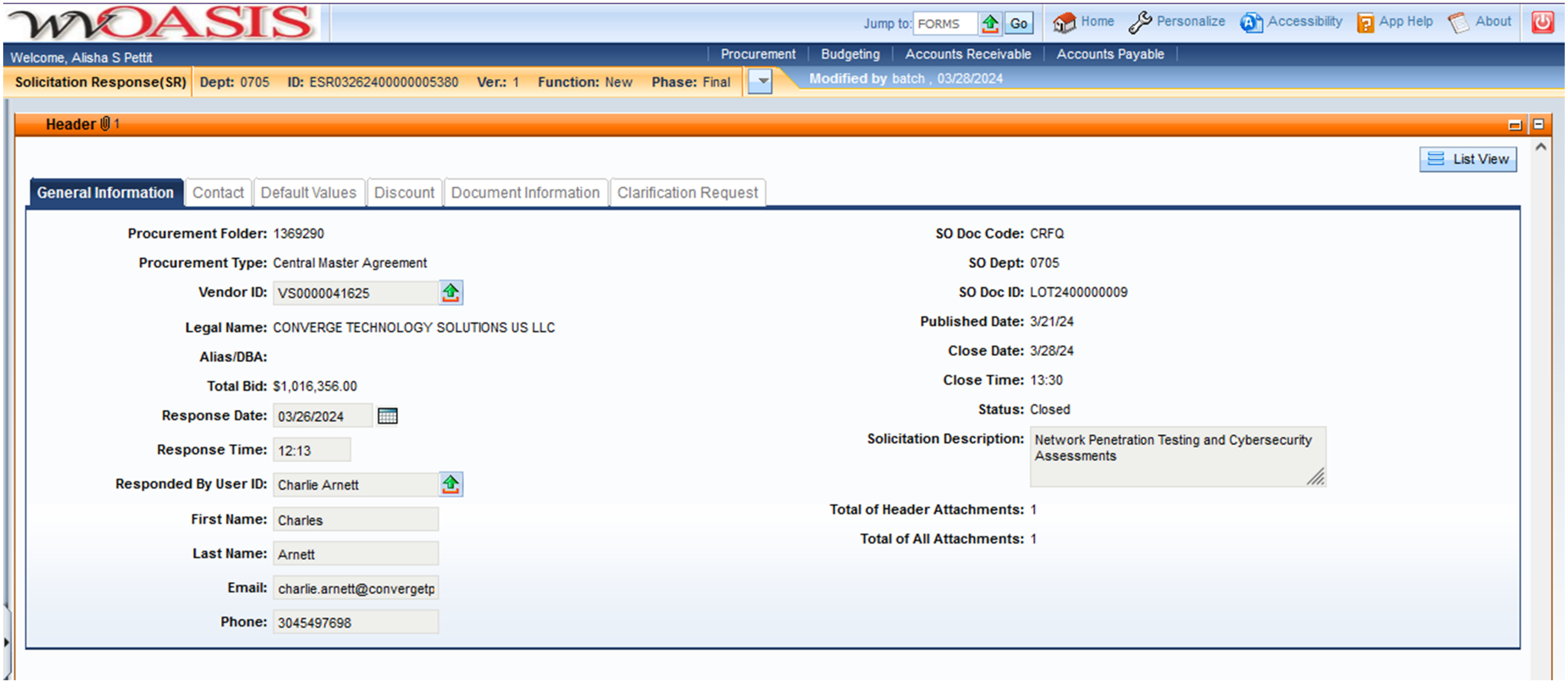
West Virginia
Purchasing Division

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: ESR03262400000005380 Ver.: 1 Function: New Phase: Final

Modified by batch , 03/28/2024

Header 1

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: VS0000041625

Legal Name: CONVERGE TECHNOLOGY SOLUTIONS US LLC

Alias/DBA:

Total Bid: $1,016,356.00

Response Date: 03/26/2024

Response Time: 12:13

Responded By User ID: Charlie Arnett

First Name: Charles

Last Name: Arnett

Email: charlie.arnett@convergetp

Phone: 3045497698

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: 1

Total of All Attachments: 1

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 ESR03262400000005380	1

VENDOR

VS0000041625
CONVERGE TECHNOLOGY SOLUTIONS US LLC

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 1016356 **Response Date:** 2024-03-26 **Response Time:** 12:13:32

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				184132.00

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				187296.00

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				348480.00

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				296448.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

CONVERGE
TECHNOLOGY SOLUTIONS

Due Date: March 28, 2024

Response to: State of West Virginia on behalf of West Virginia Lottery

Request for Quote: Network Penetration Testing and Cybersecurity Assessments

Submitted By:
Charlie Arnett, Account Executive
Address: 130 Technology Parkway, Suite 100, Peachtree Corners, GA 30092
Phone: 304.549.7698
Email: Charlie.Arnett@convergetp.com

© Converge Technology Solutions | convergetp.com

CONVERGE
TECHNOLOGY SOLUTIONS

March 28, 2024

Mr. Brandon L. Barr, Buyer
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305

Dear Mr. Barr,

Please find attached the Converge Technology Solutions (Converge) response for CRFQ 0705 LOT2400000009 due March 28, 2024. Converge understands the requirements of the RFQ and is submitting a response that meets the specifications.

At Converge, we prioritize safeguarding data, users, and brand integrity by staying relentlessly focused on our clients' cybersecurity needs. We understand the critical nature of protecting the diverse technological environment of the Lottery, which spans across multiple locations with various network devices and endpoints.

