STATE BOARD OF ADMINISTRATION
INVITATION TO NEGOTIATE
NETWORK SECURITY ASSESSMENT SERVICES
QUESTIONS WITH ANSWERS IN ITALICS

General Questions

1. Are there socio-economic preference points allocated to small businesses, disadvantaged small businesses, economically disadvantaged women-owned small businesses (EDWOSB), women-owned small businesses (WOSB), and/or minority owned small businesses?

Answer: Please see the evaluation and scoring process outlined in Section VI of the ITN. Short answer is we encourage minorities to apply but there are no special points allocated to the above request.

2. Is this the first time that you will contract a vendor for the services in question? If not, then would a copy of the final contract and amount of the previous successful vendor be available?

Answer: No, this is not the first time. Request for the contract constitutes a public records request. All public records request must follow the established process in order to facilitate the request. Contact information can be found at www.sbafla.com

3. Given the COVID-19 pandemic, can work be performed remotely to the maximum possible extent? Will this work be performed remotely or are vendors required to be on site to perform the required services?

Answer: Both for some areas work can be performed remotely but other areas may require vendor to be onsite. Majority of the testing can be done remotely.

Scope of Work

NOTE: Answers below are associated with SBA's HQ Site (unless noted otherwise).

4. How many systems, networks, workstation etc. does SBA want to be tested?

Answer: Details are discussed with the selected vendor.

5. What is the total IPS number and how many active?

Answer: If Intrusion Prevention System - 1. If IP addresses refer to question 10 response.

6. What is the approximate breakdown of the number of each externally facing device that are *in scope*? –

NOTE: Answers below refer to SBA's External Network / DMZ (RESPONSE: ~ 50 Devices).

a. Servers [>10 <20]
b. Web applications or Other internal applications used for processing transactions
c. Workstations [0]
d. Firewall / Routers / Switches [<3 for each]
e. Wireless Access Points / Controllers [0]
f. Network segments [1]

7. Any cloud environments in scope i.e. Azure or AWS? If so, what systems/devices are in the cloud?

Answer: Response – Yes. TBD – O365

8. What is the expected effort for vulnerability scanning: Nmap scans or Nessus scans or Other?

Answer: Nessus scans (or a greater effort)

9. Is manual verification and exploitation of all identified vulnerabilities required?

Answer: Verification is required (manual is unknown). No exploitation will be performed.

10. Approximately how many of the following are in scope:

a. IP ranges and size of ranges
b. IP addresses
c. Remote access endpoints/frontends
d. Web applications

Answer: The range of IPs are within 1 or 2 (IPv4) Class C subnets (198.160.242.0 /24). The number of external "Remote access endpoints/frontends" may be 0). There is only one Website however we will test 3 Applications. Web applications scope is agreed in the SOW executed each year with the vendor.

11. Are any of the applications hosted by 3rd parties where testing might be prohibited?

Answer: 3rd Party hosted applications are not in scope.

12. Will the testing (testers) IP's be whitelisted?

Answer: The tester's IP (address) will be whitelisted (though not necessarily any specific protocols).

13. Number of External Hosts?

Answer: See response to #5 and #10

14. Can testing be performed during business hours?

Answer: Some (though not all) testing can be performed during business if approved.

15. Are there any targeted objectives?

Answer: Targeted objectives will be executed in the Statement of Work.

16. How many VPN termination points exist?

Answer: <3

17. How many different remote access termination points and types exist (RDP, Citrix)?

Answer: 1 Citrix, no external RDP

18. Do you want on-site social engineering tests? If so, at how many locations?

Answer: Yes , 1

19. How many applications are in scope for the Web Application Testing (names)?

Answer: Refer to response for #10.

20. What types of data do each scoped web application process (by name)?
Answer: The SBA is an investment management organization, as described in Section I.B. of the ITN. Financial data, Participant data, Insurer data.

21. Are these applications secured with SSO technology?
Answer: No (With respect to Web Applications).

22. Can Application testing be performed during business hours?
Answer: Some (though not all) testing can be performed during business if approved.

