NYSIF

PO BOX 66699; ALBANY, NY 12206
| **nysif.com**

June 23, 2025

The following (Q&A) will serve as Amendment #1 to NYSIF’s Request for Quotes (RFQ) for 2025 Penetration testing, bid number 2025-49-IT. Material in this Amendment supersedes any contradictory material in the RFQ.

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

All bids are due 7/1/2025, by 2:00 p.m.(eastern).

Sincerely,

Ryan K. Cerone

Ryan Cerone
Contract Management Specialist II

2025 Penetration Testing
RFQ # 2025-49-IT
Amendment 1

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
1	8,9	14- Technical Specs/Scope	What's the number of internal/external IP addresses for the pen test?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided to the winning bidder.
2	N/A	General	What is the budget for this Project?	This is not material to the solicitation.
3	N/A	General	What was the annual spend for the previous year on this Project?	This is not material to the solicitation.
4	N/A	General	If this is a new Contract, What is the annual Budget for this?	This is not material to the solicitation.
5	N/A	General	Are you open to a hybrid delivery model with a mix of offshore and onshore resources?	All testers must work from the Continental US.
6	N/A	General	Work will be Onsite or Remote ?	As needed for the testing.
7	N/A	General	Can you please provide us with the extension to submit our response by 1-2 weeks.	At this time no extension will be granted. If NYSIF deems an extenstion is necessary, a separate amendment will be issued.
8	N/A	M/WBE	We are interested in submitting a response to this RFP, but we are M/WBE certified in Texas, not in New York. Can you please let us know if we are eligible to bid on this RFP? If not, can we take a subcontractor as an M/WBE certified vendor from New York?	The prime bidder must be a New York State certified M/WBE vendor at the time of proposal. Having a subcontractor who is New York State certified M/WBE does not meet this requirement.
9	6	USE OF GENERATIVE ARTIFICIAL INTELLIGENCE (GenAI) BY BIDDERS/CONTRACTORS	Page 6 of this RFQ prohibits the use of AI, but there is a specific requirement on page 9 for "AI Enhanced Security Research". Please confirm whether suppliers are permitted to use AI as part of this initiative.	If a Bidder/Contractor will be using GenAI technology, tool or solution, either directly or indirectly, to provide any part of the services under this solicitation, the Bidder/Contractor must disclose this within their proposal submission. Failure to disclose the use of GenAI in your proposal may result in the disqualification of your proposal.
10	8	Scope	While this section indicates the types of tests that NYSIF requires as part of the engagement, it does not mention the size of the environment. Roughly how many live Internet-facing hosts exist in the environment? Roughly how many endpoints and servers exist on the internal network? How many wireless SSIDs exist?	The awardee will be provided with the relevant information at the kickoff meeting.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
11	9	Coordination	This section refers to coordination of attacks with the Blue Team. Should suppliers infer that this means that NYSIF also desires a Red Team (advanced persistent threat) approach to penetration testing, potentially including phishing or social engineering?	To be discussed during kickoff. Some examples are Wi-Fi, USB drops or Business email compromise attempt.
12	8	Scope	Would NYSIF like the supplier to perform validation retesting after the identified vulnerabilities have been remediated?	No retesting required. However, remediation clarification will be required.
13	N/A	1.4	What are the primary goals of this penetration test (e.g., identify vulnerabilities, test incident response, validate controls)?	The primary goal is to identify vulnerabilities.
14	N/A	1.4	What is the scope of this engagement in terms of systems, applications, and networks to be tested?	The awardee will be provided with the relevant information at the kickoff meeting.
15	N/A	1.4	For the External Threat Simulation, what are the boundaries or IP ranges to be targeted?	The domain NYSIF.com is all that will be provided the discovery is part of the external test.
16	N/A	1.4	For the Internal Threat Simulation, how will access be granted (e.g., on-site presence, VPN)?	For the internal portion of the pentest ip ranges will be provided.
17	N/A	1.4	For the Wireless Testing, are there specific wireless networks or SSIDs that should be targeted?	There is one location - To Be Discussed at kickoff meeting.
18	N/A	1.6	Should social engineering be included in either the internal or external threat simulations?	To be discussed during kickoff. Some examples are Wi-Fi, USB drops or Business email compromise attempt.
19	N/A	1.6	What types of AI-enhanced tools will be employed, and are there any restrictions on automated scanning or analysis?	We do not allow any tools which will collect and then publicly expose our potential vulnerabilities. AI tools should not exceed the boundaries of standard pentest, like excessive traffic generation. All tools should be monitored and controlled by a person.
20	N/A	1.6	How will the results of AI-enhanced research be validated or cross-verified?	Any results will be compared to public industry vulnerability information, such as CVEs.
21	N/A	1.6	For the External Black Box test, are there any rules of engagement or legal boundaries we must observe (e.g., no DoS attacks)?	Yes. We will discuss during kickoff.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
22	N/A	1.6	For the Internal Grey Box test, what level of access or knowledge will be provided (e.g., network diagrams, credentials, source code)?	For the internal portion of the pentest ip ranges will be provided. Vulnerabilities identified during scanning will be in-scope for exploitation phase.
23	N/A	1.6	Are there any systems or assets explicitly out of scope for either Black Box or Grey Box testing?	Yes. We will discuss during kickoff.
24	10	Deliverables	Can all penetration testing activities, both external (black box) and internal (grey box), be performed remotely using secure VPN or virtual access, or is any on-site presence required at NYSIF facilities	Yes, according to our requirements to be discussed during kickoff.
25	7	Mandatory Requirements	Is the use of subcontractors permitted for this engagement, including for core testing roles, provided that all mandatory requirements (certifications, experience, etc.) are met and proper documentation is submitted?	Yes.
26	7	Mandatory Requirements	If subcontractors are used, can their resumes and certifications be submitted in lieu of full-time staff credentials? Are they subject to the same insurance and reporting requirements as the prime contractor?	The prime contractor has full responsibility for any subcontractors. The process of conducting the pentest is up to the awardee. The prime contractor insurance is what will be required.
27	7	Mandatory Requirements	Is there any flexibility in the certification requirement for penetration testers (e.g., CEH, CISSP, OSCP, etc.)? Can equivalent practical experience or alternate certifications be accepted in place of one of the specified credentials?	Yes.
28	10	Deliverables	Is there any flexibility in the proposed 3-week testing duration, or must all phases (planning, discovery, attack, reporting) be completed within that timeline?	Flexibility options will be discussed during kickoff.
29	10	Deliverables	Can the Executive-Level Presentation be conducted virtually (e.g., Zoom or MS Teams), or is an in-person presentation required if requested by NYSIF?	Virtual meetings are acceptable.

