1. For the requirement: Review configuration settings of current security products. Identify risks and recommend configuration modifications or products to enhance the general security posture. **- Can the Lottery provide an overview of scope, including number of security products in use, and number of system configurations in scope?**
Tripwire IP360, FortiNet security fabric with FortiSandbox, Telemetry and Compliance with FortiClient Endpoint Management, Symantec Endpoint Protection and Malwarebytes. Windows Defender AV on some devices. The Lottery has 2 FortiGate 61F firewalls and a pair of FortiGate 600D firewalls.

2. For the requirement: Review network architecture design and compare to best practices including a review of network device configurations and security settings. Review firewall configurations. Identify risks and make recommendations to improve network security**. - Can the Lottery provide an overview of scope, including the number of environments, and devices per environment?**
35 servers, 100 workstations, 50 iPads, 8 printers, 2 mobile phones. The Lottery has 2 FortiGate 61F firewalls and a pair of FortiGate 600D firewalls (managed by the ICN), Juniper switches at HQ (managed by the ICN) and Cisco equipment in the regional offices and central warehouse (managed by Scientific Games).

3. For the requirement: Provide an assessment of remote access infrastructure for accessing internal resources using VPN and of devices connecting to the ILOT network. **- Can the Lottery provide insight into the assessment of 'devices connecting to the network'?**
40 Laptops owned by Lottery and operated by staff, Lottery owned and managed iPads and personal computers owned by staff that can only RDP to Lottery owned and managed workstations. Newer laptops (~10) are configured to establish the VPN connection and then have direct access to network resources.

4. For the requirement: Review configuration and perform risk assessment on infrastructure servers (i.e. Domain Controllers, SQL DB servers, file servers, web servers). Identify risks and make recommendations. - **Can the Lottery provide insight into the scope and scale of this effort, in terms of the number of devices and number of unique configurations to be reviewed and assessed?**
There are 3 Domain Controllers and 4 file servers. The internal applications server "APPS" is SQL Server 2019 on WIndows Server 2022 with SQL and IIS functions combined. There is a test APPS server as well. There is a development IIS server and development SQL server that both host dev versions of ialottery.com. There is also a Great Plains server, a Jira server, and SFTP server.

5. For the requirement: Perform a scan of the Lottery's internal network, including servers, for presence of malware, viruses, and/or rouge software and indicate detections. - **Can the Lottery provide insight into the scope and scale of this effort, in terms of the number of networks/subnets, and number of hosts/IPs on those networks and subnets?**
There are ~10 subnets, 29 servers, approximately 100 workstations which include our remote locations and 8 printers. On the security subnet there are 5 video servers, 50 cameras, 1 SFTP server, 1 physical access control appliance (S2 Netbox), 1 privileged access management appliance (BeyondTrust), and 3 Windows 10 jump points.

6. For the requirement: Conduct a secure code review for web application source code - **Can the Lottery provide insight into the scope and scale of this effort, in terms of the number of unique code sets, and an approximate number of lines of code?**
We have approximately 3,000 pages on the main website and 200 pages on the mobile site, which included PDF files for game rules, etc. Our pages are usually under 100 lines of code, although there are a few that are larger.

7. For the requirement: Conduct a review of server and workstation baseline configuration of security settings **- Can the Lottery provide insight into the scope and scale of this effort, in terms of the number of unique configurations?**
The Lottery has 4 different server levels. Server 2012, Server 2016, Server 2019 and server 2022. Workstations range from Windows 10 (Ver 2004) to Windows 11 Due to the fact that Lottery personnel numbers are limited and each user has specific and shared tasks, there is no standard config. There is at least one Windows 7 workstation.

8. Can the Lottery provide insight into the scope and scale of the environment, including approximate server, workstation, and other devices (network, endpoints such as mobile devices, etc.?
35 servers, 100 workstations, 50 iPads, 8 printers, 2 mobile phones. The Lottery has 2 FortiGate 61F firewalls and a pair of FortiGate 600D firewalls (managed by the ICN), Juniper switches at HQ (managed by the ICN) and Cisco equipment in the regional offices and central warehouse (managed by Scientific Games).

9. For the deliverable of a network diagram - Can the Lottery clarify if an accurate and current network diagram exists? We believe the Lottery desires a proposed/future state network diagram (assuming there are recommended changes), is the creation of a current state network diagram included in this effort? If so, are there requirements around electronic format, file type, or other requirements related to the format of the diagram?
We do have some diagrams currently. We would like a future state network diagram if changes are recommended.

10. For the policy review, can you identify the number of policies, procedures are in place to review?
~10

11. For mobile device review, is the scope mobile phones or all mobile device types (laptop/tablet/phone)?
All mobile devices.

12. Is there a centralized logging and monitoring system in place for all locations or does each location have its own system and process?
No centralized logging. Some Security systems send logs to SYSLOG server. We use PRTG for monitoring.