23. Are APIs in scope for testing? If so, estimate how many APIs are in scope.
Answer: Not at this time

24. How many applications are protected by a WAF.
Answer: All

25. What types and how many VPN concentrators/Firewalls are in Scope?
Answer: <3

26. Number of Live IPs in scope for testing?
Answer: See response to #5 and #10 (The number of Live IPs will be < 50).

27. Number of external network ranges and size?
Answer: See response to #5 and #10.

Internal Network Information [Page 5 – Section II: Scope of Services (b)]

28. How many internal IPS, Servers and Workstations? Are there multiple locations? If multiple locations, are all IPS centrally connected?
Answer: <3 IPS, Server and Workstation counts are subject to discussion. 1 Location.

29. Please provide names of these (ii, iii, iv, and v) to determine whether CIS benchmarks are available (referencing Item B Internal Network Assessment Number 2). Are these specific to the software or system? Is the version of exchange on Prem or in the cloud?
Answer: Names will not be provided. However, CIS benchmarks do exist.

30. Is internal penetration testing in scope? Is external penetration testing in scope?
Answer: Refer to ITN Section II Scope of Services.

31. How many live/active **internal** IPs are in scope?
Answer: ~ 500

32. How many live/active **external** IPs are in scope?
Answer: ~ 50

33. What is the approximate breakdown of the number of each internally facing device that are *in scope*?

a. Servers: *150*
b. Web applications or Other internal applications used for processing transactions: *Refer to #10 response*
c. Workstations: *250*
d. Firewall / Routers / Switches: *<3 each*
e. Wireless Access Points / Controllers: *24 / 1*
f. Network segments: *50*

34. How many data centers do you have? Are any hosted by 3rd party?

Answer: 1 data center. None [0] are hosted by 3rd party.

35. What is the expected effort for vulnerability scanning: Nmap scans, Nessus scans, etc…?

Answer: Nessus scans (or a greater effort.)

36. Will credentials be provided to conduct the scans, or will they be uncredentialed?

Answer: Both

37. What is the approximate number of servers, workstations, firewalls, routers, or other network devices on the internal corporate network?

Answer: See response to #33.

38. If it is a big Windows environment, how many workgroups/domains/forests are on the network?

Answer: <3

39. Are there segmentations within the internal corporate network itself or is it a flat network where majority of hosts are reachable from a single location?

Answer: Internal Network is Segmented.

40. Is the main intent to (1) identify technical vulnerabilities or (2) to assess your detection and response capabilities?

Answer: 1

41. I would like to know if we need to physically send proposal/Quote or if we can send via email?

*Answer: You can send via email and **do not** need to send physical copies if sent via email.*

42. What is the approximate number of each of the devices that are in-scope:

Answer: [See Below]

a) Exchange Servers: *<3*
b) Firewalls*: <3*
c) Switches: *<3*
d) VPN: *<3*
e) Wireless 802.11x infrastructure: *<3*

f) Endpoint Security (AV, host firewall, etc.): *<3*

43. Is a sampling approach acceptable for each of the above? If allowed, how many per each of the above?
Answer: Yes (Responses above are based on sampling).

44. Please provide a brief description of the in-scope applications and their functionality.
Answer: Web Sites, refer to #10 response.

45. What is the approximate number of dynamic pages for each in-scope application?
Answer: 10-25 per Application

46. How many user levels/roles are within scope (e.g., User, manager, admin, etc)?
Answer: 2-3

47. Are any applications accessible from the Internet, or only from an internal network? If internal only, is there a way to provide remote access to reach the application for testing or would we be required to be onsite to test the application?
Answer: Yes. If Internal Application are in scope, internal access will be provided remotely.

48. Are any of the applications hosted by a 3rd party?
Answer: No

49. If available what is the historical level of effort? Hours?
Answer: Depends on Vendors level of expertise.

50. Will you require a State RAMP 3PAO to perform this work?
Answer: No

51. What percentage of the work will be conducted on-site? Remote?
Answer: Approximately 20%/80%. Will be specified in SOW.

52. Please list your perimeter defense technologies currently used (e.g. Cisco ASA, CKP WAF):
Answer: Will not be provided.

