Virginia Lottery | 600 E. Main St. | Richmond, VA 23219 | ph: 804.692.7100 | fax: 804.692.7102 | valottery.com

ADDENDUM NO. 1 TO ALL OFFERORS:

Reference: Request for Proposal: **RFP# 7710MS**

Commodity: **Security Operations Center and Managed Detections & Response**

Dated: **November 2, 2022**

All offerors are required to acknowledge all RFP addenda in their proposals.

*The Lottery has created a Technology Summary to provide additional environment and workload information that can be provided on an individual basis by email request to Matt Sullivan.

**The Lottery has received numerous questions in reference to workload and metrics. While the Lottery has answered many of these in the Technology Summary, it is recognized that not all have been provided. The Lottery is actively working on gathering more information to provide a complete Technology Summary based on questions asked and will provide that to Offerors who have requested the Technology Summary once it is complete.

1st Round of Questions and Answers

1. Q: Total host inventory count for:
   a. # Of Servers and type, application, database, and operating systems
   b. # Of Workstations/laptops, on prem or remote
   c. # Of Firewalls / and Total number of network devices
   d. # Of syslog servers

   A: See Technology Summary

2. Q: What is the daily log file ingest size?

   A: Unknown, this is a new installation.

3. Q: Other App's to monitor

   A: Please clarify the question

4. Q: Total employee count

   A: See Technology Summary

5. Q: Total number of IP's to be monitored, logged, etc

   A: See Technology Summary

6. Q: What is vulnerability scanning and management?

   A: See Technology Summary

7. Q: Will the scanning tools or process change?

   A: See Technology Summary

8. Q: Total number of IP's to be monitored, logged, etc

   A: See Technology Summary

9. Q: What is vulnerability scanning and management? Will the scanning tools or process change? What is the retention policy for log files?

   A: See Technology Summary – The Lottery will retain log files within its Azure Sentinel instance and configure the organizational defined retention for log files.

10. Q: Other than host logs ingested into SEIM, what other logs are to be ingested into SEIM for monitoring?

    A: See Technology Summary

11. Q: Does "dedicated" mean that the assigned resources cannot support any other customers? If no, would you approve of resources that support a maximum of 2-3 clients?

    A: Dedicated means the Lottery interacts with the same Cybersecurity Advisor or Technical Account Manager. The Cybersecurity Advisor or Technical Account Manager can support other accounts, the Lottery requires consistency in who handles our account rather than speaking to a different resource each interaction with the service provider.

12. Q: Alliance Technology Group is a partner of Arctic Wolf. We believe strongly in their managed SOC. Arctic Wolf is the industry leader in Managed Detection & Response. Would the VA Lottery consider a replacement for Azure Sentinel?

    A: No

13. Q: Please specify the average daily volume of log data ingested in the SIEM solution. Additionally, please specify the approximate yearly growth volume of log data

    A: Unknown, this is a new installation of Sentinel SIEM.

14. Q: Please provide the number and type of log sources integrated with your SIEM.

    A: See Technology Summary

15. Q: Please provide the number of additional data sources that Virginia Lottery requires the vendor to integrate with SIEM. Please provide details of non-integrated log sources/systems for monitoring.

    A: See Technology Summary

16. Q: Please specify the number of use cases / rule sets are currently enabled and actively monitored/used

    A: See Technology Summary, however it is expected the provided numbers will grow and the Lottery is seeking guidance from the awarded vendor on specific use cases

17. Q: Please specify if you have any threat intelligence data feeds integrated and used within the SIEM solution. Kindly share the threat intelligence data feeds

    A: The Lottery currently does not have threat intelligence feeds incorporated into its Azure Sentinel instance.

18. Q: Please specify the average monthly volume of alerts (total volume of alerts L1/2 would need to triage, analyze, escalate, support)

    A: Unknown, this is a new installation of Sentinel SIEM.

19. Q: Please specify the false positive rate for alerts that are monitored

    A: Unknown, this is a new installation of Sentinel SIEM.

20. Q: What is the average incident / tickets volume over the last three months?

    A: This is a new installation of Sentinel SIEM.

21. Q: Please specify your ticketing/workflow system. Are monitoring alerts integrated with the ticketing/workflow system? If not, do you expect the vendor to perform this integration?

    A: No expectation for integration with Lottery ticketing system.

22. Q: Please specify if you have an established escalation/response runbooks for the vendor to follow or expect the vendor to create them as part of this effort.

    A: The Lottery has a current internal escalation procedure defined. It is expected the vendor will assist in the creation of more thorough automated runbooks as part of this effort.