13. Is there an expectation for the testing team to scan and perform vulnerability assessments on cloud providers?

Not necessarily the cloud provider, but we do have instances of servers in the cloud (AWS) that need security review.

14. Does the lottery make use of a hardening guideline for their systems and equipment? If so, are systems all configured the same (for example, Windows 10 desktops would all be configured the same way)?
Considering expanded use of Group Policy to harden servers and workstations. PCs are all set up using a basic configuration but are specialized depending on department and use.

15. As it pertains to the requirements for "Review configuration settings of current security products. Identify risks and recommend configuration modifications or products to enhance the general security posture," can you confirm if the Lottery is looking for a risk based configuration assessment based on critical asset data flow or a vendor assessment. If the objective is more a vendor assessment, please provide a list of the vendor security products in scope.
Tripwire IP360, FortiNet security fabric with FortiSandbox, Telemetry and Compliance with FortiClient Endpoint Management, Symantec Endpoint Protection and Malwarebytes. The Lottery has 2 FortiGate 61F firewalls and a pair of FortiGate 600D firewalls. Windows Defender AV on some devices.

16. As it pertains to the requirement for "Perform a scan of the Lottery's internal network, including servers, for presence of malware, viruses, and/or rouge software and indicate detections," can you confirm if the Lottery has a CMDB solution that has approved software? If not, will the proponent be provided with a list of what the Lottery already considers to be rogue/unsanctioned software?
No CMDB. There is currently no list of rogue/unsanctioned software.

17. Does the Lottery have an existing AV solution in place. If so, which vendor/solution is the Lottery using?
Yes. We use FortiClient Endpoint Management System along with Fortinet Security Fabric FortiNet Sandbox including Telemetry and Compliance, Symantec Endpoint Protection and Malwarebytes. Windows Defender AV on some devices.

18. As it pertains to the requirement for "Conduct a secure code review for web application source code," can you provide the number of applications in scope and the type of code (i.e., programming language)
1 external public-facing site and 1 internal site.

19. What MDM solution is the Lottery currently using?
Citrix Endpoint Management Xenmobile.

20. Would the Lottery consider extending the response deadline an additional week or two to allow for vendors to provide a more informed response?
Yes.

21. The services listed in this RFP will most likely take more than 30 business days to complete upon execution of the contract. What is driving that timeframe? Is there any flexibility?

Yes.

22. Will Iowa Lottery allow the vendor to use a remote testing solution to complete many of the technical phases being requested within this RFP?
Yes.

23. Approx. how many systems (workstations, servers, network devices, etc) does Iowa Lottery have?
40 laptops, 100 workstations, 6 esx hosts, 6 Juniper switches, 4 Cisco switches, 2 Cisco routers.

- Approx. how many people would you anticipate us needing to talk for the risk assessment phase to cover the domains listed within the RFP (i.e. asset / device management, patch management, etc)
  ~5

24. Is the IT / IS function centralized within Iowa Lottery?
Yes.

25. Have policies and procedures been developed and centralized?
Yes.

26. Are cloud services being used? If so, please describe.
Google Drive. Tripwire IP360 using a local device that sends data to the cloud. Our ialottery.com website is hosted at AWS with vendor eWay. Malwarebytes and FortiNet security fabric use cloud data.

27. **Review configuration settings of current security products:** List the products (including version) which would be in-scope for this testing.
Tripwire IP360, FortiNet security fabric with FortiSandbox, Telemetry and Compliance with FortiClient Endpoint Management, Symantec Endpoint Protection and Malwarebytes. Windows Defender AV on some devices. The Lottery has 2 FortiGate 61F firewalls and a pair of FortiGate 600D firewalls.

28. **Review of network device configurations and security settings**. List the # of devices including type and version that would be in-scope for this testing (e.g. 2 Cisco 5500s, 1 Juniper MX480, etc).
2 FortiGate 61F firewalls
1 FortiGate 600D firewall
2 Juniper switches at HQ
4 Cisco routers
4 Cisco switches

29. **Review firewall configurations**: List the # of firewalls including type and version included within scope of this review.
2 FortiGate 61F firewalls
1 FortiGate 600D firewall

30. **Provide an assessment of remote access infrastructure –** What remote access solutions are currently in-place that would be in-scope for this phase?
Currently we use FortiClient VPN with MFA enabled. 20 Laptops owned by Lottery and operated by staff, Lottery owned and managed iPads and personal computers owned by staff that can only RDP to Lottery owned and managed workstations. Newer laptops (~10) are configured to establish the VPN connection and then have direct access to network resources.

