HESAA 2024 Request for Proposals
Managed Securities Services (RFP)
Potential Contractor's Questions & HESAA's Answers

Below are the responses to questions received which were relevant to the present procurement:

1. Can the Authority provide more guidance on the budget allocated for the cybersecurity services and any limitations or constraints?

   The budget will be determined based on the selected vendor.

2. Are there any cost breakdowns or pricing structures that bidders should be aware of?

   There are no specific cost breakdowns or pricing structures.

3. What specific cybersecurity services are included in the scope of the contract?

   The contract includes, but is not limited to, the following specific cybersecurity services:
   - **DNS Monitoring, Filtering, and Response Service and Management;**
   - **Managed Endpoint Detection and Response;**
   - **Next-Generation Firewall Installation, Configuration, and Management;**
   - **Managed Vulnerability Scanning and Assessment;**
   - **24/7 Threat Monitoring, Detection, and Response;**
   - **Managed Security Information and Event Management (SIEM) Solution; and**
   - **Intrusion detection and prevention (IDS/IPS).**

4. Can the Authority provide more details on its current cybersecurity infrastructure and challenges?

   The Authority's current cybersecurity infrastructure includes the above mentioned services. Challenges include limited human resources. The selected vendor shall manage the various security services to supplement the in-house cybersecurity personnel that the Authority employs.

5. Are there any specific compliance requirements or regulations that the cybersecurity services need to adhere to?

   The selected vendor shall comply with all applicable New Jersey and Federal laws and regulations apply.

6. How many users are expected to access the systems or services covered by the cybersecurity contract?

   HESAA estimates up to 300 users will access the systems or services covered by the cybersecurity contract.

7. Are there different categories of users (e.g., internal staff, external partners) that need to be accounted for separately?

   All end-users are internal staff.

8. Are the users primarily located within a single physical location (e.g., campus) or distributed across multiple sites?

   All end-users are primarily located in a single physical location with remote access through VPN when needed.

9. Do any users work remotely or access systems from off-campus locations?

   Yes. Users work remotely several times a week through VPN technology and a virtual desktop environment.

10. Are there specific tasks or activities that must be conducted on-site, or can they all be done remotely?

    Cybersecurity activities can be conducted remotely with the appropriate security measures in place.

11. How many users do you have?

    The Authority expects to have approximately 250 users.

12. What is the total quantity of Endpoint Detection & Response (EDR) endpoints to be deployed in the environment? (Total endpoint quantity should include servers and workstations/laptops that will have EDR agents installed.)

    HESAA estimates that there will be up to 400 EDR endpoints deployed in the environment.

13. How many total IP addresses will be included in the Managed Vulnerability Scanning and Assessment?

    Approximately 400 IP addresses will be included in the Managed Vulnerability Scanning and Assessment.

14. How many IP based network devices are there in your environment (routers, switches, printers, IOT, other?

    The Authority has approximately 550 IP-based network devices within its environment.

15. Are you interested in patching devices as well? If so, please provide details on which devices you would like to have patched through the service (Servers, Workstations, etc.)

    The Authority will not require patching services.

16. For NGFW firewalls, please provide total # of make/models and whether they are deployed in an HA pair.

    HESAA currently has two ASA's 5555 firewall configured in Active/Standby. HESAA also uses FirePower modules for IPS.

17. For NGFW firewalls, how are they managed (individual, manager, etc.)?

    ASA are individually managed. FirePower is managed by HESAA's current third-party managed security services provider.

18. Are you utilizing Microsoft Cloud Security? If so, how many O365 users are licensed in the environment? What type of Microsoft licensing to you have (e.g. E5)?

    No, the Authority is not utilizing Microsoft Cloud Security.

19. Can you please confirm that you wish to execute a 2-year agreement but want the ability to terminate for convenience with 30-day notice? If yes, are payment terms to be monthly or annually?

    Yes. The Authority confirms that it wishes to execute a 2-year agreement, but maintains the discretion to terminate for convenience with 30-day notice. Payments can be monthly, quarterly, or annually.