We have noted the specifications required for the contract, particularly the need for external network, website, and web application penetration testing as well as internal network vulnerability assessments. Converge is well-equipped to deliver these services, leveraging years of frontline experience and advanced technical knowledge.

Our advanced testing services are designed to uncover weaknesses before they can be exploited by attackers. We specialize in application testing and are proficient in identifying emerging threats through rigorous penetration testing. Additionally, our governance, risk, and compliance strategies will ensure that the West Virginia Lottery stays ahead of cloud security compliance and regulatory demands.

In the event of a security incident, our incident response framework will prepare your team to respond effectively and recover swiftly. Furthermore, Converge's strategic approach to architecture and integration will ensure that the cybersecurity solutions we implement align seamlessly with your business operations.

Converge also offers strategic staffing solutions to augment the West Virginia Lottery's cybersecurity resources and leadership, ensuring that your daily operations and executive strategy are fortified against cyber threats. Finally, our managed security services provide around-the-clock SOC monitoring and threat management, offering an additional layer of protection for your operations.

We look forward to the opportunity to discuss how Converge can support the West Virginia Lottery in achieving a robust and resilient cybersecurity posture.

Sincerely,

Charles D. Arnett
Senior Client Executive
charlie.arnett@convergetp.com

© Converge Technology Solutions | convergetp.com

Table of Contents

Confidentiality Notice: *This document may contain non-public, confidential information and shall neither be disclosed outside of Customer nor be duplicated, used or disclosed in whole or in part by Customer except to evaluate the services described herein or as provided by applicable law, including without limitation as may be required to respond to FOIA requests. This restriction does not limit the right to use the information contained in this document if it is obtained from another source without confidentiality restrictions.*

Forms

Following this page, please find Converge’s completed forms.

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:

Vendor Name : Converge Technology Solutions US, LLC

Address : 130

Street : Technology Parkway

City : Peachtree Corners

State : GA **Country :** US **Zip :** 30092

Principal Contact : Charlie Arnett

Vendor Contact Phone: 304.549.7698 **Extension:**

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

Vendor Signature X DocuSigned by: Karen Smallwood FD6598FB840A4D2... **FEIN#** 82-2782457 **DATE** 3/25/2024

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

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) Charlie Arnett, Account Executive

(Address) 130 Technology Parkway Peachtree Corners, GA 30092

(Phone Number) / (Fax Number) 304.549.7698

(email address) Charlie.Arnett@convergetp.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.

Converge Technology Solutions US, LLC
(Company)

DocuSigned by:
Karen Smallwood
FD6598FB840A4D2...
(Signature of Authorized Representative)

Karen Smallwood 3/25/2024
(Printed Name and Title of Authorized Representative) (Date)

866-910-4425
(Phone Number) (Fax Number)

contractscompliance@convergetp.com
(Email Address)

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:

Vendor Name : Converge Technology Solutions US, LLC

Address : 130

Street : Technology Parkway

City : Peachtree Corners

State : GA **Country :** US **Zip :** 30092

Principal Contact : Charlie Arnett

Vendor Contact Phone: 304.549.7698 **Extension:**

FOR INFORMATION CONTACT THE BUYER

Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

Vendor Signature X DocuSigned by: Karen Smallwood FD6598FB840A4D2... **FEIN#** 82-2782457 **DATE** 3/25/2024

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

DocuSign Envelope ID: A3875AFD-0236-4D17-ABC3-47B7D0A68337

	Document Phase	Document Description	Page 4
LOT2400000009	Final	Network Penetration Testing and Cybersecurity Assessments	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

Addendum Acknowledgement

Following this page, please find Converge’s acknowledgement of Addendum 1.

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:

Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration a..... See Page 2 for complete info

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 : Converge Technology Solutions US, LLC

Address : 130

Street : Technology Parkway

City : Peachtree Corners

State : GA **Country :** US **Zip :** 30092

Principal Contact : Charlie Arnett

Vendor Contact Phone: 304.549.7698 **Extension:**

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

Vendor Signature X DocuSigned by: Karen Smallwood FD6598FB840A4D2... **FEIN#** 82-2782457 **DATE** 3/25/2024

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 PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON US	WV	CHARLESTON 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 PO BOX 2067		LOTTERY 900 PENNSYLVANIA AVE	
CHARLESTON US	WV	CHARLESTON 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 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.

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 "Prior to Award both parties, the Vendor and Lottery must sign".**

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. The WV Tax Department.
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. 6
[ ] Addendum No. 2	[ ] Addendum No. 7
[ ] Addendum No. 3	[ ] Addendum No. 8
[ ] Addendum No. 4	[ ] Addendum No. 9
[ ] Addendum No. 5	[ ] 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.

Converge Technology Solutions US, LLC
Company

DocuSigned by:
Karen Smallwood
FD6598FB840A4D2...
Authorized Signature

3/25/2024
Date

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

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.

