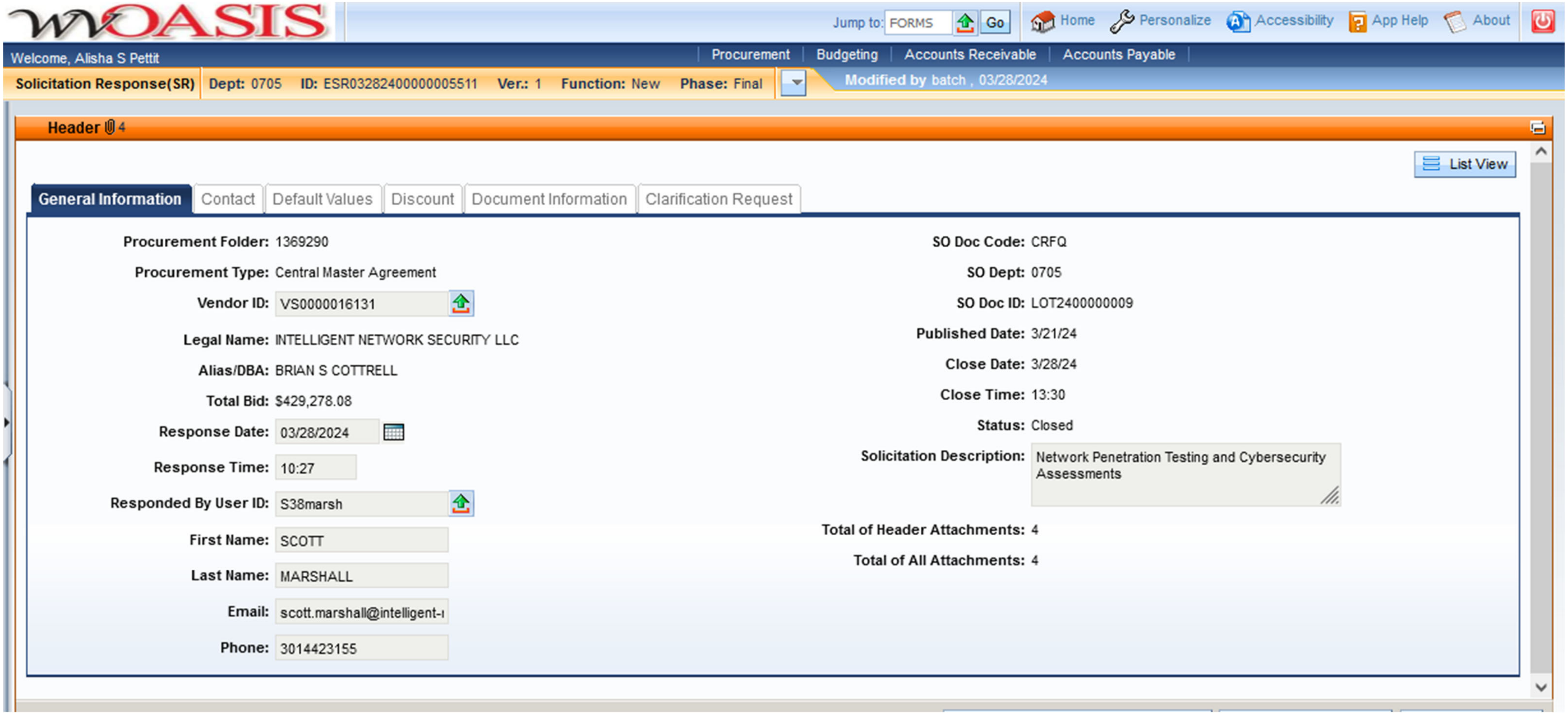
# West Virginia Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Welcome, Alisha S Pettit

Solicitation Response(SR) Dept: 0705 ID: ESR03282400000005511 Ver.: 1 Function: New Phase: Final

Modified by batch , 03/28/2024

Header 4

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: VS0000016131

Legal Name: INTELLIGENT NETWORK SECURITY LLC

Alias/DBA: BRIAN S COTTRELL

Total Bid: $429,278.08

Response Date: 03/28/2024

Response Time: 10:27

Responded By User ID: S38marsh

First Name: SCOTT

Last Name: MARSHALL

Email: scott.marshall@intelligent-i

Phone: 3014423155

SO Doc Code: CRFQ

SO Dept: 0705

SO Doc ID: LOT2400000009

Published Date: 3/21/24

Close Date: 3/28/24

Close Time: 13:30

Status: Closed

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Total of Header Attachments: 4

Total of All Attachments: 4

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

# State of West Virginia
# Solicitation Response

| | |
|---|---|
| **Proc Folder:** | 1369290 |
| **Solicitation Description:** | Network Penetration Testing and Cybersecurity Assessments |
| **Proc Type:** | Central Master Agreement |

| Solicitation Closes | Solicitation Response | Version |
|---|---|---|
| 2024-03-28 13:30 | SR 0705 ESR03282400000005511 | 1 |

**VENDOR**

VS0000016131
INTELLIGENT NETWORK SECURITY LLC

**Solicitation Number:** CRFQ 0705 LOT2400000009

**Total Bid:** 429278.08000000000162981450557 **Response Date:** 2024-03-28 **Response Time:** 10:27:52

**Comments:**

**FOR INFORMATION CONTACT THE BUYER**
Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

**Vendor Signature X** **FEIN#** **DATE**

**All offers subject to all terms and conditions contained in this solicitation**

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Ln Total Or Contract Amount |
|---|---|---|---|---|---|
| 1 | External Network Penetration Testing | | | | 91537.60 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Commodity Line Comments:**

**Extended Description:**

See Attached Specifications and
Exhibit - A Pricing Page

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Ln Total Or Contract Amount |
|---|---|---|---|---|---|
| 2 | Website Penetration Testing | | | | 91537.60 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Commodity Line Comments:**

**Extended Description:**

See Attached Specifications and
Exhibit - A Pricing Page

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Ln Total Or Contract Amount |
|---|---|---|---|---|---|
| 3 | Internal/Client-Side Network Penetration Testing | | | | 123101.44 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Commodity Line Comments:**

**Extended Description:**

See Attached Specifications and
Exhibit - A Pricing Page

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Ln Total Or Contract Amount |
|---|---|---|---|---|---|
| 4 | Wireless Penetration Testing | | | | 123101.44 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Commodity Line Comments:**

**Extended Description:**

See Attached Specifications and
Exhibit - A Pricing Page

# Appendix A

Executive Summary Example

Technical Report

Findings Presentation

Table of Contents

# 1.0 Executive Summary Example

1 Overview of testing results section
2 Summary report of the scope and approach
3 Findings
4 Key points of strength in the assessed infrastructure
5 Recommebndations

## 2.0 Technical Report Example

1. Detail of each vulnerability type discovered along with a critical, high, medium or low risk rating
2. How the vulnerability was discovered
3. The potential impact of its exploitation
4. Recommendations for remediation
5. Vulnerability references

After performing the penetration test of the WV Lottery website, INS found [fill in the blank] evidence of penetration based on analysis of provided logs and external scanning activities.

- **Finding Number:** The unique application-generated security finding number.
- **IoC:** A piece of forensic data that can indicate malicious activity on a system or network.
- **Status:** The computational lifecycle status associated with the finding. If the finding is linked to a weakness for remediation management, the finding status is computed based on the completed status of the weakness. Finding status described below:
- **Unlinked** – The finding is not linked to a weakness.
- **Active** – The finding has been linked to a weakness that has an open status.
- **Completed** – The finding has been linked to a weakness where remediation has been completed successfully (i.e., the weakness is in completed status).
- **Rejected** – The finding has been rejected either as a false positive or risk accepted (i.e. risk-based decision). No remediation is required for the security finding.
- **Source:** The finding type such as vulnerability assessment, security audit, compromise assessment, etc., and the failed security control in which the finding was created.
- **Risk:** The finding description. This is the description of the finding as defined from the vulnerability assessment, security audit report, or from the results of an internal security review.
- **Business Impact Statement:** Impact of the finding to the organization if exploited.
- **Likelihood:** The likelihood that the finding will be exploited (High, Moderate, or Low).
- **Impact:** The impact to the organization if the finding is exploited (High, Moderate, or Low).
- **Risk Level:** The computed risk level associated with the finding based on the selected likelihood and impact. Risk Exposure Ratings for details.
- **Recommended Corrective Action:** The recommended control(s) needed to remediate the finding.
- **Reference:** Hyperlink to an external source in which the IoC is listed.

# 3.0 Findings Presentation

Note: This presentation will be provided in Power point

Areas to be covered in the Presentation will include:

1. Summary
2. Findings
3. Recommendations
4. Summary

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

# State of West Virginia
# Centralized Request for Quote
# Service - Prof

| | | |
|---|---|---|
| **Proc Folder:** | 1369290 | **Reason for Modification:** |
| **Doc Description:** | Network Penetration Testing and Cybersecurity Assessments | Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration a..... See Page 2 for complete info |
| **Proc Type:** | Central Master Agreement | |

| **Date Issued** | **Solicitation Closes** | **Solicitation No** | **Version** |
|---|---|---|---|
| 2024-03-21 | 2024-03-28 13:30 | CRFQ 0705 LOT2400000009 | 2 |

**BID RECEIVING LOCATION**

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

**VENDOR**

**Vendor Customer Code:**

**Vendor Name :**

**Address :**

**Street :**

**City :**

**State :** **Country :** **Zip :**

**Principal Contact :**

**Vendor Contact Phone:** **Extension:**

**FOR INFORMATION CONTACT THE BUYER**
Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

**Vendor Signature X** **FEIN#** **DATE**

**All offers subject to all terms and conditions contained in this solicitation**

**Reason for Modification:**

Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration and bid submittal compliance

| ADDITIONAL INFORMATION |
|---|
| The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery to establish a contract for Network Penetration Testing and Cybersecurity Assessments per the terms and conditions, Exhibit A Pricing Page and Exhibit B NDA, and specifications as attached. |

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| LOTTERY | | LOTTERY | |
| PO BOX 2067 | | 900 PENNSYLVANIA AVE | |
| CHARLESTON | WV | CHARLESTON | WV |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | External Network Penetration Testing | | | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Extended Description:**

See Attached Specifications and
Exhibit - A Pricing Page

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| LOTTERY | | LOTTERY | |
| PO BOX 2067 | | 900 PENNSYLVANIA AVE | |
| CHARLESTON | WV | CHARLESTON | WV |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 2 | Website Penetration Testing | | | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Extended Description:**

See Attached Specifications and
Exhibit - A Pricing Page

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| LOTTERY<br>PO BOX 2067 | | LOTTERY<br>900 PENNSYLVANIA AVE | |
| CHARLESTON<br>US | WV | CHARLESTON<br>US | WV |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 3 | Internal/Client-Side Network Penetration Testing | | | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Extended Description:**
See Attached Specifications and
Exhibit - A Pricing Page

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| LOTTERY<br>PO BOX 2067 | | LOTTERY<br>900 PENNSYLVANIA AVE | |
| CHARLESTON<br>US | WV | CHARLESTON<br>US | WV |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 4 | Wireless Penetration Testing | | | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Extended Description:**
See Attached Specifications and
Exhibit - A Pricing Page

**SCHEDULE OF EVENTS**

| Line | Event | Event Date |
|---|---|---|
| 1 | Questions due by 10:00am ET | 2024-03-21 |

# SOLICITATION NUMBER: CRFQ LOT2400000009
## Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

**Applicable Addendum Category:**

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[✓] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[✓] Other

**Description of Modification to Solicitation:**

Addendum No. 1 is issued for the following:

1) To attach vendor questions and Agency responses.

2) To attach "Doing Business - Vendor Registration and Bid-Submittal Compliance" instruction sheet.

--No Other Changes--

**Additional Documentation:** Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

**Terms and Conditions:**

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

# ATTACHMENT A

# CRFQ LOT2400000009

# Addendum No. – 1

# Vendor Questions & Agency Response

1. We have a question in regard to Section 3 Qualifications; 3.1 that requires vendors to have been in business for at least fifteen (15) years. Just to be sure, is this a requirement for the vendor (i.e., business), or for the vendor staff?

   **A1) No, this only applies to the organization. See section 3.3 and 3.4 for vendor staff requriements.**

2. Would the West Virginia Lottery consider accepting vendor submissions (or allow a waiver) who may fall short of the 15-year requirement, but can show evidence of their organization's Network Penetration Testing and Cybersecurity Assessments competence through other means rather than tenured years of service, such as accreditation through organizations such as ISO/IEC?

   **A2) No, the 15 year requirement is mandatory.**

3. **Opinion:** The competitive nature of this RFQ, requirement 4.3.1., inadvertently places highly qualified remote teams at a disadvantage. **Question:** Would the Lottery consider waiving this requirement to level the playing field for all qualified bidders?

   **A3) Clarification:** 4.3.1 of the specifications states "Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited"; **Answer: No, Vendor qualifications for this solicitation are defined in section 3. QUALIFICATIONS, specifically section 3.1.**

4. Could the Lottery agree to exclude the costs associated with visas, travel, and lodging in the eight WV locations from the financial evaluation process?

   **A4) No, vendors must submit a fixed price cost for each service on the pricing page. Separate fees are prohibited.**

5. Understanding this will help us tailor the proposals to better meet the needs, do you have preferences or restrictions on the geographical location of the consultants?

   **A5) External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.**

6. Is Data Residency in Canada acceptable?

   **A6) No, all information obtained during assessments must be stored in the continental United States. E.g. IP addresses, usernames, passwords, vulnerabilities, proof of exploitability, etc. Please note, assessments are prohibited from performing data exfiltration.**

# CRFQ LOT2400000009
# Addendum No. – 1
# Vendor Questions & Agency Response

7. Does the lottery want separate (4) Executive Summary Reports, (4) Technical Reports delivered and findings presentations after each test (External, Internal, Wi-Fi, and Website and Web Applications)?

   **A7) Correct, each type of report and findings presentation is required and separate for each type and instance of an assessment. Reports and presentations cannot be combined across assessments.**

8. Is it acceptable to provide (1) Executive and (1) Technical Report and (1) findings presentation upon conclusion of the testing?

   **A8) No, each type of report and findings presentation is required and separate for each type and instance of an assessment. Reports and presentations cannot be combined across assessments.**

9. For the Website: how many static and dynamic pages are hosted on it? And how many user roles?

   **A9) Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, and discovery phases of the service. See section 4.2.3. No roles or authenticated testing will be performed. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.**

10. For the Cisco network devices & other servers in scope: Are they wanting any build reviews, or configuration reviews performed against these?

