NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
1	RFP Requirements	RFP Page 8, Section 7: Proposer must be a managed security services provider with at least 10 plus years of experience in providing MSS for the financial/banking sector. Will the NYS Housing Finance Agency accept at least 10 years of proven experience in providing Managed Detect and Response Services for like verticals, such as the Federal Government?	Yes, provided the Federal Government Agency/Agencies are equivalent to NYSHFA at the Federal level in providing mortgages and issuing of bonds.	1
2	RFP Requirements	As a NYS verified SDVOSB state vendor, our team can certainly meet ALL and in some sections, surpass the SECaas and MSS solutions that are required on this RFP. The only reservations we have is that the RFP wants 5 engagements within the financial and banking sector (RFP Section 9.2.1 Experience and Qualifications of the Proposer, Page 13). Within this sector we can provide numerous references/engagements, but two that are truly within the financial sector. Though one of these (financial/banking) references we will submit has over 35,000 employees. The team wanted me to ask you if you would let us submit an RFP with 5 or more engagements, but two that are truly within the financial/banking sector. We will provide others within the medical sector, educational, state and large corporate agencies to show we can certainly accommodate what is on the RFP.	The five engagements must be in the financial/banking sector.	1
3	Scope of Work	Does NY HFA have existing IDS/IPS and SIEM tool or is the MSSP expected to procure them?	The IPS/IDS and SIEM to be provided in the MSS solution.	1
4	Scope of Work	How does the agency receive the notifications regarding threats and vulnerabilities in the current state and what tools are used for monitor threats? Place?	Through the tools and SOC provided by our current MSSP.	1
5	Scope of Work	How many Agency's public facing web applications are in scope of penetration testing?	5 public Web facing applications.	1
6	Scope of Work	How often is the penetration testing expected to be performed on Agency's Wi-Fi?	As stated in the RFP, minimally once a year. Additional requests for penetration may be requested during the year if required.	1
7	Scope of Work	Who performs the periodic incident response exercises in the current state?	NYSHFA IT with the MSSP.	1
8	RFP Requirements	Pursuant to Section 14 of the RFP, "[t]he successful Proposer will be required to execute an agreement that incorporates (i) HFA's Standard Clauses for Contracts, Appendix I, ….." Some of the terms, such as a very broad indemnification obligation and the lack of a limitation on damages, appear to be significantly out-of-market, particularly with regards to State of New York contracts. May proposers submit proposed changes to the terms in their submission?	HFA's Standard Clauses for Contracts mirror NYS's Standard Clauses for Contracts; however, Proposers may submit proposed changes to the terms in their submission for HFA's consideration.	1
9	Scope of Work	#1 Wireless Network Testing: A) How many sites (locations) will be tested? B) Number of SSIDs for location#	A) 1 B) 2	1
10	Scope of Work	Or was New York State Housing Finance Agency looking instead an External PEN test? If so: A) How many external Ips are in scope? B) How many principal DNS domains are included?	Both penetration testing of the web apps and external IPs. A) Approximately 20 B) 1	1
11	RFP Requirements	Will NYS allow the ten years requirement stated in section 8.1.1 to be from an offeror that has a teaming partner with this experience? We are also referencing section 6.0 that has the following statement which we interpret as allowing such teaming to be considered (including all team members experience) in order to meet the State's requirements.	The MSSP must have 10 years experience.	1
12	Administrative	Is there an incumbent and if so will NYS please identify the incumbent as well as provide the contract information for the incumbent?	The The Agency declines to respond to this question.	1

NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
13	Scope of Work	We meet all the requirements listed in section 8 "Scope of Services ("Scope of Work")". However, there is one requirement that we need some clarifications about. It's the section 8.1.1 "… The MSSP must be able to provide SOC1/SOC2 certifications upon notice". We have SOC1 certification and ISO 27001 in lieu of SOC2 because of more international recognition. Also, ISO 27001 covers almost all that is covered by SOC2. We also have experience where SOC1 certification and ISO 27001 has been accepted as meeting the requirements where the requirements was for SOC1 and SOC2. And we believe that you would also find it meeting the requirements. It will be very helpful if you could kindly clarify.	Our Auditing standards prefers SOC1/SOC compliance, but ISO 27001 can be accepted.	1