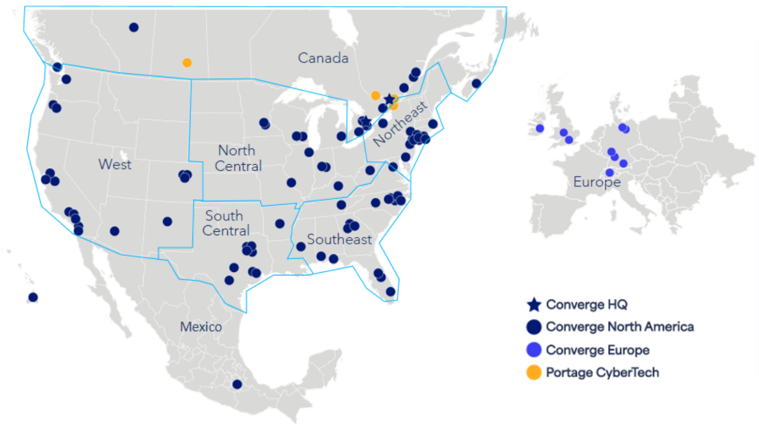
Converge Technology Solutions US, LLC ("Converge") is a services-led, software-enabled, IT & Cloud Solutions provider focused on delivering industry-leading solutions. Converge's global approach delivers advanced analytics, artificial intelligence, application modernization, cloud platforms, cybersecurity, digital infrastructure, and digital workplace offerings to clients across various industries. Converge supports these solutions with advisory, implementation, and managed services expertise across all major IT vendors in the marketplace. This multi-faceted approach enables Converge to address the unique business and technology requirements for all clients in the public and private sectors.

Converge is comprised of 35 entities that make up the organization's Portfolio of Companies. This structure allows Converge a wide-reaching team and deep, ever-expanding solutions and services capabilities. An overview of Converge's structure and portfolio of companies can be found here: Our Story (convergetp.com)

In 2022 Converge bolstered the Cybersecurity practice with a strategic and dedicated acquisition around cyber, in CBI. Today our cyber security practice has over 200 practitioners that enable our account executives, and ultimately our clients, to solve business problems through cyber solutions and have been doing it for over 25 years. This team is focused on top vendor and platform capabilities so we can advise and consult on technology itself, but also where our core services can help deliver those secure outcomes. Our core services are Advanced Testing Services, Governance Risk & Compliance, Data Protection, Identity & Access Management, Staff Augmentation and Managed Security Services. The practice holds an impressive NPS rating of 81 and we hold many top clearances and certifications as we go to market under our AIM methodology - Assess, Implement, and Manage.

Converge Platform

Scaled Footprint with Strong Partner Relationships and Capabilities



60+ Global Office Locations

500+ Global Sales Personnel

1,500+ Global Technical Resources

60+ Pre-Sales Solution Architects

35 Solution Specialists

with

1,000+ Certifications

4,000+ Customers

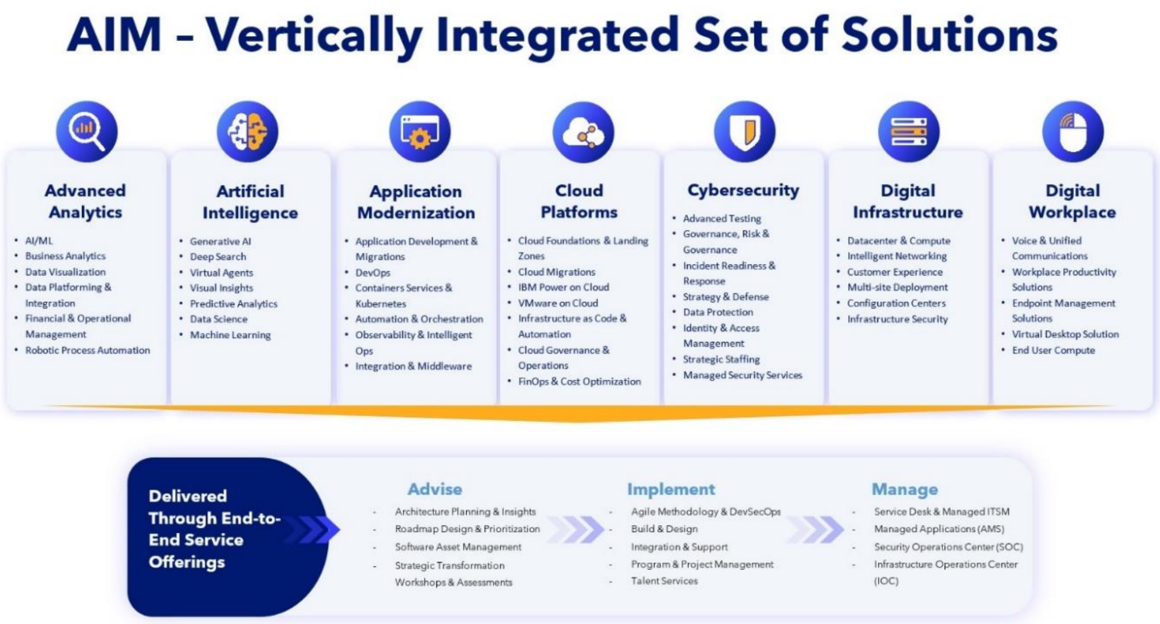
Our goal is to provide a trusted partner that brings together world-class solutions and services to help reduce costs, increase efficiency, and create competitive advantages.

Converge Solutions & Services

- Advanced Analytics: Utilizing mathematical and statistical methods, we provide clients with intelligent insight into their data, and enable enterprises to forecast trends, predict future behavior, and better navigate toward success.
- Artificial Intelligence (AI): Unlock scalability for your operations, empower your team, and redirect focus to tasks that demand human expertise – let the robots handle the rest.
- Application Modernization: Updating older software for newer computing approaches, including newer languages, frameworks, and infrastructure platforms, we deliver improved performance and security for modern applications.
- Cloud Platforms: Multi-faceted Cloud Solutions enable the adoption of new strategies and approaches that embrace Cloud technologies and evolve the way clients save, store, and access data.
- Cybersecurity: Offering defense tools, risk management approaches, technologies, end-user training, and best practices, Converge tailors solutions to protect critical networks, infrastructure, devices, applications, cloud platforms, and data from attacks or unauthorized access.
- Digital Infrastructure: Delivering applications through secure, mobile, reliable access, we enable clients to achieve enhanced business outcomes. Digital transformation is the core tenet of Converge's approach to digital infrastructure.