2025 Penetration Testing
RFQ # 2025-49-IT
Amendment 1

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
30	N/A	M/WBE	Can a firm be in process of receiving M/WBE certification, or must certification be held at the time of submission.	A firm must be New York State certified M/WBE or SDVOB at the time of submission.
31	General	General	What is NYSIF's budget for this project?	This is not material to the solicitation.
32	1	2. Purpose of this Request for Quotes	We are not located in New York State but are certified by NYS as a minority-owned business. Could NYSIF please confirm that we are eligible for this award?	If a firm has New York State certification they are eligible to bid on this opportunity.
33	7	13. Mandatory Requirements 2. Vendor must provide three samples of penetration testing of a similar size and scope.	Could NYSIF please clarify the meaning of "samples"? Should proposals include three previous project descriptions, three sample reports, or both?	Three previous projects with size, scope, brief summary and conclusion.
34	8	14. Technical Specifications, Scope, External	For the external network assessment, approximately how many IPs are active?	The domain NYSIF.com is all that will be provided the discovery is part of the external test.
35	8	14. Technical Specifications, Scope, Internal	For the internal network assessment, approximately how many IPs or subnets are in scope?	For the internal portion of the pentest IP ranges will be provided during kickoff.
36	8	14. Technical Specifications, Scope, Internal	Can all internal network testing be done from a single location?	Yes.
37	8	14. Technical Specifications, Scope, Wireless	Is the wireless network controller-based or access point-based?	To be discussed during kickoff.
38	8	14. Technical Specifications, Scope, Wireless	How many locations are in scope for the wireless assessment?	One location, specifics to be discussed at kickoff meeting.
39	8	14. Technical Specifications, Scope, AI-Enhanced Security Research	Acceptable Use of AI Technologies: The provided link is broken. Could NYSIF please provide a working link and clarify how you wish AI to be used in this project?	Please refer to the scope section of the RFQ and USE OF GENERATIVE ARTIFICIAL INTELLIGENCE (GenAI) BY BIDDERS/CONTRACTORS for AI use clarification. https://its.ny.gov/system/files/documents/2025/04/nys-p24-001-acceptable-use-of-artificial-intelligence-technologies.pdf
40	8	14. Technical Specifications / Scope / External	How many external/public-facing IPs are expected to be in-scope?	The domain NYSIF.com is all that will be provided the discovery is part of the external test.
41	8	14. Technical Specifications / Scope / External	How many FQDNs are expected to be in-scope?	NYSIF.com