14	Administrative	Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so- are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?	The The Agency declines to respond to this question.	1
15	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: How many physical locations?	2 physical locations. 1 Primary and 1 DR site. And 2 AWS instances.	1
16	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Do you manage your own data center, or do you utilize any 3rd- party/colocation facilities?	Yes, NYSHFA IT manages our primary and DR datacenters, however the DR site is co-located.	1
17	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Are any security products installed? If yes, please provide product name 1) Security Incident & Event Management (SIEM)? If yes, which SIEM product name and is internally or externally managed? 2) Endpoint Detection and Response (EDR) 3) Vulnerability management 4) Email Security 5) Network threat analytics	Yes to all. The proposer is expected to provide the listed products. Our products are provided by our current MSSP.	1
18	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Can you provide the number of security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each: Endpoint •Number of endpoints? •Count of Windows/Mac/Linux Desktops/servers (rough)?	The number of endpoints and servers are mentioned in the RFP section 8.3.	1
19	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Can you provide the number of security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each: Network •Number of ingress/Egress Points •Type of media connectivity •Average and Max Mbps at each Ingress/Egress point •High Level network diagram, if available	See the numbers provided in the RFP . The The Agency declines to provide our network diagrams at this stag, the diagrams will provided to the successful proposer .	1
20	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Can you provide the number of security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each: Email •How many mailboxes? •Are you currently using Office 365? If so are you using EOP/ATP?	Mailboxes are monitored by a different NYS Agency and are out of scope for this RFP.	1
21	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Can you provide the number of security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each: Current and projected number of users. •How many network users (at a workstation most of the day)? •How many users are not on the network most of the day, but authenticate with a domain controller (such as remote workers, maintenance staff, etc.)?	Numbers provided in RFP already.	1

NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
22	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Can you provide the number of security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each: Servers/Desktops •Windows Servers - HIGH EPS (~50 eps) •Windows Servers - Low EPS (~2 eps) •Windows Workstations (5 / 1k users) •Windows AD Servers •Linux Servers •DNS (enter # per 1000 users)	Numbers provided in RFP already.	1
23	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Can you provide the number of security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each: Network Infrastructure (# of devices) •Routers •Switches (NetFlow not supported) •Wireless LAN •Network Load-Balancers •WAN Accelerator •Other Network Devices	See section 8.3 in the RFP.	1
24	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Can you provide the number of security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each: Security Infrastructure •Firewall - Internet (Enter # in 1000's of users) •Network Firewalls (Partner / extranets) •Network Firewalls (DMZ) •Network IPS/IDS •Network VPN - Enter # in 100's of users •Email AntiSpam - Enter # in 100's of users •Network Web Proxy (enter # in 100's of users) •Other Security Devices	see RFP 8.3	1
25	Scope of Work	Page 9 of 34 Section 8.2 Scope of Work: Can you provide the number of security devices and other log sources to be monitored per the categories listed below? Just need the Device Qty for each: Applications (Device count assumed with numbers above) •Web Servers (IIS, Apache, Tomcat) •Database (MSSQL, Oracle, Sybase - indicate # of instances) •Email Servers (Enter # in 1000's of users) •Antivirus Server (Enter # in 1000's of users) •Other Applications (Email, DB, AV, etc.)	See section 8.3 in the RFP. The specific details will not be shared at this time, but will be shared to the successful proposer .	1
26	Administrative	Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?	The Agency declines to respond to this question.	1
27	Scope of Work	The questions below refer to the following bullet points (page 9 and 10, Section 8.2): • Periodic firewall reviews with a report and debriefing upon completion; • Periodic network health check reviews with a deliverable report and debriefing upon completion; • Periodic Deep Dark Web scanning to determine any unauthorized usage of the Agency's information or data with a deliverable report and debriefing upon completion; • Periodic Information Security Assessments ("ISA") on the Agency's Information Technology's infrastructure to include providing ISA ratings for each category in a deliverable report and debriefing upon completion 1) Could you please define "periodic" - how frequently are each of these to be performed?	Annual Firewall rules review, quarterly network health checks, bi-annual deep dark web searches, and annual ISA review.	1

NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
28	Scope of Work	(page 9 and 10, Section 8.2): 2) How many and what type (platform, version) of firewalls are the reviews to be performed on? And how many rules does each have?	2 Firewalls. The Agency declines to provide the FW details at this time..	1
29	Scope of Work	(page 9 and 10, Section 8.2): 3) What characteristics are you looking for in a “network health check”?	System life cycle, Device OS life cycle. Patch levels etc.	1
30	Scope of Work	(page 9 and 10, Section 8.2): 4) Could you provide the total footprint of the “network” for the health check?	Total number of endpoint provided in RFP section 8.3.	1
31	Scope of Work	(page 9 and 10, Section 8.2): 5) Could you define “Deep Dark Web scanning”?	Scan dark web to see if any of the Agency data have been exfiltrated and sold on the dark web.	1
32	Scope of Work	(page 9 and 10, Section 8.2): 6) Could you provide the total footprint of “the Agency’s Information Technology’s infrastructure”?	Total number of endpoint provided in RFP section 8.3.	1
33	Scope of Work	(page 9 and 10, Section 8.2): 7) Must these 4 bulleted scope items be included in the Proposal or would HFA consider another provider to fulfil just this particular scope?	The MSSP can team with a subcontractor to fulfill those items.	1
34	Scope of Work	Can you please confirm if HFA mainly use Microsoft products and technologies?	Microsoft and Linux are utilized.	1
35	Scope of Work	What are the end points you have which would be monitored? Vendor, device type, etc.	Total number of endpoint provided in RFP section 8.3.	1
36	Scope of Work	RFP Page 9 Section 8.1.2: Do you require the resources/personnel to be US-based only? If no, are there any countries where support cannot come from?	US based only.	1
37	Scope of Work	RFP Page 9 Section 8.2: Do you require management of firewall devices or just monitoring? If management, can you please provide further details, e.g. inventory, product name, product type, OS, etc.?	Monitoring only	1
38	Scope of Work	RFP Page 9 Section 8.2: What specifically is required around "Intrusion Prevention and Detection" systems? If management, can you provide further details, e.g., inventory, product name, etc.?	The MSSP should have IPS/IDS included in their solution for monitoring. The current solution is provided by our current MSSP.	1
39	Scope of Work	RFP Page 9 Section 8.2: What specific requirements are needed around "network health checks"?	System life cycle, Device OS life cycle. Patch levels etc.	1
40	Scope of Work	RFP Page 9 Section 8.1.3: Is there an existing SIEM in place? If so, can you provide details on the environment (product, appliances, log sources, EPS, etc.)?	Yes, our current MSSP provides the Agency with a SIEM. The successful proposer will be expected to provide their own SIEM solution.	1
41	Scope of Work	RFP Page 9 Section 8.1.3: If a SIEM is to be built, is there a choice on platform? What devices/applications/endpoints will need to feed into the SIEM?	Yes, the SIEM be a known and reputable platform. Cisco devices, database logs, endpoint NetFlow data.etc	1
42	Scope of Work	RFP Page 9 Section 8.1.3: Do you have a MDR platform already in place? If yes, what are the details of the implementation? If not, do you have a preference on platform?	The Agency declines to respond to this question at this time.	1
43	Scope of Work	RFP Page 9 Section 8.1.3: Do you have a vulnerability scanning platform already in place? If yes, what are the details of the implementation? If not, do you have a preference on platform?	Yes we have a vulnerability scanning platform in place which provided by our current MSSP. The successful proposer will be expected to provide their own vulnerability scanning platform.	1
44	Scope of Work	RFP Page 9 Section 8.2: How many IP addresses / assets / applications are in scope for vulnerability scanning?	approximately 1700	1
45	Scope of Work	RFP Page 9 Section 8.2: Are any operational technology (OT) or industrial control systems (ICS) assets in scope? If so, please provide details, count, etc.	No ICS or OT to monitor.	1
46	Scope of Work	RFP Page 9 Section 8.2: Are there any specific compliance mandates being satisfied or required to be satisfied with the vulnerability scanning program? (e.g. PCI DSS, NY State cybersecurity standards, etc.)	Yes to both	1
47	Scope of Work	RFP Page 9 Section 8.2: Is there a current process in place for ranking or prioritizing vulnerability data? If so, please describe it.	Yes . IT Policies, and categories based on scanning tool classification.	1