    **A10) Yes, configuration reviews.**

11. For the Active Directory Domain: Is this part of one of the internal IP address blocks, or is it a separate network? If it is a separate network, roughly how many IPs are in this, or how many active directory users are there?

    **A11) Additional information on the AD server will be provided to the successful vendor. There are approximately 200 active directory users.**

12. 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?

    **A12) No incumbent vendor, no past contract for Lottery; Yes, if there were an incumbent vendor they would be eligible to bid unless otherwise debarred.**

## CRFQ LOT2400000009

## Addendum No. – 1

## Vendor Questions & Agency Response

**13.** Specify the VLAN details how many are included in the Scope?

**A13) 62 total VLANS across all Lottery sites.**

**14.** How much (%) of the infrastructure is in the cloud?

**A14) 0%**

**15.** In the IT department/environment, how many employees work?

**A15) This information is not for bidding purposes, neither the Purchasing Division nor the Lottery can disclose this information to the bidders at any time prior to the conclusion of the procurement process.**

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

**A16) All data centers are owned and operate by the WV Lottery.**

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

**A17) This information is not for bidding purposes, neither the Purchasing Division nor the Lottery can disclose this information to the bidders at any time prior to the conclusion of the procurement process.**

**18.** External: Estimated number of IPs/Services per assessment?

**A18) 15 external IP addresses (approximate) please see the Existing Technology Environment section.**

**19.** Internal: Estimated number of IPs/Services per assessment?

**A19) 500 internal IP addresses (approximate) please see the Existing Technology Environment section.**

**20.** Website: Estimated number of websites per assessment?

**A20) One (1), Please see the Existing Technology Environment section.**

**21.** Wireless: Estimated number of access points and IPs per assessment?

**A21) Currently 11, with a future total estimate 32 in the next 12 months. IP addresses served on the wireless access points must be authoritatively determined in the reconnaissance, mapping, and discovery phases of the service.**

# CRFQ LOT2400000009
# Addendum No. – 1
# Vendor Questions & Agency Response

22. Which Contract Vehicle, if any, would this be procured through?

**A22) Open-End Centralized Master-Agreement (CMA) with delivery orders (release orders) against the master agreement authorizing services to be delivered, and will be processed as an Agency Delivery Order (ADO).**

23. Would there be any requirements at all for having a resource on-site through any of the Pen Testing?

**A23) Yes, External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.**

24. How many dynamic pages are hosted on your website?

**A24) Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, discovery phases of the service. See section 4.2.3.**

25. Would you like authenticated testing against your website? If so, how many unique user roles are to be tested?

**A25) Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, discovery phases of the service. See section 4.2.3. No roles or authenticated testing will be performed. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.**

26. Will you require after-hours testing?

**A26) See sections 4.1.2, 4.2.2, 4.3.2, and 4.2.2 which state: Hours of operations, testing schedule, and exclusions will be determined in conjunction with the successful vendor.**

27. For the web application assessment, would you provide URL or login credentials if behind login portal to understand scope?

**A27) www.wvlottery.com Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, discovery phases of the service. See section 4.2.3. No roles or authenticated testing will be performed. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.**

# CRFQ LOT2400000009

# Addendum No. – 1

# Vendor Questions & Agency Response

28. How in-depth would you like the web application testing (i.e., basic or in-depth)?

**A28) In depth.**

29. Would the work be conducted remotely or on site?

**A29) External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.**

30. On page 40 of "CRFQ LOT24-09 Solicitation Documents.pdf", it lists 8 separate external pen-tests, internal pen-tests, website penetration tests, and wireless penetration tests. Are these per location or can some tests be shared across locations?

**A30) Clarification:** The Background Information section states the Lottery expects to consume at least one of each service annually. The pricing page lists two (2) of each type of four (4) assessments to allow the vendor to identify the fixed price cost per assessment based on potential total consumption. This number is separate and independent from the number of locations to be tested. **Answer:** Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations and are considered one assessment per consumption. **i.e.** One Wireless penetration assessment will test the wireless infrastructure at all eight (8) Lottery locations.

31. If we must test on-site from each Lottery location, are there 8 locations that must be visited?

**A31) Yes, see the Existing Technology Environment section for locations and addresses.**

32. How far apart are the 8 locations from which testing must be conducted?

**A32) Travel time can be calculated from Lottery Main Office see addresses in Existing Technology Environment.**

**Approximate times from Lottery Main Office: Mardi-Gras – 15 minutes; Bridgeport – 2 hours; Weirton – 4 hours; Greenbrier – 2 hours; Hollywood – 6 hours; Mountaineer 4 hours; Wheeling – 4 hours.**

33. If you select one internal network penetration test annually, will it include one site or all 8?

**A33) All eight (8) for each Internal/Client Side Network Penetration assessment.**

# CRFQ LOT2400000009

# Addendum No. – 1

# Vendor Questions & Agency Response

34. Are wireless tests to be conducted for all 8 locations each year? If not, for how many annually?

**A34) Yes, all eight locations must be tested for each Wireless Penetration assessment.**

35. Are we to include the CRFQ form (pages 1-3) in our proposal?

**A35) Yes, if not submitting electronically through wvOASIS fill out pages 1-3 accordingly.**

36. Are we to include the entire CRFQ in our response?

**A36) All qualified vendors SHOULD provide all requested information stated in section 3. QUALIFICATIONS with their bid, and MUST provide all information requested in section 4. MANDATORY REQUIREMENTS.**

37. Are we to submit a signed NDA (Exhibit B) with our response or is it to be submitted post-award?

**A37) You may submit with bid, however section 3.7 states "Prior to Award both parties, the Vendor and Lottery must sign".**

38. The pricing form requests pricing for 8 instances of each assessment. Is that for each of the 8 locations, or is it because Lottery intends to repeat each assessment, say, up to two times a year, over the course of a multi-year contract?

**A38) Correct, the pricing page uses an estimated consumption of two (2) assessments of each of the four (4) types per year.**

39. Is Lottery looking for detailed configuration reviews of any of the following: Firewalls, Routers/switches, VPN appliances, Windows workstations, and Windows servers?

A39) Yes

40. Is this a portal or hard copy submission? RFP section 6 states both. If this is a hard copy submission, should vendors submit 1 technical proposal and 1 cost proposal?

**A40) Yes, you may submit through wvOASIS VSS Portal at https://prd311.wvoasis.gov/PRDVSS1X1ERP/Advantage4 sign-in or sign-up and create an account; or hand delivery, as well as USPS, UPS or FEDX; you may also FAX your bid. Vendors should submit technical and cost proposals as one bid submission. Please read the RFQ thoroughly.**

# CRFQ LOT2400000009

## Addendum No. – 1

## Vendor Questions & Agency Response

41. Please specify the process for ensuring confidentiality of certain information within the proposal. Sections that contain methodologies and/or reporting pages could harm our business if they were to be disclosed to the public. Similarly, client names that are disclosed to the public could violate privacy agreements with said clients.

**A41) Please see specification section 3.7 Non-Disclosure (NDA) and Exhibit – B; also see Section 21 YOUR SUBMISSION IS A PUBLIC DOCUMENT in the INSTRUCTIONS TO VENDORS SUBMITTING BIDS (page-9).**

**(A41-continued)** ***Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.***

***DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.***

***Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled confidential, proprietary, trade secret, private, or labeled with any other claim against public disclosure of the documents, to include any trade secrets as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.***

42. Will authenticated testing be required? Will credentials be required or is the app self-register?

**A42) No, roles and authenticated testing will not be tested. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.**

43. What is the app?

**A43) There is no app, only a website.**

44. What does the app do?

**A44) There is no app, only a website.**

45. What type of data does the app handle?

**A45) There is no app, only a website.**

46. Page 31, section 4.2.4 -- RFP says any environment can be tested. Will there be a client preference?

**A46) The Lottery will designate which environment will be tested for each assessment.**

# CRFQ LOT2400000009

# Addendum No. – 1

# Vendor Questions & Agency Response

47. Page 31, section 4.2.4 -- RFP says each environment will be assessed separately. Will all need to be tested?

**A47) This will be determined at the discretion of the Lottery.**

48. Page 33, section 4.2.8 -- RFP says DoS attacks will be required as a part of testing. SCA wants to confirm they WANT an actual DoS attack to test their defenses?

**A48) Correct. Per section 4.2.8 Denial of Service Attacks are required to be included in the pricing for Website Penetration testing. The use of DoS attacks is at the discretion of the Lottery, and requires Lottery approval.**

49. Does the State Lottery anticipate that key infrastructure components will be both similar and accessible at each site? For example, each site connects to the same Domain Controller, uses primary similar file shares, etc.

**A49) For security purposes, this information will be provided to the successful vendor.**

50. The RFP explicitly forbids "Assessing locations remotely or from one central location". Can onsite personnel be augmented by a remote workforce to lower travel costs? For example, the onsite tester will facilitate a connection for a remote employee to conduct scans, thereby freeing the onsite tester to begin wireless assessments.

**A50) No**

51. Would the State Lottery accept all work to be done remotely?

**A51) No, External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.**

52. The RFP states, "The Lottery expects to consume at least one of each service annually." Clarification on this phase would be appreciated. Is it fair to assume that all onsite testing will be executed in a logistically feasible consecutively schedule (e.g. back-to-back test events)? This question is intended to predict travel costs to/from onsite testing locations.

**A52) No, different assessments are not required to be scheduled concurrently or adjacently. Pricing should reflect independent assessments.**

53. Per the Exhibit-A Pricing Page, could you please describe or expand upon the need for 8 individual assessments?

**A53) The Background Information section states the Lottery expects to consume at least one of each service annually. The pricing page lists two (2) of each type of four (4) assessments to allow the vendor to identify the fixed price cost per assessment based on potential total consumption.**

# CRFQ LOT2400000009

# Addendum No. – 1

# Vendor Questions & Agency Response

**54.** "The vendor must have been in business for at least fifteen (15) years, performing and delivering information technology cybersecurity assessments." Does this requirement apply to individuals performing the work, or to the corporate entity? Will the purchaser revise this qualification to require the corporate entity to have been in business for at least six (6) years, performing and delivering information technology cybersecurity assessments?

**A54) Applies to the corporate entity; No, the 15 year requirement is mandatory.**

**55.** Is it sufficient to include only one example executive summary report and one example technical report, or is the bid response required to include one example executive summary report and one example technical report for each service (External Network Penetration Testing, Website Penetration Testing, Internal/Client-Side Network Penetration Testing, and Wireless Penetration Testing) to be provided?

**A55) One example per report.**

**56.** Is it true that a single Assessment & Report for Internal/Client-Side Network Penetration Testing or Wireless Penetration Testing services requires onsite visits to all eight (8) Lottery locations, therefore the "Extended Amount" for each of these services should represent bidders' costs for 64 total onsite visits to Lottery locations?

**A56) No, the pricing page identifies the consumption of two (2) of each type of assessment. In this scenario that would results in two (2) each of two (2) assessments involving eight (8) sites each for a total of 32 onsite visits. (2*2*8=32)**

**57.** How many hosts would you like to have included for the External Penetration Test?

**A57) 15 external IP addresses (approximate) please see the Existing Technology Environment section.**

**58.** How many web applications are to be included in testing?

**A58) There is no app, only a website.**

**59.** What is the name of the web application(s)?

**A59) There is no app, only a website.**

**60.** How many user roles will be tested per application?

**A60) No roles or authenticated testing will be performed. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.**

## CRFQ LOT2400000009

## Addendum No. – 1

## Vendor Questions & Agency Response

61. How many dynamic pages are there per application?

    **A61) Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, discovery phases of the service. See section 4.2.3.**

62. As an estimate, how many hosts are there on the internal network?

    **A62) 500 internal IP addresses (approximate) please see the Existing Technology Environment section.**

63. How many subnets exist that need to be tested?

    **A63) 27 (approximate) please see the Existing Technology Environment section.**

64. For the internal test, will you be able to provision a non-administrator account to test assumed breach scenario?

    **A64) Yes, see section 2.12 which states, Part one simulates an attack by an untrusted outsider or an unauthenticated user without working knowledge of the Lottery's network. Part two will be performed with the low-level credentials of an authenticated user.**

65. How many wireless access points exist?

    **A65) Currently 11, with a future total estimate 32 in the next 12 months. IP addresses served on the wireless access points must be authoritatively determined in the reconnaissance, mapping, and discovery phases of the service.**

66. Is there a guest network in addition to a corporate network?

    **A66) Yes**

67. Are there multiple locations / buildings that have access points?

    **A67) Yes, see the Existing Technology Environment section for locations and addresses.**

68. Are there any unique nuances to any of these assessments that you feel is important for the testers to know before hand?

    **A68) No**

69. What are the expectations for the report?

    **A69) See sections 4.1.10 – 4.1.13; 4.2.10 – 4.2.13; 4.3.6 – 4.3.9, and 4.4.6 – 4.4.9. Please read the RFQ thoroughly.**

# CRFQ LOT2400000009

# Addendum No. – 1

# Vendor Questions & Agency Response

**70.** When are each of the assessments expected to be performed by and delivered?

**A70) See sections 4.1.2, 4.2.2, 4.3.2, and 4.2.2 which state: Hours of operations, testing schedule, and exclusions will be determined in conjunction with the successful vendor.**

**71.** Is there an expectation of these assessments to be conducted on-site? Or can they be conducted remotely?

**A71) External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.**

**72.** Is "off hours" testing acceptable?

**A72) See sections 4.1.2, 4.2.2, 4.3.2, and 4.2.2 which state: Hours of operations, testing schedule, and exclusions will be determined in conjunction with the successful vendor.**

**73.** How many total locations will be in scope for wireless testing?

**A73) All eight (8) locations must be tested for each Wireless Penetration assessment.**

**74.** Is the external website in scope for the overall external penetration test or to be considered as part of a separate Web Application Security Assessment?

**A74) No, the external website is only in scope for the Website Penetration Testing assessment.**

**75.** Please confirm that this bid response can be submitted via *wv*OASIS.

**A75) Yes, you may submit through wvOASIS VSS Portal at <u>https://prd311.wvoasis.gov/PRDVSS1X1ERP/Advantage4</u> sign-in or sign-up and create an account; or hand delivery, as well as USPS, UPS or FEDX; you may also FAX your bid. Vendors should submit technical and cost proposals as one bid submission.**
**Please read the RFQ thoroughly.**

**76.** Do we need to include the following filled out and/or signed pages with our bid response, or are these not needed at this time?

