



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.

Header @ 1

[List View](#)**General Information** | [Contact](#) | [Default Values](#) | [Discount](#) | [Document Information](#) | [Clarification Request](#)

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: VS0000009518

Legal Name: VTECH SOLUTION INC

Alias/DBA:

Total Bid: \$710,080.00

Response Date: 03/28/2024

Response Time: 12:39

Responded By User ID: vTechadmin

First Name: Vishnu

Last Name: Naruka

Email: vtech.sled@vtechsolution.

Phone: 2029026321

SO Doc Code: CRFQ

SO Dept: 0705

SO Doc ID: LOT240000009

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 ESR03272400000005469	1

VENDOR
 VS0000009518
 VTECH SOLUTION INC

Solicitation Number: CRFQ 0705 LOT2400000009
Total Bid: 710080
Response Date: 2024-03-28
Response Time: 12:39:29
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				340560.00

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				100000.00

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				151360.00

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				118160.00

Comm Code	Manufacturer	Specification	Model #
81111801			

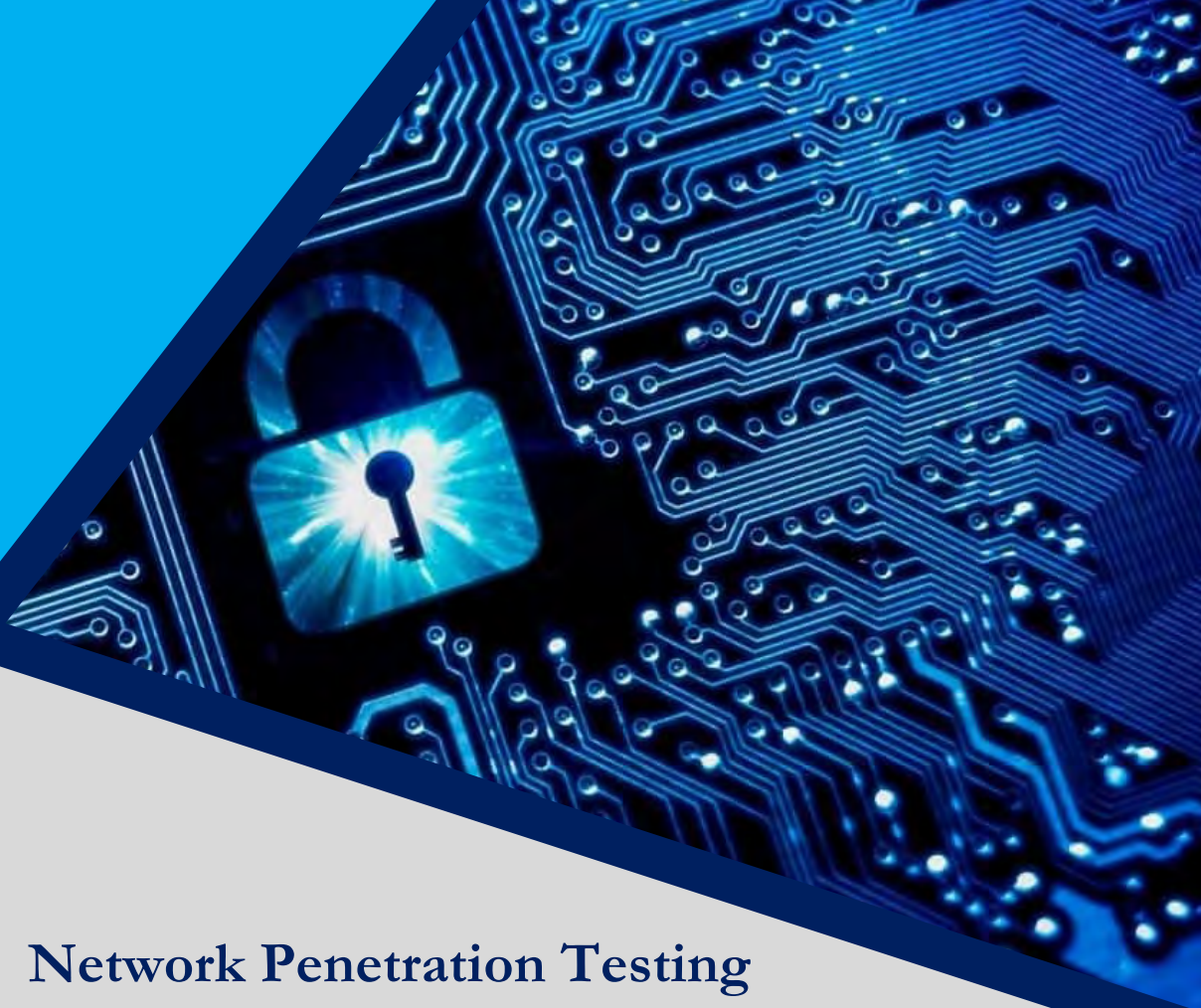
Commodity Line Comments:

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page



VTECH SOLUTION™
You Seek, We Deliver.



Network Penetration Testing & Cybersecurity Assessments

Solicitation #: CRFQ 0705 LOT2400000009

Due Date: March 28th, 2024 at 1:30 PM Local Time

Submitted To:

West Virginia Lottery
State of West Virginia
2019 Washington Street, East
Charleston, WV 25305
Fax: (304) 558-3970
Attn: Brandon Barr, Buyer
Phone: 304-558-2652
Email: Brandon.L.Barr@wv.gov

Submitted By:

vTech Solution, Inc.
1100 H Street N.W. Suite 750
Washington DC 20005
Contact Person: Anisha Vataliya
Phone: 202.644.9774
Email: rfp.vtech@vtechsolution.com

**Secure, Protect, Prevail
Partnering for Unbreakable Cyber Security**

Table of Contents

1.0 Cover Letter 3

2.0 vTech’s Qualifications 5

 2.1 Executive Summary..... 5

3.0 vTech meeting State’s Minimum Qualification..... 6

 3.1 vTech been in business for at least fifteen (15) years, performing and delivering information technology cybersecurity assessments..... 6

 3.1.1 vTech’s General Overview..... 8

 3.2 vTech’s References 11

 3.3 Overview of vTech’s project team 13

 3.4 vTech staff performing IT cybersecurity assessments current certification from a source of accreditation 19

 3.5 vTech’s Compliance with the Center for Internet Security methodology 23

 3.6 Background Checks..... 23

 3.7 Non-Disclosure Agreement (NDA)..... 24

4.0 vTech’s Project Plan 27

 4.1 Project Management..... 36

 4.2 Executive Summary Report..... 42

 4.3 vTech meeting State’s Mandatory Requirements..... 45

5.0 Exhibit A – Pricing Page 57

6.0 Appendix: Forms 58

7.0 Certificate of Insurance 60

1.0 Cover Letter

March 28th, 2024

State of West Virginia
2019 Washington Street, East
Charleston, WV 25305

Re: vTech’s Response for Network Penetration Testing & Cybersecurity Assessments - Solicitation #: CRFQ 0705 LOT240000009

Dear Brandon,

vTech Solution Inc. (“vTech”) is honored to submit this response in provision of the opportunity to provide Network Penetration Testing & Cybersecurity Assessments to the State of West Virginia (“State”) under Solicitation #: CRFQ 0705 LOT240000009. Our proposal is aligned with all the terms and conditions outlined in the solicitation and any subsequent amendments.

Established in 2006, vTech was founded by a group of highly qualified IT professionals headquartered in Washington DC, with 24 offices across the United States, including Washington. Our mission is to empower government organizations through technology and services, enabling seamless digital experiences for the people they serve. Over the years, we have evolved into a world-class solution provider, offering end-to-end solutions for government and commercial agencies.

In the realm of Network Penetration Testing and Cybersecurity Assessments, vTech has been at the forefront, delivering a wide spectrum of IT services that cater to the unique needs of our diverse clientele. We take pride in our successful collaborations with public agencies such as Metropolitan Washington Airport Authority (MWAA), Virginia Housing Development Authority (VHDA), and DC Government, which have fortified our understanding of the intricate security requirements of both public and private entities. Our Penetration Testing solution is meticulously designed to safeguard company data, websites, and web applications from a myriad of cyber threats. With attackers constantly evolving in their tactics and capabilities, our cybersecurity project team is well-equipped to assist with risk assessment, remediation, and compliance efforts. At vTech, we guide organizations through every stage of the security lifecycle, from preparation and protection to detection, response, and recovery.

Cybersecurity challenges vary across industries, requiring tailored solutions that address specific needs and threats. Leveraging our global resources and advanced technologies, we offer integrated, turnkey solutions designed to bolster cyber resilience across your entire value chain. Whether defending against known cyberattacks, detecting and responding to the unknown, or managing an entire security operations center, vTech is committed to helping you grow with confidence in your cybersecurity posture. Our team at vTech comprises experienced professionals with a minimum of 18 years of industry experience and the requisite certifications to perform assessments, penetration testing, and risk mitigation planning in the public sector. We pride ourselves on our expertise and capabilities, delivering unparalleled penetration testing services to nationwide clients for many years.

vTech is not subcontracting with any firm for the referenced opportunity, ensuring direct and focused engagement with State. With our extensive experience and commitment to excellence, we are confident in our ability to support State in achieving its penetration testing & cybersecurity objectives effectively.

Thank you for considering vTech for this critical initiative. We look forward to the opportunity to collaborate with State and contribute to the enhancement of its Network Penetration Testing and Cybersecurity Assessments posture. We are firmly committed to performing the services as requested by the State within the stipulated time if awarded with this solicitation. Should you have any questions regarding the negotiations/quotation/proposal, please do not hesitate to contact Vishnu Naruka at rfp.vtech@vtechsolution.com.

Sincerely,



Anisha Vataliya
President,
vTech Solution Inc.

2.0 vTech's Qualifications

2.1 Executive Summary

Our Understanding of the scope

vTech understands that the State of West Virginia requires comprehensive cybersecurity assessments, including external network, website, wireless, and internal/client-side penetration testing assessments. These assessments must adhere to the Center for Internet Security methodology and incorporate techniques and guidelines from the OWASP Top 10 Project and NIST SP 800-115. The assessments aim to identify exploitable vulnerabilities in the Lottery's infrastructure using a combination of automated tools and manual techniques.



vTech acknowledges the requirement for a four-phased structure methodology for each type of testing, including reconnaissance, mapping, discovery, and exploitation. This involves various activities such as WHOIS, ARIN, and DNS lookups, OSINT searches, building custom password lists, vulnerability scanning, and exploiting discovered vulnerabilities.

vTech understands the necessity of providing executive summary reports, technical reports, and findings presentations to the Lottery management team upon the conclusion of each assessment. These reports should detail discovered vulnerabilities, their potential impact, and recommendations for remediation, categorized by risk rating.

vTech recognizes the importance of conducting social engineering exercises, such as phishing simulations targeting Lottery staff, and obtaining prior approval for heavy load brute force or automated attacks. vTech is also aware of the prohibition of denial-of-service attacks for external network penetration testing but acknowledges their requirement for website penetration testing with prior Lottery approval.

vTech acknowledges the requirement for onsite internal/client-side network penetration testing and wireless penetration testing at all Lottery locations. These assessments must include a thorough reconnaissance phase, mapping of network assets, discovery of vulnerabilities, and exploitation of identified weaknesses.

vTech comprehensively understands and acknowledges the State of West Virginia's requirements for network penetration testing and cybersecurity assessments for the West Virginia Lottery.

Why vTech?