53. Is your infrastructure self-managed? If not, by whom?
Answer: Yes

54. For every environment (Google, AWS, Azure, etc.), please provide the following:
Answer: Information not to be provided. Will be discussed with the selected vendor.

a) A network schema or logical diagrams is available upon request
b) Number of regions for Azure services:
c) Number of tenants in this cloud provider:
d) Number of application services used in this provider:

55. Please describe the cloud strategy for each provider (Google, AWS, Azure, etc.), how the environment is used and its purpose.

Answer: The proposed Cloud Environment will be used for Tertiary Backups.

56. How much technical documentation is there? How many pages?
Answer: Not to be provided

57. How many users are in scope?
Answer: Users in scope for what, phishing? If so, 250.

58. How many physical sites are in scope?
Answer: 1

59. Which best describes the infrastructure: On-prem only, cloud only, or hybrid?
Answer: Initially on-prem only (possibly hybrid in the not too distant future).

60. Regarding manufacturers, quantities and versions in use:
Answer: Answers will be provided to the selected vendor during contract negotiations

a) Exchange
   - What operating system is Exchange running on?
   - What version of Exchange?
   - Is this a single server or is this setup in a cluster? If setup in a cluster, how many servers are part of the Exchange environment?

b) Firewalls/Switches
   - How many firewalls will be part of the review?
   - How many switches will be part of the review?
   - What are the makes and models of the firewalls and switches?
   - What versions of the firmware are in use on the firewalls and switches?

c) VPN
   - Is this software or hardware based VPN appliance?
   - Who is the manufacturer and model of the VPN appliance?
   - What version of firmware is in use on the VPN appliance?
   - Is there only one appliance in use or what is the quantity of VPN appliances?

d) Wireless Infrastructure
   - How many wireless access points exist in the environment?
   - How many wireless controllers exist in the environment?

e) What are the makes and models of the wireless access points and controllers?

f) What versions of the firmware are in use on the wireless access points and controllers?
   - How many SSIDs exist?

g) Endpoint Security (AV, firewall, etc.)
   - What are the versions in use for endpoint security?
   - Who are the manufacturers/vendors in use?
   - Is everything centrally managed for all endpoints?

61. How many firewalls are in scope for configuration review?
Answer: <3

62. How many switches are in scope for configuration review? Are all switches the same manufacturer?
Answer: <3 – Yes

63. How many VPN servers are in scope for configuration review? Please provide a high-level description of the remote access infrastructure in scope.
Answer: VPN <3

64. How many wireless access points are in scope for configuration review?
Answer: <3

65. In addition to configuration reviews of the wireless access points, are you also looking for a wireless network penetration test? If so, how many locations and how many access points per location?
Answer: Yes – 1 Location (HQ/24)

66. How many anti-virus solutions are in scope for configuration review?
Answer: <3

67. Please provide a high-level description of your technical infrastructure, information assets, and overall technical environment (including, if possible, brand names/types of infrastructure elements in place) so that we can get a better idea of the risk assessment scope.
Answer: Responses to other questions in this list should answer this one.