2025 Penetration Testing
RFQ # 2025-49-IT
Amendment 1

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
42	8	14. Technical Specifications / Scope / External	How many public-facing web applications are expected to be in-scope?	The domain NYSIF.com is all that will be provided the discovery is part of the external test.
43	8	14. Technical Specifications / Scope / External	Do any public-facing web applications allow self-registration? If so, how many?	To be discussed during kickoff.
44	8	14. Technical Specifications / Scope / External	Do you leverage an existing cloud service providers (e.g., AWS, Azure, GCP, Okta, Salesforce, etc.)? If so, which ones and what types (e.g., IaaS, PaaS, SaaS)?	To be discussed during kickoff.
45	8	14. Technical Specifications / Scope / Internal	How many internal domains will be in-scope?	For the internal portion of the pentest ip ranges will be provided during kickoff.
46	8	14. Technical Specifications / Scope / Internal	How many IPs will be in-scope?	For the internal portion of the pentest ip ranges will be provided during kickoff.
47	8	14. Technical Specifications / Scope / Wireless Testing	How many facilities are in-scope and what are their locations?	One Location.
48	8	14. Technical Specifications / Scope	Are the facilities entirely occupied by NYSIF or are they shared with other tenants?	To be discussed during kickoff.
49	8	14. Technical Specifications / Scope	How many SSIDs are in-scope?	To be discussed during kickoff.
50	N/A	Incumbent	Could you please confirm whether there is an incumbent currently performing under this contract? If so, kindly provide the name of the incumbent and the total contract spend to date. Also, please mention what testing tools or frameworks were used by the incumbent, both internally and externally?	This is not material to the solicitation.
51	2	Submission Mode	Could you please specify the mode of submission? Is email an acceptable method for submitting this opportunity?	Yes, email is an acceptable method for bid submission.