- **a.** CRFQ Page 1 – **Yes**
- **b.** CRFQ Page 23 – **Yes**
- **c.** CRFQ Page 39 – **Yes**
- **d.** CRFQ Exhibit B – **You may submit with bid, however section 3.7 states "<u>Prior to Award</u> both parties, the Vendor and Lottery <u>must sign</u>".**

# CRFQ LOT2400000009
# Addendum No. – 1
# Vendor Questions & Agency Response

77. Is it acceptable to the Lottery to submit one sample executive summary report to represent all four categories (External Network Penetration Testing, Website Penetration Testing, Internal/Client-Side Network Penetration Testing, and Wireless Penetration Testing)?

**A77) Yes, one example per report.**

78. Is the Lottery seeking an overview of our methodology and approach to each of the four categories of penetration testing in our bid response?

**A78) No, per section 3.5 which states Vendor must comply with the Center for Internet Security methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide. Vendors must provide information and evidence how they comply with the CIS methodology, OWASP Top 10 and NIST SP 800-115.**

79. Will this be a single or multivendor award?

**A79) Single award to one vendor.**

80. If at time of execution of the contract our shared staff in the proposal response aren't available, can we replace them?

**A80) Yes, must still follow the requirements in section 3. QUALIFICATIONS for vendor staff to be assigned to the project.**

## Doing Business - Vendor Registration and Bid-Submittal Compliance:

**Solicitations out for bid can be viewed by going to www.wvoasis.gov, click on Vendor Self Service, If you are using Vendor Self Service for the first time, please click on the 'SIGN UP' button to create your user account. Once account is created and the site has loaded SEARCH providing the solicitation number (*Example:* CRFQ: LOT2200000001). To the right are the closing date and time, and the time remaining to submit a bid.**

**Find the solicitation and click on Details, there you will need to click on attachments to find the specifications, terms and conditions, etc.**

**In order to submit an electronic bid, Vendors must create your user account, when prompted to pay Vendor Registration Fee, you may select "pay later" to allow the submission of electronic bids.**

**However, the vendor of the winning bid must pay a $125 vendor registration fee either by completing the application in VSS user account and paying via credit card, or by calling 304-558-2311 with credit card information, or mailing a check to:**

***Vendor Registration Section***
***WV Purchasing Division***
***2019 Washington Street East, Charleston, WV 25305.***

VENDOR REGISTRATION:
**The following is optional, not required, when submitting bids. However, Vendors who have received Notice of Apparent Bid Award are required to meet the following:**
**To conduct business in this state, according to West Virginia Legislative Rule 148 CSR1.6.1.7 agencies must verify Vendor registration status with the West Virginia Purchasing Division, West Virginia Secretary of State's Office (WVSOS) and West Virginia Tax Department (WVTD).**

**All West Virginia Agencies are prohibited from issuing a purchase order to any vendor until Vendor compliance can be verified that it has been properly registered with:**

**1. The Purchasing Division.**
**As stated above, the fee is $125 annually and can be paid with a credit card when registering in VSS. Otherwise, you may complete a WV-1 form and submit with a check to: WV Purchasing Division. www.state.wv.us/admin/purchase/forms.html**

**2. The Secretary of State's Office.**
**Registration with the WV Secretary of State's Office is required for all Vendors doing business with the State of West Virginia and may incur a fee of $100.00 depending on the business registration category.**
**Business registration with the Secretary of State falls into one of Two (2) categories:**
**a. Domestic (formed in West Virginia), or**
**b. Foreign (formed out-of- state)**

**Vendors may complete an Application for Exemption from Certificate of Authority with the WVSOS if you feel your company qualifies. Please mail the completed form and include a check for $25.00, made payable to WVSOS, along with a copy of the company's home state issued Certificate of Good Standing / Certificate of Corporation.**

**NOTE: You may also contact the WV Secretary of State's Office with your questions @ 304-558-8000**

**3. <u>The WV Tax Department.</u>**
**All entities doing business in the State of West Virginia must be registered with WVTAX and pay a one-time fee of $30.00.**
**An exemption with WV Secretary of State does not mean you are exempt from registering with the WV Tax Department.**
**If you need to speak to someone at the West Virginia Tax Department, please call 304-558-8693. NOTE: If you are using the Business4WV website to register with the WV Secretary of State and the WV Tax Department, you may do it on-line at www.business4wv.com. Please note there is a one-time fee of $130.00.**

# ADDENDUM ACKNOWLEDGEMENT FORM
## SOLICITATION NO.: LOT2400000009

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

**Addendum Numbers Received:**
(Check the box next to each addendum received)

[X] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

INTELLIGENT NETWORK SECURITY LLC
Company

Authorized Signature

3/28/2024
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

# State of West Virginia
# Centralized Request for Quote
# Service - Prof

**Proc Folder:** 1369290

**Doc Description:** Network Penetration Testing and Cybersecurity Assessments

**Proc Type:** Central Master Agreement

**Reason for Modification:**

| Date Issued | Solicitation Closes | Solicitation No | Version |
|---|---|---|---|
| 2024-03-08 | 2024-03-28 13:30 | CRFQ 0705 LOT2400000009 | 1 |

## BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

## VENDOR

**Vendor Customer Code:** **VS0000016131**

**Vendor Name :** **Intelligent Network Security LLC**

**Address :**

**Street :** **550 Hamric Lane**

**City :** **Spencer**

**State :** **West Virginia** **Country :** **USA** **Zip :** **25276**

**Principal Contact :** **Scott E Marshall**

**Vendor Contact Phone:** **301-442-3155** **Extension:**

**FOR INFORMATION CONTACT THE BUYER**
Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

**Vendor Signature X** **FEIN#** [redacted] **DATE** March 28, 2024

**All offers subject to all terms and conditions contained in this solicitation**

| ADDITIONAL INFORMATION |
|---|
| The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery to establish a contract for Network Penetration Testing and Cybersecurity Assessments per the terms and conditions, Exhibit A Pricing Page and Exhibit B NDA, and specifications as attached. |

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| LOTTERY | | LOTTERY | |
| PO BOX 2067 | | 900 PENNSYLVANIA AVE | |
| | | | |
| CHARLESTON | WV | CHARLESTON | WV |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | External Network Penetration Testing | | | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Extended Description:**
See Attached Specifications and
Exhibit - A Pricing Page

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| LOTTERY | | LOTTERY | |
| PO BOX 2067 | | 900 PENNSYLVANIA AVE | |
| | | | |
| CHARLESTON | WV | CHARLESTON | WV |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 2 | Website Penetration Testing | | | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Extended Description:**
See Attached Specifications and
Exhibit - A Pricing Page

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| LOTTERY | | LOTTERY | |
| PO BOX 2067 | | 900 PENNSYLVANIA AVE | |
| CHARLESTON | WV | CHARLESTON | WV |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 3 | Internal/Client-Side Network Penetration Testing | | | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Extended Description:**
See Attached Specifications and
Exhibit - A Pricing Page

| INVOICE TO | | SHIP TO | |
|---|---|---|---|
| LOTTERY | | LOTTERY | |
| PO BOX 2067 | | 900 PENNSYLVANIA AVE | |
| CHARLESTON | WV | CHARLESTON | WV |
| US | | US | |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 4 | Wireless Penetration Testing | | | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81111801 | | | |

**Extended Description:**
See Attached Specifications and
Exhibit - A Pricing Page

## SCHEDULE OF EVENTS

| Line | Event | Event Date |
|---|---|---|
| 1 | Questions due by 10:00am ET | 2024-03-21 |

## INSTRUCTIONS TO VENDORS SUBMITTING BIDS

**1. REVIEW DOCUMENTS THOROUGHLY:** The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

**2. MANDATORY TERMS:** The Solicitation may contain mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

**3. PREBID MEETING:** The item identified below shall apply to this Solicitation.

☑ A pre-bid meeting will not be held prior to bid opening

□ A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

**4. VENDOR QUESTION DEADLINE:** Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted emails should have the solicitation number in the subject line.

Question Submission Deadline: March 21, 2024 at 10:00am ET

Submit Questions to: West Virginia Purchasing Division c/o Brandon Barr, Buyer
2019 Washington Street, East
Charleston, WV 25305
Fax: (304) 558-3970
Email: Brandon.L.Barr@wv.gov

**5. VERBAL COMMUNICATION:** Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

**6. BID SUBMISSION:** All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through *wv*OASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through *wv*OASIS at its sole discretion. Such a prohibition will be contained and communicated in the *wv*OASIS system resulting in the Vendor's inability to submit bids through *wv*OASIS. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via email. Bids submitted in paper or facsimile form must contain a signature. Bids submitted in *wv*OASIS are deemed to be electronically signed.

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

**For Request for Proposal ("RFP") Responses Only:** Submission of a response to a Request for Proposal is not permitted in *wv*OASIS. In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal prior to the bid opening date and time identified in Section 7 below, plus ________N/A________convenience copies of each to the Purchasing Division at the address shown below. Additionally, the Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

**Bid Delivery Address and Fax Number:**
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:
BUYER: Brandon L. Barr
SOLICITATION NO.: CRFQ LOT2400000009
BID OPENING DATE: March 28th, 2024
BID OPENING TIME: 1:30pm EDT
FAX NUMBER: 304-558-3970

**7. BID OPENING:** Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by *wv*OASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time: March 28th, 2024 @ 1:30pm ET

Bid Opening Location: Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

**8. ADDENDUM ACKNOWLEDGEMENT:** Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

**9. BID FORMATTING:** Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

**10. ALTERNATE MODEL OR BRAND:** Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

□ This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

**11. EXCEPTIONS AND CLARIFICATIONS:** The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

**12. COMMUNICATION LIMITATIONS:** In accordance with West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

**13. REGISTRATION:** Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the $125 fee, if applicable.

**14. UNIT PRICE:** Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

**15. PREFERENCE:** Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

**15A. RECIPROCAL PREFERENCE:** The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

**16. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES:** For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37 and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women- owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.

**17. WAIVER OF MINOR IRREGULARITIES:** The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.6.

**18. ELECTRONIC FILE ACCESS RESTRICTIONS:** Vendor must ensure that its submission in *wv*OASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

**19. NON-RESPONSIBLE:** The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1-5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance."

**20. ACCEPTANCE/REJECTION:** The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.5. and § 148-1-6.4.b."

**21. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**22. WITH THE BID REQUIREMENTS:** In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

**23. EMAIL NOTIFICATION OF AWARD:** The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor *wv*OASIS or the Purchasing Division's website to determine when a contract has been awarded.

**24. ISRAEL BOYCOTT CERTIFICATION:** Vendor's act of submitting a bid in response to this solicitation shall be deemed a certification from bidder to the State that bidder is not currently engaged in, and will not for the duration of the contract, engage in a boycott of Israel. This certification is required by W. Va. Code § 5A-3-63.

## GENERAL TERMS AND CONDITIONS:

**1. CONTRACTUAL AGREEMENT:** Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

**2. DEFINITIONS:** As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

**2.1. "Agency"** or **"Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

**2.2. "Bid"** or **"Proposal"** means the vendors submitted response to this solicitation.

**2.3. "Contract"** means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

**2.4. "Director"** means the Director of the West Virginia Department of Administration, Purchasing Division.

**2.5. "Purchasing Division"** means the West Virginia Department of Administration, Purchasing Division.

**2.6. "Award Document"** means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

**2.7. "Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

**2.8. "State"** means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

**2.9. "Vendor"** or **"Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

**3. CONTRACT TERM; RENEWAL; EXTENSION:** The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☑ **Term Contract**

**Initial Contract Term:** The Initial Contract Term will be for a period of ONE (1) ________________________. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as ___________________________________), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

**Renewal Term:** This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to Three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

> □ **Alternate Renewal Term** – This contract may be renewed for ___________________ successive __________ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

**Delivery Order Limitations:** In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

□ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within __________________________days.

□ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _________________ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

□ the contract will continue for _________________ years;

□ the contract may be renewed for __________________ successive __________ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

□ **One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

□ **Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as __________________________________), and continues until the project for which the vendor is providing oversight is complete.

□ **Other:** Contract Term specified in ________________________

**4. AUTHORITY TO PROCEED:** Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

**5. QUANTITIES:** The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

☑ **Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

☑ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

□ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

□ **One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

□ **Construction:** This Contract is for construction activity more fully defined in the specifications.

**6. EMERGENCY PURCHASES:** The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

**7. REQUIRED DOCUMENTS:** All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

☑ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

☑ See Section 3. QUALIFICATIONS of the Specifications

□

□

□

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

**8. INSURANCE:** The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

☑ **Commercial General Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

☑ **Automobile Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

☑ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: $1,000,000.00 per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

□ **Commercial Crime and Third Party Fidelity Insurance** in an amount of: ________________ per occurrence.

☑ **Cyber Liability Insurance** in an amount of: $1,000,000.00 per occurrence.

□ **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

□ **Pollution Insurance** in an amount of: _________________ per occurrence.

□ **Aircraft Liability** in an amount of: _________________ per occurrence.

□

□

□

□

**9. WORKERS' COMPENSATION INSURANCE:** Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

**10. VENUE:** All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

**11. LIQUIDATED DAMAGES:** This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

□ ____________________________ for ____________________________________.

□ Liquidated Damages Contained in the Specifications.

☑ Liquidated Damages Are Not Included in this Contract.

**12. ACCEPTANCE:** Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

**13. PRICING:** The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

**14. PAYMENT IN ARREARS:** Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

**15. PAYMENT METHODS:** Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

**16. TAXES:** The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

**17. ADDITIONAL FEES:** Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

**18. FUNDING:** This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

**19. CANCELLATION:** The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

**20. TIME:** Time is of the essence regarding all matters of time and performance in this Contract.

**21. APPLICABLE LAW:** This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

**22. COMPLIANCE WITH LAWS:** Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

> **SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**23. ARBITRATION:** Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

**24. MODIFICATIONS:** This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

**25. WAIVER:** The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

**26. SUBSEQUENT FORMS:** The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

**27. ASSIGNMENT:** Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

**28. WARRANTY:** The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

**29. STATE EMPLOYEES:** State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

**30. PRIVACY, SECURITY, AND CONFIDENTIALITY:** The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in www.state.wv.us/admin/purchase/privacy.

**31. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**32. LICENSING:** In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

> **SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**33. ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

**34. VENDOR NON-CONFLICT:** Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.

**35. VENDOR RELATIONSHIP:** The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

**36. INDEMNIFICATION:** The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

**37. NO DEBT CERTIFICATION:** In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

**38. CONFLICT OF INTEREST:** Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

**39. REPORTS:** Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

☑ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

□ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.division@wv.gov.