- Digital Workplace: Providing the ability to work securely, collaboratively, and productively from everywhere, we help deliver IM, email, file collaboration, voice and video collaboration, end-user management, and subscription services.

Through our Full Spectrum of Services we "AIM" to support these solutions with advisory, implementation, and managed (AIM) services expertise across all major IT vendors in the marketplace. This multi-faceted approach enables Converge to address the unique business and technology requirements for all our clients both in the public and private sectors.


AIM – Vertically Integrated Set of Solutions
Advanced Analytics
• AI/ML
• Business Analytics
• Data Visualization
• Data Platforming & Integration
• Financial & Operational Management
• Robotic Process Automation
Artificial Intelligence
• Generative AI
• Deep Search
• Virtual Agents
• Visual Insights
• Predictive Analytics
• Data Science
• Machine Learning
Application Modernization
• Application Development & Migrations
• DevOps
• Containers Services & Kubernetes
• Automation & Orchestration
• Observability & Intelligent Ops
• Integration & Middleware
Cloud Platforms
• Cloud Foundations & Landing Zones
• Cloud Migrations
• IBM Power on Cloud
• VMware on Cloud
• Infrastructure as Code & Automation
• Cloud Governance & Operations
• FinOps & Cost Optimization
Cybersecurity
• Advanced Testing
• Governance, Risk & Governance
• Incident Readiness & Response
• Strategy & Defense
• Data Protection
• Identity & Access Management
• Strategic Staffing
• Managed Security Services
Digital Infrastructure
• Datacenter & Compute
• Intelligent Networking
• Customer Experience
• Multi-site Deployment
• Configuration Centers
• Infrastructure Security
Digital Workplace
• Voice & Unified Communications
• Workplace Productivity Solutions
• Endpoint Management Solutions
• Virtual Desktop Solution
• End User Compute
Delivered Through End-to-End Service Offerings
Advise
- Architecture Planning & Insights
- Roadmap Design & Prioritization
- Software Asset Management
- Strategic Transformation Workshops & Assessments
Implement
- Agile Methodology & DevSecOps
- Build & Design
- Integration & Support
- Program & Project Management
- Talent Services
Manage
- Service Desk & Managed ITSM
- Managed Applications (AMS)
- Security Operations Center (SOC)
- Infrastructure Operations Center (IOC)

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.

In the event that we are intended to be awarded, we will provide references. Just as we will treat West Virginia Lottery business with the highest of confidentiality, and due to current NDAs in place with our clients and the public nature of this RFQ, we are unable to provide references at this time. However, if West Virginia Lottery would like to speak with our past and current clients prior to award, we will work with West Virginia Lottery to arrange introductions with our clients on a one-on-one basis to discuss our work and past performance with clients of like size and similar scope.

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.

Converge will assign a project team upon the successful award of the Lottery assessments; however, we are pleased to submit the following qualifications for your consideration. We perform over two hundred (200) assessments like yours annually; one-hundred fifty (150) of those are by unique clients with many using our advanced testing services repeatedly and year-over-year. We have thirty (30) penetration testers on staff – all full-time Converge employees – and fifteen (15) of those FTEs maintain active Top Secret clearance. Converge is a good steward to the cybersecurity community and has discovered five (5) CVEs, aka zero-days, in commercial products within the last six (6) months. We also frequently contribute to open-source projects.

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

Converge penetration testers hold the following certifications: OSCP, OSEP, OSWA, OSWE, CRTO, PNPT, GPEN, GWAPT. Please see our response in 3.3.1 to learn more about our red team.

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.

Our proposed penetration test will adopt a systematic technical approach aligned with industry-standard frameworks and will use components from the Penetration Testing Execution Standard (PTES) and National Institute of Standards and Technology (NIST) SP800-115, with our tactics, techniques, and procedures (TTPs) aligned to the MITRE ATT&CK framework. The web application penetration testing will align to the Open Web Application Security Project (OWASP) Top 10 Project. Our typical test methodology will encompass reconnaissance, initial access, privilege escalation, lateral movement, and exfiltration – mirroring the common TTPs observed in real-world cyberattacks. These techniques and the tools used will be designed to be evasive, providing access, persistence, lateral movement, and privilege escalation that eludes most commodity incident detection and response capabilities. Most importantly, our testers mimic the tenacity of real-world threat actors. We use open-source, commercial, and internally developed custom tooling that will be uniquely tailored to each IT environment to maximize impact in search for crown jewels.

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.

Converge will comply.

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.

Converge will comply.

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.

Please see Attachment 1 for the Budgetary Services Estimate (BSE) for responses to the above Mandatory Requirements

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

Please see pricing page.

Performance

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.

Converge confirms and agrees.

Payment

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.

Per the Pricing Page requirements, Converge has provided a unit cost per Assessment & Reports.

