NYSIF
New York State Insurance Fund
Procurement Unit

March 21, 2019

The following Q&A will serve as Amendment #1 to NYSIF's Request for Quotes (RFQ) for Penetration Testing, bid number 2019-13-IT. Material in this Amendment supersedes any contradictory material in the RFQ.

In addition, the attached Appendix E, New York State Standard Vendor Responsibility Questionnaire (Contracts less than $100,000) hereby replaces the Appendix E, Vendor Responsibility Questionnaire attached to the RFQ.

Please note that the due date for the submission of bids **remains unchanged**.

All bids are due 3/29/19, by 2:00 p.m.(eastern).

Sincerely,

Alexandria Romano

Alexandria Romano
Contract Management Specialist 2

15 Computer Drive West • Albany, New York 12205
Phone (518) 437-4360 • Fax (518) 437-4209

Penetration Testing
RFQ # 2019-13-IT
Amendment 1

#	Question	NYSIF Response
1	I am working on RFQ #2019-13-IT proposal and I am curious how you would like us to respond. It requires an SDVOB utlization plan, but we are planning to prime and we are also an NYS certified SDVOSB	There is a 6% SDVOB goal for this procurement. Bidders must complete Appendix S, Form S-100: SDVOB Utilization Plan based on your information. Bidder should note in your Appendix S that you are a certified SDVOB firm.
2	Technical Specifications/Assets - What are the total number of internal and external IP addresses being tested?	Externally approximately 25 IP's. Internally we are not looking for a vulnerability scan so the total number of IP addresses are out of scope. We are looking for a penetration test, so the tester will do scans as needed to find a vulnerability that they could exploit to gain a foothold and pivot from there.
3	Technical Specifications/Assets - What are the total number of web pages and authentication contexts being tested?	Nysif.com and 5 web applications
4	If the prime bidder is a SDVOB, what % of the contract is the SDVOB allowed to sub-out ?	There is a 6% SDVOB goal for this procurement. If the prime is a certified SDVOB, the firm is not required to subcontract any of the work to an SDVOB firm as the SDVOB goals are being met through the prime. However, any firm whether SDVOB or not, is encouraged subcontract services to an SDVOB.
5	If the prime bidder is a SDVOB, is the SDVOB required to sub out 30 % of the contract to a MWBE ?	NYSIF has established a 30% MWBE goal for this procurement. Bidders must subcontract 30% of the work to an MWBE firm or complete Appendix M, Form 104 'Request for Waiver' Form.
6	11-4 Assets-a. Internal Pen Test - Approximately how many IP addresses are to be tested on the Internal network ?	Internally we are not looking for a vulnerability scan so the total number of IP addresses are out of scope. We are looking for a penetration test, so the tester will do scans as needed to find a vulnerability that they could exploit to gain a foothold and pivot from there.
7	11-4 Assets-b. External Pen Test - Approximatly how many IP addresses are to be tested on the External network ?	Approximately 25
8	11-4 Assets-b. External Pen Test - Approximately how many web-sites are to be tested on the External network ?	Just one: www.nysif.com
9	11-4 Assets-b. External Pen Test - Please define " a few additional physical security tests will be required to be performed at three NYSIF offices" Physical security tests could mean attempts to gain physical entry or simply a physical location risk assessment.	Attempt to gain physical access into the building
10	11-4 Assets-b. External Pen Test - Please define " a few additional physical security tests will be required to be performed at three NYSIF offices" What are the specific locations of the three NYSIF physical security tests that are to take place? The cost of traveling to Albany vs the cost to travel to NYC varies considerably.	NYSIF's Albany 15, Rochester, Syracuse locations.
11	13-1- Project Plan - What is the specific location of where the kickoff meeting is to take place ? The cost of traveling to Albany vs cost of traveling to NYC varies widely	Meeting could be virtual. No specific need for an onsite meeting.
12	11-1-c. Wireless - What is the specific location of where the wireless testing will be performed ? The cost of traveling to Albany vs cost of traveling to NYC varies widely	Albany
13	11-1-c. Wireless - How many buildings are at the specific location of where the wireless testing will take place ? A single building or campus with multiple buildings will impact the cost.	One.
14	11-1-c. Wireless - Approximately how many Access Points will be tested at the location of the wireless test?	Not controller based, only 1 location, which should be done while internal assessment is being done.
15	11-1-b. Internal - Will the Internal assessment be completed on-site or can remote access technologies be utilized to connect to the Internal network?	On-site. No remote testing for internal assessment.
16	11-1-b. Internal - If Internal testing is to be completed onsite, what specific location will be utilized for the testing? The cost of travelling to Albany vs the cost of travelling to NYC varies widely	Albany
17	13. Deliverables - Can online file sharing systems such as Dropbox or OneDrive be used to share resources between the client and the vendor? If not, what is the expected method of data sharing?	NYSIF will initiate secure encrypted email to transfer reports. We will not accept encrypted emails initiated by third party.
18	6. Disaster Recovery Plan - Can NYSIF provide a template as to the level and format for the disaster recovery plan	Please refer back to Appendix C, Clause 6 as to what is required. The plan should include but not be limited to a description of the Plan Assumptions, Recovery Strategy, Disaster Declaration, Plan Notification and Activation, and Recovery Resources.