**40. BACKGROUND CHECK:** In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

**41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS:** Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.

b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.

c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

    1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or

    2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

**42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL:** In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars ($50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

**43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE:** W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least $1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

**44. PROHIBITION AGAINST USED OR REFURBISHED:** Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

**45. VOID CONTRACT CLAUSES:** This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

**46. ISRAEL BOYCOTT:** Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

**DESIGNATED CONTACT:** Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) **Scott E Marshall**

(Address) **2028 Scarlet Pine Road, Dumfries, VA 22026**

(Phone Number) / (Fax Number) **301442-3155** **304-927-1649**

(email address) **scott.marshall@intelligent-network-security.com**

**CERTIFICATION AND SIGNATURE:** By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

*By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.*

__Intelligent Network Security LLC__________________________________________
(Company)

_______________________________________________________________
(Signature of Authorized Representative) _
Scott E Marshall/Executive Vice President March 28,2024____________________ _
(Printed Name and Title of Authorized Representative) (Date)
_301-442-3155/304-927-1649_______________________________________________
(Phone Number) (Fax Number)
**scott.marshall@intelligent-network-security.com**
(Email Address)

Revised 8/24/2023

## SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery (Lottery) to establish a contract to perform and deliver information technology cybersecurity assessments, including external network, website, wireless, and internal/client-side penetration testing assessments. These assessments must follow the Center for Internet Security methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide. The services provided must thoroughly assess and evaluate the Lottery infrastructure to identify areas that present an exploitable vulnerability available to attackers using a combination of automated tools and manual techniques.

**BACKGROUND INFORMATION:**

- The Lottery expects to consume at least one of each service annually.
- Physical instruction and Text Smishing are not in scope for these services.
- Source code will not be provided.
- A password analysis is not required.
- Retesting after vulnerabilities are remediated is out of scope. Each assessment stands alone.
- Sampling approaches are prohibited.
- Written information security policies are not in scope.

**EXISTING TECHNOLOGY ENVIRONMENT:** The following is a listing of the Lottery's current technology environment:

- The Lottery operates technology assets in eight (8) locations:
  - Main Office – 900 Pennsylvania Ave, Charleston, WV 25302
  - Bridgeport – 64 Sterling Drive, Bridgeport, WV 26330
  - Weirton – 100 Municipal Plaza Bldg. 34, Weirton, WV 26330
  - Greenbrier – 101 W. Main Street, White Sulphur Springs, WV 24986
  - Hollywood – 750 Hollywood Drive, Charles Town, WV 25414
  - Mardi Gras – 1 Greyhound Drive, Cross Lanes, WV 25313
  - Mountaineer – 1420 Mountaineer Circle, New Cumberland, WV 26047
  - Wheeling Island – 1 Stone Street, Wheeling, WV 26003
- One (1) externally accessible website hosted by a third party
- One (1) Active Directory domain
- Two (2) external IP address blocks, 15 external IP addresses (approximate)
- 27 internal IP address blocks, 500 internal IP addresses (approximate)
- 200 active users (approximate)

- Cisco network devices (approximate)
  - 10 Firewall appliances
  - 15 Routers
  - 35 Switches
  - 4 VPN appliances
- 250 Windows operating system endpoints, various versions
- 120 Voice over IP (VOIP) phones
- 40 Windows servers, various versions
  - These are replicated to redundant servers at the hot site
- Two (2) Linux storage appliances
- 30 Networked Printers with onboard operating systems and storage

**2. DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

**2.1 "Contract Items"** means the information technology cybersecurity assessments as more fully described in these specifications in Section 3.1 below and on the Pricing Page.

**2.2 "Pricing Pages"** means the schedule of prices, estimated order quantity, and totals contained in wvOASIS or attached hereto as Exhibit A and used to evaluate the Solicitation responses.

**2.3 "Solicitation"** means the official notice of an opportunity to supply the State with goods or services published by the Purchasing Division.

**2.4 "Holidays"** means days designated by WV State Code CSR 2-2-1 as legal holidays.

**2.5 "NDA"** means Non-Disclosure Agreement, attached hereto as Exhibit B, to ensure the confidentiality of the information exposed and proprietary tools and techniques used during these assessments.

**2.6 "Reconnaissance"** means passively gathering as much information about the Lottery infrastructure as possible to build attack profiles. During this phase, efforts are made to map identifying information about the infrastructure.

**2.7 "Mapping"** means activities that facilitate an understanding of the lottery's business logic, flow, and organization.

2.8 **"Discovery"** means actively probing the Lottery to identify vulnerabilities at various operational layers.

2.9 **"Exploitation"** means the Culmination of the information gathered in the previous phases to verify and confirm any identified vulnerabilities.

2.10 **"External Network Penetration Test"** means an iterative, four-phased assessment employing techniques and guidelines from the NIST SP 800-115 Information Security Testing and Assessment technical guide. It comprises activities to identify vulnerabilities of externally available hosts accessible from the Internet. Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.

2.11 **"Website Penetration Testing"** means an iterative, four-phased assessment employing techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project to verify the Lottery website security status independently. This assessment determines whether websites present an exploitable risk to the organization. Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.

2.12 **"Internal/Client Side Network Penetration Testing"** means an iterative, four-phased assessment employing techniques and guidelines from the NIST SP 800-115 Information Security Testing and Assessment technical guide, comprising activities to identify vulnerabilities at each operational layer of the target network. This includes two-part testing to assess the security of all networked assets, including but not limited to servers, desktops, firewalls, other network devices, and network monitoring & management. Part one simulates an attack by an untrusted outsider or an unauthenticated user without working knowledge of the Lottery's network. Part two will be performed with the low-level credentials of an authenticated user.

2.13 **"Wireless Network Penetration Testing"** means an iterative, four-phased assessment employing techniques and guidelines from the NIST SP 800-115 Information Security Testing and Assessment technical guide. It comprises activities to identify vulnerabilities at each target wireless network operational layer.

2.14 **"DoS"** means Denial of Service, an attack that occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

2.15 **"SAN"** means Storage Area Network is a specialized, high-speed network that provides block-level network access to storage.

**2.16** **“PTES”** means Penetration Testing Execution Standard and consists of the initial communication and reasoning behind a pen test, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it

**2.17** **“CISSP”** means Certified Information Systems Security Professional certification granted by the International Information System Security Certification Consortium.

**2.18** **“GPEN”** means GIAC Penetration Tester certification validates a practitioner's ability to properly conduct a penetration test using best-practice techniques.

**2.19** **“OSCP”** means Offensive Security Certified Professional hands-on penetration testing certification, requiring holders to successfully attack and penetrate various live machines in a safe lab environment.

**2.20** **“CEH”** means Certified Ethical Hacker is a qualification given obtained by demonstrating knowledge of assessing the security of computer systems.

**2.21** **“CPTE”** means Certified Penetration Testing Engineer presents information based on the 5 Key Elements of Pen Testing; Information Gathering, Scanning, Enumeration, Exploitation and Reporting.

**2.22** **“CEPT”** means Certified Expert Penetration Tester, has deep knowledge of web hacking techniques and methodologies.

**2.23** **“CRTOP”** means Certified Red Team Operations Professional uses tactics, techniques, and procedures that threat actors use to infiltrate IT systems and stay under the detection radar.

**2.24** **“ECSA”** means Certified Security Analyst an advanced security certification that complements the Certified Ethical Hacker (CEH) certification by validating the analytical phase of ethical hacking.

**2.25** **“CPPT”** means Certified Professional Penetration Tester utilizes a variety of methodologies to conduct a thorough penetration test, and write a complete report as part of the evaluation.

**2.26** **“CWSP”** means Certified Wireless Security Professional an advanced level certification that measures the ability to secure any wireless network.

**2.27** **"CMWAPT"** means Certified Mobile and Web Application Penetration Tester certification using pen testing methodologies and tools to conduct tests on Web and mobile apps and asses their security.

**3. QUALIFICATIONS:** Vendor, or Vendor's staff, if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

**3.1** The vendor must have been in business for at least fifteen (15) years, performing and delivering information technology cybersecurity assessments.

**3.1.1** Vendor should provide, with their bid, a general company overview that must include information regarding the professional services offered and the number of dedicated security staff resources.

**3.2** Vendor should provide, with their bid, a minimum of three (3) references for projects of similar or greater size and scope of the assessments to be performed for the Lottery.

**3.2.1** References shall include contact information and brief details of the services performed for each reference.

**3.3** Vendor should provide, with their bid, an overview of the project team and documentation of qualifications for each project team member assigned to Lottery cybersecurity assessments.

**3.3.1** Documentation shall consist of information regarding the prior security assessments completed, resumes, and documentation of certifications, which should be provided as stated below in section 3.4.

**3.4** Vendor staff performing information technology cybersecurity assessments must hold a current certification from a source of accreditation and should provide the certification credentials with their bid response. Allowable certifications include:

**3.4.1** Certified Information Systems Security Professional (CISSP)
**3.4.2** GIAC Penetration Tester (GPEN)
**3.4.3** Offensive Security Certified Professional (OSCP)
**3.4.4** Certified Ethical Hacker (CEH)
**3.4.5** Certified Penetration Testing Engineer (CPTE)
**3.4.6** Certified Expert Penetration Tester (CEPT)
**3.4.7** Certified Red Team Operations Professional (CRTOP)
**3.4.8** Certified Security Analyst (ECSA)
**3.4.9** Certified Professional Penetration Tester (CPPT)
**3.4.10** Certified Wireless Security Professional (CWSP)

**3.4.10.1** This certification is only applicable to Wireless Penetration Testing Services

**3.4.11** Certified Mobile and Web Application Penetration Tester (CMWAPT)

**3.4.11.1** This certification is only applicable to Website Penetration Services

**3.5** Vendor must comply with the Center for Internet Security methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide.

**3.6 Background Checks:** Prior to award and upon request, the Vendor must provide names, addresses, and fingerprint information for a law enforcement background check for any Vendor staff working on the Lottery project team.

**3.7 Non-Disclosure Agreement (NDA):** Prior to award both parties, the Vendor and Lottery must sign a mutual Non-Disclosure Agreement (NDA), attached as Exhibit – B, to ensure the confidentiality of the information exposed and proprietary tools and techniques used during these assessments.

## 4. MANDATORY REQUIREMENTS:

### 4.1. External Network Penetration Testing

**4.1.1.** External Network Penetration Testing may be performed remotely.

**4.1.2.** Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.

**4.1.3.** Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.

**4.1.3.1. Reconnaissance should include:**

**4.1.3.1.1.** Perform WHOIS, ARIN, and DNS (public server) lookups

**4.1.3.1.2.** OSINT - Public Searches/Dorks

**4.1.3.1.3.** Build custom password lists

**4.1.3.1.4.** DNS lookups (entities server)

**4.1.3.1.5.** Gather information from entities network resources

**4.1.3.1.6.** Analyze metadata

**4.1.3.2. Mapping should include:**

**4.1.3.2.1.** Network Discovery (ICMP sweeps, traceroutes, bypass firewall restrictions, etc.)

**4.1.3.2.2.** Port/Protocol Scanning (Scan for accepted IP protocols, open TCP/UDP ports)

**4.1.3.2.3.** OS/Version Scanning (Identify underlying OS and software and their versions)

**4.1.3.3. Discovery should include:**

**4.1.3.3.1.** Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner)

**4.1.3.3.2.** Enumerating Network Services (Connect and interact with services to disclose information, gain access, identify misconfigurations, etc.)

**4.1.3.3.3.** Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)

**4.1.3.4. Exploitation should include:**

**4.1.3.4.1.** Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force)

**4.1.3.4.2.** Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)

**4.1.3.4.3.** Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the penetration test steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope).

**4.1.4.** Must identify exploitable vulnerabilities and demonstrate organizational impact.

**4.1.5.** Denial of service (DoS) attacks are prohibited for External Network Penetration Testing services.

**4.1.6.** A social engineering exercise must be included. This will consist of a single phishing email scenario targeting approximately 200 active Lottery staff. The content must be designed to maximize successful phishing, and the email content and target addresses must be verified and approved by the Lottery.

**4.1.7.** Heavy load brute force or automated attacks will only be performed with prior Lottery approval.

**4.1.8.** Must notify Lottery of any portion or portions of the assessment resulting in service disruption.

**4.1.9.** The Lottery must be notified immediately upon identifying any security vulnerability threatening critical business processes or IT services.

**4.1.10.** Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.

**4.1.10.1.** The vendor shall provide a sample of the executive summary report with their bid response.

**4.1.10.2.** The report must be submitted to the Lottery electronically for review.

**4.1.11.** Upon conclusion of the assessment the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

**4.1.12.** Reports must include specific details for each vulnerability found, including:

**4.1.12.1.** How the vulnerability was discovered

**4.1.12.2.** The potential impact of its exploitation.

**4.1.12.3.** Recommendations for remediation.

**4.1.12.4.** Vulnerability references

**4.1.12.5.** The vendor shall provide a sample of the technical report with their bid response.

**4.1.12.6.** The report must be submitted to the Lottery electronically for review.

**4.1.13.** Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

**4.1.13.1** The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

### 4.2. Website Penetration Testing

**4.2.1.** Website Penetration Testing may be performed remotely.

**4.2.2.** Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.

**4.2.3.** The successful vendor must determine static and dynamic page counts.

**4.2.4.** Any environment, such as production, development, quality assurance, etc., may be tested. Each environment will be assessed separately.

**4.2.5.** Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.

**4.2.5.1. Reconnaissance should include:**

**4.2.5.1.1.** Perform WHOIS, ARIN, and DNS (public server) lookups

**4.2.5.1.2.** OSINT - Public Searches/Dorks

**4.2.5.1.3.** Build custom password lists

**4.2.5.1.4.** DNS lookups (entities server)

**4.2.5.1.5.** Gather information from entities web applications

**4.2.5.1.6.** Analyze metadata

**4.2.5.2. Mapping should include:**

**4.2.5.2.1.** SSL/TLS Analysis (Identify accepted SSL/TLS ciphers)

**4.2.5.2.2.** Virtual Hosting & Load Balancer Analysis

**4.2.5.2.3.** Software Configuration Discovery (Identify HTTP version, web services, scripting languages, third-party web applications, etc.)

**4.2.5.2.4.** HTTP Options Discovery (Identify accepted HTTP methods)

**4.2.5.2.5.** Web Application Spidering (gather/follow all links)

**4.2.5.2.6.** Directory Browsing (Identify web directory listings, brute force common web directory names)

**4.2.5.2.7.** Web Application Flow (Identify the business logic, flow, organization, and functionalities of the app)

**4.2.5.2.8.** Session Analysis (Identify locations where session cookies are set and analyze predictability)

**4.2.5.3. Discovery should include:**

**4.2.5.3.1.** Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner)

**4.2.5.3.2.** Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)

**4.2.5.3.3.** Identify Web Application Specific/Web Service Specific Vulnerabilities (Command/XML/XXE/SQL Injection, File Inclusion, Directory Traversal, File Upload, XSS, CSRF, etc.)

