second Stage items.

54. What is the anticipated start date for year 2 and year 3 of the agreement?
    See the TORFP.

55. What applications are in scope?
    Answered in the TORFP.

56. Are those applications off the shelf or homegrown?
    Answered in the TORFP.

57. What is the allocated budget for this engagement?
    Will not be made available.

58. Is there any leeway for the expected turnaround?
    No.

59. What is the total number of IP's in scope on the two (2) Internet-facing computing environments mentioned in the TORFP?
    Already answered.

60. What is the total number of locations that are in scope for the WLAN assessment and pen test identified in the TORFP?
    1 WiFi, 2 PEN test.

61. Has this type of assessment been completed in the past?

    Yes, multiple times.

62. If so, will the results be made available to the winning vendor prior to the engagement?

    No.

63. What % of the work will be complete onsite for security/vulnerability assessment of the Agency's internal Wireless Local Area Network (WLAN/WiFi) infrastructure?

    The WiFi assessment is small in scope compared to the web application assessment/PEN test. Estimated to be 15-20%.

64. Section 2.3.2 – Application Testing
    Application penetration testing is usually performed on a replica of the Production instance.
    - Does MSRA require the application penetration testing to be performed on the Production instance or a QA or Pre-Prod instance that mirrors the Production instance?
      Testing will be performed on production instances of the applications.
    - Does MSRA require application penetration testing on non-Production instances?
      No non-production testing will be performed.

65. Section 2.1.2.1 - Are these applications listed as part of 2.1.2.1 or these are over and above the 3 apps listed in 2.1.2.2?

    They are the same, not over and above.

66. Section 2.1.2.2 - Are we expected to use credentialed assessment? If so, how many such user roles are expected as part of the testing in each application?

    (See #39): More thorough testing of the web applications is possible using an authenticated account. One will be provided. 1-2 Roles

67. Section 2.1.2.3 - How many SSIDs are in Scope? Number of Access points and area of the real estate to be covered as part of the assessment?

    Wireless: 8AP's (access points), 4 floors at 120 E. Baltimore St.

68. Section 2.1.2.3 – Is there a need to review the Access Controller configuration?

    Yes

69. Section 2.3.1 – External PEN Testing - Is the DoS attacks expected to be performed at network layer or at the application / OS layer?

    Network layer.

70. Section 2.3.2 – Point A - To quantify the security code review efforts, can the agency share the lines of code in each application?

    Already answered, see #43.

71. Section 2.3.2 – Point A - To perform code review, will the Agency share code to be run from our systems?

    The Agency will share the Visual Studio project solution files containing the application code and database scripts (schema, stored procedures, etc.) for each.

72. Section 3.9.1 – Point F – Do we need to deploy the Key Personnel (Specific Individuals) identified in the TO Proposal or the agency will allow the Key Personnel identified at the time of award?

    The State requires the evaluation of only Key Personnel in the evaluation process. Therefore Key Personnel must be disclosed at the time of submittal.

73. Section 3.9.5 states up to 5 Key Personnel, however section 3.9.6 states up to 4 Key Personnel to be identified. Please clarify. Also, can we propose less than 4 or 5 key personnel?

    3.9. 5 States "Offerors shall propose up to five (5) personnel …"
    While 3.9. 6 States "Master Contractors may only propose **up to four (4) Key Personnel** …"

74. Page 3, section 2.3.1 Infrastructure Penetration (PEN) Testing. The fifth bullet € indicates that wireless access points are included in the penetration test. Since you indicated on page 2 in section 2.1.2 in the note that the wireless infrastructure may be a future task, do you simply want the access points identified? Would the penetration testing be included in the future work?

    Item 2.3.1 is accurate. The future task note relates to item 2.1.2.2 application testing. Section 2.5 describes this future work order.

75. Page 4, section 2.3.2 Application Testing, bullet A. How many lines of code will need to be code reviewed?

    Already answered, see #43

76. 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?

    We anticipate acceptance within two (2) weeks of submittal.

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

    Employer Payroll is a single page application (SPA), the others have 2-4.

78. Page 10, section 2.5, Optional Work. Are you expecting pricing for this potential work to be included in this proposal?

    No, SRA will follow the Work Order process for any other possible future requests under the current TO.

79. Page 15, 3.6.4, Cyber Security/Data Breach Insurance. We carry $5,000,000 of cyber liability insurance in addition to liability of $5,000,000. We request that the $10,000,000 limit be adjusted down to $5,000,000, particularly since in a penetration test, your confidential data (which could be subject to a breach) is not removed offsite.

    Please see Addendum No. 2 for revision to TORFP.

80. We would like to know if a referenced contract (as it relates to providing relevant past performance) commenced more than 3 years ago but ended within the last 3 years, can be considered a valid past performance (i.e. no older than 3 years). For example, one of our penetration testing projects at the Maryland Judiciary started in Jun 2015 but ended in Sep 2015. Can this project be considered a valid past performance that is no older than 3 years?

    Yes

81. Section 5.4.2.J.3, states that any services furnished from third party entities shall include current Letters of Authorization. Would you kindly define the "furnished services "and provide an example? If the vendor decides to use a software tool for this project, will they need to provide a letter of authorization for such services/tools?

    This is template language. Please disregard for this TORFP.

82. Section 5.4.2.J.4 requires the vendor to provide a Letter of Authorization on the authorizing entity's letterhead or through the authorizing entity's e-mail. We would like to know the purpose of the Letter of Authorization?

    This is template language. Please disregard for this TORFP.

83. It appears that no internal private network testing is required. Only externally-facing testing and external wireless networking equipment is in scope however the inclusion of section 2.3.1 item D specifies routers and switches. Please confirm there is not an internal network test requirement.

    This is for **internal** wireless networking See item 2.1.2.3.