Penetration Testing
RFQ # 2019-13-IT
Amendment 1

#	Question	NYSIF Response
19	Appendix S: SDVOB - Is the contract a SDVOB Set Aside?	No.
20	Section 9 - We are a registered MWBE. In order to meet the SDVOB goal of 6%, can we utilize SDVOB firms located outside NY state and registered as SDVOB with either their specific state of operation or recognized as SDVOB by the Federal government?	The SDVOB subcontractor must be a NYS certified SDVOB. Firms can search certified NYS SDVOB's on the following website: https://online.ogs.ny.gov/SDVOB/search
21	Section 10.2 - When you say "provide three samples of penetration testing", our understanding is that you mean that we need to provide references of the 3 such penetration tests and not actual reports. Can you please confirm?	Sanitized reports of past pen-tests performed.
22	Section 7 - It is our understanding that a certificate of insurance that meets the stated requirements needs to be submitted at a later date by the successful vendor. Is that correct? Or do bidders need to submit said certificate of insurance along with bid responses?	Correct, they will be submitted at a later date by the awarded firm.
23	Section 17 - Which of the mentioned appendices and exhibits, specifically, need to be completed and sent back with the bid response? Given that certain appendices (such as Appendix A and Appendix B, for instance) appear to be more for reference rather than completion; hence the question. If you could specify the ones that need to be completed and sent back, that would leave little room for errors/omissions.	Appendix D-Z and Attachment 3 should be submitted with your quote.
24	Appendix E states that it applies to contracts greater than $100,000. However, Page 1 of the RFP states that the resulting contract from the procurement will not exceed $50,000. Wouldn't that mean that Appendix E does not apply?	Please see the attached revised Appendix E that should be submitted with your quote.
25	Is there a budget or not-to-exceed amount that NYSIF has penciled for this project that you can share?	The value of the resulting contract from this procurement has a maximum not-to-exceed price of $50,000.
26	Please provide the total number of live external IP addresses that are in the scope of the project.	Approximately 25
27	Please provide the total number of live internal IP addresses that are in the scope of the project.	Internally we are not looking for a vulnerability scan so the total number of IP addresses are out of scope. We are looking for a penetration test, so the tester will do scans as needed to find a vulnerability that they could exploit to gain a foothold and pivot from there.
28	Is internal penetration testing expected to be done onsite or can it be done remotely via a VPN connection and virtual scanner that can be installed by NYSIF?	On-site. No remote testing for internal assessment.
29	Please confirm that web application penetration testing is also in the scope of this project. If so, please provide the total number of web applications that are in scope and if test account credentials will be provided for these.	No credentials will be provided. Following Webapps do not require a login: Get a quote, where's my check, efroi, validate certificate of insurance, premium audit scheduling system, find my underwriter, case manager.
30	Section 11.1. - For the wireless testing, please provide the number of locations where wireless testing will need to be performed. If there is more than one location, please provide the physical locations (addresses) of these locations. Alternatively, please let us know the approximate distance between these locations.	Albany
31	Section 11.1. - For the physical security testing, please provide the addresses of these 3 locations mentioned. Alternatively, please let us know the approximate distance between these locations.	NYSIF's Albany 15, Rochester, Syracuse locations.
32	Section 11.1. - For the physical security testing, we understand that you are looking for us to perform physical security penetration exercises (similar to social engineering scenarios) wherein we try methods including impersonation, misdirection, and so on, to break your physical security defenses. Can you please confirm?	Yes, attempt to gain physical access.
33	Appendix T. Data Privacy a) - Will the customer consider allowing remote participation by a cybersecurity expert team in Israel who is a designated Qualified Security Assessor by the PCI Counsel and who holds an ISO 27001 certificate?	No.