**4.2.5.3.4.** Identify Authentication/Authorization Issues/Bypasses (Weak access control, weak password policy, session management, etc.)

**4.2.5.4. Exploitation should include:**

**4.2.5.4.1.** Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force)

**4.2.5.4.2.** Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)

**4.2.5.4.3.** Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the pentest steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope).

**4.2.6.** Must provide identification of prioritized remediation needs, requirements, and associated risks.

**4.2.7.** Testing shall determine if website vulnerabilities exist by testing each website, including server operating systems, application platforms, and databases.

**4.2.8.** Denial of Service (DoS) attacks are required for Website Penetration Testing and require notification to the Lottery and Lottery approval before the attack commences.

**4.2.9.** Heavy load brute force or automated attacks will only be performed with prior Lottery approval.

**4.2.10.** Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.

**4.2.10.1.** The vendor shall provide a sample of the executive summary report with their bid response.

**4.2.10.2.** The report must be submitted to the Lottery electronically for review.

**4.2.11.** Upon conclusion of the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

**4.2.12.** Reports must include specific details for each vulnerability found, including:

**4.2.12.1.** How the vulnerability was discovered

**4.2.12.2.** The potential impact of its exploitation.

**4.2.12.3.** Recommendations for remediation.

**4.2.12.4.** Vulnerability references

**4.2.12.5.** The vendor shall provide a sample of the technical report with their bid response.

**4.2.12.6.** The report must be submitted to the Lottery electronically for review.

**4.2.13.** Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

**4.2.13.1.** The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

**4.3. Internal/Client-Side Network Penetration Testing**

**4.3.1.** Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited.

**4.3.2.** Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.

**4.3.3.** Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.

**4.3.3.1. Reconnaissance should include:**

**4.3.3.1.1.** Identify software versions along with potentially useful software configurations or settings

**4.3.3.1.2.** Identify any anti-malware, firewall, and IDS products on the system

**4.3.3.1.3.** Gather information about the network (i.e., domain user/group information, domain computers, password policy)

**4.3.3.1.4.** Verify the ability to execute scripts or third-party programs

**4.3.3.2. Mapping and Discovery should include:**

**4.3.3.2.1.** Identify possible vulnerabilities affecting the provided host

**4.3.3.2.2.** Determine the possibility of receiving and executing various malicious payloads

**4.3.3.3. Exploitation should include:**

**4.3.3.3.1.** Attempt to bypass anti-malware solutions and security restrictions, escape restricted environments, and escalate privileges

**4.3.3.3.2.** Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)

**4.3.4.** Must identify prioritized remediation needs, requirements, and associated risks.

**4.3.5.** Testing shall assess the security of all networked assets, including but not limited to servers, endpoints, firewalls, network devices, and network monitoring and management.

**4.3.6.** Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.

**4.3.6.1.** Vendor shall provide a sample of the executive summary report with their bid response.

**4.3.6.2.** Report must be submitted to Lottery electronically for review.

**4.3.7.** Upon conclusion of the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

**4.3.8.** Reports must include specific details for each vulnerability found, including:

**4.3.8.1.** How the vulnerability was discovered.

**4.3.8.2.** The potential impact of its exploitation.

**4.3.8.3.** Recommendations for remediation.

**4.3.8.4.** Vulnerability references.

**4.3.8.5.** The vendor shall provide a sample of the technical report with their bid response.

**4.3.8.6.** The report must be submitted to the Lottery electronically for review.

**4.3.9.** Upon conclusion of the assessment, the Vendor must provide a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

**4.3.9.1.** The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

**4.4. Wireless Penetration Testing**

**4.4.1.** Wireless Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited.

**4.4.2.** Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.

**4.4.3.** Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.

**4.4.3.1. Reconnaissance should include:**

**4.4.3.1.1.** Perform WHOIS, ARIN, and DNS (public server) lookups

**4.4.3.1.2.** OSINT - Public Searches/Dorks

**4.4.3.1.3.** Build custom password lists

**4.4.3.1.4.** DNS lookups (entities server)

**4.4.3.1.5.** Gather information from entities web applications

**4.4.3.1.6.** Analyze metadata

**4.4.3.2. Mapping should include**:

**4.4.3.2.1.** Sniffing (establish a baseline of traffic, sniff Wi-Fi, Bluetooth, Zigbee, and other RF)

**4.4.3.2.2.** War Walk (map location of access points and their coverage, identify leakage)

**4.4.3.2.3.** Identify Rogue Access Points* (Friendly, malicious, or unintended access points)

**4.4.3.2.4.** Full access to the buildings will be granted to the testing team

**4.4.3.3. Discovery should include:**

**4.4.3.3.1.** Identify Points of Attack (Identify WEP networks, capture WPA/WPA2 PSK key exchanges, identify clients for evil-twin and MiTM attacks

**4.4.3.3.2.** Enumerating Services (Connect and interact with services on APs, Bluetooth Devices, and other RF devices to disclose misconfigurations

**4.4.3.3.3.** Vulnerability Scanning (Identify vulnerabilities)

**4.4.3.4. Exploitation should include:**

**4.4.3.4.1.**AP Attacks (Exploit hotspots, perform MiTM attacks, crack WEP, crack WPA/WPA2 PSK, etc.)

**4.4.3.4.2.**Client Attacks (Perform Evil-Twin attacks, perform rogue AP attacks, MiTM, etc.)

**4.4.3.4.3.**Denial of Service where applicable and with prior Lottery approval

**4.4.3.4.4.**Bluetooth/Zigbee/SDR Attacks where applicable and with prior Lottery approval

**4.4.4.** Must identify prioritized remediation needs, requirements, and associated risks.

**4.4.5.** Testing shall assess the security of all wireless assets.

**4.4.6.** Upon conclusion of the assessment, the Vendor must provide an Executive Summary Report. This report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.

**4.4.6.1.**Vendor shall provide a sample of the executive summary report with their bid response.

**4.4.6.2.**Report must be submitted to Lottery electronically for review.

**4.4.7.** Upon completing the assessment, the Vendor must provide a Technical Report. This report details each vulnerability type discovered and assigns a critical, high, medium, or low risk rating.

**4.4.8.** Reports must include specific details for each vulnerability found, including:

**4.4.8.1.**How the vulnerability was discovered.

**4.4.8.2.**The potential impact of its exploitation.

**4.4.8.3.**Recommendations for remediation.

**4.4.8.4.**Vulnerability references.

**4.4.8.5.**The vendor shall provide a sample of the technical report with their bid response.

**4.4.8.6.**The report must be submitted to the Lottery electronically for review.

**4.4.9.** Upon the conclusion of the assessment, the Vendor must present a Findings Presentation to the Lottery management team. This presentation shall provide an overview of the strengths, weaknesses, and vulnerabilities identified throughout the assessment.

**4.4.9.1.** The findings presentation shall be presented to Lottery in person or via a conference call presentation, to be determined by Lottery upon competition of the project.

## 5. CONTRACT AWARD:

**5.1 Contract Award:** The Contract is intended to provide Agency with a purchase price for the Contract Services. The Contract shall be awarded to the Vendor that provides the Network Penetration Testing and Cybersecurity Assessments meeting the required specifications for the lowest total bid amount as shown on the Pricing Pages.

**5.2 Pricing Page:** Vendor should complete the Pricing Page by entering the unit cost per assessment and reports as a fixed amount for all penetration testing, vulnerability assessments, reports and findings presentation to calculate the extended amount. Then add all extended amount line items together to get the total bid amount. Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

The Pricing Page contains an estimated number for assessments. The estimates represent an amount that will be utilized for evaluation purposes only. No future use of the Contract or any individual item is guaranteed or implied.

Vendor should type or electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document. In most cases, the Vendor can request an electronic copy of the Pricing Pages for bid purposes by sending an email request to the following address: brandon.l.barr@wv.gov

**6. PERFORMANCE:** Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

7. **PAYMENT:** Agency shall pay the hourly rate, as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

8. **TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.

9. **FACILITIES ACCESS:** Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:

   **9.1.**Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.

   **9.2.**Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.

   **9.3.**Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.

   **9.4.**Anyone performing under this Contract will be subject to Agency's security protocol and procedures.

   **9.5.**Vendor shall inform all staff of Agency's security protocol and procedures.

10. **VENDOR DEFAULT:**

    **10.1.** The following shall be considered a vendor default under this Contract.

    **10.1.1.** Failure to perform Contract Services in accordance with the requirements contained herein.

    **10.1.2.** Failure to comply with other specifications and requirements contained herein.

    **10.1.3.** Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

    **10.1.4.** Failure to remedy deficient performance upon request.

**10.2.** The following remedies shall be available to Agency upon default.

**10.2.1.** Immediate cancellation of the Contract.

**10.2.2.** Immediate cancellation of one or more release orders issued under this Contract.

**10.2.3.** Any other remedies available in law or equity.

## 11. MISCELLANEOUS:

**11.1. Contract Manager:** During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

**Contract Manager: Scott E Marshall**
**Telephone Number: 301-442-3155**
**Fax Number: 304-927-1649**
**Email Address: scott.marshall@intelligent-network-security.com**

## EXHIBIT A - Pricing Page

| Item # | Section | Description of Service | *Estimated Number of Assesments* | Unit Cost per Assesment & Reports | Extended Amount |
|---|---|---|---|---|---|
| 1 | 4.1 | External Network Penetration Testing | 8 | $ 11,442.20 - | $ 91,537.60 - |
| 2 | 4.2 | Website Penetration Testing | 8 | $ 11,442.20 - | $ 91,537.60 - |
| 3 | 4.3 | Internal/Client-Side Network Penetration Testing | 8 | $ 15,387.68 - | $ 123,101.44 - |
| 4 | 4.4 | Wireless Penetration Testing | 8 | $ 15,387.68 - | $ 123,101.44 - |
| | | | | TOTAL BID AMOUNT | $ 429,278.08 - |

***Please note the following information is being captured for auditing purposes and is an estimate for evaluation only***

**Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.**

**Any product or service not on the Agency provided Pricing Page will not be allowable.**

**The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.**

| | |
|---|---|
| **Vendor Name:** | Intelligent Network Security LLC |
| **Vendor Address:** | 550 Hamric Lane, Spencer, WV 25276 |
| **Email Address:** | scott.marshall@intelligent-network-security.com |
| **Phone Number:** | 301.442.3155 |
| **Fax Number:** | 304-9274-1649 |
| **Signature and Date:** | 3/28/2024 |
| | |

# EXHIBIT B
# NON-DISCLOSURE AGREEMENT (NDA)

## MUTUAL NON-DISCLOSURE AGREEMENT

This Mutual Non-Disclosure Agreement ("Agreement") is entered into by and between the West Virginia Lottery, with its principal offices located at 900 Pennsylvania Avenue Charleston, WV 25302 ("Lottery"), and ___________________________________________, with its principal offices located at ___________________________________ ("Party of the second part"), with an Effective Date of ____________________. Lottery and Party of the second party also are referred to herein individually as a "party", or collectively as the "parties".

WHEREAS, the parties to this Agreement may wish to exchange certain information related to the provision of certain information or communication technology services by one party of interest to the other party; and

WHEREAS, the parties agree that improper disclosure of either party's Confidential Information, as defined below, by the other party could cause material harm to the party whose Confidential Information was improperly disclosed;

NOW THEREFORE, in order to protect certain Confidential Information that may be disclosed between the parties, Lottery and Alpha agree to maintain the confidentiality of the Confidential Information as follows:

**I.** **Definition of Confidential Information**. The "Confidential Information" disclosed under this Agreement is defined as follows:

Any data or information that is proprietary to the disclosing party and not generally known to the public, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to: (i) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated companies; (ii) plans for products or services, and customer or supplier lists; (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, intellectual property, and trade secrets; (v) solicitation for proposals, responses to proposals, bids, or information disclosed in connection with such solicitation, response, or bid; (vi) any other information that should reasonably be recognized as confidential information of the disclosing party.

**II.** **Disclosure Period and Term**. This Agreement protects against the disclosure of Confidential Information which is disclosed between the parties during each party's performance of its obligations associated with that certain CRFQ Agreement executed between the parties on _________________ (the "Effective Date") and 3 year(s) after the termination of such Agreement ("Disclosure Period"). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure

## EXHIBIT B
## NON-DISCLOSURE AGREEMENT (NDA)

Period. Upon termination of this Agreement or upon the disclosing party's request, the recipient shall cease use of Confidential Information and return or destroy it.

**III.** **Use of Confidential Information**. A party hereunder receiving Confidential Information shall use such Confidential Information solely for the purposes of, as applicable to the recipient, understanding current business activities of a party, soliciting a proposal for certain information technology services, responding to such proposal solicitation, reviewing solicitation responses, tendering a bid, or discussions or negotiations related to such solicitation, proposal, or bid.

**IV.** **Protection of Confidential Information**. Each party shall not disclose the Confidential Information of the other party to any third party. The recipient shall protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the recipient uses to protect its own confidential information of a like nature. A recipient shall restrict disclosure of Confidential Information to its employees, provided that such employees (i) have a need to know, and (ii) are bound by obligations of confidentiality equally as restrictive as the terms of this Agreement.

**V.** **Exclusions**. This Agreement imposes no obligation upon the recipient with respect to Confidential Information which: (a) was in the recipient's possession before receipt from the disclosing party; (b) is or becomes a matter of public knowledge through no fault of the recipient; (c) is rightfully received by the recipient from a third party without a duty of confidentiality; (d) is disclosed by the disclosing party to a third party without a duty of confidentiality on the third party; (e) is independently developed by the recipient; (f) is disclosed under operation of law; or (g) is disclosed by the recipient with the disclosing party's prior written approval.

**VI.** **Miscellaneous**. Neither party to this Agreement shall acquire any intellectual property rights nor any other rights under this Agreement except the limited right to use as set forth in this Agreement. This Agreement does not prevent either Party from competing with one another for work or clients unless the parties specifically agree otherwise, in writing, as to a specific client. Each disclosing party warrants and represents that the Confidential Information and other information provided which is necessary to the purposes described hereunder, are true and correct to the best of the disclosing party's knowledge and belief. Nothing in this Agreement shall be construed to preclude either party from developing, using, marketing, licensing, and/or selling any software or other material that is developed without reference to the Confidential Information.