31. **Review configuration and perform risk assessment on infrastructure servers –** List the # of servers including type and version included within scope of this testing (e.g. 1 Server 2016 AD Domain Controller, 1 SQL Server 2019, etc). Sampling would be the recommended approach to execute on this phase.
There are 3 Domain Controllers and 4 file servers. The internal applications server "APPS" is SQL Server 2019 on WIndows Server 2022 with SQL and IIS functions combined. There is a test APPS server as well. There is a development IIS server and development SQL server that both host dev versions of ialottery.com. There is also a Great Plains server, a Jira server, and SFTP server.

32. **Penetration testing –** List the approx. # of live external and internal systems that would be included within scope of this testing.
1 domain with workstations and servers (~150 total devices). 1 public facing website, 1 internal site, and ~10 public IP addresses.

33. **Perform a scan of Lottery's Internal network for presence of malware –** This would most likely be performed by using an agent based solution that requires installation on all in-scope systems. Please confirm that this would be an acceptable approach and how many systems would likely be included in-scope for this phase.
We would prefer to not have additional software installed on Iowa Lottery systems.

34. **Conduct a secure code review for web application source code and perform a scan of all internal and external IP addresses for OWASP Top 10 vulnerabilities and indicate deficiencies***:* How many applications are included in-scope for both the static code review and the application vulnerability scanning? It should be noted that RSM partners with 3rd party provider Veracode to perform static code analysis. Support depends on the coding language and framework used for each in-scope applications. That information does not need to be provided now.
1 external public-facing site and 1 internal site.

35. **Conduct a review of server and workstation baseline configuration of security settings***:* How many domains are in-scope for this testing? What workstation operating systems are in-scope for this testing?
1 domain. The Lottery has 4 different server levels. Server 2012, Server 2016, Server 2019 and server 2022. Workstations range from Windows 10 (Ver 2004) to Windows 11 and at least 1 Windows 7 workstation.

36. **Review mobile device configuration and management system:** List the product including type and version.
iPads - devices that are in the MDM currently

37. **Review log management and auditing system:** List the product including type and version.
For some security systems we currently use Kiwi Syslog v.9.8.0 as a log repository.

38. **Evaluate effectiveness of current vulnerability management system:** List the product including type and version.
Tripwire IP360. Effectiveness is medium.

39. **Perform discovery on Lottery Wi-Fi network***:* How many sites are in-scope for this testing?
One.

40. In regards to the following service, “Conduct a secure code review for web application source

code and perform a scan of all internal and external IP addresses for OWASP Top 10

vulnerabilities and indicate deficiencies”:

Typically, clients have their own tools for source code scanning and generally do not

grant access to the vendor. Would the vendor review the results of the client source

code scans, or is the client allowing the vendor to perform code scans?

We would allow code scans.

41. What is the context in terms of the size of the environment (e.g., # of servers, operating system and database versions, web applications, internal/external IP address, firewalls, etc.)?
1 domain across 5 locations within Iowa. 1 backup/DR site. 35 servers, 100 workstations, 50 iPads, 8 printers, 2 mobile phones. The Lottery has 2 FortiGate 61F firewalls and a pair of FortiGate 600D firewalls (managed by the ICN), Juniper switches at HQ (managed by the ICN) and Cisco equipment in the regional offices and central warehouse (managed by Scientific Games). There are 3 Domain Controllers and 4 file servers. The internal applications server “APPS” is SQL Server 2019 on WIndows Server 2022 with SQL and IIS functions combined. There is a test APPS server as well. There is a development IIS server and development SQL server that both host dev versions of ialottery.com. There is also a Great Plains server, a Jira server, and SFTP server.

42. Will testing need to be performed during off normal business hours?
Doubtful.

43. Will the client provide testing credentials to perform scans?
Yes.

44. Will scanning also include Scientific games and MUSL systems?
No.

45. Is there an anticipated timeline for when the Lottery would like to complete this project? Is there any flexibility or ability to discuss the 30-day requirement for the final deliverable to be provided after the commencement of the project?
Yes. Fiscal year.

46. What is the total number of internal AND external IPs being tested? (If unsure, CIDR notations will suffice). **192.168.25.0/24, 192.168.32.0/24, 192.168.40.0/24, 192.168.9.0/24, 192.168.16.0/24, 192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24, 192.168.5.0/24**

47. Is the penetration test required for a specific compliance standard? (If yes, what standard).
Not necessarily.

48. For internal Pen test, should the testing occur as a trusted domain user?
Prefer both, otherwise as a trusted user.

49. For external, should testing occur as an untrusted outsider?
Yes.

50. Will testing be done during or after business hours?
Depends. Any test/dev systems can be tested during regular hours. Production systems may need to wait until after business hours.

51. In the event the system is penetrated, should the testers proceed? (no further tasks, perform a local vulnerability assessment, or attempt to gain the highest privileges).
Perform a local vulnerability assessment and report.