23. Q: Does the state expect the vendor to perform remediation, containment, or response actions? Please specify the average monthly volume of such actions

    A: Yes, the Lottery expects guidance from the vendor in defining remediation, containment and response actions as part of the resulting Contract.

24. Q: Please specify the total number of endpoints (including servers) in your environment

    A: See Technology Summary

25. Q: Please specify the total number of servers in your environment

    A: See Technology Summary

26. Q: Please specify the number of endpoints where the Endpoint Detection and Response (EDR) solution is enabled. Additionally, please specify if the EDR alerts are integrated and monitored within the SIEM solution.

    A: See Technology Summary

27. Q: Please specify the total number of employees and contractor staff in your organization.

    A: See Technology Summary

28. Q: Please specify the current staffing level for the different capabilities within your Security Operations. E.g., Number of 24X7 analysts and associated levels (L1, L2, L3), Number of content engineers, 24X7 Threat hunting team, Dedicated Incident response team, % that is offshore if any?

    A: The purpose of this RFP is to establish 24x7 security operations capability

29. Q: Please specify if the state has an existing Continuity of Operations (COOP) for security operations that vendor can use to update with our service capability

    A: Yes

30. Q: Does the Lottery have the expectation of achieving or maintaining a security compliance standard (e.g., SOC, GDPR, NIST, ISO, other)?

A: Yes, the Lottery has the expectation of being compliant with the Commonwealth of Virginia Security Policy and Standards which closely aligns with NIST. See Link: Policies, Standards & Guidelines | Virginia IT Agency

31. Q: What is the estimated number of endpoints that will be monitored? An endpoint is a computer, server (virtual or physical), switch, etc., that the Lottery intends to be covered by the monitoring services.

    A: See Technology Summary

32. Q: How many on-premises locations will be monitored?

    A: See Technology Summary

33. Q: Are local and/or remote users permitted to use personally owned devices (e.g., computers, phones, tablets) to access Lottery IT Systems? Is Lottery anticipating installing monitoring agents on those devices?

    A: Yes, BYOD is allowed via limited access unless additional access is granted. Installation of monitoring on those devices would be under review.

34. Q: When was the last security assessment conducted?

    A: Calendar Year - Q1 2022

35. Q: Have there been breaches or attacks on Lottery IT Systems in the past? Were any of these successful?

    A: Like all organizations the Lottery is under constant attack from bad actors. Because of the current security measures in place, to the best of our knowledge and validated by our current threat detection tools, none of these attacks have been successful.

36. Q: Does the Lottery have any expectation of monitoring and analyzing operational lottery-specific data and transactions?

    A: No

37. Q: 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?

    A: No incumbent or previous incumbent company.

38. Q: How many physical locations?

A: See Technology Summary

39. Q: Specify the VLAN details how many is included in the Scope?

    A: See Technology Summary

40. Q: How much (%) of the infrastructure is in cloud?

    A: See Technology Summary

41. Q: In the IT department/environment, how many employees work?

    A: See Technology Summary

42. Q: Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

    A: The Lottery manages its own data center.

1. Q: Are any security products installed? If yes, please provide product name
    - A. Security Incident & Event Management (SIEM)? If yes, which SIEM product name and is it internally or externally managed?
    - B. Endpoint Detection and Response (EDR)
    - C. Vulnerability management
    - D. Email security
    - E. Network threat analytics

    A: See Technology Summary

2. Q: Can you provide the number of the 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)?

    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

    Email
    - How many mailboxes?
    - Are you currently using Office 365? If so, are you using EOP/ATP?

    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)?

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)

Network Infrastructure (# of devices)

- Routers
- Switches (netflow not supported)
- Wireless LAN
- Network Load-Balancers
- WAN Accelerator
- Other Network Devices

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

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)

A: See Technology Summary – Detail of number of users is not available at this time, Lottery is continuing to work through a complete answer.

43. Q: Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?

A: This information is not available.

44. Q: Does an out-of-state MBE from Massachusetts have the same advantage as a Virginia SwaM?

A: Yes, but must be registered with Virginia Department of Small Business and Supplier Diversity SBSD

45. Q: Is there a budget identified for this project that you can share?

    A: See answer to question 43

46. Q: What are the key drivers for establishing a 24/7 security monitoring service? (select all that apply)
    a. Compliance requirement □
    b. Critical component of business cyber security strategy/program/roadmap □
    c. Requirement was highlighted by a previous cyber security compromise □

    A: A and B

47. Q: Is monitoring required across multiple geographical regions? If so, what are the locations?

    A: No

48. Q: Do you have any data retention requirements (EG PCI)?

    A: Question needs clarification for relevancy

49. Q: What is the makeup of your current security team, if any?

    A: The Lottery does not have a SOC, however there is a security team made up of Information Security Manager, Information Security Analyst, Network Security Specialist

50. Q: Do you have an incident response plan? What is your process for responding currently if not?

    A: Yes

51. Q: Is Microsoft Defender Endpoint Detection and Response (EDR) deployed to 100% of your environment?
    a. If not, what is the estimated % of coverage.