Penetration Testing
RFQ # 2019-13-IT
Amendment 1

#	Question	NYSIF Response
34	Section 10.1. In order to provide samples of similar scope, will the customer provide the number of IP addresses and the number of VLAN internal and external assets in order to properly scope this project?	Approximately 25 DMZ IP's. Internally we are not looking for a vulnerability scan so the total number of IP addresses are out of scope. We are looking for a penetration test, so the tester will do scans as needed to find a vulnerability that they could exploit to gain a foothold and pivot from there.
35	Section 11.1.d. - Can testing of IP addresses and ACL Devices be done remotely or does the scope of the physical testing include locks and access points to the building?	External assessment can be remote, internal assessment must be performed on-site in Albany.
36	Section 11.2.For the Black and Gray box test: If we are testing both at the application layer (internal web servers and web services) and infrastructure layer (firewall, segmentation, servers, OS versions etc.). could the customer please provide some kind of a rough estimation on how many internal web servers/services and how many infrastructure related components?	Approximately 25 DMZ IP's. Internally we are not looking for a vulnerability scan so the total number of IP addresses are out of scope. We are looking for a penetration test, so the tester will do scans as needed to find a vulnerability that they could exploit to gain a foothold and pivot from there. nysif.com with 5 external web apps.
37	Section 11.2. Black box external test – If only application layer is required, is this the only URL we will be testing? https://ww3.nysif.com/ or does the customer have a list of URLs to cover?	nysif.com with 5 external web apps.
38	Section 11.2.d. "Reporting occurs through the penetration process." Does this mean with artifacts?	Yes
39	Section 13.4. Where will the onsite Executive Level Presentation be held? The different locations would be priced differently.	This could be done remotely.
40	We do not plan to utilize contractors and are a WBE firm ourselves. Must we hire a subcontractor specifically to meet this goal?	Vendor should submit their WBE certification with their bid and complete Appendix M as requested in the RFQ. MWBE subcontracting is not required if the prime can meet the 30% MWBE goal.
41	We do not plan to utilize contractors and are a WBE firm ourselves. Must we hire a subcontractor specifically to meet this SDVOB goal?	There is a 6% SDVOB goal for this procurement, which needs to be met as either the prime or subcontractor for this procurement.
42	Mandatory Requirements, Item 1. - Please clarify how you want Appendix T submitted. Can we include it in our proposal response or is it to be submitted as a separate document?	Appendix T, and any substantiating documents, even if included or referenced elsewhere in a bidder's response, must be submitted as one file and labeled separately in the electronic copy. See Section 16 for additional information.
43	Mandatory Requirements, Item 4. ii. - Do you want copies of certificates included in our response?	If the question is about qualification certificates, no we don't need copies of them.
44	Technical Specifications, Item 2.c. - Is the executive report required to be a separate report or may it be a section within the main report?	It should be a separate report
45	Section 13, Deliverables, Item 2 - Does the three weeks of testing allowed account for elapsed time or is this the limit for work-effort of testing?	3 weeks for work effort of active testing
46	Section 18, Due Date, Last Paragraph - It states that an electronic copy of the Fee Schedule is to be submitted as a separate file. Are we to submit one hard copy of our proposal that does not include the Fee Schedule, i.e. we will submit three documents in hard copy - those being the proposal, the Fee Schedule and Appendix T. Please clarify.	Yes, submissions must include one (1) hard copy of the proposal and one (1) exact electronic copy (CD/DVD-rom or USB flash) of proposal. The exact electronic copy must include a copy of the Bidders Fee Schedule in a separate file from the Bidders proposal.
47	Appendix E - Since your budget maximum is $50,000.00, and this Appendix states that this questionnaire is for all projects over $100,000.00 is there a requirement to complete this questionnaire?	Please see the attached revised Appendix E that should be submitted with your quote.
48	Does this RFP have a minority owned / woman owned mandatory requirement?	Please refer back to Section 8 of the RFQ.
49	Does this RFP have a mandatory SDVOSB requirement?	Please refer back to Section 9 of the RFQ.
50	Appendix T - For the Substantiating Documents, are anonymized reports from other clients sufficient or is there a need for additional documents such as a SANS GPEN cert?	Sanitized reports of past pen-tests performed.
51	Section 11. Technical Specs - How many targets / IPs is the black box and gray box testing going against?	Approximately 25 DMZ IP's. Internally we are not looking for a vulnerability scan so the total number of IP addresses are out of scope. We are looking for a penetration test, so the tester will do scans as needed to find a vulnerability that they could exploit to gain a foothold and pivot from there.
52	Section 11. Technical Specs - Where are the physical locations for the physical security tests and how many locations are there?	NYSIF's Albany 15, Rochester, Syracuse locations.