By understanding these specific goals, we have tailored our cybersecurity solution to precisely meet State's requirements and contribute to the robustness and resilience of their digital infrastructure. Our team is committed to delivering innovative solutions that align with State's objectives and ensure the highest level of security and protection against evolving Network Penetration Testing & Cybersecurity services. vTech offers a comprehensive array of cybersecurity services and sets itself apart through a combination of vital strengths. Our team of professionals possesses relevant certifications, industry knowledge, and expertise in utilizing advanced cybersecurity tools and techniques. Our team holds an impressive array of certifications, including CISSP (Certified Information Systems Security Professional) and CISA (Certified Information Systems Auditor), which demonstrates their mastery in designing and implementing effective security measures. Additionally, we boast certifications like CEH (Certified Ethical Hacker) and CompTIA Security+ that exemplify our in-depth knowledge of offensive and defensive cybersecurity methodologies. With extensive familiarity in the deployment of cutting-edge cybersecurity tools, such as SIEM (Security Information and Event Management) systems, IDS/IPS (Intrusion Detection/Prevention Systems), and DLP (Data Loss Prevention) solutions, we are poised to proactively monitor, detect, and mitigate potential threats for State. Furthermore, our team's expertise in penetration testing and ethical hacking enables us to simulate real-world cyber-attacks, pinpoint vulnerabilities, and reinforce the resilience of State's infrastructure. To



ensure seamless project delivery, we integrate proven project management methodologies, including PMI's PMBOKs (Project Management Body of Knowledge), into our workflow. Our project management professionals adeptly manage timelines, budgets, and resources, ensuring that cybersecurity projects are executed efficiently and effectively. We have demonstrated in our proposal through our detailed project approach, implementation plan and prior experience to prove how vTech Solution, Inc. (vTech), can offer the best value and quality service to meet and exceed all the requirements of State.



By choosing vTech for this project, State of West Virginia will benefit from our commitment to delivering exceptional results, our collaborative approach, and our customer-centric focus. We understand the importance of this project to your organization and are fully dedicated to its success. We look forward to partnering with you and making a significant impact through our services.

3.0 vTech meeting State's Minimum Qualification

3.1 vTech been in business for at least fifteen (15) years, performing and delivering information technology cybersecurity assessments

As a seasoned provider of Network Penetration Testing and Cybersecurity Assessments, vTech is well-prepared to meet the rigorous requirements set forth by State. With over a decade of experience cybersecurity services, vTech has honed its expertise in crafting innovative and user-centric solutions tailored to the needs of diverse clients. Our commitment to excellence extends to ensuring compliance with the latest standards and regulations. Below, we detail how vTech's extensive experience and proficiency align with each of state's minimum qualification requirements, guaranteeing the delivery of a robust and reliable website solution. Our extensive track record of over 250+ government contracts and collaboration with more than 50 contracting agencies underscores our ability to meet the requirement of having been in business for at least fifteen (15) years, performing and delivering information technology cybersecurity assessments. Organizations that have trusted vTech to provide similar services include:

Project	Summary of Scope	Client Name
IT Audit and Cybersecurity Assessment	vTech provided IT Audit and security assessment to the town. Our team identified and mitigated the security risks to the town's network, systems, and applications including Core Network Devices, VPN, Email Server, Company Website, and FTP Server. We also performed Dynamic Application Security Testing (DAST) for the company website and FTP Server. The methodology was based on the guidelines of OWASP (Open Web Application Security Projects), OSSTMM (Open-Source Security Test Methodology Manual), and ISO 27001/2 ISMS, PCI Standards. vTech performed Security Assessment of internet services like SMTP, naming services (DNS), HTTP, Proxy, etc. Our security team accessed the risk of allowing traffic to enter the town's network from external sources, such as VPN tunnels.	Town of Smyrna, DE  Duration: July 2021- Feb 2023
Vulnerability Assessment & SIEM Services	vTech provided 24x7x365 eyes-on screen security event monitoring, analysis, and alert management. The primary focus of our SIEM analysts was to respond to alerts generated by the SIEM system as well as data mining functions. Over time, as the system was tuned and new rules were developed, the SIEM analyst was more focused on data mining as opposed to responding to alerts. When not	Virginia Housing Department Authority, VA 

	<p>working on active Offenses within the customer environment, our SIEM Analyst:</p> <ul style="list-style-type: none"> • Reviewed security event data within the SIEM to identify anomalous or suspicious activity • Escalated anomalous or suspicious security event data to the TIER II and/or vTech SDF, as required. <p>At all times, at least one vTech SIEM analyst worked on active Offenses or reviewed security event data within the SOC to identify anomalous or suspicious activity.</p> <p>Our correlation engineer provided input and guidance to the SDF to define enhancements to existing SIEM rules, as appropriate, including but not limited to reduction of false positives, suggestions for new rules, suggestion for modifications to existing rules based on VHDA data, threat intelligence and data.</p>	<p>Duration: August 2019 – August 2022</p>
IT Audit	<p>We performed IT audit for Florida – City of Jacksonville. Our objective was to ensure that IT infrastructure was secure, that network hardware was configured appropriately, and that IT general controls were operating effectively. Our review included analyses of key IT processes, internal wireless network security, the configuration of the internet-facing firewall, and compliance with HIPAA and the PCI Data Security Standards.</p>	<p>City of Jacksonville, FL</p>  <p>Duration: Jan 2000 – Jan 2002</p>
Vulnerability Identification and Reporting and Network Security Review	<p>vTech conducted an information systems risk assessment and network security review. Our objective was to determine if the policies and standards governing the management of technology environment were adequate to protect the security and integrity of its information assets. We reviewed the design and functionality of risk management framework, governance policies and key IT processes, including disaster recovery, change and patch management, user provisioning, physical access controls and database controls over enterprise systems. We also tested the external and internal network, and databases for vulnerabilities; reviewed internal LAN architecture; analyzed the configuration of the internet-facing firewall.</p> <p>The team at vTech was in charge of organizing and carrying out continual vulnerability testing, which also included proactive threat hunting and monthly vulnerability assessments. In order to find and investigate potential weaknesses in the City's information security protection plan, our team used methods, techniques, and tools that are frequently used by the adversary community in addition to proprietary tools. The results of this team's vulnerability assessment program were fed into the ATAC and SOC, when necessary, to create a clear and thorough understanding of the infrastructure's weaknesses. Our team</p>	<p>City of Bristol, TN</p>  <p>Duration: Jul 2004 – Jul 2008</p>

	<p>then identified necessary resources who had the knowledge and expertise to carry out particular tests and/or research. We used a variety of techniques, such as human processes and automated tools, to provide greater context and recommendations in order to enable the ATAC fill in the intelligence gaps. The teams were able to swiftly connect the dots for assaults for malware, assets, vulnerabilities, and threat actors, which enabled orchestration platform ensuring quick transitions from incident response to threat response and a minimum of dwell time for the SOC analyst.</p>	
--	--	--

3.1.1 vTech’s General Overview

Legal Name of the Company: vTech Solution, Inc.
Street Address: 1100 H Street N.W. Suite 750, Washington DC 20005
legal incorporation status: C- Corporation, Active
Number of dedicated security staff resources: 05



vTech Solution, Inc. (vTech) is a distinguished small business headquartered in Washington, DC, specializing in network penetration testing & managed security services. vTech was incorporated in January 2006 in the Commonwealth of Virginia with a primary focus on Enterprise level Cyber security services, professional services, and Cloud solutions. We operate at the intersection of business and technology to drive performance improvement and create lasting value for our clients and stakeholders.

As a minority-owned and woman-owned business, vTech holds the distinction of being appraised with CMMI Level 3 and certified as an 8(a) small business. Our commitment to excellence and customer satisfaction is evident in our track record and certifications. We are proud to be an accredited company with an A+ rating from the Better Business Bureau (BBB), underscoring our commitment to maintaining the highest standards of business practices. Additionally, our consistent inclusion in the prestigious Inc. 5000 ranking for eight consecutive years solidifies our position as one of the fastest-growing companies in the United States.

In 2010, vTech expanded our focus to encompass penetration testing and cybersecurity services, leveraging our expertise in program and project management to establish a dedicated project delivery team. This strategic move has further strengthened our position in the market.

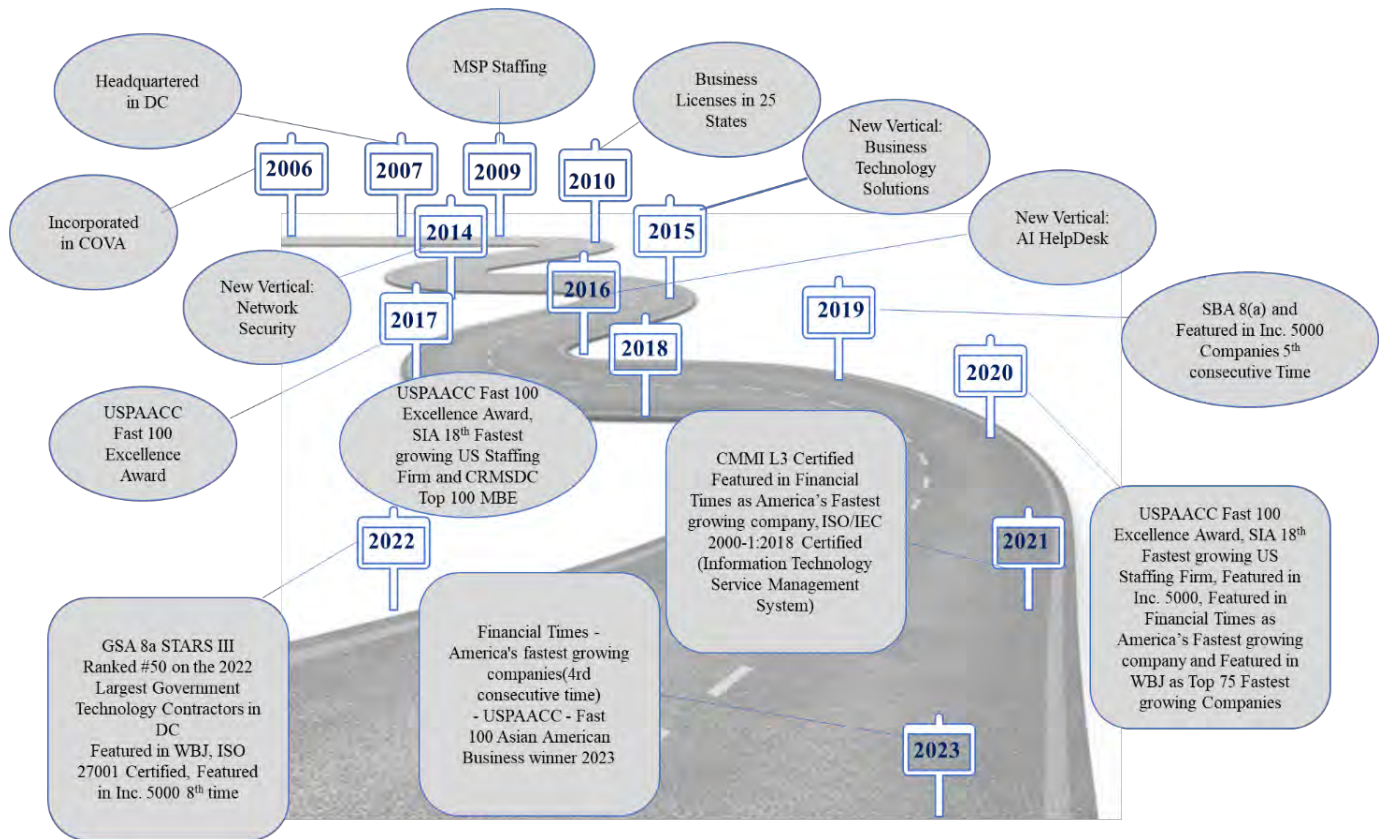
With a proven track record spanning over 18 years, vTech excels in delivering top-tier IT security Services to a diverse range of clients. Our comprehensive solutions facilitate streamlined services, enhanced governance, and efficient management. We have successfully served numerous State, Local, Commercial, and Federal clients, earning their trust and satisfaction. Our extensive experience includes over 250+ Government Contracts and collaboration with more than 50 Contracting across various cities, counties, and states. The figure below demonstrates our history and evolution in the industry.

Why Team vTech? – Quick Facts!