48	Scope of Work	RFP Page 9 Section 8.2: Are services for remediation management and/or governance considered to be in scope?	No	1
49	Scope of Work	RFP Page 9 Section 8.2: Is there any ticket integration already in place today for vulnerability scanning activities? If not, is this required?	No	1

NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
50	Scope of Work	RFP Page 9 Section 8.2: What is the specific driver for requiring weekly vulnerability scanning? or can that be performed monthly?	Agency IT Policies requires weekly scans.	1
51	Scope of Work	RFP Page 9 Section 8.2: For "Real-time threat intelligence especially with zero-day or emerging threats" - Is this requirement a capability of the MSSP or does the client expect to receive the threat intelligence into their threat intelligence platform?	This is referring to general weekly threat intelligence report which is expected to be provided by the successful proposer 's solution.	1
52	Scope of Work	RFP Page 9 Section 8.2: How many keywords or phrases would the client use to find unauthorized usage of the Agency's information or data in the Deep Dark Web scan?	Minimally 8	1
53	Scope of Work	RFP Page 9 Section 8.2: Related to Threat Modeling, How many applications? Does technical documentation exist? e.g. Architecture and data flow diagrams What is it's risk classification? (e.g. web facing, sensitive data-PII, financial data, privileged operations)	The Agency declines to respond to this question at this time.	1
54	Scope of Work	RFP Page 9 Section 8.2: What cloud environment is your organization using?	The Agency declines to respond to this question at this time.	1
55	Scope of Work	RFP Page 9 Section 8.2: "Continuous notifications to the Agency concerning latest and ongoing Cybersecurity threats and vulnerabilities" - does a quarterly report with the latest threats and vulnerabilities trend and recommendations meet this requirement?	No, the Agency wants the report weekly to allow the Agency to be as proactive as possible.	1
56	Scope of Work	RFP Page 9 Section 8.2: "Real-time threat intelligence especially with zero-day or emerging threats" Is this requirement a capability of the MSSP or does the client expect to receive the threat intelligence into their threat intelligence platform?	Yes it should be part of the MSS.	1
57	Scope of Work	RFP Page 9 Section 8.2: How many keywords or phrases would the client use to find unauthorized usage of the Agency's information or data in the Deep Dark Web scan?	Minimally 8	1
58	Scope of Work	RFP Page 9 Section 8.2: How many applications are in scope for pen testing and do you have a list of these sites so that we can possibly check for sizing of testing efforts if Internet facing and accessible?	We cannot provide this at this time, But based on previous Pentest its considered a 'Small'.	1
59	Scope of Work	RFP Page 9 Section 8.2: On average, how many different privilege roles exist per applications (regular user, Admin, supervisor etc.)?	The Agency declines to respond to this question at this time.	1
60	Scope of Work	RFP Page 9 Section 8.2: Is any data captured on these sites which would need to adhere to any sort mandate such as PCI, HIPAA or any sort of PII processing / storage or transmission?	Minimally PCI/PII standards	1
61	Scope of Work	RFP Page 9 Section 8.2: Are any of these apps hosted in cloud providers such as AWS, Azure, or Google Cloud?	The Agency declines to respond to this question at this time.	1
62	Scope of Work	RFP Page 9 Section 8.2: Wifi Testing - Number of locations? Number of buildings per location? Number of floors per building? What is the square footage of each building (estimate)? How many APs do you have? How many SSIDs?	The Agency declines to respond to this question at this time, but based on previous Wi-Fi Pen tests its considered a 'Small'.	1
63	Scope of Work	Technical: What are the Agency's specific technical requirements for the SECaaS solution? For example, what specific SIEM, EDR, and threat intelligence platforms does the Agency use?	The Agency declines to respond to this question at this time. MSSP to propose their own solution.	1
64	Scope of Work	Technical: How does the Agency want to integrate the SECaaS solution with its existing IT infrastructure?	The 'how to integrate' should be part of the proposal's solution by taking in consideration section 8.3 of the RFP.	1
65	Scope of Work	Technical: What are the Agency's performance requirements for the SECaaS solution? For example, what is the expected latency for incident response?	SLAs to be agreed upon.	1
66	Scope of Work	Technical: How does the Agency want to handle security incidents? For example, does the Agency have a specific incident response plan (IRP) that the MSSP must follow?	The successful proposer and the Agency will use a combined and agreed upon IRP.	1
67	Scope of Work	Technical: What are the Agency's requirements for reporting and communication? For example, how often does the MSSP need to provide status reports?	Statuses are to be provided in bi-weekly threat hunt meetings, quarterly protection review meetings and during Security trends meetings.	1