Penetration Testing
RFQ # 2019-13-IT
Amendment 1

#	Question	NYSIF Response
53	Appendix T - We can answer 'fully' to every one of these questions but since it is only for a pen test do we only have to answer the pen test box	Bidder must complete the attached Appendix T, Vendor Security Survey. Appendix T, and any substantiating documents, even if included or referenced elsewhere in a bidder's response, must be submitted as one file and labeled separately in the electronic copy. See Section 16 for additional information.
54	Section 11.1.a.Approximately how many assets exist in your DMZ?	25
55	Section 11.1.a. Do any assets exist in the cloud (such as AWS or Azure) or are all assets on premise? (Cloud based tests usually require authorization from 3rd parties)	None.
56	Section 11.1.a. What is the goal of the external penetration test? Identify what the external footprint is and what vulnerabilities can be exploited? Gain a foothold into the internal network/DMZ network?	Identify what the external footprint is and what vulnerabilities can be exploited. Gain a foothold into the internal network/DMZ network
57	Section 11.1.a. Is targeted spear-phishing permitted?	Yes.
58	Section 11.1.c. What is the SSID of the wireless networks that we need to assess? This is required as we will not be authorized to "guess" and attempt to compromise adjacent wireless networks.	This will be provided, if needed, during the kickoff meeting.
59	Section 11.1.b. What is the goal of the internal penetration test? Breach a particular network? Access a workstation/server/application? Compromise sensitive data sets?	Assess the strength of internal network, VLANs, ACLs from Dev/test into production networks, password strength
60	Section 11.1.b.What is the protected network segment that is intended to be segmented from networks of lower security requirements? What types of sensitive data resides within this network?	This will be provided, if needed, during the kickoff meeting.
61	Section 11.1.b. Is the intention of the assessment to assess the capabilities of the blue team to detect, respond and contain a sophisticated threat? To what level? Will a full incident response process take place? Are there third-party incident handlers on retainer which will be brought in?	Identify what the external footprint is and what vulnerabilities can be exploited. Gain a foothold into the internal network/DMZ network
62	Section 11.1.b.How should the internal penetration test be performed? Will *Vendor Name Redacted* work under the guise of a "consultant" or regular employee that has been onboarded? Will *Vendor Name Redacted* presence be known to the wider defensive team? Will Nettitude work from a NYSIF workstation?	The pen-tester will assess the external portion remotely and the internal location is to be done on-site. NYSIF will provide a workplace but will not provide a workstation and pen-tester will be required to obtain an ip-address and perform the assessment.
63	Section 11.1.b. What is the goal of the physical social engineering assessment? Is the intention to breach into a secure office space?	Attempt to gain physical access into the building
64	Section 11.1.b. Once in a secure office space, what is permitted? Document introduction/exfiltration? Photographs? Device introduction/exfiltration?	Photograph insecure document storage, unlocked workstations, but no exfiltration and no device introduction
65	Section 11.1.b. Are there any on-premise armed security guards that we should be made aware of?	No armed security guards.
66	Section 11.1.b. Are there any impersonation techniques that we should not attempt?	None.
67	11. 1. Technical specifications Is the IT organization centralized or decentralized?	Decentralized
68	When was your last assessment of this nature performed?	2018
69	12. 2. Rules of engagement - Are there documented policies, procedures, standards, and guidelines in place? If so, how many?	Yes, we have policies and standards, Rules of engagements will be set during kickoff.
70	Is there an incumbent and are they eligible to bid on this project? If so, who was the incumbent and what was the value of the contract?	Not material to this RFQ.
71	10. 2. Mandatory requirements - We respond to a large number of bid requests and appreciate our clients' generosity in providing references for our firm. However, we do not want to overwhelm our customers with reference requests. Will NYSIF accept letters of recommendation in place of references with contact information? Alternatively, can we redact the contact information for our references in our proposal? If named a finalist for this RFP, we will provide full contact information upon NYSIF's request.	We do not need references from your past pen-tests. We need sanitized reports of three past pen-tests performed. You may redact sensitive information.