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	$23,016.50 -	$ 184,132.00 -
2	4.2	Website Penetration Testing	8	$ 23,412.00 -	$187,296.00 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ $43,560.00 -	$ 348,480.00 -
4	4.4	Wireless Penetration Testing	8	$37,056.00 -	$ 296,448.00 -
				TOTAL BID AMOUNT	$ 1,016,356.00 -

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:	Converge Technology Solutions US, LLC
Vendor Address:	130 Technology Parkway Peachtree Corners, GA 30092
Email Address:	local contact: Charlie.Arnett@convergetp.com corporate: contractscompliance@convergetp.com
Phone Number:	local contact: 304.549.7698 corporate: 866-910-4425
Fax Number:	859.977.4747
Signature and Date:	DocuSigned by: Karen Smallwood FD6598FB840A4D2... 3/25/2024

Travel

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.

We will accommodate onsite work and have built travel into the fixed cost.

Facilities Access

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.

We will accommodate onsite work and have built travel into the fixed cost.

Vendor Default

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.

10.3 Any other remedies available in law or equity.

Converge has reviewed and confirms.

Miscellaneous

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: ______________________
Telephone Number: _________________________
Fax Number: ________________________________
Email Address: _____________________________

Please see following page.

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: Charlie Arnett
Telephone Number: 304.549.7698
Fax Number: 859.977.4747
Email Address: Charlie.Arnett@convergetp.com

Attachments

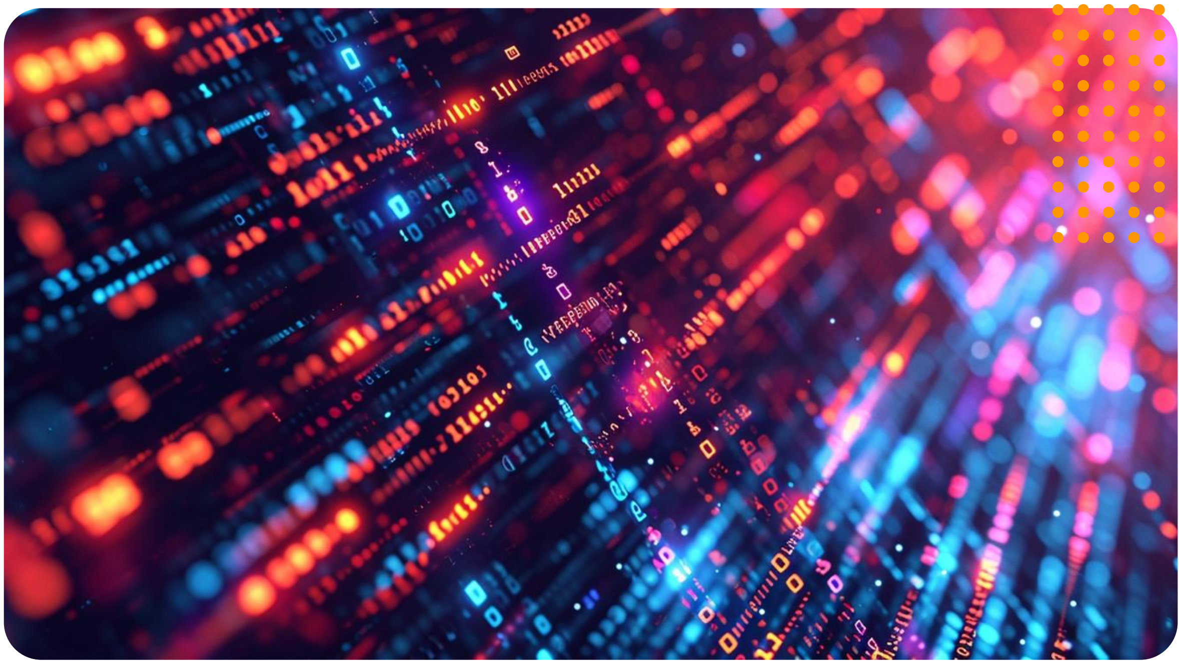
Attachment 1 – Budgetary Services Estimate (BSE)

Attachment 1 – Budgetary Services Estimate (BSE)

CONVERGE
TECHNOLOGY SOLUTIONS

Budgetary Services Estimate:

Penetration Test



Prepared by:

Phil Traversa, Cybersecurity Solutions Architect
Converge Technology Solutions
March 22, 2024

Version: 1
PSR-026429

Protect What You've Built.
Collaborate. Connect. Converge.

Contact Information

Legal Company Name	West Virginia Lottery
Primary Point of Contact (Name)	Brandon L Barr
Email	brandon.l.barr@wv.gov
Phone	(304) 558-2652
Address	2019 Washington St E, Charleston, WV 25305
Primary Domain/Website	https://wvlottery.com
Industry	Government
Account Executive	Charlie Arnett
Solution Specialist	Eric Potvin
Solution Architect	Phil Traversa

Summary

West Virginia Lottery ("Client") has engaged Converge Technology Solutions ("Converge") to assist with a penetration test (the "Services").

Based on our understanding of your needs, Converge has identified the following objectives that you would like assistance to address:

- Perform thorough testing to meet specific compliance mandates and due diligence requirements.
- Leverage advanced and manual techniques that more effectively identify critical threats.
- Use the testing to measure the effectiveness of controls, tools, processes, and response.
- Provide prioritized tactical and strategic recommendations based on identified vulnerabilities to allow the organization to quickly remediate discovered threats.
- Build a framework for continuous security improvement.