**VII.** **Export Administration**. Each party to this Agreement agrees to comply fully with all relevant export laws and regulations of the United States and other countries to assure that no Confidential Information or any portion thereof is exported, directly or indirectly, in violation of such laws.

**VIII.** **No Obligation to Purchase or Offer Products or Services**. Neither party has an obligation under this Agreement to purchase or otherwise acquire any service or item from

## EXHIBIT B
## NON-DISCLOSURE AGREEMENT (NDA)

the other party. Neither party has an obligation under this Agreement to commercially offer any products using or incorporating the Confidential Information. The disclosing party may, at its sole discretion, offer such products commercially and may modify them or discontinue such offerings at any time.

**IX.** **General**. The parties do not intend that any agency or partnership relationship be created between them by this Agreement. This Agreement sets forth the entire agreement with respect to the Confidential Information disclosed herein and supersedes all prior or contemporaneous agreements concerning such Confidential Information, whether written or oral. All additions or modifications to this Agreement must be made in writing and must be signed by both parties. This Agreement and all matters arising out of or relating to this Agreement shall be governed by the laws of the State of West Virginia. The parties agree that the information provided as allowed by this Agreement will not contain any proprietary technical or confidential contractual information, or any financial information related to the relationship between Alpha and its partners. As a result, damages will not be included as a remedy.

The undersigned authorized representatives of each party have agreed to be legally bound by the terms of this Agreement as of the Effective Date shown above.

**WEST VIRGINIA LOTTERY**

By: ________________________________

Name: _______________________________

Title: ________________________________

**______________________________ (VENDOR)**

By:_________________________________

Name: ______________________________

Title: _______________________________

Network Penetration Testing and Cybersecurity Assessments
Solicitation Number: CRFQ LOT2400000009

West Virginia Lottery

Technical Proposal

Point of Contact:
Scott E Marshall
Executive Vice President
301.442.3155
scott.marshall@intelligent-network-security.com

*Intelligent Network Security, LLC | 550 Hamric Lane, Spencer, WV 25276*

*This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Intelligent Network Security.*

## Table of Contents

# Specifications

## Purpose and Scope

Intelligent Network Security LLC is submitting this response to Solicitation Number: CRFQ-0705-LOT2400000005-1 to provide Network Penetration Testing and Cybersecurity Assessments for the West Virginia Lottery. The resulting contract will require INS to perform and deliver information technology cybersecurity assessments, including external network, website, and web application penetration testing and internal network vulnerability assessments.

Intelligent Network Security LLC certifies that we are not currently engaged in, and will not for the duration of the contract, engage in a boycott of Israel.

INS has prepared pricing based on the below existing technology environment:

- The Lottery operates technology assets in eight (8) locations:
  - Main Office- 900 Pennsylvania Ave, Charleston, WV 25302
  - Bridgeport- 64 Sterling Drive, Bridgeport, WV 26330
  - Weirton - 100 Municipal Plaza Bldg. 34, Weirton, WV 26330
  - Greenbrier - 101 W. Main Street, White Sulphur Springs, WV 24986
  - Hollywood- 750 Hollywood Drive, Charles Town, WV 25414
  - Mardi Gras - 1 Greyhound Drive, Cross Lanes, WV 25313
  - Mountaineer- 1420 Mountaineer Circle, New Cumberland, WV 26047
  - Wheeling Island - 1 Stone Street, Wheeling, WV 26003
- One (1) externally accessible website hosted by a third party
- One (1) Active Directory domain
- Two (2) external IP address blocks, 15 external IP addresses (approximate)
- 27 internal IP address blocks, 500 internal IP addresses (approximate)
- 200 active users (approximate)
- Cisco network devices (approximate)
  - 10 Firewall appliances
  - 15 Routers
  - 35 Switches
  - 4 VPN appliances
- 250 Windows operating system endpoints, various versions
- 120 Voice over IP (VOIP) phones
- 40 Windows servers, various versions
- These are replicated to redundant servers at the hot site
- Two (2) Linux storage appliances
- 30 Networked Printers with onboard operating systems and storage.

## Qualifications

### Intelligent Network Security, LLC ("INS")

INS is a Center for Veterans Enterprise (CVE) certified Service-Disabled Veteran-Owned Small Business (SDVOSB) and Small Business Administration (SBA) Certified HUBZone specializing in providing information technology professional and cybersecurity services. **Founded, registered and headquartered in Spencer, WV (Roane County) in 2005, INS has nineteen continuous years** of professional and cybersecurity experience in government, state and commercial network cybersecurity operations and in building, deploying, and monitoring network firewalls; performing penetration testing; wireless network testing and assessments; conducting vulnerability assessments; monitoring Intrusion Detection Systems (IDS); building, deploying, and monitoring host and network based IDS; network support and IT outsourcing; network security engineering and implementation; digital forensics; threat analysis; forensic analysis; flow analysis; large dataset analysis; forensic log analysis; malicious code analysis; malware reverse engineering; compromise assessment and cyber hunt by utilizing Advanced Persistent Threat Detection technologies to combat computer adversaries from extracting knowledge or data from network systems.

### Certifications

It is understood that the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award. Additional information will be submitted as requested. Intelligent Network Security LLC considers this information proprietary with personally identifiable information.

### Personnel

It is understood that the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award. Additional information will be submitted as requested. Intelligent Network Security LLC considers this information proprietary with personally identifiable information.

### References

It is understood that the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award. Additional information will be submitted as requested. Intelligent Network Security LLC considers this information proprietary with personally identifiable information.

## Compliance with Penetration Testing Execution Standard (PTES)

Our team will follow the engagement PTES methodology detailed in Table 1 for external, internal and website and web application penetration testing. The process we will follow in the below table conforms to the requirement that our testing methodology includes enumeration, vulnerability assessment and exploitation.

| Phase | Details |
|---|---|
| 1 – Rules of Engagement and Pre-Engagement Interactions | Prior to performing any security testing or accessing WV Lottery's networks, INS will collaborate with lottery personnel to determine the appropriate rules of engagement (ROE) based on the work to be performed and the level of exploitation requested. This phase ensures both parties understand the nature and risks involved with the engagement. |
| 2 – Intelligence Gathering, reconnaissance, mapping and discovery | Once the ROE is communicated and agreed upon, INS will perform intelligence gathering and reconnaissance activities to profile and understand the scope of the environment. We will conduct open-source intelligence (OSINT) to detect network/account compromise. The extent of intelligence gathering is dependent upon the scope of the environment but may include documentation reviews, |

| | |
|---|---|
| | public information searches, network mapping and discovery, application spidering, and network device configuration best practices, etc. |
| 3 - Risk/Vulnerability Identification | INS will use a variety of methods and toolsets (including open-source tools, Rapid7 and Tenable Nessus) to precisely identify and specify points of a security weakness that may be exploited from the viewpoint of malicious entities. These toolsets are designed to acquire a comprehensive picture and list of vulnerability exposures and threats while ensuring minimal impact. |
| 4 – Analysis | In the analysis phase, INS will review and validate the results from the previous phases and apply specific techniques to validate identified risk/vulnerabilities. An essential part of this phase is false-positive identification and removal which will be conducted by subject matter experts using custom, manual techniques. By removing false-positive information, we will be able to focus our support on remediating real vulnerabilities and threats in the environment. |
| 5 – Exploitation | Once validation and analysis have been completed, INS will then attempt to exploit any security weaknesses identified using sophisticated techniques designed to mimic real-world attackers.<br>Examples of exploits INS may use within this phase covering penetration testing include but are not limited to network exploitation, application exploitation, network exploration, social engineering, and public presence research. If application testing is required, we will verify common attack techniques. |
| 6 – Reporting | After the exploitation phase is performed, INS will analyze resultant findings, extent of our penetration activities, categorize vulnerability types by class, and point out high-risk vulnerabilities that exist on multiple systems that should be addressed with the highest priority. INS' reports will summarize overall risk attributed to the vulnerabilities identified, describe vulnerabilities requiring your attention and how they were exploited or could be exploited. Our reports will provide actionable results specific to the WV Lottery network. |

Table 1

## Compliance with Open Web Application Security Project (OWASP) Top 10 Project

INS will follow the best practices contained in the OWASP Top 10 listing top security risks producing web application vulnerabilities. It is commonly understood that these vulnerabilities include:

- A01:2021 – Broken Access Control
- A02:2021 – Cryptographic Failures
- A03:2021 – Injection
- A04:2021 – Insecure Design
- A05:2021 – Security Misconfiguration
- A06:2021 – Vulnerable and Outdated Components
- A07:2021 – Identification and Authentication Failures
- A08:2021 – Software and Data Integrity Failures
- A09:2021 – Security Logging and Monitoring Failures

- A10:2021 – Server-Side Request Forgery (SSRF)

## Penetration Testing/Vulnerability Assessment Tools/Platforms

Upon award, INS will perform penetration testing services using the following subscription and open-source tools, at a minimum, to conduct the penetration testing services:

**Rapid 7:** This is a well know penetration testing software. Rapid7's Metasploit Pro saves time, automates exploitation, evidence collection, and enhances reporting. Metasploit Pro also can conduct client-side attacks, with advanced brute forcing techniques and phishing attacks. The product will stealthily conceal our exploits and pivot around the WV Lottery network. Metasploit Pro will simulate a real attack on networks, and continuously assess network defenses. **Rapid7 leverages the Open-Source Security Testing Methodology Manual (OSSTMM), the Penetration Testing Execution Standard (PTES), and for application testing, the Open Web Application Security Project (OWASP) as foundation for assessments.**

Rapid7's penetration testing capabilities include comprehensive reporting features that provide detailed insights into identified vulnerabilities, exploited systems, and recommended remediation actions.

**Tenable Nessus:** Tenable Nessus is a remote security scanning tool that INS will use to scan for vulnerabilities in devices, applications, operating systems, and cloud services. It can also scan network resources. Nessus can detect vulnerabilities such as:

- Unauthorized access to sensitive data
- Misconfiguration, such as open mail relay
- Denials of service (DoS) vulnerabilities

**Shodan** (Sentient Hyper-Optimized Data Access Network). Shodan is a search engine designed to map and gather information about internet-connected devices and systems. INS will use its functions to detect devices that are connected to the internet at any given time, the locations of those devices and their current users. Will leverage its capabilities to grab banners which will help us to identify vulnerabilities in WV Lottery systems.

**Nmap**. We will use Nmap, an open-source network mapper, to detect open ports. We will use this tool to send packets to identified hosts and then analyze responses regarding network topography for our exploration efforts. Specifically, it will be used to scan UDP ports, find all the live hosts in a range of IPs, and run scripts to find common vulnerabilities in applications among other actions.

**Nikto**. We will use Nikto to assess and perform comprehensive tests to detect the web server's vulnerabilities. Specifically, we will use it to scan for dangerous files/CFGIs, outdated server software and other problems.

**Whois**. We will use Whois for information gathering on the WV Lottery website. The enumeration information uncovered is then used to find vulnerabilities in the target for exploitation.

**Wireshark**. Wireshark is a widely used open-source network protocol analyzer we will use to capture, analyze, and interactively browse the traffic running on a computer network. We will leverage Wireshark's capabilities for network troubleshooting, analysis, software, and protocol development.

## Penetration Test Overview:

INS will provide penetration testing services using standard, accepted and ethically based processes and procedures.

As demonstrated in our response to the mandatory requirements, we are in compliance and follow the guidance contained in NIST Special Publication 800-115, "Technical Guide to Information Security Testing and Assessment". This includes:

- Implementing a repeatable and documented assessment methodology
- Determine the objectives of each security assessment, and tailor the approach accordingly
- Analyze findings, and develop risk mitigation techniques to address weaknesses

INS will conduct penetration testing on WV Lottery's external network, website, wireless and internal/client-side network. This process will help the WV Lottery address potential hostile attempts by exposing weaknesses through penetration testing exploitation activities across their systems and networks. INS' penetration testing process follows the Penetration Testing Execution Standard (PTES), the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide. Our assessments will include reconnaissance, mapping, discovery, and exploitation using our automated tools and manual techniques.

Prior to commencement of testing activities, a rules of engagement (ROE) will be developed, coordinated and approved. The purpose of this document is to establish and formalize the parameters for the cybersecurity services and assessment activities, which will be conducted by Intelligent Network Security (INS) for the West Virginia (WV) Lottery. The ROE will include a scope section that details the specifics of the assessment; the assessment environment; the methodology. These sections will be followed by specific permissions the WV Lottery will grant INS to conduct active penetration tests. Personnel and points of contact will be included. After agreement is reached on the ROE by the lottery and INS, the document will be signed.

INS will review WV Lottery's network device configuration for best practices. We will look for standardized configuration for each device category:

- if automation is being used to implement configuration and change management tasks
- are firmware and drivers regularly updated
- are the firewall settings updated and properly configured
- have insecure protocols been disabled.

INS will evaluate computer network defenses and measure the attack capabilities of potential threats. We will assist in finding exposed information and vulnerabilities in all cyber environments and provide recommendations to improve security measures to minimize susceptibility to future network attacks.

INS has conducted many penetration tests, for both government and commercial entities. Through our experience gained over the course of many years, we have developed a trusted reputation. For this assessment, INS will actively attack external network, website and web application, wireless network and internal/client-side network to expose any viable threat vectors.

INS will participate in the contract kick-off meeting. This meeting will include WV Lottery personnel, the INS program/contract manager, and INS subject matter expert. We will discuss points of contact and responsibilities. We will also discuss the delivery schedule milestones and timelines.

**General Requirements**: INS will perform the testing in a timely and professional manner. In accordance with the CRFQ, we will perform tests on all networked assets, including but not limited to websites, servers, endpoints, firewalls, network devices, wireless infrastructure and network monitoring and management. Based on the capabilities of our tools, we will conduct tests on each asset and will not test smaller, representative samples. INS will provide all task and deliverables on time while adhering to our quality standards. We will target our testing services on activities and locations, as required, to include internal and external facing targets for the WV Lottery. INS understands the complexity of attacking targets that encompass a spectrum of external and internal targets. We possess the tools and expertise to successfully conduct testing in these varied settings and geographic locations.

### Team Accreditations

It is understood that the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award. Additional information will be submitted as requested. Intelligent Network Security LLC considers this information proprietary.