    A: No, not all of our devices, see Technology Summary

52. Q: Do you use any other cloud environments in addition to Microsoft Azure?
    a. Amazon Web Services □
    b. Google Cloud Platform □
    c. Other (please specify):

    A: No

53. Q: Estimated total number of EPS (Event Per Second) or GB/day of logs generated (if known).

54. A: Unknown, this is a new installation of Sentinel SIEM.

55. Q: *If using EPS, what is the average log size, or type of log?*
    a. Preferred delivery model
    b. Consumption/as-a-Service ☐
    c. Own the SIEM platform ☐

    A: Unknown TBD

56. Q: Is the Lottery open to consider non-US based options to provide these 24 /7 services - Delivery model can either be fully offshore (3 shifts remote with a dedicated TAM in US) or hybrid model (1 shift in US SOC , other 2 non-US SOC)

    A: Yes

57. Q: Please share the details of assets that are currently integrated with McAfee SIEM and expected to be transitioned to sentinel? (Device type / count of devices/Ingestion rate)

    A: See Technology Summary

58. Q: Please share the details of assets that are NOT integrated with sentinel and must be newly integrated with Sentinel
    (Device type / count of devices/Ingestion rate)

    A: See Technology Summary

59. Q: Please share the breakdown of your log sources in the sheet named " Sentinel SIEM - Sizing Details" that Lottery expect to have them integrated to Sentinel

    A: All relevant information is included in the Technology Summary

60. Q: What is the timeline lottery expecting to complete this migration after project kick off - Both transition from McAfee and new integration to Sentinel?

    A: TBD

61. Q: Does lottery have the license in place to use Logic Apps as a SOAR or expect the offeror to bring our 3rd party SOAR

    A: Yes, the Lottery isM365 E5 licensed

62. Q: What is the expected year on year growth in the Lottery infrastructure that you anticipate? This will be in terms of

    A: TBD

63. Q: What existing software delivery mechanisms in place (like SCCM) to distribute the agent across all in scope systems?

    A: The Lottery uses SCCM and Intune

64. Q: How many locations exist for all in scope systems to integrate with Sentinel?

    A: Approximately 10, See Technology Summary for actual locations

65. Q: We assume VA Lottery, presently having M365 E5 license for all their users and deployed (MDE, MDO, MDI, MCAS,
    MIP, AAD, Intune etc). Please confirm our understanding.

    A: Yes

66. Q: Can you please share the number of log Analytics workspaces and location (on-prem, Azure, AWS, GCP, etc), and the number of subscriptions/tenants?

    A: See Technology Summary

67. Q: Please confirm if "Defender for the cloud" is rolled across all your cloud (Azure, AWS, GCP) and on-prem workloads?

    A: No, Defender for cloud is not currently deployed for On-Prem devices, however Lottery is evaluating a future roll out.

68. Q: Please provide clarity on current Azure Arc implementation. Does VA Lottery require the Azure Arc full capability as Hybrid Multi-cloud Management Platform (Features like provisioning, MACD, monitoring, automation, and end-to- end management of Azure, AWS, GCP etc)? or does VA Lottery require using Azure Arc to only provision Defender for cloud for non-Azure workloads?

    A: The Lottery is moving toward the implementing Azure Arc and may require assistance

69. Q: Under Pricing section, there is a line item on Implementation price for assets currently on Sentinel – Our understanding is to evaluate Lottery's current Sentinel Implementation and assess if the Log source configuration are in line with best practices and this line item do not include onboarding additional devices. Pls confirm if this understanding, correct?

    A: This is correct, that line item is for reviewing and correcting the Lottery current sentinel instance

70. Q: On page 28 of the RFP document, under PRICING section - we understand Lottery is requesting for MDR and IR pricing separately. However, Our MDR offering includes Incident response services and we usually offer "Incident Response Retainer" hours under Labor category. Is lottery ok to include 24 / 7 Monitoring + Incident Response + Threat hunting under MDR pricing and "Retainer hours” (breach response / crisis management) under IR labor category?

    A: Offerors can provide additional pricing models as long as the pricing model in RFP is completed as provided.