Scope of Work

Asset/Component	Description	Scope Detail
External Penetration Test	Penetration testing against the external (WAN) environment.	In scope Up to 50 IPs
Internal Penetration Test	Penetration testing against the private (LAN) environment.	In scope Up to 500 IPs 8 locations
Lateral Movement & Privilege Escalation	When a system is compromised, the next attack vector is to move laterally and escalate privileges.	In scope
Wireless Penetration Test	Penetration testing against the wireless (WLAN) environment.	In scope Up to 2 SSIDs per location 8 locations
Social Engineering (Email) Test	Security awareness testing through a simulated social engineering campaign via email.	In scope 1 scenario Up to 300 test targets
Web Application Penetration Test	Web application assessment with unauthenticated testing using the Open Web Application Security Project (OWASP) framework.	In scope 1 application Up to 40 dynamic pages

Supporting Details		
Delivery Model	Testing to be conducted remotely or onsite.	Hybrid – both remote and onsite as per the WV Lottery
Testing Hours	Timeframe in which the testing will be conducted (normal business hours, after hours, weekend)	Normal business hours
Penetration Test Methodology	The approach in which the penetration test will be conducted. 1. White Box (full information provided) 2. Black Box (no information provided) 3. Gray Box (some information provided)	Gray Box

Penetration Testing Methodology

Established security assessment and penetration testing methodologies are followed that are based on industry standards and best practices that include components from the National Institute of Standards and

Technology (NIST) SP800-115, the Penetration Test Execution Standard (PTES), and the MITRE ATT&CK Framework (MITRE).

The processes performed for each component of the testing are outlined in the service descriptions included in the Scope of Work sections that follow. No activities that would intentionally cause an outage or denial of service (DoS) or damage, corrupt, or delete any systems or confidential information will occur.

External Penetration Test

The penetration test process will include the following tasks:

- **Reconnaissance:** A search and review is performed of public data and open-source intelligence (OSINT) available on the Internet that can reveal information about Client that could be leveraged to attack Client's IT environment, systems and technology.
- **Network Discovery and Enumeration:** An extensive identification and port-scanning process is performed to map out active systems on the network. ICMP and listening TCP and UDP ports are identified for these hosts and devices, along with the associated services being provided.
- **Vulnerability Scanning:** Using vulnerability scanning tools, potential vulnerabilities are found on the systems. These initial scans are run in a "safe mode" to avoid potential impact to system availability.
- **Manual Testing and False-Positive Validation:** Using various tools, along with manual tests and techniques, the validity of the discovered vulnerabilities is verified.
- **Penetration Testing:** For higher risk issues, controlled attempts to exploit the vulnerabilities to better qualify the true level of risk and potential compromise. During the testing process, various tools along with manual methods are used for the exploitation testing, but denial-of-service testing will NOT be performed.
- **Advanced Penetration Testing:** If access is gained to a system during this penetration testing it will be used to escalate access as well as pivot and attack other systems where applicable.
- **Data Analysis and Reporting:** The results of the testing are reviewed and analyzed, and a report is created that documents the findings, identifies critical- and high-risk vulnerabilities, and provides recommendations and guidance on how to remediate the vulnerabilities and strengthen information security. The report developed is peer-reviewed by another penetration tester, and also sent through a QA review before delivery to the Client.

Internal Penetration Test

The penetration test process will include the following tasks:

- **Network Discovery and Enumeration:** An extensive identification and port-scanning process is performed to map out active systems on the network. ICMP and listening TCP and UDP ports are identified for these hosts and devices, along with the associated services being provided.
- **Vulnerability Scanning:** Using vulnerability scanning tools, potential vulnerabilities are found on the systems. These initial scans are run in a "safe mode" to avoid potential impact to system availability.
- **Manual Testing and False-Positive Validation:** Using various tools, along with manual tests and techniques, the validity of the discovered vulnerabilities is verified.
- **Penetration Testing:** For higher risk issues, controlled attempts to exploit the vulnerabilities to better qualify the true level of risk and potential compromise. During the testing process, various tools along with manual methods are used for the exploitation testing, but denial-of-service testing will NOT be performed.
- **Advanced Penetration Testing:** If access is gained to a system during this penetration testing it will be used to escalate access as well as pivot and attack other systems where applicable.

- **Data Analysis and Reporting:** The results of the testing are reviewed and analyzed, and a report is created that documents the findings, identifies critical- and high-risk vulnerabilities, and provides recommendations and guidance on how to remediate the vulnerabilities and strengthen information security. The report developed is peer-reviewed by another penetration tester, and also sent through a QA review before delivery to the Client.

Wireless Penetration Test

Testing attempts for unauthorized network access through wireless network discovery and penetration testing of the wireless network(s) at the scoped locations. Without authorized authentication, attempts to enumerate and access the wireless infrastructure will be performed. Using scans, tools, and testing techniques, the following will be performed:

- Enumeration of wireless device information and configuration.
- Penetration testing to attempt to gain unauthorized access to the wireless network(s) and where successful identify the level of corporate network access gained.

Social Engineering (Email) Test

Common social engineering techniques and phishing attempts will be performed to discover gaps in user awareness, security policy, and access controls. Security awareness is reviewed through interaction with Client employees using email and web phishing.

Communication and close coordination with the designated Client project contacts will be performed, but other Client staff are not notified of the social engineering so that stealth can be maintained and the social engineering truly effective. Attempts are made to get employees to divulge confidential information, including login credentials, passwords, and other critical data.