2025 Penetration Testing
RFQ # 2025-49-IT
Amendment 1

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
52	N/A	Penetration Testing Tool Preferences & Licensing	Please confirm if NYSIF currently have preferences for specific penetration testing tools (e.g., Metasploit, Nmap, Nessus, Burp Suite), or existing licenses that a vendor may leverage during the engagement to avoid tool redundancy?	Yes, any tool may be used for the testing. Further clarification will provide if necessary during the kickoff meeting.
53	N/A	Clarification on Target Assets & Test Scope	Could you kindly confirm the estimated volume and types of assets in-scope for penetration testing? For example: -Number of public-facing web applications/IPs? -Quantity of internal servers, firewalls, switches, routers? -Wireless networks and mobile devices, if any?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.
54	N/A	Onsite vs. Remote Delivery & Offshore Restrictions	Could NYSIF please clarify: Whether parts of the work (such as planning or reporting) may be performed remotely? Whether any portion of the work can be offshored, or must all services be delivered within the Contiguous U.S. (CONUS), as stated in Section 14?	As Needed for the testing. All services must be delivered within the Contiguous U.S. (CONUS)
55	N/A	Tool Licensing Responsibility	For any penetration testing tools not provided by NYSIF, are vendors expected to cover the cost of licenses, or will NYSIF reimburse or provision them?	No.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
56	N/A	Key Personnel Availability and Substitution	If our proposed personnel become unavailable during interview or implementation due to scheduling conflicts, will NYSIF permit substitution of equally qualified alternate resources, subject to prior approval?	Yes.
57	1 of 14	3. CONTRACT TERMS & APPROVAL	**Would the NYSIF please clarify:** Are there preferred dates or planned blackout periods for the Penetration Test between the contract start and the 12/31/2025 completion date?	The awardee will be provided with the relevant information at the kickoff meeting.
58	1, 6, 12, 14	Appendix C, 30. USE OF GENERATIVE ARTIFICIAL INTELLIGENCE (GenAI) BY CONTRACTORS	**Would the NYSIF please clarify:** The RFQ states the contractor will "Use Artificial Intelligence enhanced security research tools to uncover additional risks". However, Section 11 prohibits the use of Generative AI without prior written approval. Can NYSIF clarify this potential conflict and provide examples of the types of AI-enhanced tools it expects the contractor to use?	Please refer to the scope section of the RFQ and USE OF GENERATIVE ARTIFICIAL INTELLIGENCE (GenAI) BY BIDDERS/CONTRACTORS for AI use clarification. https://its.ny.gov/system/files/documents/2025/04/nys-p24-001-acceptable-use-of-artificial-intelligence-technologies.pdf See Q 19
59	2 of 14	4. CALENDAR	**Would the NYSIF please:** Provide the primary physical location for the on-site portions of this work? The RFQ lists an Albany address for bid submission, assume this is acquisition only, but NYSIF has multiple locations, to include the Manhattan HQ address.	One location - To Be Discussed at kickoff meeting.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
60	8, 9 of 14	14. TECHNICAL SPECIFICATIONS	**Would the NYSIF please list:** All requirements, meetings, events, other than those listed "Internal", that cannot be performed remotely in order to plan travel estimate? *We will use the NYSIF HQ address to estimate travel. If there are NYSIF sites outside of a 50 mile radius of HQ that require physical presence, Would the State please provide?	NYSIF has many district offices around state and 2 main offices (one upstate and one downstate). To Be Discussed at kickoff meeting.
61	8, 9 of 14	14. TECHNICAL SPECIFICATIONS	**Would the NYSIF please provide:** Approximate number of external-facing IP addresses, web applications, and other services to be tested to support our ability to properly scope the external black box test?	The domain NYSIF.com is all that will be provided the discovery is part of the external test.
62	8, 9 of 14	14. TECHNICAL SPECIFICATIONS	**Would the NYSIF please provide:** Estimated number of internal subnets, IP addresses, and applications that are within scope of this RFQ, regarding internal grey box assessments?	For the internal portion of the pen test Ip ranges will be provided during kickoff.
63	8, 9 of 14	14. TECHNICAL SPECIFICATIONS	**Would the NYSIF please provide:** High-level overview of the technology environment in this scope, to include the number and types of assets (e.g., servers, workstations, routers, switches, firewalls, and cloud environments)?	To be discussed during kickoff.
64	9 of 14	14. TECHNICAL SPECIFICATIONS	**Would the NYSIF please clarify:** The RFQ mentions "Wireless Testing" can be performed with either the External or Internal component. What is the scope of this "Wireless Testing", including the number of wireless networks and physical locations?	One location - To Be Discussed at kickoff meeting.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
65	8, 9 of 14	14. TECHNICAL SPECIFICATIONS	**Would the NYSIF please clarify:** The RFQ states the test is "estimated to take three (3) weeks". Does this 3-week estimate cover only the "Attack" phase, or all project phases from Planning through Reporting?	Flexibility options will be discussed during kickoff.
66	8 of 14	14. TECHNICAL SPECIFICATIONS	**Would the NYSIF please clarify:** For the "Internal Grey Box" test, the level of information and access (e.g., network diagrams, user credentials) will be provided to the testing team?	For the internal portion of the pen test Ip ranges will be provided during kickoff.
67	9 of 14	14. TECHNICAL SPECIFICATIONS	**Would the NYSIF please clarify:** If NYSIF will provide dedicated technical Points of Contact (POCs) to act as the "Blue Team" for coordination during the assessment?	NYSIF will provide a point person to be in contact with the vendors testing team.
68	8	14. TECHNICAL SPECIFICATIONS	Would NYSIF be open to extending the estimated testing period from 3 weeks to up to 5 weeks, if needed?	Flexibility options will be discussed during kickoff.
69	8	14. TECHNICAL SPECIFICATIONS	What's the number of Physical Locations, Servers and Firewalls	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pen test Ip ranges will be provided during kickoff.
70	8	14. TECHNICAL SPECIFICATIONS	What Cloud Environments the Fund uses, which Email Platform and Email Protection has in place, EDR/Anti-Virus?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.
71	8	14. TECHNICAL SPECIFICATIONS	Currently the fund has an Intrusion Detection System/IntrusionPreventionSystem?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.
72	8	14. TECHNICAL SPECIFICATIONS	What's the number of Web Applications, Web pages and APIs ?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.