Penetration Testing
RFQ # 2019-13-IT
Amendment 1

#	Question	NYSIF Response
72	11. 1. Technical specifications - What is the approximate number of active IPs to be tested during the external penetration testing?	25
73	11. 1. Technical specifications - Is a detailed firewall configuration analysis in scope? If so, what is the number of firewalls, and, of those, are any in HA pairs?	No. Only attempts to exploit any vulnerability on the firewall to gain a foothold into the internal network.
74	11.1. What is the approximate number of active IPs to be tested during internal network vulnerability assessment and penetration testing?	Internally we are not looking for a vulnerability scan so the total number of IP addresses are out of scope. We are looking for a penetration test, so the tester will do scans as needed to find a vulnerability that they could exploit to gain a foothold and pivot from there.
75	11.1. For the wireless network assessment, how many controllers are in scope? If not controller-based, please provide the number of locations.	Not controller based, only 1 location, which should be done while internal assessment is being done.
76	11.1. Is penetration testing of web applications in scope? How many applications and URLs are to be tested?	nysif.com with 5 external web apps
77	11.1. How many appliances will be tested during the VPN/remote access review?	There is no separate VPN/remote access review. It should be part of the pen-test.
78	11.1. Is physical social engineering included in the physical security testing (e.g., baiting, tailgating)? If so, is this to be done at only three locations?	Yes, and yes.
79	Our insurance carrier cannot endorse the policies to provide written notice prior to cancellation, non-renewal, or material change. However, we will provide prior written notice to NYSIF in the event of cancellation, non-renewal, or material change in any of the applicable policies. As such, we request that the second paragraph of this section be modified as follows: All insurance required by the RFP shall be obtained at the sole cost and expense of the Bidder, shall be maintained with insurance carriers licensed to do business in New York State and acceptable to NYSIF and shall be primary and non-contributing to any insurance or self-insurance maintained by NYSIF. The Contractor will provide written notice to NYSIF at least thirty (30) days prior to the cancellation, non-renewal, or material alteration of such policies, which notice, evidenced by return receipt of United States Certified Mail, shall be sent in accordance to the 'Notice' provision of the Agreement.	The requested change is acceptable and incorporated by this Amendment to the RFQ.
80	We request that the following coverages be removed from the Commercial General Liability Insurance requirements: "liability assumed in a contract (including the tort liability of another assumed in a contract) and explosion, collapse & underground coverage."	Should your firm be awarded, this may be reviewed during contract negotiations.
81	Because our consultants use ride-sharing services for transportation to and from work sites, we do not have any company-owned vehicles. As such, our business automobile liability insurance policy covers hired and non-owned vehicles only. We request that the Comprehensive Business Automobile Liability Insurance requirements be modified to apply to hired and non-owned vehicles only, as opposed to "any automobile including owned, leased, hired and non-owned vehicles."	Should your firm be awarded, this may be reviewed during contract negotiations.