68	Scope of Work	Security: What are the Agency's specific security requirements? For example, does the Agency have any specific compliance requirements (e.g., PCI DSS, HIPAA)?	PCI/PII standards	1
69	Scope of Work	Security: Are there currently Cybersecurity Governance Policies and Standards in place?	Yes	1

NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
70	Scope of Work	Security: Is there a POA&M security policy (Plan of Action and Milestones security policy) in place?	Informal standards current exist. A formal plan will be put in place with assistance with the successful proposer .	1
71	Scope of Work	DR/Failover: What is the physical layout of the primary and DR sites?	The Agency declines to respond to this question at this time.	1
72	Scope of Work	DR/Failover: What types of security controls are in place at each site?	The Agency declines to respond to this question at this time.	1
73	Scope of Work	DR/Failover: How is data replicated between the primary and DR sites?	The Agency declines to respond to this question at this time.	1
74	Scope of Work	DR/Failover: What is the Agency's failover plan for the primary and DR sites?	The Agency declines to respond to this question at this time.	1
75	Scope of Work	DR/Failover: How often is the failover plan tested?	The Agency declines to respond to this question at this time.	1
76	Scope of Work	DR/Failover: What are the Agency's requirements for network bandwidth and latency between the primary and DR sites?	The Agency declines to respond to this question at this time.	1
77	Scope of Work	DR/Failover: What are the Agency's requirements for security logging and monitoring at the primary and DR sites?	The Agency declines to respond to this question at this time.	1
78	Scope of Work	DR/Failover: What are the Agency's requirements for access control to the primary and DR sites?	The Agency declines to respond to this question at this time.	1
79	Scope of Work	DR/Failover: What are the Agency's requirements for disaster recovery testing?	The Agency declines to respond to this question at this time.	1
80	Scope of Work	Additional: What operating systems and software applications are running on the Agency's endpoints?	The Agency declines to respond to this question at this time.	1
81	Scope of Work	Additional: What are the Agency's patch management procedures?	Standard monthly patch management and critical patches done on demand.	1
82	Scope of Work	Additional: How does the Agency currently monitor and secure its endpoints?	Through the current MSS solution.	1
83	Scope of Work	Additional: Is there an adopted and used Change Management Policy in place?	Yes	1
84	Scope of Work	Additional: Is it a must to have SOC2 certifications? Having an equivalent ISO 27001 is accepted by many agencies.	Our Auditing standards prefers SOC1/SOC compliance, but ISO 27001 can be accepted.	1
85	Scope of Work	Additional: What kind of servers are in place today?	See RFP section 8.3	1
86	Scope of Work	Are we going to manage the current security stack (EDR, SIEM, Vulnerability Management) or is this new technology with licenses? If so, what is the stack?	MSSP to provide the complete solution.	1
87	Scope of Work	What are the Data sources that will be feeding into the SIEM? (Quantities, Type, Role and function of device) See attached gathering sheet	See RFP section 8.3	1
88	Scope of Work	Approximately how many IP addresses are in use with technology behind them? (will respond to vulnerability scan).	1700	1
89	Administrative	Page 7: Can a 2-3 week extension be granted?	No	1
90	Administrative	Page 17: Are you open to proposed changes to the contract terms in our response? Specifically, we are concerned that there is no limitation of liability.	Proposer may submit substitute language for HFA's consideration.	1
91	Scope of Work	Page 9: Do you currently have an existing EDR technology deployed? If so, please confirm which technoloty. If not, do you want us to make a recommendation and plan to deploy an EDR?	MSSP to provide the complete solution.	1
92	Scope of Work	Page 9: Can you elaborate on the "Intrusion prevention and detection" requirement? E.g., should this be interpreted as managing an IPS/IDS infrastructure? If so, can you provide information on what's been deployed and the activities/role you want your MSS to provide. Or, can this simply be interpreted that you want the MSS to be able to detect threat activities and take action to prevent major impact to the organization?	Managing an IPS/IDS infrastructure, able to detect threat activities and take action to prevent major impact.	1
93	Scope of Work	Page 9: Can you expand on "Ability to conduct proactive and reactive threat hunting across all the Agency’s environments"? Are you looking for a provider that proactively develops use cases and integrates intelligence data to search for threats, and then retro-actively hunts for threats using threat indicators as part of investigations that the SOC Analysts perform? Or are you looking for provider to add additional dedicated specialized threat hunters to team that develop threat hypotheses and conduct threat hunt plans to actively search for threats?	Yes to both	1

NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
94	Scope of Work	Page 9: Will the Penetration testing be a full black box approach (No credentials) or will the app developer provide credentials and test data to the enviorment for a full penetration test?	Both approaches to be tested.	1
95	Scope of Work	Page 9: How many sites will wifi pen testing include?	1	1
96	Scope of Work	Page 9: Is there an existing NYS HFA ITSM tool to integrate the SIEM tool for auto ticketing? What is the current NYS HFA ITSM solution (if applicable)?	Currently no, but our ticketing system can be integrated with a SIEM tool.	1
97	Scope of Work	Page 9: How many applications/information systems are to be considered for ISA?	All of the Agency's systems and applications. The details of the systems/applications will be provided to the successful proposer .	1
98	Scope of Work	Page 9: Is there an already existing Control and Assessment Framework that can be extended for conducting the assessments? What are the approximate number of controls defined ?	The Agency declines to respond to this question at this time.	1
99	Scope of Work	Page 9: How many firewalls are in scope for review and types of firewalls (i.e. Palo Alto, Cisco, Fortinet, etc..)?	2 High Availability pairs	1
100	Scope of Work	Page 9: Do you currently have a tool in place for firewall reviews? If so, what?	The Agency declines to respond to this question at this time.	1
101	Scope of Work	Page 9: What scope of activities are you looking for in the network health review? Which/how many devices will be in scope for these reviews?	System life cycle, Device OS life cycle. Patch levels etc.	1
102	Scope of Work	#2 Web Application Testing: A) How many applications will be tested? B) Can our team access the application without authentication or if they need to know credentials- An example of application that does not require authentication is an online quotation service for an insurance provider. An application that does require authentication would be a banking customer portal. C) Will tests be authenticated? Y/N D) How many application roles will be tested?	A) 3 apps where 2 of the apps have 2 instances. (5 in total). B) Please rephrase your question C) Yes D) 2-3 roles for each of the applications.	2
103	Scope of Work	Periodic Deep Dark Web scanning to determine any unauthorized usage of the Agency's information or data with a deliverable report and debriefing upon completion; •What specific types of data or information are you most concerned about appearing on the dark web (e.g., financial information, personal identifying information, proprietary business information)?	Brand and product names; Internal system, project, or product names, including special projects, prototype names, and/or sensitive internal/external applications; Executive or key employee names (additional identifiers, such as email addresses and phone numbers); BIN/IIN numbers; Restricting handling caveats for sensitive/internal documents (“Confidential”, “Proprietary”, etc.); Hostile actors and actor groups known or suspected of targeting government Agencies or Financial Institutions; Malicious campaigns or operations known or suspected of targeting the Agency's Information on key executives.	2
104	Scope of Work	Periodic Deep Dark Web scanning to determine any unauthorized usage of the Agency's information or data with a deliverable report and debriefing upon completion; •How frequently would you like these scans to be conducted?	bi-annually	2
105	Scope of Work	Periodic Deep Dark Web scanning to determine any unauthorized usage of the Agency's information or data with a deliverable report and debriefing upon completion; •What level of detail are you expecting in the deliverable reports?	see 103	2
106	Scope of Work	Periodic Deep Dark Web scanning to determine any unauthorized usage of the Agency's information or data with a deliverable report and debriefing upon completion; •Who will be the primary audience for the reports and debriefings (e.g., IT team, executive leadership)? This will help us tailor the content appropriately.	see 103	2
107	Scope of Work	Periodic Deep Dark Web scanning to determine any unauthorized usage of the Agency's information or data with a deliverable report and debriefing upon completion; •Would you prefer these debriefings to be in-person, or are virtual meetings acceptable?	Virtual meetings are acceptable.	2

NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
108	Scope of Work	Periodic Information Security Assessments (“ISA”) on the Agency’s Information Technology’s infrastructure to include providing ISA ratings for each category in a deliverable report and debriefing upon completion; •Could you please specify the scope of the infrastructure that will be assessed? Are there any specific systems, networks, or applications of particular concern?	Standard type ISA subjected to banking industry, See RFP section 8.3 for number of devices.	2