2025 Penetration Testing
RFQ # 2025-49-IT
Amendment 1

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
73	8	14. TECHNICAL SPECIFICATIONS	Where is the Application Hosted?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.
74	8	14. TECHNICAL SPECIFICATIONS	there is any Web Application Firewall (WAF) in place?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.
75	8	14. TECHNICAL SPECIFICATIONS	Is the Source Code Available? What's the Programming Language?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.
76	8	14. TECHNICAL SPECIFICATIONS	What's the number of User Roles	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.
77	8	14.TECHNICAL SPECIFICATIONS	Please clarify if all the phases of the project(planning, discovery, attack, reporting, executive) are expected to be completed within 3 weeks.	Flexibility options will be discussed during kickoff.
78	8	14.TECHNICAL SPECIFICATIONS - Scope	What specific systems or assets should be explicitly excluded or included in the test? - network, end points etc. Please share the volumes of the systems/assets in scope for penetration testing.	To be discussed during kickoff.
79	7	13.MANDATORY REQUIREMENTS	Please confirm if sub-contracting allowed.	Yes, provided they meet the stated requirements of the contract.
80	105	Appendix S - I. Contract Goals	Please confirm if overall goal of 6% for SDVOB participation a mandatory requirement.	A bidder must be either an NYS certified, MWBE or SDVOB vendor. The bidder must submit the waiver request for the certification type it does not possess.
81	8	14.TECHNICAL SPECIFICATIONS - Scope	Are user endpoints in scope for testing?	The awardee will be provided with the relevant information at the kickoff meeting