Penetration Testing
RFQ # 2019-13-IT
Amendment 1

#	Question	NYSIF Response
82	Appendix A 10. Records Section 10, Records, states that the State will have access to the books, records, documents, accounts, and other evidence pertaining to performance under this contract ("Records"), for purposes of conducting an audit or inspection. We are inclined to provide direct access to our accounting system but will provide the State with copies or other evidence of the Records. We request that this section be modified to state that: "the State Comptroller, the Attorney General and any other person or entity authorized to conduct an examination, as well as the agency or agencies involved in this contract, shall have access to copies or other evidence of the Records during normal business hours at an office of the Contractor within the State of New York or, if no such office is available, at a mutually agreeable and reasonable venue within the State, for the term specified above for the purposes of inspection, auditing, and copying."	No comments, limitations or changes are permitted with respect to any of the terms and conditions contained in Appendix A.
83	Appendix C 17. Right to Audit We are not inclined to provide NYSIF direct access to our accounting system for purposes of conducting an audit. As such, we request that this clause be modified to state that: "Contractor shall furnish or make available copies or other evidence of such supplemental accounts, records or other information as required to substantiate any estimate, expenditures or report as required by NYSIF (or its designee), or as may be necessary for auditing purposes or to verify that expenditures were made only for the purpose authorized by this agreement and consistent with all requirements as stated in the Request for Proposal."	Should your firm be awarded, this may be reviewed during contract negotiations.
84	Appendix C 21. Remedies for Breach a. Cover/Substitute PerformanceWe request the addition of the following sentence: "Contractor will not reimburse NYSIF for purchases in excess of the value of this Contract."	Should your firm be awarded, this may be reviewed during contract negotiations.
85	Appendix C 21. Remedies for Breach d. Reimbursement of Costs Incurred We request the addition of the following sentence: "Contractor will not reimburse NYSIF for amounts in excess of the value of this Contract."	Should your firm be awarded, this may be reviewed during contract negotiations.
86	Appendix C 21. Remedies for Breach e. Deduction/Credit We request the addition of the following sentence: "Contractor will not be responsible for amounts in excess of the value of this Contract."	Should your firm be awarded, this may be reviewed during contract negotiations.

Appendix E

New York State
Standard Vendor Responsibility Questionnaire
(Contracts less than $100,000)

VENDOR RESPONSIBILITY Within the past five years has your firm, any affiliate, any predecessor company or entity, owner, director, officer, partner or proprietor been the subject of:	ANSWER ALL QUESTIONS
A. an indictment, judgment, conviction, or a grant of immunity, including pending actions, for any business-related conduct constituting a crime under governmental law?	☐ YES ☐ NO
B. a government suspension or debarment, rejection of any bid or disapproval of any proposed subcontract, including pending actions, for lack of responsibility, denial or revocation of prequalification or a voluntary exclusion agreement?	☐ YES ☐ NO
C. any governmental determination of a violation of any public works law or regulation, or labor law or regulation, or any OSHA violation deemed "serious or willful?"	☐ YES ☐ NO
D. a consent order with NYS Department of Environmental Conservation, or a governmental enforcement determination involving a construction-related violation of federal, state or local environmental laws?	☐ YES ☐ NO
E. a finding of non-responsibility by a governmental agency or Authority for any reason, including but not limited to the intentional provision of false or incomplete information as required by State Finance Law §139-j?	☐ YES ☐ NO

If yes to any of above, please provide details regarding the finding.

ENTITY MAKING FINDING: _____

YEAR OF FINDING: _____

BASIS OF FINDING: _____

_____

_____

_____

(ATTACH ADDITIONAL SHEETS IF NECESSARY)

USEFUL INFORMATION MAY BE ACCESSED AT:
http://www.ogs.state.ny.us
AND
http://www.osc.state.ny.us/vendrep/index.htm