68. How many Active Directory Domains and Forests are in scope
Answer: 1 – 1

69. How many workstations/laptops are in scope?
Answer: 250

70. How many servers are in scope?
Answer: ~150

71. How many Windows servers are in Scope?
Answer: ~95

72. How many Linux based servers are in scope?
Answer: ~ 30

73. How many datacenters are in scope?
Answer: 1

74. What identity and access management systems are you using?
Answer: AD / AAD

75. Are all locations, workstations and servers accessible from a central network point?
Answer: Yes

76. What operating systems are run on Workstations/Laptops?
Answer: Windows

77. Are there any tablets/mobile devices in scope?
Answer: Yes

78. How many firewalls are in scope?
Answer: <3

79. Are all firewalls the same manufacturer?
Answer: Yes

80. Are all switches the same manufacturer?
Answer: Yes

81. What Exchange roles are in use?
Answer: ServerRole; Mailbox

82. What VPN technology is in use?
Answer: Answers will be provided to the selected vendor during contract negotiations

83. How many VPN endpoints are deployed?
Answer: 1 or 2

84. Are access points controlled by a central controller?
Answer: Yes

85. How many access point configurations are in scope? Does each site have a unique configuration?
Answer: <30 No

86. How many SSIDs are in scope?
Answer: 3

87. How many sites are in scope for wireless testing?
Answer: 1

88. How many endpoints (by OS) are in scope for hardening testing?
Answer: Windows 10 – Representative Sample

Windows Server 2016 – (at least) 1

Windows Server 2019 – (at least) 1

Ubuntu – 1

RHEL – 1

89. Are there any site-specific requirements for testing (city, number of sites).
Answer: Tallahassee, 1

90. Are there any cloud services hosted by one or more cloud service providers (CSP) which will be within the scope of the assessment? If so how many CSPs?
Answer: TBD. At this time we can think of one O365.

91. Approximately how many external facing applications and systems are in scope?
Answer: Redundant question – see other responses.

92. Approximately how many internal facing systems, firewalls, databases, and endpoints are in scope?
Answer: This question is answered via other responses. Endpoints would include both workstations and servers in this context. Also, see #33.

93. How many different locations does SBA have? Where are they located? Do all sites use wireless?
Answer: 1, Tallahassee, Yes

94. Which specific Federal and State regulations related to security and the protection of PII is the SBA required to maintain compliance?
Answer: SBA works to align broadly with Federal information security regulations applicable to the financial services industry and those outlined in Florida state law.

95. Are tests such as attempting to install unauthorized peripherals to the SBA environment in scope?
Answer: Yes

96. Are there any public facing kiosks/workstations which will be in scope for the assessment? If so approximately how many and in how many locations?
Answer: No

97. What environments are within scope for testing? Is testing limited to production environments or are non-production environments (for example: development, testing, user acceptance testing) in scope?
Answer: 3 (PROD, DEV, TEST).

Web Applications

98. For the Grey Box Web App – How many internally facing web apps? (reference Section C; Page 6)
Answer: There are 35+ internal web applications.

99. How many web applications will be included in the assessment? *3*
For each web application please indicate:
a) Is the web application accessible via the Internet? *Internal apps – no, External apps – yes*

b) Number of user forms (data entry forms): *With internal applications we have 100s of forms. With external applications we have 10s of forms.*
c) Source code owned by SBA? *Yes, for web applications in scope.*
d) For vendor software, is SBA authorized to test application? *No*
e) Number of web/database/application servers for each application? *Each app is hosted on a web server and may or may not utilize 1-2 database servers.*
f) What environments are in scope for testing i.e. staging/production/test/QA? *Production*
g) For authenticated based testing please indicate by application the number of user types SBA requires to be tested. (e.g. Admin, Power User, User, etc.) *Typically, 1-2 roles*
h) Are testing of applications required for regulatory compliance program(s)? (e.g. PCI, NIST, etc.) *Not at this time, to our knowledge.*

100. Do the web applications in scope allow the ability to register one's own test account?
Answer: Internal apps – no. External app – some do with verification.

101. Grey box assessment of selected web applications –
a) How many applications are in scope? *3*
b) How many roles are there per application? *1-2*
c) Is Authenticated API testing in scope? *no*
d) What is the API technology (i.e. Rest/JSON/XML/etc) *NA*
e) Authentication Method (Basic/Bearer/Digest/OAuth/etc). *TMI*
f) How many applications are protected by a WAF? *All of them.*

Internal Network Penetration Test

102. Approximate number of:
a) Servers: *~150*
b) Devices (router, switch, network printer etc) *Need additional clarification*
c) Workstation/Desktop/Laptop: *250*

103. Are you looking for automated vulnerability scanning or manual penetration testing?
Answer: Both – the requirements include black and grey testing. This would generally include both automated vulnerability scanning to identify vulnerabilities that may be exploitable, then attempting to leverage applicable vulnerabilities to compromise the target.