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
82	9	14.TECHNICAL SPECIFICATIONS - Documentation	Links for the documents under a and c are not accessible, kindly share the files a. Acceptable Use of Artificial Intelligence Technologies (NYS-P24-001) c. Accessibility of Information Communication Technology (NYS-P08-005)	https://its.ny.gov/system/files/documents/2025/04/nys-p24-001-acceptable-use-of-artificial-intelligence-technologies.pdf https://its.ny.gov/system/files/documents/2024/10/nys-p08-005-accessibility-of-information-communication-technology_0.pdf
83	11	19.REQUIRED APPENDICES AND EXHIBITS	Please confirm if Appendix J1, Appendix O and Attachment 1 are to be submitted as part of bid response or post contract award.	Appendix J1 is to be completed by the awarded vendor. Appendix O is to be submitted as part of your submission. Attachment 1 is to be completed quarterly as outlined in Form 102 located in Appendix M.
84	12	20.BID FORMAT	We understand that the Administrative Proposal should contain appendices and forms. Please confirm.	Confirmed.
85	39	Appendix B - Administrative - 39. BIDDER CERTIFICATION REQUIREMENTS - aa.	The last statement says - "The certification required above can be found on NYSIF's Bidder Certification Form, which Bidder must submit with its bid." Please share the Bidder Certification Form.	The Bidder Certification form is not required with this solicitation.
86	12	20.BID FORMAT	Please share the checklist for submission documents	Please see the list of required Appendices and Exhibits in Section 19 for the list of required documents for your Administrative Proposal. Please see Section 14 for the requirements for the Technical Proposal.
87	N/A	N/A	How many internal/external IPs, domains, and subdomains need to be tested? If internal, how many VLANs/segments are there?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.
88	N/A	N/A	For scopes that are not publicly accessible from the internet, how does NYSIF intend to give pentesters access? What types of VPN solutions are acceptable? Would NYSIF prefer it to be vendor-provided?	The awardee will be provided with the relevant information at the kickoff meeting.
89	N/A	N/A	Is any onsite testing required?	As Needed for the testing.
90	N/A	N/A	Is subcontracting acceptable?	Yes, provided they meet the stated requirements of the contract.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
91	N/A	N/A	What are the in scope networks and applications hosted?	The domain NYSIF.com is all that will be provided the discovery is part of the external test. For the internal portion of the pentest ip ranges will be provided during kickoff.
92	N/A	N/A	Are there specific compliance requirements (PCI-DSS, GLBA, SOX) that dictate testing methodologies?	Please see Technical Requirements.
93	N/A	N/A	For the grey box portion of testing, how many roles are expected to be in scope?	The awardee will be provided with the relevant information at the kickoff meeting.
94	N/A	N/A	What is the desired or expected duration of the testing period, and are there specific time of day constraints? (i.e. when should the pentests work)?	The awardee will be provided with the relevant information at the kickoff meeting.
95	N/A	N/A	Are there any maintenance windows where testing must be performed to avoid service disruptions?	The awardee will be provided with the relevant information at the kickoff meeting.
96	N/A	N/A	Are there any regulatory or legal restrictions that may impact the testing process?	The customary and normal standards for a penetration test apply, there are no additional legal restrictions.
97	N/A	N/A	Will this be a one-time test, or do you require repeated pentests throughout the year? Beyond a year?	One time test.
98	Page 8	Scope – Internal Pentest	Can you clarify the estimated number of hosts or subnets included in the internal grey-box test?	The awardee will be provided with the relevant information at the kickoff meeting.
99	Page 8	Scope – Internal Pentest	Will internal grey-box testing include access to credentials or system documentation?	The awardee will be provided with the relevant information at the kickoff meeting.
100	Page 8	Wireless Testing	Will wireless testing require on-site presence, or will remote access (VPN or other) be granted?	As Needed for the testing.
101	Page 8	Wireless Testing	Are there specific SSIDs or wireless networks identified for testing within the scope?	The awardee will be provided with the relevant information at the kickoff meeting.
102	Pages 6, 8	AI Enhanced Security Research	Can you clarify whether AI/ML tools that are not GenAI (e.g., for risk modeling or anomaly detection) are allowed without prior approval?	Yes as long as the tool is not provided NYSIF data. Any specific tools can be discussed during kickoff or posted as a public question.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
103	Page 8	Attack Phase	What is the threshold or limitation for high-impact operations such as domain admin or simulated data exfiltration?	The awardee will be provided with the relevant information at the kickoff meeting.
104	Not specified	Rules of Engagement	Are phishing or other social engineering methods permitted during the external or internal assessment phases?	The awardee will be provided with the relevant information at the kickoff meeting.
105	Page 9	Rules of Engagement	Will penetration testing take place in a production environment, or is a separate staging/test environment provided?	The awardee will be provided with the relevant information at the kickoff meeting.
106	Page 8	Timeline	Is the estimated 3-week testing duration flexible based on the scope complexity?	Flexibility options will be discussed during kickoff.
107	Not specified	Remote Work	Will internal testing require physical presence on NYSIF premises, or will VPN or secure remote access be allowed?	As Needed for the testing.
108	Page 10	Project Plan	Will the kickoff meeting be virtual or in-person?	Virtual.
109	Pages 10-11	Deliverables	Is there a required format or standard (e.g., NIST 800-115, MITRE ATT&CK) for the technical or executive summary reports?	NIST 800- 53 Rev. 5
110	Page 11	Executive Summary Presentation	Will the executive-level presentation be virtual or in-person, and who will the audience be (e.g., IT team, executive board)?	Virtual meetings are acceptable.
111	Pages 5-6	SDVOB/MWBE Participation	Can SDVOB or MWBE participation goals be met through qualified subcontractors, and how should this be documented?	No, the prime bidder must satisfy the MWBE/SDVOB requirement.
112	Not specified	Deliverable Acceptance	What are the acceptance criteria for the penetration test findings and remediation recommendations?	See Deliverables.
113	Page 8 of 14	Scope & Objectives	What are the primary goals of this penetration test? (Compliance, risk assessment, etc.)	Identify vulnerabilities.
114	Page 8 of 14	Scope & Objectives	Which assets are in scope and count? (IP ranges, applications, cloud environments, IoT devices, etc.)	The awardee will be provided with the relevant information at the kickoff meeting.
115	Page 8 of 14	Scope & Objectives	Are third-party/vendor systems connected to your network included?	No, vendors who maintain data are outside of scope.