- Strong presence as a Network Penetration Testing & cyber security services provider firm company throughout the United States, including major Departments of the US Federal and State Governments.
- ISO 9001:2015, ISO 27001:2013, and CMMI- Level 3 certified quality processes ensure consistent performance and quality.
- Adhere to ISO/IEC 27001, NIST Cybersecurity Framework, PCI DSS, HIPAA, SOC 2, FISMA standard compliances.

Capability and Competency

- vTech employs the methodologies and processes of frameworks such as CISM, COBIT ITIL, ISMS, and Six-Sigma.
- Our team of experts deliver cyber security services based on best



vTech boasts certifications in ISO 9000:2015, ISO/IEC 20000-1:2018, and ISO 27001:2013, as well as a team of Six Sigma-certified professionals dedicated to applying quality standards and continuously improving our processes. These certifications enable us to deliver exceptional Penetration testing & Cyber security services.

<p>BBB Accreditation</p> <p>vTech is a Better Business Bureau (BBB) accredited company with an A+ rating.</p> 	<p>ISO 9001:2015 Certified Business</p> <p>vTech is now an ISO 9001-certified business. Perry Johnson Registrars, Inc. has audited the Quality Management System of vTech Solution Inc. This registration is to the IT Services and Resources to the Commercial Market, State, and Federal Government.</p> 
<p>ISO 27001:2013</p> <p>vTech's ISO 27001:2013 certification signifies that we have implemented robust information security practices and controls to protect the confidentiality, integrity, and availability of data and information assets. It demonstrates our commitment to maintaining a secure environment for our client's sensitive information and highlights our ability to effectively manage information security risks.</p> 	<p>8(a) Certified</p> <p>vTech is an 8(a) certified company. We are pleased to serve opportunities from the government in a modernized, intelligible way.</p> 
<p>CMMI Level 3 Appraised</p>	<p>ISO/IEC 20000-1:2018</p>

We are a CMMI Level 3 appraised company. We ensure to provide quality services and processes to our clients.

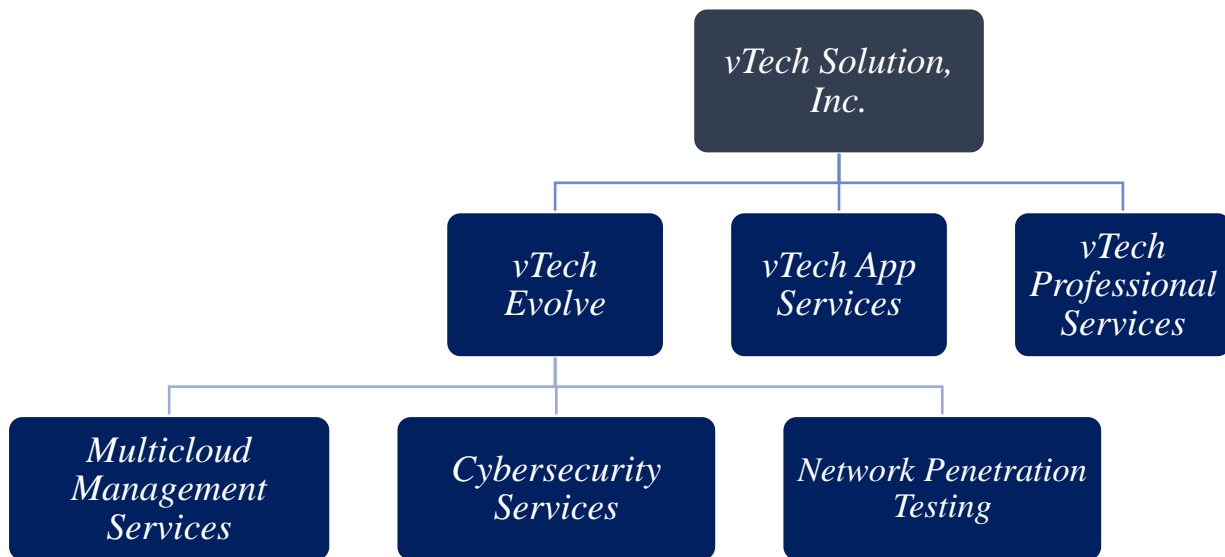


ISO/IEC 20000-1:2018 is a service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain, and improve an SMS. The requirements include the design, transition, delivery, and improvement of services to fulfill agreed service requirements.



Over the years, we have forged strategic partnerships with leading Penetration testing & cybersecurity vendors, allowing us to expand our offerings with a diverse and unbiased approach that benefits our customers. Our key partners include renowned companies such as McAfee, Checkpoint, Dell, Veeam, Microsoft, and Symantec. Our Security Operations Center comprises experts who possess in-depth knowledge of IBM Qradar, Siemplify, Splunk, Nessus, Qualys, and various other EDR solutions from our extensive technology network.

vTech is committed to providing top-quality, IT Services. From entry-level to upper-level management, vTech specializes in a variety of industries including the following:



At vTech, we take pride in our impressive customer retention rate which serves as a testament to our unwavering dedication to customer satisfaction. Each client account is assigned a dedicated point of contact from our client relations department, supported by a highly trained team, ensuring personalized and attentive service. vTech is a trusted partner that combines expertise, dedication, and a customer-centric approach to deliver exceptional managed staffing services, enabling the success of our clients in the ever-evolving business and technology landscape.

Our team of seasoned cybersecurity professionals, including Certified Information Systems Security Professionals (CISSP), possesses extensive expertise in managing and mitigating cyber risks. With a focus on proactive cybersecurity measures, we guide organizations in developing robust security strategies, ensuring compliance with industry standards and regulations.

Our cybersecurity services include comprehensive risk assessments, security policy development, incident response planning, and ongoing monitoring of security controls. We tailor our cybersecurity consulting to align with organizational goals, addressing specific threats and vulnerabilities. vTech is committed to delivering cutting-edge cybersecurity solutions, safeguarding sensitive information and fortifying organizations against evolving cyber threats.

vTech’s Nationwide Presence:

We are headquartered in DC and having regional offices in 24 locations across US and Canada. All services requested under this solicitation would be provided from *1100 H Street, N.W. Suite 750, Washington DC 20005* as per the requirement of State. Please find below our locations across United States and Canada.


WE HAVE A STRONG PRESENCE ACROSS NORTH AMERICA WITH 24 FIELD OFFICES IN U.S. & CANADA.

OFFICES IN UNITED STATES

Washington, DC	Eaton Rapids, MI	Oklahoma City, OK
Chantilly, VA	Eden Prairie, MN	Boston, MA
Lutherville, MD	Springfield, IL	Readfield, ME
Phoenix, AZ	Trenton, NJ	Poca, WV
Wilmington, DE	Keizer, OR	Houston, TX
Loxahatchee, FL	Lexington, SC	Atlanta, GA
Des Moines, IA	Seattle, WA	

OFFICES IN CANADA

Winnipeg, MB	Vancouver, BC
Toronto, ON	Calgary, AB



▼ DATA CENTERS

3.2 vTech’s References

At vTech, our Network Penetration Testing and Cybersecurity Assessments professional division comprises seasoned professional strategists with an average of 18 years of a profound experience. Our diverse team is driven by challenging projects, problem-solving, exceptional customer service, continual education, and a dedication to quality. With a strong track record in similar projects, we bring the expertise needed to meet your requirements effectively. Since past performance is the best indicator of future performance, we are citing below experience references for similar projects to the requirement of the State:

Reference #1

Client Name	Town of Smyrna
Contact name	Gene Brinkley
Phone/Email	302.389.2362 gbrinkley@smyrna.delaware.gov
Project Name and Scope	Cybersecurity Assessment
Project start date and end date	July 2021-Feb 2023
Description of the project	vTech provided security assessment to the town. Our team identified and mitigated the security risks to the town’s network, systems, and applications including Core Network Devices, VPN, Email Server, Company Website, and FTP Server. They also performed Dynamic Application Security Testing (DAST) for the company website and FTP Server.

	<p>The methodology was based on the guidelines of OWASP (Open Web Application Security Projects), OSSTMM (OpenSource Security Test Methodology Manual), and ISO 27001/2 ISMS, PCI Standards. vTech performed Security Assessment of internet services like SMTP, naming services (DNS), HTTP, Proxy, etc. Our security team accessed the risk of allowing traffic to enter the town’s network from external sources, such as VPN tunnels. Town’s infrastructure was tested and exploited “but not limited to” against the following threats:</p> <ul style="list-style-type: none"> • Zero-Day Attacks • Social Engineering • Denial of Service (DoS) and Distributed DoS (DDoS) • Database Vulnerabilities Content Spoofing • Systems / Networks Brute Force Attack • Buffer Overflows, Heap Overflows, Stack Overflows • Bypassing Authentication and Authorization • Network and DNS Reconnaissance • Other vulnerabilities as per the latest security threats reported on international and local security forums and reports <p>Determined the impact of a security breach on:</p> <ul style="list-style-type: none"> ➤ The integrity of the town’s systems. ➤ The confidentiality of the town’s Information. ➤ The internal infrastructure and availability of Information. ➤ The results of this assessment will be used by the client to drive future decisions as to the direction of their information security program. ➤ All tests and actions would be performed in a controlled environment.
--	--

Reference #2

Client Name	Obverse, Inc
Contact name	James Detherage
Phone/Email	202-213-3422 jdetherage@obverse.net
Project Name and Scope	Cybersecurity Services
Project start date and end date	October 2021-December 2022
Description of the project	vTech offered a comprehensive approach to ransomware protection and recoverability by aligning capabilities to the National Institute of Standards and Technology (NIST) Cybersecurity Framework for the obverse. This helped the organization better in identifying and protecting, detecting and mitigating, and recovering from ransomware attacks.

Reference #3

Client Name	Metropolitan Washington Airport Authority (MWAA)
Contact name	Kevin James
Phone/Email	Kevin.james@mwaa.com
Project Name and Scope	Ransomware Impact Assessment
Project start date and end date	February 2022 – September 2022

Description of the project	Assess the readiness against ransomware impact and perform gap analysis, business impact analysis, tabletop exercise, SCRM
-----------------------------------	--

3.3 Overview of vTech’s project team

vTech offers the indispensable capabilities required for the successful implementation of Network Penetration testing & Cyber Security Services for the State. We possess a winning combination of highly skilled professionals, efficient processes, and cutting-edge tools, all of which are essential for delivering exceptional Cyber Security Services. Our primary objective is to assist the State in establishing a robust talent foundation that sets you up for success.

To ensure the utmost dedication and expertise for each contract, we propose a dedicated team of experts who are fully committed to meeting our client's objectives. Also, our well-structured management system guarantees that every contract is overseen by a senior staff member, mitigating any concerns regarding inexperienced project managers. Our team members are not only adaptable and resilient, but they also possess a wealth of knowledge across various cyber fusion domains. This enables them to contribute valuable institutional insights, drive operational efficiencies, and continuously improve project performance.

We have established long-term partnerships with industry-leading product companies. These partnerships bolster our ability to provide exceptional cyber solutions that surpass State expectations. For this specific contract, we have assigned the following key personnel who will remain intact for the duration of this contract and contribute to its successful execution:

Name of Key Personnel	Proposed Role for this Contract
Troy A. Postin	Program Manager
Kartik Hirpara	Project Manager
Okpo Kalu	IT Security Engineer
Tushar Dudhat	Security Specialist
Abdu Kiyaga	Security Specialist
Vishnu Naruka	Contract Specialist
Stefan James	Information Technology Specialist

Please find the Resumes of Our proposed Staff:



Key Personnel Name: Troy A. Postin
Title: Program Manager
Number of Relevant Experience: 20+ Years



SUMMARY

Mr. Postin is a Program Manager for vTech Solution. He has been working in the Federal Space for 18+ years. He has 22 years of real-world experience in industry and information technology. He has been heavily involved in program management, project management, identifying requirements, performing business analysis/strategy/implementation, and change management. He has also assisted in software development, IT Service Management, and Asset Management, and has performed at every level of management, including executive. His ability to align the company’s activities, talent, and assets with the leader’s vision and the customer’s expectations has allowed him to increase profits, reduce waste, and increase overall efficiency. As a self-starter, Mr. Postin leverages creative and critical thinking in problem-solving and is very adept at integrating his training, education, and experience into solutions that meet the immediate needs of the client as well as building the foundation for sustaining long-term performance.