109	Scope of Work	Periodic Information Security Assessments (“ISA”) on the Agency’s Information Technology’s infrastructure to include providing ISA ratings for each category in a deliverable report and debriefing upon completion; •What is your preferred frequency for these assessments?	Annually	2
110	Scope of Work	Periodic Information Security Assessments (“ISA”) on the Agency’s Information Technology’s infrastructure to include providing ISA ratings for each category in a deliverable report and debriefing upon completion; •Are there any specific standards or frameworks that you would like us to use for the ISA ratings (e.g., NIST, ISO 27001)?	Preferably NIST aligned	2
111	Scope of Work	Periodic Information Security Assessments (“ISA”) on the Agency’s Information Technology’s infrastructure to include providing ISA ratings for each category in a deliverable report and debriefing upon completion; •Could you provide further details about the categories for which you'd like ISA ratings?	See 108	2
112	Scope of Work	Periodic Information Security Assessments (“ISA”) on the Agency’s Information Technology’s infrastructure to include providing ISA ratings for each category in a deliverable report and debriefing upon completion; •Who will be the primary audience for the reports and debriefings (e.g., IT team, executive leadership)? This will help us tailor the content appropriately.	Yes IT management and executive management.	2
113	Scope of Work	Periodic Information Security Assessments (“ISA”) on the Agency’s Information Technology’s infrastructure to include providing ISA ratings for each category in a deliverable report and debriefing upon completion; Would you prefer these debriefings to be in-person, or are virtual meetings acceptable?	Virtual meetings are acceptable.	2
114	Scope of Work	Page 10, Section 8.3: How many Domain Controllers?	The Agency declines to respond to this question at this time.	2
115	Scope of Work	Page 10, Section 8.3: How many DNS/DHCP Servers?	The Agency declines to respond to this question at this time.	2
116	Scope of Work	Page 10, Section 8.3: How many Firewalls (If you can, can you please include models)?	2 HA Pairs. The Agency declines to share make and models at this time.	2
117	Scope of Work	Page 10, Section 8.3: What type of applicances are they using (11)?	The Agency declines to respond to this question at this time.	2
118	Scope of Work	Page 10, Section 8.3: Out of (100) networking devices, how many are routers, switches, WAPS?	The Agency declines to respond to this question at this time.	2
119	Scope of Work	Page 10, Section 8.3: For Penetration Testing, how many times a year (Yearly, twice a year, quarterly, etc..?)	Once annually or if there is a major change	2
120	Scope of Work	How many discrete network sites are in-scope, and how are they interconnected?	The Agency declines to respond to this question at this time.	2
121	Scope of Work	How many users are in your in-scope network(s)?	The Agency declines to respond to this question at this time.	2
122	Scope of Work	Are you using any virtual infrastructure? If yes, which virtual technology are you using?	The Agency declines to respond to this question at this time.	2
123	Scope of Work	Do you have cloud infrastructure deployed? If yes, which cloud infrastructure architecture are you using, i.e. Azure, GCP, AWS, private?	AWS	2
124	Scope of Work	Are you using O365 or M365? What license type are you utilizing, i.e. E3, E5, etc? How many employees have mailboxes?	Not in scope	2
125	Scope of Work	If you are using Micrsoft Azure, are you under one tenant or several tenants?	Not applicable.	2
126	Scope of Work	Are you using SIEM today? If yes, which one? Is it managed in-house or via an external vendor?	MSSP to provide their SIEM Solution.	2
127	Scope of Work	Are there requirements for log retention? If yes, how long do you need to retain logs and for what purpose?	Yes, 3 years	2
128	Scope of Work	What is the Event(s) Per Second generated by your current security technology infrastructure set, e.g., total EPS generated by your firewalls, servers, applications?	20 MB internet traffic	2

NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
129	Scope of Work	Do you have compliance requirements which must be met on a periodic basis, e.g. PCI-DSS, GDPR, etc?	PCI-DSS	2
130	Scope of Work	What is the size of your current Security Operations team, and what roles/responsibilities are fufilled by them?	The Agency declines to respond to this question at this time.	2
131	Scope of Work	What is the current security technology tool set you use today, e.g. anti-virus, firewalls, IDS/IPS, NDR, etc? Please provide as much detail as possible indicating the brand and quantities	The Agency declines to respond to this question at this time.	2
132	Scope of Work	Do you require hands-on device management for your existing infrastructure, i.e., your firewalls, etc?	No	2