2025 Penetration Testing
RFQ # 2025-49-IT
Amendment 1

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
116	Page 8 of 14	Testing Approach	•Threat Simulation: oScope includes External, Internal and Wireless network. Correct? oShould we use AI-enhanced tools for vulnerability discovery?	Yes to both questions.
117	Page 8 of 14	Testing Approach	•Analysis & Preparation: oBlack Box (no prior knowledge) for External or Grey Box (limited knowledge) for Internal tests? oWill you provide credentials for grey-box testing?	Yes, to the questions regarding testing requirements. NYSIF will NOT provide credentials.
118	Page 9 of 14	Rules of Engagement	•Are there restricted hours for testing (to avoid business disruption)?	The awardee will be provided with the relevant information at the kickoff meeting.
119	Page 9 of 14	Rules of Engagement	•Any off-limits systems/attack methods (e.g., no DoS, no social engineering)?	The awardee will be provided with the relevant information at the kickoff meeting.
120	Page 9 of 14	Rules of Engagement	•Is Blue Team coordination required (defenders aware of the test)?	NYSIF will provide a point person to be in contact with the vendors testing team.
121	Page 8 of 14	Logistics & Access	Will you provide VPN/network access for internal testing?	The awardee will be provided with the relevant information at the kickoff meeting.
122	Page 8 of 14	Logistics & Access	Do we need onsite presence for wireless/physical testing?	As Needed for the testing.
123	Page 8 of 14	Logistics & Access	Who is the primary contact for coordination?	NYSIF will provide a point person to be in contact with the vendors testing team.
124	Page 10 of 14	Reporting & Deliverables	What level of detail is needed in the technical report?	See Deliverables.
125	Page 10 of 14	Reporting & Deliverables	Is an executive summary required for management?	See Deliverables.
126	Page 10 of 14	Reporting & Deliverables	Preferred remediation guidance format ?	See Deliverables.
127	Page 8 of 14	Compliance & Standards	Any specific regulatory frameworks to align with? (PCI DSS, ISO 27001, NIST, etc.)	NIST 800- 53 Rev. 5
128	Page 8 of 14	Compliance & Standards	Should testing follow OSSTMM/PTES/NIST SP 800-115 methodologies?	NIST 800- 53 Rev. 5
129	Page 8 of 14	Post-Testing Support	Will there be a remediation validation phase?	No validation required. However, review and remediation clarification will be required.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
130	Page 8 of 14	Post-Testing Support	Is retesting expected after fixes are applied?	No retesting required. However, review and remediation clarification will be required.
131	Page 8/14	External	Please provide the average number of active externally facing IP addresses for the organization?	Two blocks of /24.
132	Page 8/14	External	Please provide the number of externally exposed websites or web applications that are in-scope for the external test?	The domain NYSIF.com is all that will be provided the discovery is part of the external test.
133	Page 8/14	Internal	Please provide the approximate number of servers in-scope for the internal test?	For the internal portion of the pentest ip ranges will be provided during kickoff.
134	Page 8/14	Internal	Please provide the approximate number of workstations in-scope for the internal test?	The awardee will be provided with the relevant information at the kickoff meeting.
135	Page 8/14	Internal	Please provide the approximate number of network devices and other (printers, etc.) in-scope for the internal test?	The awardee will be provided with the relevant information at the kickoff meeting.
136	Page 8/14	Wireless	Please provide the approximate number of SSID's in scope for the wireless test?	The awardee will be provided with the relevant information at the kickoff meeting.
137	Page 8/14	Wireless	Please provide the number of locations in scope for the wireless test?	One location - To Be Discussed at kickoff meeting.