Mr. Postin's experience in industry has allowed him to multi-task operations at every level; from the tactical to the strategic. He has driven and monitored progress with multidisciplinary teams and staff in fast-paced environments ensuring milestones and deliverables were met on time and within budget. His ability to forecast, and integrate cross-domain operations, resources, and administrative support were key to enabling customer success and satisfaction. He communicates effectively with, stakeholders, leaders, staff, clients, and other team members facilitating both internal and external meetings across multiple time- zones and countries when necessary. He is also effective at presenting complex information in easy-to-understand language and identifying strengths, weaknesses, opportunities, and risks. He is and has been a practitioner of Business Analytics, Lean Six Sigma, AGILE, Composite Risk Management, Project Management, and Program Management.

CORE COMPETENCIES

- A skilled negotiator who relies heavily on building and sustaining high-trust relationships.
- Familiar with strategic leadership, National Security Policy and Strategy, Contemporary Security Issues, Performance Management, and best business practices.
- The process-oriented manager understands accountability and the desired effects of a client's plan or program and how the execution should occur down to the user level.
- Possesses keen understanding - with years of experience performing analysis in business and process refinement and integrating all company domains toward a common goal.
- Working individually or as part of a team he has a keen focus on developing a successful outcome.

EXPERIENCE

- Program Manager at vTech Solution Inc, Feb 2023 – Present
- Senior Project Manager at Technical and Project Engineering LLC (TAPE), Sept 2021 – Jan 2023
- Program Manager at Agile Defense Inc, Sept 2020 – Aug 2021
- Project Manager at Directviz Solutions LLC, Sept 2017 – Sept 2020
- Requirements Manager at Advanced Computing Technologies, Nov 2015 – Apr 2016
- Senior Consultant at IBM Corporation, June 2006 – Oct 2015
- General Manager at RWI, Marlow Heights, Feb 2005 – May 2006
- Operations Officer at US Army Reserves, deployments to Iraq, Kuwait, and Afghanistan, April 1980 – Aug 2019

EDUCATION AND CERTIFICATIONS

- Top Secret (SCI), through 2025
- M.S., Strategic Studies, US Army War College, Carlisle, PA, 2014
- B.S., Management, Park University, Parkville, MO, 2005
- AGILE Training Certificate
- Scrum Product Owner Certification (In progress)
- Project Management Training and Certification (PMP)
- Certified Military Trainer
- Over 40 Military Schools, Courses, and Certifications, most notable;
- US Army War College, 2014
- Army Associate Logistics Executive Development Course, Fort Lee, VA, 2005
- Army Command & General Staff College, Fort Leavenworth, KS, 20075

Resume –
Project Manager

Key Personnel Name: Kartik Hirpara
Title: Project Manager
Number of Relevant Experience: 8+ Years



SUMMARY

- Over 8 years of experience in the IT Services domain supporting diverse technology stacks including Infrastructure, Security, and Cloud Operations.
- Creating, and Managing service portfolio for Managed Services including Managed Security, IaaS, PaaS and SaaS, and Infrastructure.
- Experience leading IT operations teams to deliver quality results to SLED, Federal, and commercial clients for Managed IT Service projects.
- Expertise working with Business Development and Marketing teams to prepare, document, and go to market with Managed Services solutions.
- Strong technical writeup and solution architecture development skills including Cloud, and Cybersecurity solutions - Risk Assessments, SOC (Security Operations Center), and Implementation Strategies.
- Solid Understanding of Internal IT operations management, leadership, and cost optimization for internal use applications.

CORE COMPETENCIES

- IT Operations and Service Management
- ITIL process, ITSM lifecycle management
- Architecture Design, Implementation, and Improvement
- Simultaneous project management
- NIST, HIPAA, PCI, FISMA, and FedRAMP
- ISO 27001, ISO 9001, and ISO 2000-1
- EDR, MDR, Compliance automation technology, Assessment, and testing
- Hybrid and Cross-Cultural Team Management
- Go to Market, Strategic Solution Development, and Sales
- RFP/RFQ/RFI technical write-ups, Solution Pricing Development experience
- Executive reporting, Finance, and Budget Management
- OEM & Partner Channel Management

TOOLS & TECHNOLOGIES

- Windows 10, Windows 2012 Server, Windows 2016 Server, Linux OS
- CCNA - Networking - Routing and Switching
- Aviatrix - Multi-cloud networking platform
- Morpheus - Multi-cloud management platform
- Nessus Professional - Vulnerability Scanning
- Checkpoint Harmony Suite - EDR, Email Security, Endpoint Security, Mobile Security, CloudGuard IaaS
- Orca - Cloud Security and Compliance Management
- PlexTrac - Purple teaming platform
- Scythe - Platform for Attack Emulation and Behavioral Analysis
- Security + Concepts and OWASP standards basic knowledge
- Azure Administration

- Basic PowerShell Scripting Knowledge
- PSA (Professional Service Automation tools)
- AvePoint Migration tool

EXPERIENCE

- Project Manager, vTech Solution, Inc., August 2017 – Present

Key Projects:

- Government Customer- Ransomware Impact Assessment and Response Planning
- Government Customer - Network Infrastructure Assessment
- Government Customer - Data Center relocation
- Government Customer- Cybersecurity Audit and IT Risk Assessment
- Commercial Customer: Managed IT Services
- Government Customer: Office 365 Migration and Deployment
- Government Customer: Microsoft Azure Support

EDUCATION & CERTIFICATIONS

- Stratford University, Virginia - MS, Networking, and Telecommunications, Jan 2016 - June 2017
- UVPCE, Ganpat University, Gujrat, India - B.Tech, Electronics and Communications, Jan 2011 - Jan 2015
- Aviatrix Certified Engineer - Multi-cloud Network Associate
- Sandblast Mobile Specialist - Checkpoint Software Ltd
- CloudGuard SaaS administrator - Checkpoint Software Ltd
- Sandblast Mobile Sales certification - Checkpoint Software Ltd
- CloudGuard IaaS Sales certification - Checkpoint Software Ltd
- Lean Six Sigma Green Belt - ASCB
- VMware VSP Foundations – 2019



Key Personnel Name: Tushar Dudhat
Title: Security Specialist
Number of Relevant Experience: 22+ Years

SUMMARY

With over 22 years of comprehensive experience in IT, I have excelled in IT Service Delivery, Operations & Management, Project Management, and Manufacturing IT. My technical expertise spans Azure cloud, VMWare, Wintel, ePO/Radia, and proficiency in monitoring tools such as NNMi and HP-OM. I have a deep understanding of ITIL processes and possess excellent network troubleshooting skills.

My IT skills cover Managed Cloud, Security, and IT Services support, multi-cloud management, IT Service Delivery, Project Management, IT Operations, IT Budgeting, Planning, Procurement, and People Management. I am well-versed in working within both global and local environments.

In addition to my IT proficiency, I have significant exposure to the automotive industry, including Powertrain, Press Shop, Body Shop, Paint Shop, General Assembly Shop, Tractor Assembly, and Design & Development. My behavioral attributes include pro-activeness, a positive attitude, strong organizational skills, and a dedication to sharing knowledge and continual technical skill enhancement.

EXPERIENCE

- Lead IT Services at vTech Solution Inc. - Jan 23 – Present
- Senior Director – IT Services at vTech Family Solution India Pvt. Ltd. - Dec 18 – Jan 23
- Manager IT at General Motors India Pvt. Ltd. - Nov 13 – Nov 17
- Principal Infrastructure Engineer - VMware & Wintel at Mphasis an HP Company - Dec 09 – Oct 13
- IT Executive at Net connect Pvt. Ltd. - Oct 07 – Dec 09
- Area Support Manager at Zenith Computers Ltd - Aug 03 – Sep 07
- Systems Officer at Indo German Tool Room – IGTR - Jun 01- Mar 03
- Network Engineer at P C Horizons - Jan 01 – May 01
- Customer Support Engineer at HASOW AUTOMATION Ltd - May 99 – Jan 01
- Customer Support Engineer at ASTER NETWORKS Pvt. Ltd - Jan 99 – May 99
- Technician Apprentice at INDIAN SPACE RESEARCH ORGANIZATION (ISRO) - Jan 98 – Jan 99

SKILLSET

Tushar is a cybersecurity professional with a strong technical skill set, specializing in Azure cloud, VMWare, Wintel, ePO/Radia, and proficiently using monitoring tools like NNMi and HP-OM. His expertise includes network troubleshooting and ITIL processes, demonstrating a comprehensive understanding of cybersecurity principles. Tushar excels in managing cloud security, IT services support, and multi-cloud environments. With a background in automotive exposure, particularly in Powertrain, Press Shop, Body Shop, Paint Shop, General Assembly Shop, Tractor Assembly, and Design & Development, Tushar brings a unique perspective to cybersecurity assessments. His behavioral skills, characterized by proactiveness, a positive attitude, and a commitment to knowledge-sharing and continuous learning, make him a valuable asset in the ever-evolving field of cybersecurity and vulnerability management.

EDUCATION & CERTIFICATIONS

- Bachelor of Business Administration at Sikkim Manipal University - 2017
- Electronics & Communication at A V Parekh Technical Institute – 1997

PROFESSIONAL DEVELOPMENT

- Microsoft Certified Professional (MCP)/Microsoft Certified Systems Engineer (MCSE) NT 4.0/2000
- Cisco Certified Network Associate (CCNA) (████████)
- Microsoft Certified Systems Administrator & MCSE 2003
- ITIL – Mphasis skill port
- VMware 5.0 – Mphasis skill port
- VMware Certified Associate Data Center Virtualization
- Six Sigma Green Belt
- AWS Cloud Practitioner



Key Personnel Name: Abdu Kiyaga
Title: Security Specialist
Number of Relevant Experience: 4+ Years

SUMMARY

As a Security Specialist, Abdu brings extensive expertise in troubleshooting and resolving intricate technical issues, with a proven track record of implementing innovative solutions to optimize system

performance and enhance overall user experience. Abdu's skill set extends to cybersecurity, assessment, and vulnerability management, where he has demonstrated a proactive approach to fortifying organizational defenses. Proficient in ITIL processes and adept at using monitoring tools such as NNMi and HP-OM, Abdu has a wealth of experience in managing diverse IT environments. His commitment to staying current with the latest developments in cybersecurity aligns seamlessly with his passion for knowledge-sharing and continual skills enhancement. Abdu is well-positioned to contribute significantly to any cybersecurity-focused role by leveraging his comprehensive skill set and dedication to staying ahead of emerging threats.

EXPERIENCE

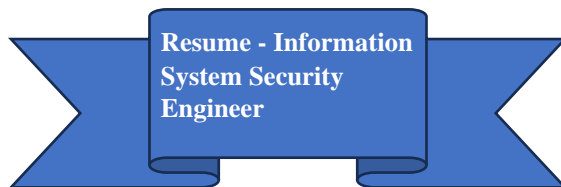
- Security Specialist at vTech Solution Inc, 10/2023 – present
- Cyber Security Analyst Jr at Washington Metropolitan Area Transit Authority, 01/2023 – 10/2023
- Radio Communication Technician at Washington Metropolitan Area Transit Authority, 07/2019 – 12/2022

SKILLSET

- Network administration
- Troubleshooting
- Asset Security
- Linux administration
- BifFix Management
- Nutanix Management
- Network Security
- Cloud Migration

EDUCATION & CERTIFICATIONS

- Computer Networks and Cybersecurity | Bachelor University of Maryland Global Campus 09/2020 – 05/2023
- Certified Incident Handler at GIAC, 02/2023
- GIAC Security Essentials at GIAC, 12/2022



Key Personnel Name: Stefan James
Title: Information System Security Engineer
Number of Relevant Experience: 15+ Years

SUMMARY

A results-driven and articulate IT Security professional with over 15 years of extensive experience, I bring a wealth of expertise in Cybersecurity, PCI DSS Framework, Information Assurance, Cloud Security (AWS), Security Compliance (GRC), Vulnerability Management, DevSecOps, Incident Response, Risk Management Framework (RMF), and Cyber Operations. Throughout my career, I have consistently delivered exceptional value to federal, private, and healthcare organizations by providing guidance in achieving and maintaining compliance while supporting business continuity.