20. Can you please provide a network diagram or detailed description of your network topology so that we can quote the appropriate number of managed firewalls and managed network detection and response solution?

    For security purposes HESAA cannot provide a diagram or description of network topology without a signed agreement in place. See the response to question 16 regarding the number of firewalls.

21. How many endpoints do you have in your environment (PCs, Servers, Virtual Machines)?

    The Authority has approximately 550 endpoint users within its environment.

22. Are there any EDR or Cloud Platforms that you would like us to integrate with and support?

    The contracted vendor will need to integrate and support CrowdStrike Falcon and Cisco Umbrella.

23. How many firewalls do you have and what is the i/f of your firewall(s)? 1G / 2G / 10G / 40G? Copper? Fiber?

    HESAA has two ASA 5555 firewalls, and the interfaces are 1G.

24. Are there existing systems in place for the requested services other than the Cisco devices/services?

    Yes. Other than the Cisco devices/services, the existing system in place for the requested services is CrowdStrike Falcon.

    a) If so, does HESAA prefer to keep or replace existing systems, and can you identify the existing systems?

       The Authority prefers to keep existing systems.

    b) If so, is Cisco the preferred vendor for the NGFW even if alternatives can integrate?

       Yes, Cisco is the preferred vendor.

25. Can you provide more detail on your network, such as:

    a) Number of physical locations requiring NGFW?

       There is one physical location requiring NGFW.

    b) Is all Internet access to be routed through the NGFW?

       Yes. All Internet access is to be routed through the NGFW.

    c) Are there VPNs or dedicated routes between locations?

Yes. There are VPNs or dedicated routes between locations.

d) Network diagram?

Please see the response to Question 20.

e) Number and type of endpoints?

There are approximately 550 endpoints including laptops, virtual machines, ESXi hosts, switches, servers, and routers.

f) Wireless networks to be included in protection services?

Yes. There is one wireless network.

g) Cloud services utilized?

No. There are no cloud services to be utilized at this time.

h) Any IOT or mobile devices?

Yes. There are IOTs and/or mobile devices.

26. How many firewalls are in scope for monitoring / management? Are they in HA pairs? What model of firewall are these appliances?

HESAA has two ASA's 5555 firewall configured in Active/Standby. HESAA also uses FirePower modules for IPS.

27. How many domain controllers are in the environment?

There are two domain controllers in the environment.

28. How many users does the organization have today?

The Authority has approximately 250 users.

29. Are you leveraging Entra ID / Azure AD today? Is this setup as a hybrid environment with M365 today?

No. The Authority is not leveraging Entra ID/Azure AD. There is currently no hybrid environment with M365.

30. How many endpoints are in scope for monitoring/Managed Endpoint Detection & Response (i.e. servers and desktops/laptops)?

    There are up to 350 endpoints in scope for monitoring/Managed Endpoint Detection & Response.

31. How many Windows servers are in the environment today?

    There are up to 190 Windows servers in the environment today.

32. How many Linux/Unix servers are in the environment today?

    There are five Linux/Unix servers in the environment.

33. Are there other security controls / identity management platforms / SaaS applications in the environment that providers should include in the scope of their MDR solutions? Please list them out with associated quantities (i.e. user count, appliance count, etc.).

    Other security controls within the scope of MDR solutions include CrowdStrike Falcon, which has up to 350 endpoints.

34. Does the organization currently have an EDR solution in place? If so, what is in place today? If something is in place, is organization open to alternatives?

    The Authority's current EDR solution is CrowdStrike Falcon. The Authority is not open to alternatives.

35. How many full time employees does HESSA have?

    The Authority has approximately 250 full-time employees.

36. How many users, servers and physical sites are in scope for this engagement?

    HESAA utilizes up to 550 pieces of equipment, and there is one physical site.