138	Page 8/14	AI Enhanced Security Research	Can you describe what is intended by this research? Is it intended for the vendor to introduce AI tools into your environment, or to leverage tools that are already in the environment?	AI Enhanced Security Research– Use Artificial Intelligence enhanced security research tools to uncover additional risks.
139	9	Scope (Technical Specifications)	How many total employees are supported across all NYSIF locations?	About 2000 employees.
140	9	Scope (Technical Specifications)	How many live external IP addresses and hosts are in scope for the external black box penetration test?	Two blocks of /24.
141	9	Scope (Technical Specifications)	For the internal grey box penetration test, is the environment segmented? If so, how many segments and hosts per segment? If not, what is the total number of internal hosts?	The awardee will be provided with the relevant information at the kickoff meeting.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
142	9	Scope (Technical Specifications)	How many office locations and data centers are in scope for the internal and wireless penetration tests? Please specify addresses if possible.	The awardee will be provided with the relevant information at the kickoff meeting.
143	9	Scope (Technical Specifications)	How many wireless networks or access points are in scope for wireless testing? Are there specific locations for this testing?	The awardee will be provided with the relevant information at the kickoff meeting.
144	9	Scope (Technical Specifications)	Are there any systems, applications, or locations that are explicitly out of scope or require special handling?	The awardee will be provided with the relevant information at the kickoff meeting.
145	9	Scope (Technical Specifications)	Are there any restrictions or preferences regarding the use of AI-enhanced security research tools?	No, if used for research without sensitive NYSIF data. No preferences.
146	9	Rules of Engagement	Are there specific time windows or blackout periods when testing cannot be performed (e.g., business hours, maintenance windows)?	The awardee will be provided with the relevant information at the kickoff meeting.
147	9	Coordination / Assets	Will remote access be provided for internal testing, or is on-site presence mandatory? If on-site, at which locations?	As needed for the testing.
148	9	Reporting / Executive	Are there any specific formats or templates required for the executive summary and technical reports?	See Deliverables.
149	9	Reporting / Executive	What is the expected turnaround time for draft and final reports after testing completion? (3 weeks is mentioned in the RFQ) - Is it the complete time of delivery or just the testing?	Flexibility options will be discussed during kickoff.
150	4	Insurance Requirements	Are there any specific requirements or restrictions regarding insurance deductibles and self-insured retentions?	Insurance must meet limits and thresholds outlined in Section 8.

Question #	RFQ Page #	RFQ Section and Sub-Section Reference #/Heading	Question	NYSIF Response
151	4	Insurance Requirements	Is subcontracting permitted, and if so, are there any restrictions or approval processes for subcontractors?	Yes, provided they meet the stated requirements of the contract.
152	3	Contract Terms & Approval	Are there any additional legal or contractual clauses (beyond Appendix A) that may impact the engagement?	Appendices B, B1, and C as well as the terms outlined in the RFQ govern the terms of the engagement.
153	9	Scope (Technical Specifications)	Does the external penetration test need to be conducted as a blind test across a fixed time period and as a best effort approach?	The domain NYSIF.com is all that will be provided the discovery is part of the external test.
154	9	Scope (Technical Specifications)	Does the internal penetration test need to be conducted as an assumed breach and blind test across a fixed time period and as a best effort approach?	For the internal portion of the pentest ip ranges will be provided during kickoff.
155	9	Scope (Technical Specifications)	Do any of the applications or, APIs hosted on the external or, internal assets be explicitly tested with separate reports? If yes, please share the count.	One report including everything. See Deliverables.