My robust knowledge encompasses preparing organizations for PCI DSS compliance audits, safeguarding IT infrastructure, and assessing client-facing security challenges. I excel in communicating risks, vulnerabilities, and security control assessments with key stakeholders at all levels, ensuring quick dissemination of pertinent information to mitigate security risks effectively. Certified at IAT Levels I - III,

IAM Levels I - II, and IASAE Levels I - II in compliance with DoD 8570/8140, I am committed to continuous learning and hold numerous Cyber and Cloud-related certifications. My passion for improving skill sets and relentless pursuit of knowledge underscore my dedication to staying at the forefront of the ever-evolving field of IT Security.

EXPERIENCE

- Information System Security Engineer (ISSE) at Accenture Federal Services, U.S. Department of Veteran Affairs – Annapolis, MD, May 2021 - Present
- Information Security Consultant at James Consulting Group, LLC – Bowie, MD Jun 2020 - Present
- Security Control Assessor (SCA) at Veterinarian Electronic Assistant (VEA) – Bowie, MD, Jan 2018 – Jan 2020
- Cyber Security Specialist at Grove Research Solutions, Inc, National Institutes of Health (NIH) – Bethesda, MD Mar 2016 – Jan 2018
- Sr. Information Technology Specialist at Medical Science & Computing, LLC, National Institutes of Health (NIH) – Bethesda, MD Mar 2014 – Mar 2016
- Information Security Analyst at Collabera, Inc. – Washington, DC, Oct 2013 – Mar 2014
- Information Technology Analyst at U.S. Department of Agriculture – Beltsville, MD, Aug 2007 – Aug 2013

SKILLSET

Stefan James is a seasoned IT Security professional with 15+ years of expertise across Security Compliance, Security Control Assessments (SCA), Vulnerability Management, Cloud Security, Incident Response, and DevSecOps. His proficiency includes validating FedRAMP security controls, contributing to policy and compliance development, and conducting audits. Stefan excels in technical assessments aligned with RMF, Web Application Security Assessments (WASA), and is well-versed in various security frameworks. His strength lies in efficient Vulnerability Management using tools like Tenable, Qualys, and AWS services. In Cloud Security, Stefan secures cloud infrastructure, ensuring compliance with industry standards. He brings a wealth of experience in Incident Response, using tools like Splunk and AWS Security Hub. In DevSecOps, Stefan collaborates with developers, identifying and remediating vulnerabilities early in the SDLC using tools like Prisma Cloud and AWS services.

EDUCATION & CERTIFICATIONS

High School Diploma in Information System **2002**
Laurel High School Laurel MD

CERTIFICATION & TRAINING

- | | |
|--|------|
| • Certified Information Systems Auditor (CISA) | 2022 |
| • Certified Information Security Manager (CISM) | 2022 |
| • CompTIA Advanced Security Practitioner (CASP+) | 2021 |
| • CompTIA Security+ | 2020 |
| • AWS Certified Solutions Architect Associate | 2019 |
| • AWS Certified Developer Associate | 2019 |
| • Qualys Certified Specialist | 2022 |

3.4 vTech staff performing IT cybersecurity assessments current certification from a source of accreditation



**Resume - Information
System Administrator**

Key Personnel Name: Okpo Kalu
Title: Information System Administrator
Number of Relevant Experience: 15+ Years

SUMMARY

With several years of proven expertise in Information Systems and Administration, Okpo possesses a robust skill set to manage multiple projects independently, ensuring efficiency and timeliness. Their experience spans across NIST and FedRAMP risk management frameworks, Cybersecurity governance, and compliance, encompassing system scope definition, analysis, business case development, testing, production, maintenance, and technical documentation. Proficient in implementing RMF Security controls, conducting vulnerability scanning and remediation, and overseeing Data Loss governance and prevention, Okpo excels in FIPS categorization, data analysis, and mapping.

Okpo's background in Security Engineering and consulting, coupled with expertise in systems and accounts management, risk mitigation, and customer service, enriches their capabilities. Okpo is recognized for exceptional organizational, time management, and analytical skills, enabling them to function adeptly in leadership or managerial roles. With a knack for establishing and nurturing effective business relationships, they consistently achieve desired outcomes, exhibiting a keen eye for detail and adaptability in operational and technical environments. Proficient in MS Office Suite and SharePoint, Okpo is poised to contribute effectively to organizational success.

EXPERIENCE

- Senior Associate Cyber Enterprise and Cloud Security at Price Waterhouse Coopers LLP (PWC), Baltimore, MD, Apr 2022 – Apr 2023
- Cybersecurity FISMA/FISCAM Compliance Lead and Security Assessor at Department of Health and Human Services (HHS), US Government, Rockville, MD, Apr 2021- Apr 2022
- Cybersecurity Manager/Sr. Security Administrator at Maryland Department of Transport State Highway Administration, Baltimore, MD, Aug 2018 – April 2022
- Computer Network Specialist at Department of Human Services (DHS), Columbia, MD, Jan 2018 – Jul 2018
- Security Analyst/Sr. IT Operational Support Specialist III at Amazon Bwi2, Baltimore, MD, Jun 2015 – Jan 2018
- IT Support Advance Technician (Secondary Employment) at CMS/Leidos/Dell Contract (PART TIME), Baltimore, MD, Feb 2017 – Jun 2017
- Cyber Security Analyst at Dalnet Services Inc Pikesville, MD, Dec 2013 – Nov 2015
- Software Tester at Endress + Hauser, Maulburg, Germany, Mar 2012 – Oct 2012

SKILLSET

- Audit Readiness Assessment and Gap analysis
- Microsoft Suit (Word, Excel, PowerPoint, Access, Project, Visio)
- OMB Circulars A-123, A-127, A-134, A-136 and other OMB policies
- Federal Information Security Management Act (FISMA)
- Business Continuity Planning & Incident Response
- NIST 800-53, NIST 800-171, NIST 800-39, NIST 800-37
- Risk Management Framework (RMF/FedRAMP)
- Categorization of Information Systems (FIP 199)

- Selection of Security Controls (FIPS 200)
- Security Control Implementation
- Data Loss Prevention (DLP) and File Removal Protection (FRP)
- Security Control Assessment
- Privacy Protection & Regulations - GDPR, HIPPA, SOX, GLBA
- Information System Authorization
- Monitoring of Security Controls
- Cyber security Framework (CSF)
- Vulnerability Remediation Asset Manager (VRAM)
- Network Patch Management (Shivalik & SCCM)
- RSA Archer, Nessus, Nexpose, CounterAct, MacAfee ePO
- Auditing, Security exceptions and POAMS
- Retina, Security Content Automation Protocol
- OWASP & CIS Application Security
- Software/Databases: Microsoft Suit (Word, Excel, PowerPoint, Access, Project, Visio), Azure O365, Nessus, Nexpose, CounterAct, MacAfee ePO
- Others: Cyber security Framework (CSF), Vulnerability Remediation Asset Manager (VRAM), Retina, Security Content Automation Protocol, OWASP & CIS Application Security

EDUCATION & CERTIFICATIONS

MSc. Cyber Security University of MD – University College (UMUC), 2016

BSc. Telecommunication & Information TURKU University of applied Science Finland, 2012

CERTIFICATION & TRAINING

- | | |
|--|------|
| • Certified Information System Security Professional (CISSP) | 2019 |
| • CompTIA Security + CE | 2014 |
| • CompTIA Network + | 2014 |
| • CompTIA A+ | 2014 |
| • CCNA Routing & Switching | 2011 |
| • Gartner Security & Risk Management Summit | |
| • SAN Security Monitoring and Security Operations | 2018 |



Candidate Name: Okpo Kalu

ID/Examination number: [REDACTED]

March 25, 2019

CISSP



Dear Okpo Kalu:

Congratulations! We are pleased to inform you that you have provisionally passed the Certified Information Systems Security Professional (CISSP®) examination. Your examination result is provisional in that it may be subject to further psychometric and forensic evaluation before a certification decision is reached.

Please allow 2-5 business days for your examination result to be transmitted to (ISC)². If you have applied to become an Associate of (ISC)², no further action is necessary at this time. A welcome letter with the requirements for maintaining your Associate status will follow. If you are seeking certification as a CISSP, you must successfully complete the endorsement process. Instructions will be provided once your examination result has been processed.

For more information concerning our credentialing process, including the endorsement requirement noted above, please visit www.isc2.org/about-isc2-credentials. Information related to our Associate program may be found at www.isc2.org/associate.

Should you have any questions, please feel free to contact us via email at membersupport@isc2.org. Live chat is also available on the member homepage at www.isc2.org/memberhome. For detailed (ISC)² contact information, including regional information, please visit <https://www.isc2.org/contactus>.

Again, congratulations on your achievement and we look forward to serving you as a member of (ISC)².

Sincerely,
(ISC)²

3.5 vTech's Compliance with the Center for Internet Security methodology

vTech acknowledges and confirms its commitment to comply with the Center for Internet Security methodology and adhere to the techniques and guidelines outlined by the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide. We understand the importance of these industry-standard methodologies and guidelines in conducting comprehensive cybersecurity assessments for the West Virginia Lottery. By incorporating these best practices into our assessment approach, vTech aims to ensure the highest level of security for the Lottery's infrastructure and safeguard against potential vulnerabilities.

3.6 Background Checks

vTech agrees to provide names, addresses, and fingerprint information for a law enforcement background check for any vTech staff working on the Lottery project team, upon request prior to award.

3.7 Non-Disclosure Agreement (NDA)

EXHIBIT B NON-DISCLOSURE AGREEMENT (NDA)

MUTUAL NON-DISCLOSURE AGREEMENT

This Mutual Non-Disclosure Agreement (“Agreement”) is entered into by and between the West Virginia Lottery, with its principal offices located at 900 Pennsylvania Avenue Charleston, WV 25302 (“Lottery”), and vTech Solution, Inc, with its principal offices located at Washington DC 20005 (“Party of the second part”), with an Effective Date of 3/25/2024. Lottery and Party of the second party also are referred to herein individually as a “party”, or collectively as the “parties”.