133	Scope of Work	Which endpoint technology are you using on your workstations and servers?	The Agency declines to respond to this question at this time.	2
134	Scope of Work	What is the operating system of your workstations and servers?	Windows workstations, and Windows and Linux servers.	2
135	Scope of Work	Do you have a vulnerability scanning tool in place today? If yes, which one?	MSSP to provide their vulnerability management solution.	2
136	Scope of Work	Please elaborate on the "periodic deep dark web scanning" requirement. What exactly do you require?	See question 105	2
137	Scope of Work	Are you using a network detection and response tool today? If yes, which one?	Yes, but MSSP to provide their detection solution.	2
138	Scope of Work	How many applications are in-scope for penetration testing? Are these transaction applications which require user credentials to access? Is credit card information accepted through these applications? How many user roles are in play for each application? What type of testing is required – black box or grey box testing?	3 external applications, no credit card transactions, both black and grey box testing.	2
139	Scope of Work	Do you require infrastructure penetration testing? How many public facing IP addresses are in-scope for testing?	The Agency declines to respond to this question at this time. But from previous PenTests its considered a "small"	2
140	Scope of Work	Please detail the Wi-Fi infrastructure in place today and that's in-scope for testing. Is this Wi-Fi network located in one place or distributed across a geography, i.e., throughout NY?	one location.	2
141	Scope of Work	What frequency of testing is required for the applications, Wi-Fi network, and infrastructure?	once annually.	2
142	Scope of Work	Please detail the FW reviews that are needed. Should the reviews cover the FW rules only, or be more complete to include any patches that are required to address vulnerabilities? What is the frequency of these reviews?	FW rules and vulnerabilities. Once annually	2
143	Scope of Work	Please elaborate on the "network health check reviews" that is required. What is the exact ask, and what aspect of the network is in-scope for this? What is the frequency of these reviews?	System life cycle, Device OS life cycle. Patch levels etc.	2
144	Scope of Work	Please elaborate further on "Information Security Assessments on the Agency's Information Technology's infrastructure". Is this an assessment of People-Process-Technology or a security architecture assessment? If the latter, is the assessment specific to the Agency's on-premises, cloud, or hybrid infrastructure? What is the frequency of these assessments?	Standard type ISA subjected to banking industry, See RFP section 8.3 for number of devices. Once annually	2
145	Scope of Work	Do you have an incident response plan and team already in place? Please detail the "periodic incident response exercises" that are required. Is this a periodic tabletop exercise for the Agency to ensure the incident response plan works or do you need to an incident response plan because one does not exist?	We will utilize a combination of MSSP and Agency internals to for IRP. IRP to be done once annually,	2
146	Scope of Work	What is the level of interaction and effort expected between the selected security vendor and the Agency? 100% effort from the Vendor inclusive of remediation or a collaborative approach between the vendor and the Agency?	MSSP provides reporting, and agency staff does remediations.	2
147	Scope of Work	Does the Agency require that security monitoring and the provision of other services be from the US only or can these services be provided from elsewhere, e.g., Canada?	US based only.	2
148	Scope of Work	Does the Agency require that the vendor and its staff have and/or maintain security clearances specific to the US?	No, US government clearences are not required.	2
149	Scope of Work	What is the anticipated service term, i.e., 1 year, 3 years, etc?	5 Year contract with options to extend to 10 years.	2
150	Scope of Work	Do you require us to leverage your existing security controls such as IDS,IPS,WAF,FW, etc., to respond and mitigate attacks and threats, or just the EDR?	MSSP is required to provide IDS. IPS, EDR.	2

NEW YORK STATE HOUSING FINANCE AGENCY

Request for Proposals (RFP) for Managed Security Services

Questions and Answers - Updated November 27, 2023

Number	Topic	Questions	Answers	Posted Round
151	Scope of Work	Do you want to have access to the security platform for yourself to view the dashboards, etc?	YES we require access to security platform.	2
152	Scope of Work	Are we solely relying on established frameworks such as OWASP Top 10 and MITRE ATT&CK for threat modeling, or do we also need to construct our own threat modeling output based on the unique requirements and context of our system and operations?	Yes to all. We will also accept outputs based on each unique systems or operations.	2