DLP

104. Are you concerned with access control or actual extraction of data and the detection of extraction?
Answer: Yes

105. Which DLP technology is in use?
Answer: Various (endpoint and network based), but none are stand-alone DLP systems

106. Will Presidio have access to speak with the DLP team?
Answer: SBA has no dedicated/specific DLP team, but assessors will have access to relevant SBA employees

107. How many endpoint agents are deployed?
Answer: Depends on the technology.

108. How many DLP Policies are deployed?
Answer: Redundant question – see other responses.

109. Is a CASB or similar technology also deployed?
Answer: Yes

110. What tools or application is used for DLP?
Answer: Redundant question – see other responses.

111. What types of data are in scope for testing DLP?
Answer: PII, Financial,

Social Engineering

112. Is social engineering limited to the SBA employees only?
Answer: No

113. Are email phishing attempts expected for all or would a sampling be sufficient?
Answer: All

114. How many employees will be included in the phishing test?
Answer: Approximately 250

115. Is physical impersonation (e.g. impersonating a vendor to gain physical access to restricted/locked areas) in scope? *Yes*
a) If yes, how many locations will be tested? *1*

116. For the social engineering assessment, how many scenarios would you like us to perform?
Answer: Not clear on the question

117. Is the Board of Directors within testing scope? Are SBA contractors in scope?
Answer: No

118. Is physical impersonation (e.g. impersonating a vendor to gain physical access to restricted/locked areas) in scope? If yes, how many locations will be tested?
Answer: One

119. For the social engineering assessment, how many scenarios would you like us to perform?
Answer: Redundant question – see also response #117.

120. How many targets will be included in the social engineering testing?
Answer: Redundant question – see also response #119.

Phishing

121. How many targets in scope
Answer: Redundant question – see other responses.

122. Will SBA provide targets or will vendor need to perform OSINT
Answer: SBA will provide.

123. Are you looking for targeted or untargeted campaigns?
Answer: Ideally, a mix of both.

124. Are you looking for vendor to create custom payload or evasion development?
Answer: No

125. Will the phishing domain be whitelisted?
Answer: Yes, for phishing test designed to test SBA information system users' abilities to detect phishing. No, for tests designed to test our phishing detection systems.

Black Box Web Application

126. How many externally facing web applications are in scope for the black box test? (reference section 2; Item A4) Number of applications in scope for non-authenticated testing.
Answer: 9-10. See other responses answered above.

127. Do all of the applications require authentication?
Answer: (The ones that we would prefer to test do, there are a couple publicly accessible sites, not sure if those are in scope)

Device Configuration

128. How many exchange servers are in scope for configuration review?
Answer: See response to #42.

129. How many firewalls are in scope for configuration review?
Answer: <3

130. How many switches are in scope for configuration review?
Answer: <3

131. How many VPN servers are in scope for configuration review? Please provide a high-level description of the remote access infrastructure in scope.
Answer: <3

132. How many wireless access points are in scope for configuration review?
Answer: 24

133. In addition to configuration reviews of the wireless access points, are you also looking for a wireless network penetration test? If so, how many locations and how many access points per location?
Answer: Yes. 1 location (Tallahassee) which utilizes ~ 24 Aps.

134. How many anti-virus solutions are in scope for configuration review?
Answer: 1

135. Please provide a high-level description of your technical infrastructure, information assets, and overall technical environment (including, if possible, brand names/types of infrastructure elements in place) so that we can get a better idea of the risk assessment scope.
Answer: Redundant question – see other responses.

136. Do you currently have a data loss prevention system/software in place?

Answer: Redundant question – see also responses #107-110.

Email Phishing

137. Will target email addresses be provided, or is the expectation for the vendor to perform discovery via Internet harvesting?
Answer: Redundant question – see other responses.

Vishing

138. Will target phone numbers be provided, or is the expectation for the vendor to perform discovery via Internet harvesting?
Answer: Harvesting

139. How many target email addresses / phone numbers would you like to be included in this exercise?
Answer: Up to 50 phone numbers / 250 email addresses.

140. Are payloads that allow remote access allowed?
Answer: No – All payloads should be inert/benign and designed only to demonstrate POC.

141. Is credential harvesting allowed?
Answer: Yes

142. What types of a exploitation activities are allowed?
Answer: Question is too vague.

143. How many targets in scope
Answer: Redundant question – see other responses.

144. Will SBA provide targets or will vendor need to perform OSINT
Answer: Redundant question – see other responses.

Remote Access Assessment

145. Number of targets in scope
Answer: This question doesn't make sense in the context of a black box remote access assessment.