## Mandatory Requirements

### External Network Penetration Testing

#### Reconnnaissance

We will use Whois for information gathering on the WV Lottery external network. We will use the enumeration information uncovered to find vulnerabilities in the target for exploitation. The WHOIS lookup will retrieve specific network information regarding ownership, registration date, expiration date and other information we will need to assess the network. INS will do an ARIN (American Registry for Internet Numbers) lookup to retrieve information about IP addresses using arin.net and other viable sources and processes. We will conduct a public and entity server DNS lookup using command-line tools or our subscription software to gather accurate information on IP addresses.

We will conduct open-source intelligence (OSINT) to detect network/account compromise. The extent of intelligence gathering is dependent upon the scope of the environment but may include documentation reviews, public information searches, network mapping, application spidering, and network device configuration best practices, etc.

INS will build a custom password list through a systematic approach, including generating patterns reflective of common password user habits, to use for password strength testing and cracking.

INS will collect and categorize metadata which we will review with the goal of identifying meaningful insights and patters. We will look for inconsistencies and exploitable errors.

#### Mapping

INS will leverage the capabilities of Nmap to conduct network mapping activities. We will use this tool to send ICMP echo requests and analyze the responses from hosts. Its capabilities include port scanning to determine open or closed TCP and UDP ports and accepted IP protocols. We will use various scanning techniques including TCP connect scan, SYN stealth scan, UPD scan, among others.

We will conduct OS detection through Nmap's ability to find differences in TCP/IP stack implementations.

We will conduct service version detection by analyzing responses obtained from open port probes. This will assist us in understanding potential software/operation system vulnerabilities.

We will use a structured process to gather information on the WV Lottery's external network infrastructure, devices, services to detect potential, exploitable vulnerabilities. We will use Nmap as a network mapper to detect open ports. It will be used to scan UDP ports, find all the live hosts in a range of IPs, and run scripts to find common vulnerabilities in applications. We will use this information to assess security risks to identify potential threats.

## Discovery

INS will conduct Vulnerability scans using our Tenable Nessus tool in multiple network systems areas or facilities, such as in firewalls, application servers, Web servers, and operating systems.

Our focus will be on whether a vulnerability has the potential to be exploited by a threat, which depends on a number of variables including (but not limited to):

- The strength of the security controls in place
- The ease at which a human actor could purposefully launch an attack
- The probability of an environmental event or disruption in each local area

We will conduct enumerating network services by systematically identifying and cataloging the services running on network hosts to understand the lottery's network attack surface and assess potential vulnerabilities using Nmap and Tenable Nessus. We will scan for known vulnerabilities and misconfigurations to gain access.

We will conduct username/email enumeration using active enumeration techniques. These include email format guessing based on common patterns, directory enumeration by probing directory to discover user profiles, email aliases or hidden resources, and email harvesting using scripts to gather email addresses from various sources, including webpages, forms, or online directories.

## Exploitation

Once enumeration efforts are complete (including reconnaissance, footprinting and vulnerability scanning), INS will attempt to exploit identified vulnerabilities to gain unauthorized access to WV Lottery's external network. All testing will be conducted from INS Corporate locations. We will leverage Rapid7, Tenable Nessus and other custom scripts and open-source tools, to gain a foothold and elevate privileges to external network.

INS will immediately notify WV Lottery officials if a service disruption is caused by our testing efforts. If we find a critical vulnerability that could adversely affect the lottery's business process or services, we will immediately notify lottery officials. We will not conduct a denial of service (DoS) attack on the external network.

INS will obtain prior approval, in accordance with the rules of engagement (ROE), prior to conducting brute force logins. We will leverage information about usernames and email addresses from information gathered from our enumeration activities. We will conduct the brute force attack using Rapid7, Tenable Nessus, open-source tools and other custom scripts. Our tools will send login requests to the lottery's network to guess a useful system login to gain access or exhaust all combinations.

We will attempt to exploit vulnerabilities we found using Tenable Nessus, open-source tools and INS custom scripts to gain or elevate unauthorized access to the lottery's external network. This may also involve leveraging known/published vulnerabilities to bypass security controls to gain a foothold within the external network.

Once we gain unauthorized access to the external network, we will attempt post-exploitation and pivot by seeking to expand our control, escalate privileges and move laterally within the external network.

We will attempt to escalate privileges gained through exploitation to gain higher access. We will use various techniques, involving exploiting discovered vulnerabilities, misconfigurations, or other weaknesses we discovered. Once we obtain elevated privileges, we will conduct additional enumeration and discovery to obtain information regarding network resources, user accounts, system configuration and potential avenues for further exploitation. We will attempt to move latterly within the external network to expand our foothold. We will attempt to pivot to access other parts of the network that are not directly connected to the external network.

A targeted social engineering exercise will be conducted via a single phishing email scenario. This exercise will be coordinated and pre-approved by WV Lottery officials prior to execution. We will use standard techniques to create the email to create a false sense of urgency on the part of the recipient. This could involve spoofing – making the email appear to be sent from a legitimate source. The result of the phishing exercise will be to convince the recipient to click on a link.

## Website Penetration Testing

### Reconnaissance

We will use Whois for information gathering on the WV Lottery website. We will use the enumeration information uncovered to find vulnerabilities in the target for exploitation. The WHOIS lookup will retrieve specific network information regarding ownership, registration date, expiration date and other information we will need to assess the network. INS will do an ARIN (American Registry for Internet Numbers) lookup to retrieve information about IP addresses using arin.net and other viable sources and processes. We will conduct a public and entity server DNS lookup using command-line tools or our subscription software to gather accurate information on IP addresses.

We will conduct open-source intelligence (OSINT) to detect network/account compromise. The extent of intelligence gathering is dependent upon the scope of the environment but may include documentation reviews, public information searches, network mapping, application spidering, and network device configuration best practices, etc.

INS will build a custom password list through a systematic approach, including generating patterns reflective of common password user habits, to use for password strength testing and cracking.

INS will collect and categorize metadata which we will review with the goal of identifying meaningful insights and patters. We will look for inconsistencies and exploitable errors.

### Mapping

We will use a structured process to gather information on the WV Lottery's websites, network infrastructure, devices, and services to detect potential, exploitable vulnerabilities. We will use Nmap as a network mapper to detect open ports. It will be used to scan UDP ports, find all the live hosts in a range of IPs, and run scripts to find common vulnerabilities in applications. We will use this information to assess security risks to identify potential threats.

INS will begin the mapping process by manually exploring the WV Lottery's website to gain a better understanding of the structure and content. We will identify user input fields and map out the website's application flow. This will be followed by automated scanning using our Tenable Nessus tool, Rapid7, open-source tools and our own custom scripts.

We will identify the SSL/TLS cipher suites supported by the lottery's servers and assess their strength and security.

INS will perform an analysis of virtual hosting and load balancer configurations by assessing the setup, performance, and security of these components within the network infrastructure under normal and peak load conditions. We will then analyze server logs and load balancer metrics to uncover performance issues.

We will analyze and map the software configuration of the website by identifying and documenting the technologies, frameworks, libraries, and server configurations used to build and host the website. We will perform a source code analysis by reviewing source code, including HTML, CSS, JavaScript, etc. We will identify any custom scripts or third-party components. We will review HTTP response headers and procure information regarding the server software and version. We will review the web server's configuration files.

INS will conduct web application spidering/web crawling to systematically map the structure and content of the web application. We will use OWASP ZAP and/or mirroring code to download all accessible data for examination for possible data leaks to navigate through the web application, following links, submitted forms, and collecting information.

We will check if directory browsing is enabled on the web server and will look for directory listings pages that display the contents of directories when no default page is present. INS will brute-force directories, starting with common directory names and then expanding to less common ones.

INS will examine the lottery's website codebase, server configurations, and network traffic to understand how session cookies are created and managed. This will help us identify where session cookies are set within the website, analyze their predictability, and assess the security implications of session management practices.

## Discovery

INS will conduct discovery analysis on WV Lottery's website and applications to identify all authentication and authorization mechanisms used in the application, to include login forms, session management, access control lists, and role-based access controls (RBAC). We will analyze if entry point checks are performed, including URLs, API endpoints, etc. We will test for weak password policies, credential stuffing password resets and authentication bypass. We will also look for IDORs, RBAC bypass, horizontal privilege escalation and vertical privilege escalation. INS will test the security of sessions management mechanisms and verify that session tokens are securely generated.

INS will conduct vulnerability scans in multiple areas of network systems or facilities, such as in firewalls, application servers, web servers, and operating systems using our Tenable Nessus tool.

Our focus will be on whether a vulnerability has the potential to be exploited by a threat, which depends on a number of variables including (but not limited to):

- The strength of the security controls in place
- The ease at which a human actor could purposefully launch an attack
- The probability of an environmental event or disruption in each local area

We will conduct username/email enumeration using active enumeration techniques. These include email format guessing based on common patterns, directory enumeration by probing directory to discover user profiles, email aliases or hidden resources, and email harvesting using scripts to gather email addresses from various sources, including webpages, forms, or online directories.

INS will gain an understanding of the web application/web service specific vulnerabilities associated via open-source collection systems in addition to direct internet access to the source internet assigned protocol address for the target WV Lottery website through by analyzing common security issues that are unique to web applications and web services. Through our analysis, we will discover injection vulnerabilities, including SQL injection, XML injection and command injection. We will identify likely entry points for file upload attacks, HTTP headers, etc. Our tools will identify common vulnerabilities including cross-site scripting (XSS), including stored XSS and reflected XSS. We will look for indicators of cross-site request forgery (CSRF).

INS will conduct discovery analysis on WV Lottery's website and applications to identify all authentication and authorization mechanisms used in the application, to include login forms, session management, access control lists, and role-based access controls (RBAC). We will enumerate entry point checks are performed, including URLs, API endpoints, etc. We will test for weak password policies, credential stuffing password resets and authentication bypass. We will also look for IDORs, RBAC bypass, horizontal privilege escalation and vertical privilege escalation. INS will test the security of sessions management mechanisms and verify that session tokens are securely generated.

### Exploitation

Once enumeration efforts are complete (including reconnaissance, footprinting and vulnerability scanning), INS will attempt to exploit identified vulnerabilities to gain unauthorized access to WV Lottery's website, website applications, servers and databases. All testing will be conducted from INS Corporate locations. Our testing process will help the WV Lottery address potential hostile attempts by exposing weaknesses through penetration testing exploitation activities across their website and web applications. INS' penetration testing process follows standard OWASP and PTES guidelines. We will leverage Rapid7, Tenable Nessus, as well as open-source penetration testing tools and INS custom scripts to gain a foothold and elevate privileges to the network. We will supplement our automated attack procedures with manual analysis to identify vulnerabilities our automated tools may miss, including false positives, logic flaws or other authentication issues.

We will exploit web applications by identifying vulnerabilities, including SQL injection, cross-site scription (XSS) or insecure direct object references (IDOR). We will perform tests to assess the web server's vulnerabilities using a command-line vulnerability web scanner that performs comprehensive tests against web servers. Specifically, we will scan for dangerous files/CFGIs, outdated server software and other problems. The tools will with use include Rapid7, Tenable Nessus, Shodan, Nikto and Whois.

INS will immediately notify WV Lottery officials if a service disruption is caused by our testing efforts. If we find a critical vulnerability that could adversely affect the lottery's business process or services, we will immediately notify lottery officials. We will conduct a denial of service (DoS) attack on the website. INS will obtain prior approval, in accordance with the rules of engagement (ROE), prior to conducting DoS attacks.

INS will obtain prior approval, in accordance with the rules of engagement (ROE), prior to conducting brute force attacks on the website using our Rapid7 (Metasploit) tool and INS custom scripts. We will leverage information about usernames, passwords and credentials from word lists and other information gathered from our enumeration activities. Our tools will begin a brute force attack against the WV Lottery's website's login page to guess a useful system login providing unauthorized access or exhaust all combinations.

We will attempt to exploit vulnerabilities we found using Tenable Nessus, open-source tools and INS custom scripts to gain or elevate unauthorized access to the lottery's website. This may also involve leveraging known/published vulnerabilities to bypass security controls to gain a foothold within the website and avoid security measures present in the network.

Once we gain unauthorized access to the website, we will attempt post-exploitation and pivot by seeking to expand our control, escalate privileges and move laterally within the external network.

We will attempt to escalate privileges gained through exploitation to gain higher access. We will use various techniques, involving exploiting discovered vulnerabilities, misconfigurations, or other weaknesses we discovered. Once we obtain elevated privileges, we will conduct additional enumeration and discovery to obtain information regarding network resources, user accounts, system configuration and potential avenues for further exploitation. We will attempt to move latterly within the network to expand our foothold. We will attempt to pivot to access other parts of the network that are not directly connected to the website.

As a result of our exploitation efforts, we will provide a thorough vulnerability assessment of the website's security posture. We will evaluate those vulnerabilities and provide a risk assessment regarding the potential impact of the vulnerabilities. Factors we will consider include likelihood of exploitation, the sensitivity of the data or systems that could be affected. We will prioritize the vulnerabilities we discover using the common vulnerability scoring system (CVSS) included in our penetration testing/vulnerability assessment tools. We will recommend appropriate remediation/mitigation strategies that will consider each prioritized vulnerability. These may include patching, configuration control, version control, password strength, etc.

## Internal/Client-Side Network Penetration Testing

### Reconnaissance

We will use open-source and subscription tools, including Tenable Nessus Professional, Kali, and Kismet to identify software version, configurations, and potential vulnerabilities. Our tools will gather information about services and applications located on internal/client-side hosts. This will include anti-malware, firewall and IDS products located on the internal/client-side network.

INS will conduct active host reconnaissance on network hosts leveraging techniques including ping sweeps and DHCP fingerprinting. We will conduct port scanning and network mapping activities. These tactics will provide comprehensive internal network information. All testing will be conducted at WV Lottery locations.

We will conduct tests to verify if third-party programs or scripts can be executed within the network environment. This will be accomplished by testing known scripts, testing with simulated scenarios and monitoring for security events. We will evaluate the security risks associated with these risks.

## Mapping and Discovery

We will begin identifying possible vulnerabilities by creating an inventory of network assets, servers, workstations, network devices and applications using open-source, Rapid7 and Tenable Nessus tools. This will be followed by vulnerability scanning looking for known vulnerabilities and weaknesses. These scans will be configured to target specific IP ranges, ports or protocols based on the network architecture.

INS will evaluate security risk of receiving and executing various malicious payloads. This will involve malicious code detection through assessing the effectiveness of antivirus/anti-malware solutions. We will review vulnerability management practices and procedures regarding patches and updates related to scripting languages, frameworks and dependencies are being used within the internal network environment.

## Exploitation

We will conduct all internal/client-side penetration testing exploitation on-site at WV Lottery locations.