52. Is any on-site assessment or data gathering needed at the two business to business partner locations?
No.

53. For how many web applications do you want a source code review performed?
www.ialottery.com (external) and apps.iowa-lottery.com (internal)

54. How many wi-fi locations are to be tested?
One. The wi-fi network at Lottery HQ.

55. Are the wi-fi locations relatively close to each other?
Wireless access points are distributed throughout HQ.

56. How many SSIDs are to be included in the testing?
Two. Lottery-Guest and Lottery-802.1x

57. How many of the following are in-scope:
- Servers (virtual and physical)? **10 physical servers + 30 VMs**

- Mobile devices? **~50**
- ICS firewalls? **2**
- Network perimeter firewalls? **Yes.**

58. Is the Iowa Lottery HQ wireless network also within scope?
Yes.

59. Do you currently have a Lottery network drawing that can be reviewed as a starting point for the new drawing?
Yes.

60. Is the public copy of the report to be a redacted or "cleansed" report?
It will be for anyone asking for a report and the vendor does not want certain language going outside the Iowa Lottery.

61. If we have undergone recent background checks for other lotteries, will additional background checks be required?
Up to VP of Security.

62. May work be performed remotely?
Yes.

63. You request a secure code review for web application source code. How many applications are in-scope?
   a. How large is each application in-scope?
   b. Number of static pages?
   c. Number of dynamic pages?
   d. How many roles are to be analyzed?
   e. How many lines of code?

We have approximately 3,000 pages on the main website and 200 pages on the mobile site, which included PDF files for game rules, etc. Our pages are usually under 100 lines of code, although there are a few that are larger.

64. Are any of the servers to be assessed in a Cloud vendor's control?
Yes, ialottery.com is at AWS. eWay is the vendor.
- If so, has the vendor agreed to technical testing of the servers?
  No. Not yet.

65. How many servers are to be included in the baseline configuration of security settings review?
A sample is likely sufficient.

66. How many workstations are to be included in the baseline configuration of security settings review?
We have ~100 workstations total

67. Are all mobile devices of one type?
No, but mostly iPads.

68. How many different versions of each type of mobile device are in-scope?

Devices that are in the MDM.

69. How large are the in-scope log files?
Do not keep centralized log files

70. How long are log files kept?
Until overwritten

71. Does the Lottery have a written cyber security strategy?
We have written cyber security strategy goals

72. How old is the Lottery's cyber security strategy?
2 years

73. Does the Lottery have ransomware prevention software installed?
Yes.

74. Page 3, Item 13.0. Will you accept a redacted copy of our proposal to be used in the event a request for public records is made?
Yes

75. What is the budget for this project?
We have no budget for this RFP.

76. Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? If so - are they eligible to bid on this project and can you please provide incumbent contract number, dollar value and period of performance?
There was a previous incumbent who did this work for us several years ago. Yes, they are eligible to bid on this current RFP. Dollar amount was around $20,000.00.

77. Specify the VLAN details how many is included in the Scope?
~10. 192.168.25.0/24, 192.168.32.0/24, 192.168.40.0/24, 192.168.9.0/24, 192.168.16.0/24, 192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24, 192.168.5.0/24

78. Can you please provide current number of infrastructure details (Physical Server, Virtual Server, Network Devices etc.
4 Physical servers, 2 VMware UCS/San nodes (production and test) There are 28 virtual servers plus the security and bomgar servers. 1 cisco switch

79. Approximately how many computer endpoints do you have (desktop PCs, laptops, servers)?
Approximately 120 endpoints.

80. Can you tell the total number of endpoints you want protected?
All of them.

81. What's your headcount of users (employees + contractors+interns)? What number/percentage of your workforce resides within organizational facilities? What number/percentage works remotely?

112 FTE's, 3 interns, 0 contractors.

82. How much (%) of the infrastructure is in cloud?
Some file storage and sharing does occur on Google Drive.

83. What is the size of the IT environment?
29 servers (approximately 12 terabytes) SAN storage = 25 terabytes, Server network consists of 2 SQA?UCS combos 1 for production and 1 for tes/replication storage. A 3rd node is under development for DR,

84. How many physical locations?
Five locations: HQ (Clive), Region 2 (Cedar Rapids), Region 3 (Mason City), Region 4 (Storm Lake), Central Warehouse (Ankeny), backup/DR site.

85. What is the aggregate Internet Capacity per location (<300mbps, <1gbps, <4gbps, up to 10gbps)?
Regional offices and Central Warehouse have 10 Mb each back to HQ and HQ has a 20 Mb Internet connection.

86. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?
We manage our primary data center at Lottery HQ and an offsite backup data center with ICN at JFHQ.

87. What is the approximate budget?
There is no budget at this time.

88. Does the Lottery follow a specific security framework (e.g., NIST CSF, WLA-SCS:2016, etc.) that we should plan on using for the network security assessment?

Not currently, but NIST is preferred