The overall process consists of the following tasks:

- **Scenario Development:** Working with Client to develop the cover story that is used to frame the social engineering attempts. Client will approve before proceeding.
- **Phishing Attack Setup:** A phishing email that is to be sent to the targeted Client staff is created. Fake domain names may be registered to be used to facilitate the phishing. There will be no impact on Client systems from the attack simulation. If any fake domains are newly registered, a two-week delay should be expected to allow for DNS propagation and email blocklist avoidance.
- **Phishing Testing and Customer Sign-off:** The proposed phishing email is reviewed with Client to validate the approach to be used. If necessary, changes to the email may be made to meet Client requirements or concerns. The testing may also reveal that that phishing emails are being blocked by Client's security controls already in place (e.g., spam filters, suspicious website blocking). Allow-listing of test accounts and domains may be required to get the full effect of this security awareness effort.
- **Email Phishing Execution:** The phishing emails will be sent to a target list of Client staff. Client will approve the target list before proceeding.
- **Data Collection, Analysis, and Reporting:** The response to the phishing email by customer employees will monitored and tracked to see how the targeted staff responds. Statistics are collected and information gathered and presented in a report.

Web Application Penetration Test

The web application penetration test is designed to provide insight into methods of attack against a specific application, or a suite of resident applications, and present a reasonable example of what an attacker might accomplish. The assessment is intended to provide a comprehensive security evaluation of an application; it concentrates on modeling specific attack scenarios, identifying vulnerabilities, and validating exploitation possibilities.

Converge uses the Open Web Application Security Project (OWASP) framework when assessing web applications. OWASP is an industry standard security framework used to assess and protect web applications. OWASP testing requirements include, but are not limited to: Information Gathering, Configuration Management, Identity Management, Authentication Testing, Authorization Testing, Session Management, Input Validation, Error Handling, Weak Cryptography, Business Logic Testing, and Client-Side Testing. Using additional advanced and non-traditional testing techniques, Converge will be able to identify vulnerabilities that typical assessment frameworks are unable to discover.

Note: Testing may be performed against non-production copies of the web application, but Client must ensure the copies match production code for the results to be valid.

Rules of Engagement

- All scanning and testing will be scheduled and coordinated with Client prior to initiation of the testing.
- All testing will be performed remotely over the Internet.
- All testing will be performed during normal business hours (8am to 5pm), but there may be instances where it would help meet project schedule requirements by letting scans and testing proceed past 5pm. Converge will request permission and coordinate the scheduling with Client before performing any scanning or testing outside the normal business-hours window.
- All IP addresses to be tested must be provided by Client at project kickoff.
- The source IP addresses of the scanning system(s) that will be used to perform the testing will be provided to Client at project kickoff.
- Client will allow-list the scanning system's IP addresses on intrusion prevention systems (IPS), web application firewalls (WAFs) or other network-based exploit prevention services so full vulnerability testing can be performed in an efficient manner to minimize time and cost. If an IPS/WAF device is determined to be in preventative mode or otherwise identified to be interfering in testing, testing will be stopped, and Client personnel notified to troubleshoot the allow-listing configuration. Converge will work with Client personnel to test the allow-listing for up to two hours, spanning no more than two days, at which point other IPS allow-listing testing time will be billed or Converge will resume testing as-is.
- Assessment components using automated scanning tools for data gathering will NOT use evasion techniques unless specifically stated in the scope. This may result in numerous log statements captured across the assessed infrastructure, including firewall, intrusion detection, and server logs.
- If scanning or testing is being performed against systems hosted by a cloud service/hosting provider, such as Amazon Web Services (AWS) or Microsoft Azure, Client will perform any notification or authorization steps required by the hosting provider. This process may take multiple days to complete depending on the hosting provider, so to avoid delays in the project execution, Client should complete this requirement prior to project kickoff.
- **Internal Penetration Test:** The internal testing may be facilitated using a remotely accessible scanning system that will be provided. It is a requirement that this device has internet access on HTTPS (TCP 443). Assistance from Client will be required in setting up this scanning system on the Client internal network to facilitate testing.
- **Internal Penetration Test:** If applicable, after any internal testing using the supplied scanning system(s) is complete, a request to return the system(s) will be made, and a FedEx shipping label provided to

return the system(s). If the system is not returned within 45 days of that request, the Client will be charged $3,000 for lost equipment fees per system(s) not returned.

- **Wireless Penetration Test:** All wireless testing work will be performed onsite at the Client location.
- **Wireless Penetration Test:** Client will provide physical access to the site and floors where the wireless network SSIDs to be tested are located.
- **Wireless Penetration Test:** If applicable, after any wireless testing using the supplied scanning system(s) is complete, a request to return the system(s) will be made, and a FedEx shipping label provided to return the system(s). If the system is not returned within 45 days of that request, the Client will be charged $3,000 for lost equipment fees per system(s) not returned.
- **Social Engineering (Email) Test:** There may be a delay of up to two (2) weeks between the creation and approval of the fake phishing email and the execution of the phishing attack simulation to allow any created fake domains to clear security checks.
- **Social Engineering (Email) Test:** To avoid any concerns that employees are being unfairly targeted, Client may provide a full list of staff email addresses and then a random selection of staff will be chosen as targets for the phishing from the list.
- **Social Engineering (Email) Test:** Allow-listing on anti-spam and anti-phishing security controls, including at the endpoint, may be requested to ensure delivery to targeted email addresses.
- **Web Application Penetration Test:** Client will provide the URLs for the web application(s) before the test is scheduled to begin.
- **Web Application Penetration Test:** If the application test requires a credentialed role, the test accounts to be used must be provided before the scheduled start date. If the account is not provided before the start date, the assessment will be limited to a non-credentialed review of that specific application.
- **Web Application Penetration Test:** The version or instance of the application being tested should not be changed or updated during the testing period.
- **Web Application Penetration Test:** Prior to the initiation of testing, Client will perform a high-level demonstration or “walk-thru” of the application with Converge so the functionality, purpose, and use of the application by Client and Client’s customers is understood to provide context to the testing and help ensure all critical functions are tested.