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

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

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

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

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

II. Disclosure Period and Term. This Agreement protects against the disclosure of Confidential Information which is disclosed between the parties during each party’s performance of its obligations associated with that certain CRFQ Agreement executed between the parties on 3/25/2024 (the “Effective Date”) and 3 year(s) after the termination of such Agreement (“Disclosure Period”). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

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

- III. Use of Confidential Information.** A party hereunder receiving Confidential Information shall use such Confidential Information solely for the purposes of, as applicable to the recipient, understanding current business activities of a party, soliciting a proposal for certain information technology services, responding to such proposal solicitation, reviewing solicitation responses, tendering a bid, or discussions or negotiations related to such solicitation, proposal, or bid.
- IV. Protection of Confidential Information.** Each party shall not disclose the Confidential Information of the other party to any third party. The recipient shall protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the recipient uses to protect its own confidential information of a like nature. A recipient shall restrict disclosure of Confidential Information to its employees, provided that such employees (i) have a need to know, and (ii) are bound by obligations of confidentiality equally as restrictive as the terms of this Agreement.
- V. Exclusions.** This Agreement imposes no obligation upon the recipient with respect to Confidential Information which: (a) was in the recipient's possession before receipt from the disclosing party; (b) is or becomes a matter of public knowledge through no fault of the recipient; (c) is rightfully received by the recipient from a third party without a duty of confidentiality; (d) is disclosed by the disclosing party to a third party without a duty of confidentiality on the third party; (e) is independently developed by the recipient; (f) is disclosed under operation of law; or (g) is disclosed by the recipient with the disclosing party's prior written approval.
- VI. Miscellaneous.** Neither party to this Agreement shall acquire any intellectual property rights nor any other rights under this Agreement except the limited right to use as set forth in this Agreement. This Agreement does not prevent either Party from competing with one another for work or clients unless the parties specifically agree otherwise, in writing, as to a specific client. Each disclosing party warrants and represents that the Confidential Information and other information provided which is necessary to the purposes described hereunder, are true and correct to the best of the disclosing party's knowledge and belief. Nothing in this Agreement shall be construed to preclude either party from developing, using, marketing, licensing, and/or selling any software or other material that is developed without reference to the Confidential Information.
- VII. Export Administration.** Each party to this Agreement agrees to comply fully with all relevant export laws and regulations of the United States and other countries to assure that no Confidential Information or any portion thereof is exported, directly or indirectly, in violation of such laws.
- VIII. No Obligation to Purchase or Offer Products or Services.** Neither party has an obligation under this Agreement to purchase or otherwise acquire any service or item from

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

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

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

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

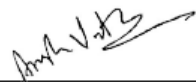
WEST VIRGINIA LOTTERY

By: _____

Name: _____

Title: _____

vTech Solution, Inc (VENDOR)

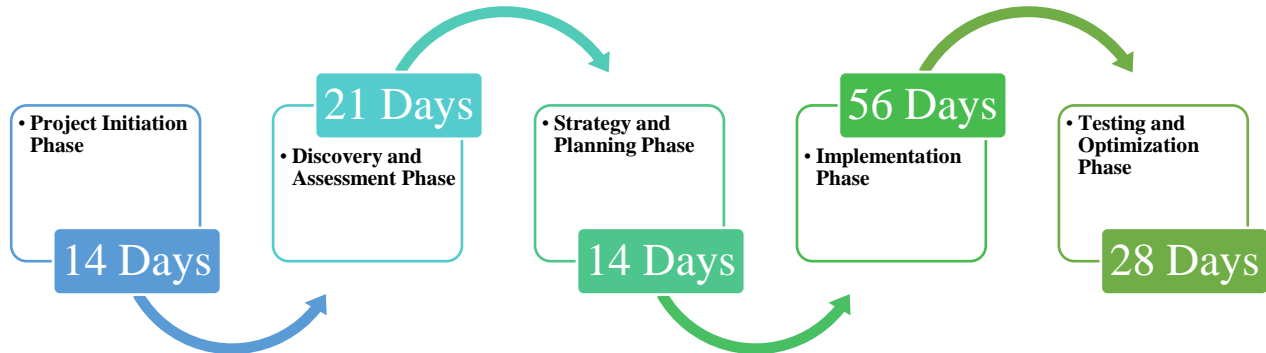
By:  _____

Name: Anisha Vataliya

Title: President

4.0 vTech's Project Plan

The project plan outlined below provides a high-level overview and may require further detailed planning and customization based on the specific requirements of State and vTech. The timelines and milestones will be determined in collaboration with State and adjusted as necessary throughout the project lifecycle.



1. Project Initiation Phase (2 Week):

- Conduct a kick-off meeting with State to discuss project objectives, expectations, and deliverables.
- Establish project governance structure, roles, and responsibilities.
- Define project milestones and timelines.
- Obtain necessary access and permissions to State network, systems, and data.

2. Discovery and Assessment Phase (3 Weeks):

- Perform a comprehensive risk assessment to identify and prioritize cybersecurity risks and vulnerabilities specific to State.
- Conduct interviews and workshops with State stakeholders to gather information on existing cybersecurity practices, policies, and procedures.
- Analyze State network infrastructure, systems, and data architecture to identify potential security gaps and weaknesses.
- Review existing cybersecurity documentation and policies.

3. Strategy and Planning Phase (2 Weeks):

- Develop a cybersecurity strategy and roadmap tailored to State specific needs and risk profile.
- Define cybersecurity policies, procedures, and standards based on industry best practices and regulatory requirements.
- Design a cybersecurity awareness training program for State staff and stakeholders.
- Create an incident response plan outlining procedures for handling cybersecurity incidents.
- Establish metrics and key performance indicators (KPIs) to measure the effectiveness of cybersecurity controls.

4. Implementation Phase: (8 Weeks)

- Deploy network security controls, including firewalls, intrusion detection and prevention systems, and other necessary security devices. (2 Weeks)
- Implement endpoint protection measures, such as antivirus, anti-malware, and anti-spyware software, on all endpoint devices. (3 Weeks)
- Establish data protection controls, including encryption, access controls, and backup procedures. (2 Weeks)

- Develop and deliver cybersecurity awareness training sessions for State staff and stakeholders. (2 Weeks)
- Configure a Security Information and Event Management (SIEM) solution for log analysis and real-time threat detection. (2 Weeks)
- Set up continuous monitoring mechanisms for State network, systems, and data. (1 week)

5. Testing and Optimization Phase: (4 Weeks)

- Conduct testing of implemented cybersecurity controls and validate their effectiveness.
- Perform vulnerability scanning and penetration testing to identify any remaining vulnerabilities.
- Optimize configurations, fine-tune security policies, and address any identified gaps or weaknesses.
- Verify the functionality of incident response procedures through tabletop exercises.
- Refine and enhance the cybersecurity awareness training program based on feedback and evaluation.

6. Ongoing Management and Support Phase: (Continuous until contractual end-date)

- Provide 24/7 monitoring and management of State cybersecurity infrastructure and systems.
- Conduct quarterly or agreed upon period for vulnerability assessments and update risk profiles as needed.
- Respond to cybersecurity incidents promptly, following the incident response plan.
- Maintain compliance with industry standards and regulatory requirements.
- Deliver periodic reports on cybersecurity activities, including compliance reports and status updates.
- Stay up to date with emerging threats and technologies, recommending improvements to State cybersecurity posture.

vTech's Project Approach

Penetration Testing: A penetration test simulates a hacker attempting to get into an organization's system through hands-on research and the exploitation of vulnerabilities both internally and externally. Skilled ethical hackers search for vulnerabilities (including those potentially not yet known or visible to vulnerability scanners), and then try to exploit said vulnerabilities. Ethical hackers often make use of similar tools and tactics employed by malicious actors.

Penetration Testing Deliverables

We will provide penetration testing as requested to meet the requirements of the State to assess and understand the areas of improvement for each State's systems. Through a detailed process State will be thoroughly tested to determine the strength of the specific component and the results of the testing will be communicated with comprehensive reporting. This methodology will assist you with improving your current cybersecurity, and proactively combat against cyber threats.

Internal Network Penetration Test

We have included Internal Network testing, as this phase is to exploit vulnerabilities and identify what information is being exposed to outsiders, after receiving full disclosure of the internal configurations, including source code, IP address, diagrams, and network protocols. This type of penetration testing attempts to find and exploit vulnerabilities of a system to steal or compromise the State's information.

External Network Penetration Test

Critical business resources such as external portals that allow access to internal systems, or to sensitive company data, are specifically tested. This phase exploits observed vulnerabilities, and identifies what information is being exposed to outsiders. This type of penetration testing attempts to find and exploit vulnerabilities of a system to steal or compromise the State's information.

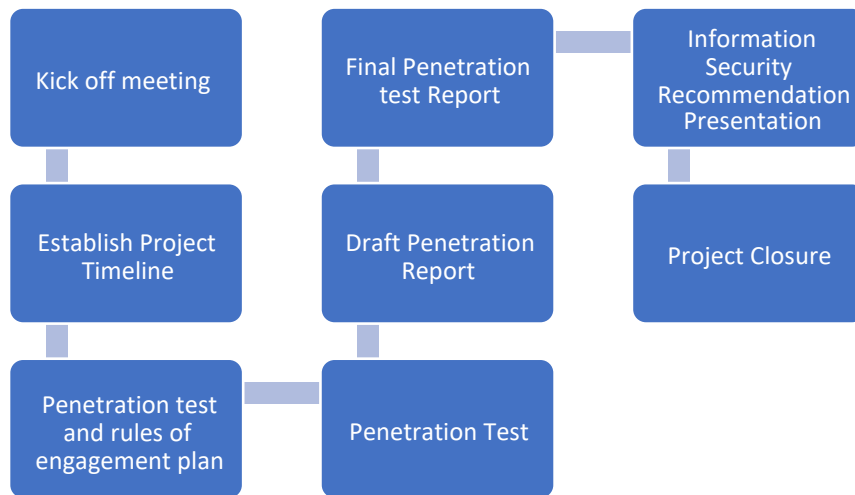
Web Application Penetration Test

This simulates a malicious actor attacking your web application using techniques outlined by OWASP, to exploit against all types of vulnerabilities that give access to private data, cardholder data, and sensitive information.

ASSESSMENT APPROACH/METHODOLOGY FOR PENETRATION TESTING

vTech Solution has extensive knowledge about performing penetration tests and our highly experienced engineers carry out penetration tests according to industry standards. During the assessment, the team will gather all relevant policy documentation, and scan networks, hosts, and applications with a variety of techniques and then perform the penetration test based on the found vulnerabilities. This yields a comprehensive insight into the IT environment, while also uncovering any gaps between the perceived state of security and the actual implementation and initiatives. A brief description of our assessment phases is laid out below:

- Discovery** – Develop a deeper understanding of State’s infrastructure, involved systems and applications
- Analysis** – Perform a detailed analysis of the current posture and identify the gaps as per the international standards and business objectives
- Assessment** – Once gaps are identified they are assessed as to their potential severity of loss and probability of occurrence
- Reporting & Strategic Remediation Plan** – Report the documented gaps, prioritized, and categorized along with a plan to help close those gaps and bring the organization to the level as per its business objective and legal and regulatory compliance.
- Sustainability** – Once the efforts have been made and a required strategic level is achieved, we make recommendations to maintain a high level of compliance for continuous improvement.



vTech’s experts follow a standard methodology to carry out a network and application penetration tests.

Intelligence Gathering

The objective of this first phase is to gain as much knowledge as possible about the target environment through a combination of non-intrusive and somewhat intrusive activities. Equipped with the results of these Intelligence Gathering activities, the team determines its execution plans for the subsequent phases.

- Project based information gathering
- Public- domain information gathering
- Network mapping

Vulnerability Scanning

The objective of this phase is to identify hosts, services and vulnerabilities in the target environment using a suite of customized tools. vTech performs two distinct steps during this phase: Host & Service Identification and Vulnerability Identification.

- Host & Service Identification
- Vulnerability Identification

Manual Verification

During this phase, vTech manually confirms the results from the automated tools. This activity serves to filter the data to improve the accuracy and relevance of our technical findings report as it eliminates false positives yielded by the tools.

While the scans effectively identify a large portion of the vulnerabilities present, vTech also executes manual testing to identify certain complex, emerging, or obscure vulnerabilities. This phase does not generally include exploitation of the identified vulnerabilities to penetrate systems. However, ‘inadvertent’ exploitation may occur when the vulnerability, by its very nature, is exploited in the process of identifying its presence or when exploitation will identify additional and/or dependent vulnerabilities.

The activities Our team performs during this phase offer significant value over the sole use of automated tools. Often, vulnerabilities identified using automated tools only are later determined to be false positives with the use of these advanced techniques. Furthermore, such techniques allow Our team to identify previously undetected vulnerabilities as they can detect countersecurity and attack techniques that obscure vulnerabilities from automated tools. For example, a common application running on a non-standard port may exhibit vulnerabilities not discovered by an automated scanner, but detectable using manual testing methods.

At the conclusion of this phase, our team will enumerate and validate vulnerabilities discovered through both automated and manual means. Within the final deliverable report, our team will note any particular vulnerability whose presence could neither be validated nor eliminated.