146. Specific type of VPN, Remote Desktop & other technologies in use
Answer: Redundant question – see other responses.

Other Questions

147. Will this review be used to meet or satisfy any regulatory or compliance requirements? If so, which one(s)?
Answer: No

148. Are there any systems currently being utilized which could be characterized as fragile (systems with tendency to crash)?
Answer: No

149. Are there systems on the network which the client does not own, that may require additional approval to test?
Answer: No

150. How many hosts (endpoints) are in the network and part of the scope?
Answer: Redundant question – see other responses.

151. Is the target environment mostly Windows based? If not, which technologies are used?
Answer: Yes

152. How many external IPs are in scope (local perimeter, cloud services, etc.)?
Answer: Redundant question – see other responses.

153. How many DNS domains are included?
Answer: Redundant question – see other responses.

154. How many web applications will need to be tested?
a. Will the tests be authenticated?
Answer: Redundant question – see other responses.

155. How many application roles will be tested (by app)?
Answer: Redundant question – see other responses.

156. Are any mobile applications in scope? Android vs. iOS
b. Is the source code available on request?
c. How many lines of code?
d. In what language is the application written?
e. For iOS, is the application available unencrypted?
Answer: None in scope

157. For API Testing, how many features?
   a. Can a swagger file be provided?

Answer: API Testing not currently in scope

158. For the Vulnerability Analysis (Vulnerability Scanning) to be included in the scope of activities, how many hosts need to be scanned/analyzed?

Answer: Redundant question – see other responses.

Security Policies

159. Please provide the following security policies from SBA:

- SBA Policy #20-404 Remote Access
- SBA Policy #20-411 Anti-Virus
- SBA Policy #10-409 Confidential/Sensitive Electronic Data Handling

Answer: Information will be provided to the selected vendor

Deliverables

160. Can status report and Presentations to the SBA committee be performed remotely? Are presentations to be conducted on-site at SBA locations or may they be performed remotely?

Answer: Status meetings can be provided remotely. Presentations to the Audit Committee may or may not be presented remotely depending on the situation.

161. How often will status reports be expected?

Answer: Bi-weekly or earlier if needed.

162. How often are the presentations to the SBA audit committee?

Answer: Twice, going over the audit scope and going over the report presentation

163. In Section V: Response Requirements, Letter E. "Response Requirements and Deadline" it states that we need to submit: #**1. Submit response electronically via email no later than 4:00 p.m. ET on January 4, 2022, to Procurement@sbafla.com** and **#4 Submit nine (9) bound copies of your response no later than 4:00 p.m. ET on January 4, 2022.** Does this indicate that we need to submit via ***both*** email and hardcopy? Due to the upcoming holidays and with potential shipping delays because of the holiday season, would it be possible to submit our response only electronically via email to ensure timely delivery?

Answer: Yes, response can be submitted electronically. Paper copies are not required if you submit electronically.

164. What is involved in on-boarding contract staff? For example, are there specific clearances, background checks, and NDA's required?

Answer: A Level 2 (or greater) background check is required for on-boarding contract staff. NDA's are required from the vendor selected.

165. REGARDING Questionnaire: In regards to #19 on the questionnaire: Does the Broward County Board of County Commissioners represent an entity under the oversight of the SBA?

Answer: No

166. Based on the upcoming holidays, does the SBA anticipate extending the proposal submittal deadline?

Answer: At this time, we don't anticipate any changes to deadlines. Refer to section D for checking SBA and SBA websites for any addenda or updates.

167. Due to current logistical issues and holidays, can the Nine (9) bound copies of the proposal be accepted late if the electronic version is on time?

*Answer: If electronic copy is provided nine (9) bound copies are **not** needed.*

168. The RFP requirements state that vendors are to submit proposals electronically. Further instructions listed under (*vendor does not complete sentence)

Answer: Refer to ITN Section E. Response Requirements and Deadline. If electronic copy is provided nine (9) bound copies are not needed.

169. Is there an incumbent for this opportunity or is this a new effort?

Answer: This is not a new effort

170. Would SBA be open to additional service areas over the 5-year contract (Wireless, Social Engineering or Physical)?

Answer: Refer to ITN Section M Contract term.