Project Methodology

Converge strives to ensure every engagement meets the business objectives of its clients. To achieve this goal, the project execution process is well defined from years of experience, but flexible and client-focused throughout the project. A project manager and one or more cybersecurity consultants will be assigned to the project, with oversight and guidance provided by the Cybersecurity Professional Services Manager.

Before executing the work detailed in this SOW, a project kickoff meeting will be held with Client, the project manager, and the assigned consultant(s) to ensure all parties are aligned regarding the project timeline, resource work schedules, project start prerequisites, travel logistics (if applicable), change management requirements, and project deliverable expectations.

Project Management

A project manager will be assigned to facilitate project success through planning, coordination, tracking, reporting, communication, and escalation as needed. In alignment with the Converge proven project management process, the project manager will complete the following tasks:

- Conduct project kick-off meeting
- Follow up on completion of project prerequisites
- Develop workplan and timeline for in-scope activities

- Manage project communications and resource scheduling
- Distribute project status dashboard
- Conduct project status meetings and/or standups/sprint ceremonies (agile)
- Identify and track project risks and issues
- Facilitate any necessary project change requests
- Ensure project deliverables are completed and meet expectations
- Conduct closeout meeting

Deliverables

Documentation Deliverable	Description
External Penetration Test & Social Engineering Report	Detailed report deliverable with an executive summary component and technical report component including results from vulnerability scanning and risk ranked as per the WV Lottery requirements.
Web Application Penetration Test Report	Detailed report deliverable with an executive summary component and technical report component including results from vulnerability scanning and risk ranked as per the WV Lottery requirements.
Internal Penetration Test Report	Detailed report deliverable with an executive summary component and technical report component including results from vulnerability scanning and risk ranked as per the WV Lottery requirements.
Wireless Penetration Test Report	Detailed report deliverable with an executive summary component and technical report component including results from vulnerability scanning and risk ranked as per the WV Lottery requirements.

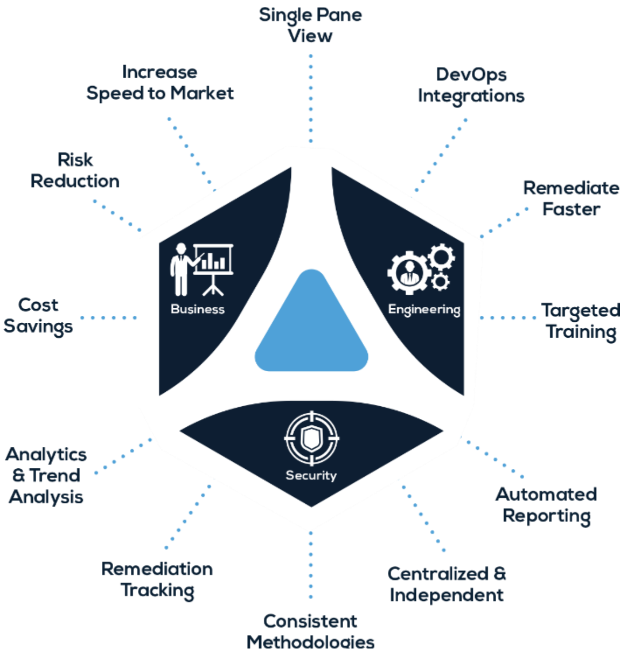
Unless otherwise stated, any documentation deliverables shall be provided in electronic format.

Red Team Portal

As part of this engagement, Converge will provide the client with access to the Red Team Portal at no additional charge. Access to the Red Team Portal will be available for up to one (1) year, and no less than thirty (30) days, beyond the end of the project. The portal connects business, technology, and security teams to reduce vulnerability remediation lead times and increase visibility into potential risks and priorities. The Red Team Portal is proven and validated in organizations large and small to help save direct costs, increase visibility, and reduce effort on every assessment.

The Red Team Portal uses a world-class, enterprise-grade solution explicitly built for penetration and application testing. The portal is secured by best-in-class features, configurations, and controls. The solution runs in a private cloud environment and meets compliance standards such as but not limited to ISO27001/27017/27018, SOC 1, 2 and 3, FIPS140-2, and GDPR. A complete overview of the security architecture, controls, and configurations is available upon request.

Get Secure Quick	•Begin remediation efforts in real-time as results from the engagement are entered into the portal by our team. Receive real-time notifications when our team finds a critical threat.
Clearer View	•See your organizations vulnerable areas and know your real priorities using detailed analytics, dashboards, and remediation tracking features.
Team Collaboration	•Our red team and your business, technology, and security teams can collaborate in one place.
Integration	•Centralized integrations via secure self service API, JIRA, exportable formats, etc.
Gain Cost Efficiencies	•Tools and workflows to reduce project overhead and costs by up to 40%



Pricing and Payment Terms

Fixed Price: Client is invoiced a fixed fee inclusive of project management and expenses for the Services. Please refer to **Exhibit A – Pricing Page** for pricing details.