Vulnerability Exploitation

During this phase, our team attempts to exploit some of the vulnerabilities identified and confirmed during the previous phases. Our team will execute exploits with the sole aim of fulfilling the specific goals of the penetration assessment; however, our team will not actively exploit any vulnerability without obtaining permission from the client. Exploitation of certain vulnerabilities may lead to the identification of additional vulnerabilities that, in turn, may require further exploitation to identify potential problems. However, please note that Our team will follow this iterative process only to the extent necessary to accomplish the goals of the assessment. Our team performs Vulnerability Exploitation using a variety of techniques, depending on the nature of the vulnerabilities. Due to the nature of some vulnerabilities, our team may not be successful in exploiting all vulnerabilities within the agreed timeframe for execution. In such cases, our team will note this in the final deliverable report.

Analysis and Reporting

During the Analysis and Reporting phase, our team analyzes the information gathered and documents the findings. Our team then assigns a rating to each risk identified, based on standards of good practice and Our team’s extensive practical assessment experience.

Specifically, our team categorizes the risk each finding poses to your enterprise as "High," "Medium," or "Low." Our team will also categorize the amount of effort required to implement each recommendation

Social Engineering Testing vTech Security will perform two different exercises to test employee's resilience to social engineering attacks.

eMail Phishing

- Send employee emails
- Track input of credentials
- Track users that opened the email
- Track users that enter their credentials
- Track users that click on links in emails

Physical Security Testing

- Testing employees face to face
- Attempt to access non- public areas without authorization
- Attempt to gain access to the internal network

Web Application Security Assessment Objectives

Our team's Web Application Security Assessment determines the extent to which an application is vulnerable to an external attack. It examines the application for use of secure coding practices and identifies the risk exposure the application represents. Our team execution of a Web Application Assessment uses a combination of automated testing practices and creative manual testing approaches. The automated portion of the assessment relies on automated tools to perform tasks such as spidering and identification of vulnerabilities that are easily detected from responses.

The artistry of the assessment service is based on the execution of numerous manual attacks. These techniques are not easily automated and exploit the discoveries from the automated assessment activities. Vulnerabilities are verified and placed in context using knowledge of the environment and prior experience with another clientele.

Methodology Our team's Web Application Assessment service identifies security concerns of each application architecture component. Our team will begin the assessment by reviewing the application architecture with the State development personnel, application administrator or other applicable IT personnel, in order to gain an understanding of the application's use and administration. Network diagrams of all hosts in question should be provided before the initial meeting so that Our team has a clear architectural representation of the application.

Our team follows a detailed approach to conducting web application testing, as described in the following sections. While this is primarily a manual test, our team does employ some automated tools in assessing the application. Our team then analyzes the data and creates the technical findings report.

Application Architecture Review

This phase of the project begins with a meeting between the appropriate State key personnel and our testing team. This meeting identifies the objectives of the application test and desired results. Following the initial objective identification, our team and State will perform a review of the application features and architectural components. The State will provide a diagram of functional components and other supporting documentation, if available, during this phase. This ensures that the team will quickly understand and focus their efforts on the specific objectives of the test. The State will also provide all URLs, and any user IDs and passwords required to access the application at this time.

Discovery

Upon the completion of the architecture review, our team will begin the discovery phase of the assessment. This phase involves crawling the application and determining pages that exist within the application and where dynamic content is likely being generated. This activity will also in ascertaining other preliminary data. This phase is generally automated; however, there are sites which spiders do not handle well, in which case the application is mapped via more manual techniques.

Results from the discovery tools are used to create an attack plan. The attack plan focuses on areas that are often susceptible to web application vulnerabilities. Areas such as the authentication pages, form fields, and dynamically generated pages are marked for focus, while files such as images (i.e. .gif) and cascading style scripts (.css) are noted less important.

Automated Testing

Executing the plan of attack begins with the employment of automated tools and scripts. These tools provide value by testing a variety of attack vectors in a reduced timeframe. Detection of potential cross-site scripting, verbose errors and forceful browsing are examples of flaws typically identified with automated tools.

Manual Validation and Testing

During this phase, our team has two main objectives – to eliminate false positives from the previous phases and to exercises the features and functions provided by the application with the aim of escalating privileges and identifying potential vulnerabilities. Our team will attempt to escalate privileges both from the perspective of a valid user with a user ID provided by the State or as a user without any assigned user ID (guest).

The following list provides potential vulnerabilities that are tested for, as they are the most likely to present the greatest risk to a web application environment. Actual testing may evaluate a number of additional types of issues.

Input Validation

The majority of web application vulnerabilities are due to the lack of properly validating input. Common vulnerabilities associated with the lack of proper input validation include Command Injection attacks such as SQL Injection, cross-site scripting (XSS), Buffer Overflows and Form Manipulation.

Input validation is the act of validating the data the application receives and insuring it is data in the format the application expects. For example, in a field that expects a username, the application should ensure only alpha characters are received and reject all other character types. If testing produces non-alpha characters, then the application should either display a generic error or remove the unwanted characters. Furthermore, a major component of Input Validation is enforcing length restrictions to ensure the space available for the data to be stored is of adequate length.

Command Injection

Using Command Injection, an attacker attempts to submit a special character to terminate the intended application function and cause the application to execute a command issued by the attacker. For example, in SQL injection, a single quote (') character is injected through an input field variable being used in a SQL query. The single quote character terminates the SQL statement normally built by the application and can allow an attacker to append additional query data to the statement. The application sends the query to the backend database, executing the attacker's appended command. This type of attack can lead to a full compromise of the server by using internal database functionality.

Cross-site Scripting

Cross-site Scripting attacks target a client web browser through the vulnerable web application. This form of attack utilizes the web applications lack of input validation to inject client-side code into the webpage. A common mistake in web applications is to pass error messages as part of the URL.

For example, <http://www.domain.com/error.asp?error=This+is+an+error> results in the message “This is an error” displayed to the user via HTML. Changing the URL to [http://www.domain.com/error.asp?error=<script>alert\(‘test’\);</script>](http://www.domain.com/error.asp?error=<script>alert(‘test’);</script>) provides a java alert message that will display with the word “test”.

At this point, an attacker can insert a variety of JavaScript and other server-side code that could allow the capture of sensitive information such as cookie data that may contain authentication credentials for the applications. The attacker would then need to find a way to get the user to execute the URL in their browser, through an email message or message board, for instance. When the target follows the link, the code runs on the user’s machine, executing the attacker’s commands.

Buffer Overflows

A buffer overflow is an anomalous condition where a program somehow writes data beyond the allocated end of a buffer in memory. Since program control data often resides in the memory areas adjacent to data buffers, a buffer overflow is used to execute arbitrary code and usually leads to a remote compromise of the server.

In web applications, buffer overflows are often found in compiled Common Gateway Interface scripts, or State’s, and processing engines. Testing for buffer overflows is not as straightforward as other tests but is usually accomplished by replacing variable and cookie data with large amounts of data. In addition, large URLs, or file names may also cause overflows. In both cases, non-alpha characters printed on the screen after submitting these long strings is usually a sign of a buffer overflow existing.

Form Manipulation

Form Manipulation usually exists in web applications that attempt to hide information using “hidden” html form tags. Early on, a majority of these vulnerabilities resided in shopping cart programs that used this tag to hide the price of an item. This allowed an attacker to manipulate the price of an item. In this example, passing an item number via the form to a database and forcing the query to return the price for that item removes the problem.

Bypassing Access Controls

In some cases, web developers have taken extra steps to implement filters into the application to handle input. However, it is possible to bypass these filters in some cases using a variety of techniques. It is common to find developers using client-side code, such as JavaScript, in forms via “onsubmit()” functions. Since JavaScript executes on the client side, an attacker can choose not to execute the code either by submitting variables directly via a URL or by saving the page locally and modifying the code.

In other cases, the filters are implemented in the wrong place within the application. For example, cookie data is commonly encoded using base64 or Unicode. An attacker can easily decode this data, modify it and then re-encode it. If the filter only checks the encoded data for validity, it misses any data the attacker has inserted.

Authentication and Authorization Authentication is the act of verifying a user’s identity. Based on the identity, the application then authorizes the user to access various parts of the application. Improper account and session management as maintained by each application can allow unauthorized users elevated access to sensitive systems.

Account and Session Management

Account and session management deals with all aspects of how a user manages their account, as well as how the application tracks active sessions. Account management may include mechanisms to remind a user of their password, change a password or personalize their account information by uploading icons and adding signatures.

Our team tests multiple aspects of an application's account and session management. Users should not be able to change their password to be the same as their login id and reminders should not be the same as their password. In addition, the application should scrutinize "special characters" to ensure that they do not introduce problems during storage and retrieval. Session tracking should use random IDs in order to thwart attempts to guess valid session numbers. Guessing session IDs may allow an attacker to spoof a valid session and obtain unauthenticated access through another person's valid account.

Error Handling and Information Leakage

Error handling is the act of catching errors returned by an applications and functions. In a web environment, this usually deals with HTTP errors such as error 404 and 500. Information leakage may occur through data returned in error messages or the source code of HTML documents. Developers should be careful to take into account what information viewable by to users. Our team will attempt to obtain information by deliberately causing applications errors and evaluating the returned messages. These error messages could contain such things as directory structure s, paths to sensitive server configuration files or database structures. In addition, comments in the code disclosing a developer's name and email address can assist an attacker with social engineering attempts.

Data Integrity and Confidentiality

Proper data integrity and confidentiality implementation protects data from unauthorized modification and viewing. An attacker will normally try to compromise the data while in transit across the network but will be equally happy to compromise the data at the storage point. In a multi- tier web application environment, sensitive data traverses not only to and from a client, but also between tiers in the environment.

In a web application environment, data stored in cookies, authentication processes and data stored in the HTML source are all areas of concern. Encrypting data in cookies, especially credential data, will help prevent tampering by the user.

Often time's developers implement base 64 encoding to protect data instead of encryption. Using algorithms such as base64 to encode data provides little added security, as a simple web search provides numerous methods to decode base64 and reveal the hidden data. In addition, developers and Information Security should perform a comparative analysis of various types of encryptions, and discard algorithms not adequate to protect the data.

Web Server and Application Configuration

Improper configuration of servers and applications can pose significant risks to a system's security. When web servers and third- party web applications ship, they often come with a number of default settings that are inherently insecure. In addition, a number of them include online documentation and interfaces installed by default. A high percentage of these have proven security flaws that usually allow an attacker to gain information about your environment or even remotely compromise the server.

Follow-up Validation

If gaps are identified, that the State prefers to correct without our team's assistance or if these issues cannot be corrected during the time frame of the assessment, our team will return to the State, once remediation is

complete to validate mitigation of gaps on a “time and materials” basis. This effort will be addressed with a separate SOW, if required.

Quarterly ASV scans for PCI compliance

We will perform a quarterly ASV Scan for State using Tenable’s Nessus, as that is an approved vendor for ASV Scans. This quarterly ASV scan will identify vulnerabilities and misconfigurations. The ASV Scanning tool will scan physical devices, servers, services, and web applications that are part of the State environment.

vTech’s quarterly ASV Scans will include scanning of systems that are externally accessible (internet facing), their system components which are used by the environment and any external facing system component that provides access to the State. vTech’s team will start the process by gathering complete information about the environment before planning the scan to ensure that all entry points are included within the scan. Therefore, our scan will ensure compliance by confirming that the ASV scope is accurate and includes connected systems, including systems involved in storing, processing, or transmission of cardholder data. We will also ensure to scan IP addresses and FQDNs that have entryways into the environment.