37. Please describe your on-prem server infrastructure.

    HESAA's on-premises server infrastructure includes: Node VXRails for Servers, 5 Node VXRails for VDI, 4 Blade VRTX Chassis. IDPA backing up the VMs, 3 Node Nutanix cluster for Servers, 3 Node Nutanix cluster for VDI, 6 R710s, and p5600 SAN VMWare system.

38. Please describe your cloud environment, if any.

The Authority does not use a cloud environment.

39. Can you provide a network diagram?

Please see the response to Question 20.

40. Is Cisco technology used for all of your DNS, EDR, Firewalls, IDS/IPS? Else please detail.

Yes, HESAA uses Cisco technology for DNS, Firewalls and IDS/IPS. HESAA uses CrowdStrike Falcon for EDR.

41. If something is in place, is organization open to alternatives?

The Authority is not open to alternatives to its existing DNS, EDR, Firewalls and IDS/IPS.

42. Which tools are leveraged currently for vulnerability Scanning, Threat Monitoring, and SIEM?

HESAA utilizes a third party for managed security.

43. What is your current solution? Would you like us to assume management, or replace it?

HESAA's current solution is managed security provided by a third-party organization, and HESAA is not looking for the selected vender to assume management.

44. Do you require full MDM for end user devices? If so, company owned, user owned, or both?

HESAA does not require full MDM services.

45. What do you use for ticketing?

HESAA's vendor provides the ticketing system and relays the security issues to HESAA.

46. What is your current rate of security tickets?

The current rate of security tickets is 20 per month.

47. What percentage of them are false positives?

The percentage of false positives is 75%.

48. Do you have requirements regarding engineering resources' residency?

The Authority does not have requirements regarding engineering resources' residency.

49. Do you own or intend to retain your current cybersecurity technology, systems, software, etc.? If so, is there an existing provider now?

HESAA owns some of its software and systems, the rest is provided by the selected vendor.

50. What is the number of endpoints you're planning to protect? How many servers versus other devices?

The number of endpoints the Authority is planning to protect is up to 550. Approximately 100 endpoints are servers.

51. Can any of the contractors or services be delivered remotely?

Yes, the services can be delivered remotely.

52. Do you know the ingest volume of alerts? Do you know how many alerts come in daily that are actionable?

HESAA does not know the ingest volume of alerts or how many alerts that come in daily are actionable.

53. What are the number of log and type of log sources? Cloud or on-prem, etc?

HESAA's current vendor manages the logs.

54. Any architecture diagrams that you would be willing to share?

Please see the response to Question 20.

55. What type of ticketing system are you using today? Will we need to integrate into that system?

Please see the response to Question 45.

56. What is your ultimate goal of this Security service?

The Authority's ultimate goal for this security service is to protect HESAA's IT environment 24-hours a day, 7-days a week, and 365-days a year.

57. Do you have a desire/requirement for on-site services, personnel, technology? Would US only be required or off-shore services allowed for any portion of the services?

    HESAA does not require on-site services or personnel. All services must be conducted within the United States.

58. Are there specific certifications or qualifications you require? E.g. Compliance or certification requirements not already mentioned?

    HESAA requires the selected vendor to comply with all applicable standard New Jersey and Federal laws and regulations.

59. Any existing solutions for IPS IPDR that we would be working with or providing the whole solution? Any cloud providers for Intrusion Prevention or solutions like Azure or OKTA, etc.

    The selected vendor shall provide the whole solution.

60. Are you using DNSSEC?

    The Authority is not using DNSSEC.

61. Do you currently subscribe to Threat Feeds? What feeds? Would you continue to subscribe to these feeds or rely on the MSSP threat feeds?

    The Authority does not currently subscribe to Threat Feeds. HESAA relies on MSSP threat feeds.

62. Do you have any required/escalated SLAs we should consider? Do all agencies have the same SLA requirements or should we consider differentiated SLA service catalogs?

    The Authority requires 24-hour SLA for standard threats and one hour SLA for mission critical threats.

63. Would SOC2 Type 2 suffice to meet requirements?

    Yes, SOC2 Type 2 is sufficient to meet HESAA's requirements.