We will leverage the information gained from our enumeration efforts to exploit the internal/client-side network. We will exploit misconfigurations including weak passwords and credentials to gain unauthorized access using our Rapid7 tool and other INS developed customer scripts. We will look for opportunities to gain a foothold and escalate privileges to achieve higher levels of access.

The scope of our penetration testing efforts, in accordance with the ROE, will cover all aspects of the internal/client-side network, to include connected devices and endpoints, servers and firewalls and other network resources and functions. Our Rapid7 tool has the capability to leverage penetration testing capabilities to provide a comprehensive assessment of all network connected components. Our subject matter experts have the experience from conducting thousands of custom script-based penetration testing efforts to interpret results, identify false positives, measure risk and recommend mitigation and radiation to harden the internal network.

We will simulate a real-world attack on the internal network, which we will conduct at WV Lottery's locations. This test will leverage capabilities to bypass security restrictions by identifying security weaknesses present in the internal network and allowing our penetration testing professionals to escalate privileges within the network.

As a result of our exploitation efforts, we will provide a thorough vulnerability assessment of the internal/client-side network's security posture using assessment and reporting feature of our Tenable Nessus tool. We will evaluate those vulnerabilities and provide a risk assessment regarding the potential impact of the vulnerabilities. Factors we will consider include likelihood of exploitation, the sensitivity of the data or systems that could be affected. We will prioritize the vulnerabilities we discover using the common vulnerability scoring system (CVSS) included in our penetration testing/vulnerability assessment tool. We will recommend appropriate remediation/mitigation strategies that will consider each prioritized vulnerability. These may include patching, configuration control, version control, password strength, etc.

INS will conduct an uncredentialed penetration test on all connected systems within the provided ranges using our Tenable Nessus and Rapid7 (Metasploit) software tools, as well as our own custom scripts. All internal network vulnerability assessments will be conducted at the locations provided in the CRFQ. The assessment will be device agnostic and include, but not limited to workstations, servers, equipment, applications, mobile devices, printers, fax machines, voice over internet protocol (VoIP), video teleconference (VTC), internet of things (IoT), supervisory control and data acquisition (SCADA), as applicable, and any additionally discovered points of entry.

INS will scan all network protocols, to include UDP and TCP ports on all provided and newly identified internet network addresses to identify vulnerabilities and any open listening daemon for which communication is possible. Once identified, the listening service or daemon will be scanned for possible vulnerabilities and communication potential.

We will review the Active Directory for best practices. Established best practices include the following:

- We will look for indications of a poorly planned OU structure.
- Choice of a model
- Determine if users and computers are set apart
- If utilizing OU nesting
- Was the OU design documented
- Displaying a minimal number of privileged users
- Use of groups to assign privileges
- Secure accounts with administrator privileges
- Enforcement of modern password policies
- Enforcement of strong passwords on service accounts
- Regular review and removal of inactive or unused user accounts
- Disabled or deleted unnecessary security groups or distribution lists
- Clean up outdated or unused Group Policy Objects
- Audit and remove unnecessary user and computer objects

Environmental disruption is usually unique to a geographic location. Depending on the risk exposure level, the successful exploitation of a vulnerability varies from disclosure of information about the host to a complete compromise of the host. Risk exposure to organizational operations can affect the business mission, functions, or organizational reputation.

The ROE will cover when our team can perform assessments and testing on network information systems. The testing schedule and hours of operation will be determined and included as part of the rules of engagement. All assessment and testing activities will be coordinated with appropriate WV Lottery personnel and will be conducted at various work sites/locations. The internal assessment and testing events will be briefed to appropriate officials prior to the commencement of any testing activities. Passive testing will be performed during regular business hours, assuming the events will not disrupt normal daily operations. The location of testing and access will be coordinated prior to any planned activity.

INS will conduct penetration testing on identified domains, internet protocol addresses, and network entry points. In addition, INS will scan the designated ranges for all ports and protocols that may provide access to the system's networks. Each entry point will be examined via commercial and open-source scanning software to identify authentication methods, authentication thresholds, configuration errors, and security design flaws. The testing will be conducted in coordination with WV Lottery's defensive system operations to validate alerting mechanisms and defensive countermeasures.

## Wireless Penetration Testing

### Reconnaissance

We will use Whois for information gathering on the WV Lottery's wireless networks. The enumeration information uncovered is then used to find vulnerabilities in the target for exploitation. The WHOIS lookup will retrieve specific network information regarding ownership, registration date, expiration date and other information we will need to assess the network. INS will do an ARIN (American Registry for Internet

Numbers) lookup to retrieve information about IP addresses using arin.net and other viable sources and processes. We will conduct a public and entity server DNS lookup using command-line tools or subscription software to gather accurate information on IP addresses.

We will conduct open-source intelligence (OSINT) to detect network/account compromise. The extent of intelligence gathering is dependent upon the scope of the environment but may include documentation reviews, public information searches, network mapping, application spidering, and network device configuration best practices, etc. All testing will be conducted at WV Lottery locations.

INS will build a custom password list through a systematic approach, including generating patterns reflective of common password user habits, to use for password strength testing and cracking.

INS will collect and categorize metadata which we will review with the goal of identifying meaningful insights and patters. We will look for inconsistencies and exploitable errors.

## Mapping

We will use a structured process to gather information on the WV Lottery's network infrastructure, devices, services to detect potential, exploitable vulnerabilities. For example, we will use Nmap as a network mapper to detect open ports. It will be used to scan UDP ports, find all the live hosts in a range of IPs, and run scripts to find common vulnerabilities in applications. We will use this information to assess security risks to identify potential threats.

We will ensure we are compliant with legal regulations and the rules of engagement (ROE) before performing any wireless sniffing activities, including intercepting communications. We will follow legal and regulatory guidance concerning personally identifiable information (PII). INS will follow best practices for securing, controlling, and disposing of captured data.

We will use open-source and subscription tools to establish a baseline of traffic and perform Wi-Fi, Bluetooth, zigbee and other RF sniffing functions. INS will begin sniffing by ensuring a suitable Wi-Fi network adapter capable of packet capture is in place. We will then configure the wireless network adapter for monitor mode to capture all wireless traffic. We will begin packet capture/log analysis of captured traffic to understand network activity, identify devices and detect potential suspicious/malicious activities.

We will employee specialized tools and functions to conduct Bluetooth, software defined radio zigbee, packet capture and other RF sniffing analysis. We will ensure our sniffing tool is compatible with the adapter installed on the WV Lottery network for the wireless function we are mapping. We will discovery nearby wireless devices and will pair or connect the sniffing device with the target device as necessary. We will capture wireless traffic, analyze data exchanges between devices and analyze captured packets to understand wireless device interactions.

INS will conduct a war walk/drive around areas of high wireless network density or potential security risks at each of the WV Lottery locations listed in the CRFQ. We will equip, install, and configure a device to detect, scan and map wireless/radio networks. After recording information on detected networks (to include SSIDs, MAC addresses, etc.), we will use mapping software/GPS devices to pinpoint geographic locations of transmitters to create a visual map where wireless networks and transmitters were detected.

We will detect and map rogue access points. This will involve establishing a baseline of known, authorized access points. We will follow this with identifying access points that do not match the baseline of known devices broadcasting SSIDs that are not part of the authorized network. We will detect and analyze signal strength and location, identify MAC address, and analyze traffic patterns and encryption algorithms. We will also perform active scanning to probe detected access points and conduct a physical inspection of the WV Lottery site to identify unauthorized devices.

### Discovery

INS will identify access points that may could be exploited. We will look at access point firmware or configuration that show potential incidents of attack or incidents of compromise. We will check for weaknesses in encryption protocols, including WEP (wired equivalent privacy) or insecure configurations of WPA/WPA2/WPA3 that show potential or actual exploitation/compromise by attackers to monitor network traffic, perform man-in-the-middle (MiTM) attacks or crack encryption keys via WiFi Pineapples.

We will perform discovery on wireless networks for evidence or potential of evil twin attacks. We will look for evidence that rogue access points were set up with the same SSID as legitimate ones to trick users into connecting to gain access and deploy malware.

We will use open-source and subscription tools to connect and perform discovery on Wi-Fi, Bluetooth, zigbee and other RF protocols. INS will identify areas with poor coverage, dead zones, or interference issues that may be caused by misconfigurations or environmental factors. We will review the security settings of wireless Aps to endure they align with best practices and policies. We will check to see if the latest firmware updates and security patches are in place.

We will begin packet capture analysis of captured traffic to understand network activity, identify devices and detect potential suspicious/malicious activities.

INS will configure our Tenable Nessus tool to detect vulnerabilities specifically in wireless network components, including access points, wireless clients, and associated protocols. We will initiate the scan, monitor progress and review the scan results. Our subject matter experts will review the findings, eliminate false positives, prioritize vulnerabilities based on severity ratings, and review detailed information regarding each vulnerability, including descriptions, affected systems, and remediation recommendations.

### Exploitation

INS will conduct all wireless penetration testing activities on-site at WV Lottery locations. Our testing will encompass all wireless protocols and devices.

We will exploit weaknesses in encryption protocols, including WEP (wired equivalent privacy) or insecure configurations of WPA/WPA2/WPA3 that were uncovered during the reconnaissance, mapping, and discovery phases of the wireless penetration test. We will use Rapid, Tenable Nessus and INS custom scripts to attempt to detect, crack and defeat encryption defenses present in WV Lottery wireless networks. We will capture and analyze packets/logs to understand wireless network devices and resources. We will conduct traffic analysis to understand and exploit device interactions, network topography, extract information from protocols and system vulnerabilities via WiFi Pineapples.

We will attempt to intercept and alter communications between a compromised user and the network server. This may take on a passive attack by eavesdropping on communications we have compromised or an active attack that affects or alters a communication using man-in-the-middle (MiTM) attacks or crack encryption keys. We could also spoof the identity of a user or server and intercept/alter those communications.

We will utilize evil twin procedures to set up rogue access points using fake SSIDs that mimic the real ones to entice users to connect. Once the user connects, we will intercept information, perform MiTM attacks or otherwise affect communications.

INS will conduct denial of service (DoS) on identified wireless networks, accordance with the rules of engagement, with prior approval of lottery officials.

We will attempt to use up all available network bandwidth ("flooding") such that legitimate traffic can no longer pass to/from targeted systems. Additionally, we may use "distributed reflection denial-of-service" (DRDoS) to trick other, unwitting systems into aiding in the attack by flooding the target with network traffic.

During the attack, we will attempt to deny access to legitimate users on the wireless network. Also, we could alter the network by targeting network infrastructure devices (e.g. switches, routers, wireless access points, etc.) such that they no longer allow network traffic to flow to/from targeted systems as usual, leading to similar denial-of-service results without the need for flooding.

We could conduct system-targeted denial-of-service that focus on undermining the usability of targeted systems. Resource depletion is a common attack vector, where limited system resources (e.g. memory, CPU, disk space) are intentionally "used up" to cripple the target's normal operations. For example, we could employ SYN Flooding, which is a system-targeted attack which will use up all available incoming network connections on the target wireless network, preventing legitimate users and systems from making new network connections.

As a result of our exploitation efforts, we will provide a thorough vulnerability assessment of the wireless network's security posture. We will evaluate those vulnerabilities and provide a risk assessment regarding the potential impact of the vulnerabilities. Factors we will consider include likelihood of exploitation, the sensitivity of the data or systems that could be affected. We will prioritize the vulnerabilities we discover using the common vulnerability scoring system (CVSS) included in our penetration testing/vulnerability assessment tools. We will recommend appropriate remediation/mitigation strategies that will consider each prioritized vulnerability. These may include patching, encryption, configuration control, version control, password strength, etc.

## Reporting

Intelligent Network Security will provide an Executive Summary Report, a Technical Report, and a Findings Presentation to the WV Lottery. We will submit these reports and presentations in conjunction with external network penetration testing, website penetration testing, internal/client-side network penetration testing and wireless penetration testing engagements. Throughout the course of the engagement, INS will participate in periodic status meetings where we will provide updates on our activities and findings.

The cost for these reports will be included with their respective pricing item #. Examples of the Executive Summary, Technical Report and Findings Presentation are included at Appendix A.

### Executive Summary

In accordance with the RFQ, we will provide an overview of results including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior lottery management after the given assessment concludes. Prior to final submission, we will submit the summary report to the WV Lottery for review. We have included a sample of our Executive Summary Report as an appendix to this bid response. This report will also detail the value WV Lottery will receive from identification of vulnerabilities the testing results will provide.

## Technical Report

In accordance with the RFQ, we will provide a technical report which details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

INS will provide a technical report that includes our findings and risk ratings derived from Rapid7, Tenable Nessus and other open-source penetration testing tools. We will detail our testing methodology and provide recommendations for network security improvement.

The report will include:

- **Finding Number:** The unique application-generated security finding number.
- **IoC:** A piece of forensic data that can indicate malicious activity on a system or network.
- **Status:** The computational lifecycle status associated with the finding. If the finding is linked to a weakness for remediation management, the finding status is computed based on the completed status of the weakness. Finding status described below:
- **Unlinked** – The finding is not linked to a weakness.
- **Active** – The finding has been linked to a weakness that has an open status.
- **Completed** – The finding has been linked to a weakness where remediation has been completed successfully (i.e., the weakness is in completed status).
- **Rejected** – The finding has been rejected either as a false positive or risk accepted (i.e. risk-based decision). No remediation is required for the security finding.
- **Source:** The finding type such as vulnerability assessment, security audit, compromise assessment, etc., and the failed security control in which the finding was created.
- **Risk:** The finding description. This is the description of the finding as defined from the vulnerability assessment, security audit report, or from the results of an internal security review.
- **Business Impact Statement:** Impact of the finding to the organization if exploited.
- **Likelihood:** The likelihood that the finding will be exploited (High, Moderate, or Low).
- **Impact:** The impact to the organization if the finding is exploited (High, Moderate, or Low).
- **Risk Level:** The computed risk level associated with the finding based on the selected likelihood and impact. Please refer to Table 3-4 Risk Exposure Ratings for details.
- **Recommended Corrective Action:** The recommended control(s) needed to remediate the finding.

- **Reference:** Hyperlink to an external source in which the IoC is listed.

### Findings Presentation

We will prepare briefing slides and present our findings to the lottery management team. In accordance with the RFQ, this presentation will provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment. We will submit the presentation to WV Lottery in the manner/medium they choose. An example of our presentation is included at Appendix A

# Appendix A

See file: Appendix A

Executive Summary Example
Technical Report Example
Findings Presentation Example