Vulnerability Scanning and Reporting:

Risk Level	Recommendation
High Risk	Pose a serious, immediate threat to the confidentiality, integrity, and availability of the environment and its users, the exploitation of these findings would lead to the compromise of security. These findings should take the highest priority when considering your remediation efforts.
Medium Risk	Pose a threat to the environment and its use, these vulnerabilities are not necessarily immediately exploitable, but should be given serious consideration when remediating. An attacker could use medium level vulnerabilities to enumerate information and could lead to further attacks to compromise the environment and its users.
Low Risk	Do not pose a serious or immediate threat to the environment but is not recommended exposure. These vulnerabilities should not be ignored and should be considered when looking to secure your environment from attacks and compromise.
Informational	Interesting facts that were found during the assessment that pose no obvious risk to the environment but should be taken into consideration.

The Final Report will be divided into several sections as detailed below:

Section	Definition
Executive Summary	High-level overview of the in-depth vulnerability assessment.
Statement of Work	An overview of the client specified parameters for the assessment and the responsibilities of each party.
Results	An overview of the objectives that were met during the in-depth vulnerability assessment (i.e., unauthorized access obtained to environment, information resource, personal identifiable information was disclosed).

Analysis and Recommendations	An overview of the number of findings with their associated risk ratings.
Conclusion	The outcome of the Vulnerability Assessment.
Methodology	A summary of our in-depth vulnerability assessment methodology is given, detailing the phases that are taken from beginning to the end of the assessment.
Vulnerability Analysis and Recommendations	The core of the vulnerability report and gives detailed technical insight on the vulnerabilities that were identified, and the recommended remediation steps to eliminate the threats.

ENGAGEMENT DELIVERABLES AND CLIENT REQUIREMENTS

This engagement will require dynamic interaction between vTech and the Port team, in order to meet the outlined goals. Specific roles and accountabilities are defined as follows:

Activity or Focus	Scope & Delivery Requirements
Kickoff Meetings	One (2) hour Kick- off/Review remote meeting Rules of Engagement, Schedule, Target Identification plus Architecture Interview, Documentation and Diagram reviews
External Penetration Testing	Perform automated and manual testing of externally available services and resources belonging to vTech: Automated and manual service discovery and identification Vulnerability investigation and identification Vulnerability exploitation If relevant and authorized, post- exploitation privilege escalation and lateral movement
Internal Penetration Testing	Perform automated and manual testing of internally available services and resources: Automated and manual service discovery and identification Vulnerability investigation and identification Vulnerability exploitation Privilege escalation Network exploitation Lateral movement Account exploitation (with provided low- privileged account)
Physical Security Testing	Attempt to gain physical access to employee only areas Test employee resistance to in- person pressure Obtain unauthorized internal network connectivity

4.1 Project Management

Our project management approach is guided by PMBOK standards, COBIT framework for governance. This approach serves as a template that is customized and adapted to meet the specific requirements of each contract. vTech’s project managers apply these practices throughout the life cycle of the project as required. Our project management practices are concentrated around continuous oral and written communications. Our major projects are managed by a project manager with an impressive record of guiding projects to success.

Systematic Approach	Methodology
Establishing performance objectives	Performance objectives are established through a combination of best and proven commercial practice and government-specified performance standards. Performance objectives are developed internally to meet contract requirements. Performance objectives are documented and include contract requirements, approved plans, QC requirements for the program and employees performing tasks associated with performance requirements.
Measuring performance	Supervisors, managers, and QC specialists routinely and randomly measure performance proactively and continuously using key performance indicators and customer service indicators that indicate the effectiveness of personnel and the preparedness of employees before performance standards are jeopardized.
Collecting, analyzing, reviewing, and reporting performance data	Supervisors, managers, and QC specialists collect, analyze, review, and report performance data internally as metrics to identify performance trends, root causes, and corrective actions.
Reporting performance data	The Program Manager routinely briefs the Corporate Office on program-specific performance data and metrics. Metrics and general performance data indicating a potential performance deficiency are flagged and tracked in our management information system for proactive management. Metrics and general performance data are presented to key government personnel along with a root cause analysis, corrective action plan, and schedule.
Using performance data to drive performance improvement	Advance indicators of potential performance deficiencies afford us the time needed to re-allocate re-sources, conduct supplemental training, or take other corrective actions to improve performance and ensure client satisfaction. Performance is constantly monitored for contract-wide project delivery to respond in a timely manner and preempt negative impacts on mission effectiveness.

Project Schedule/Plan

Project Phase	Description	Schedule
Identification	Business Discovery, Program Analysis, Framework Mix identification, System Inventory	2-4 business weeks
Assessment	Manual and Automated Risk assessment, Risk Impact Evaluation, Priority matrix development, Maturity assessment	Contingent on Scope of Systems
Planning	Security roadmap development, risk prioritization,	Contingent on Scope of Systems
Execution	Mitigation Implementation, Project Initiation	Contingent on Scope of Systems
Monitoring	Cybersecurity Program Management	Contingent on Scope of Systems

**** Project Schedule for few activities is contingent upon size of the environment.**

Key Service Differentiators:

- Extensive Federal Government Experience with Cybersecurity Program Management backed by in-house Security Operations Center intelligence.
- Access to Industry leading technology and labs
- Ability to rapidly staff/consult additional security professionals.

Key Consulting Service Differentiators:

- Diverse Cybersecurity program skills available at the fingertip
- 40+ large mitigation consulting completed across government agencies.
- Enhanced Cybersecurity posture management reviews

Key Assessment Service Differentiators:

- Access to world’s best Cybersecurity assessment workflow technologies
- Consolidated Dashboard to track and view progress of assessments.
- Fine grained access to custom assessments
- Optimized assessment time for both manual and automated assessments by 30%

Deliverables

1. Initial Maturity Gap analysis
2. Strategic cybersecurity roadmap
3. Continuous Assessment and Authorization Plan
4. Cybersecurity Program Evaluation Briefing report
5. Executive Cyber Report

Task 1: Network Penetration Test

For this project's scope, Network Penetration testing is defined as security testing in which evaluators mimic real-world attacks to identify ways to circumvent the security features of an application, system, or network. vTech will offer the State the option to select the internal and external Penetration Testing they wish to participate in that is applicable for the State’s environment. The three (3) options will include Black Box, Gray Box, and White Box Penetration Testing.

A. White Box will be defined as a test methodology that assumes explicit and substantial knowledge of the assessment object's internal structure and implementation detail.

B. Gray Box will be defined as a test methodology that assumes some knowledge of the assessment object's internal structure and implementation detail.

C. Black Box will be defined as a test methodology that assumes no knowledge of the assessment object's internal structure and implementation detail

Understanding	Proposed Solution
<p>vTech will offer the State three options for Penetration Testing: White Box, Gray Box, and Black Box.</p> <p>White Box Testing assumes explicit and substantial knowledge of the assessment</p>	<p>We will present the State with the three Penetration Testing options: White Box, Gray Box, and Black Box.</p> <p>vTech’s White Box Testing methodology will involve having detailed knowledge of the State’s systems, including internal structures and implementation details. This type of testing allows for a comprehensive assessment of the systems, targeting specific vulnerabilities and providing an in-depth understanding of potential security risks.</p>

<p>object's internal structure and implementation detail. Gray Box Testing assumes some knowledge of the assessment object's internal structure and implementation detail. Black Box Testing assumes no knowledge of the assessment object's internal structure and implementation detail.</p>	<p>Our Gray Box Testing methodology will involve having partial knowledge of the State's systems, including certain internal structures and implementation details. This type of testing provides a balance between comprehensive testing and realistic scenarios, enabling the identification of vulnerabilities while simulating an attacker with limited knowledge.</p> <p>vTech's Black Box Testing methodology will involve having no prior knowledge of the State's systems, mimicking a real-world scenario where an attacker has no insider information. This type of testing assesses the systems' resilience against external threats and helps identify vulnerabilities that may be exploited by attackers with no prior knowledge.</p>
--	--

Task 2: Penetration Results Report

The Penetration test will be followed up with an extensive written report of the penetration test findings - to include cybersecurity gaps, suggestions for mitigation and remedies for gaps, and additional hardware and software that would rectify the identified gaps for the county. The report will be submitted to the respective State's point of contact and asked to present the findings to the State Commission. Depending on the sensitivity of the information, this will be done in either a public open meeting or study session (exempt from the Open Records Act)

Understanding	Proposed Solution
<p>The Penetration test aims to identify cybersecurity gaps in the State's systems. Suggestions for mitigation and remedies will be provided. Recommendations for additional hardware and software will be made. The report will be submitted to the County's point of contact. Presentation of the findings to the State Commission may be required. Consideration of sensitivity may require the presentation to be in a public open meeting or study session.</p>	<p>vTech will conduct a thorough assessment of the State's hardware, software, and cybersecurity measures to identify vulnerabilities and potential entry points.</p> <p>We will develop a comprehensive plan to address the identified cybersecurity gaps, including implementing security patches, enhancing network security, and updating software.</p> <p>vTech will first identify and propose suitable hardware and software solutions that can enhance the State's cybersecurity defenses, such as firewalls, intrusion detection systems, and encryption tools.</p> <p>We will establish a clear communication channel with the designated State representative to ensure the timely delivery of the penetration test report.</p> <p>vTech's assigned personnel will prepare a concise and informative presentation to effectively communicate the penetration test findings, cybersecurity gaps, and recommended remediation strategies.</p> <p>We will determine the sensitivity level of the information and adhere to the appropriate protocols and regulations for public disclosure, ensuring compliance with the Open Records Act.</p>

Task 3: Retest

Within 90 days of the mitigation and remedies being implemented, we will conduct an exact retest to the one previously performed on the respective State and provide a comprehensive analysis of the new test results to determine if the previous mitigation and remedy recommendations were successful and effective

Understanding	Proposed Solution
<p>Within 90 days of implementing mitigation and remedies, a retest will be conducted. The purpose of the retest is to determine the success and effectiveness of the previous mitigation and remedy recommendations. A comprehensive analysis of the new test results will be provided. The analysis will determine if the previous recommendations were successful and effective. The retest report will assist in identifying any further actions required. The report will be submitted to the respective State’s point of contact.</p>	<p>We will conduct an exact retest that replicates the initial penetration test on the respective State’s systems to evaluate the effectiveness of the implemented mitigation and remedy measures.</p>
	<p>We will thoroughly analyze the new test results and compare them with the findings from the initial penetration test. Evaluate if the implemented mitigation and remedy measures have effectively addressed the identified cybersecurity gaps and vulnerabilities.</p>
	<p>vTech will present a comprehensive analysis of the retest results, highlighting any changes, improvements, or remaining vulnerabilities in the State’s systems.</p>
	<p>We will also evaluate the effectiveness of the implemented mitigation and remedy measures based on the retest results. Determine if the recommended actions have adequately addressed the cybersecurity gaps and vulnerabilities identified in the initial penetration test.</p>
	<p>Our team will identify any additional actions or enhancements that may be necessary to strengthen the State’s cybersecurity posture based on the retest results. Provide recommendations for further improvements to ensure comprehensive protection and resilience against potential threats.</p>
<p>We will submit the retest report to the designated State representative responsible for overseeing cybersecurity. This individual will review the findings and recommendations presented in the report and take appropriate actions to address any remaining vulnerabilities and enhance the State’s security.</p>	

Task 4: Vulnerability Assessment

For the scope of this project, Vulnerability Assessment is defined as a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. The Vulnerabilities Assessment will involve a review of the hardware and software configurations, which must be utilized to establish the Cybersecurity Program for the State.

Understanding	Proposed Solution
---------------	-------------------

<p>Vulnerability Assessment is a systematic examination of an information system or product.</p> <p>The assessment aims to identify security deficiencies and predict the effectiveness of proposed security measures. The assessment helps confirm the adequacy of implemented security measures. Review of hardware and software configurations is necessary for the assessment. The assessment will provide essential data to support the Cybersecurity Program development. The report will be submitted to the respective State’s point of contact.</p>	<p>We will conduct a comprehensive evaluation of the State’s information system and product to assess the adequacy of existing security measures.</p>
	<p>Our assigned resource will identify potential vulnerabilities and security gaps within the hardware and software configurations utilized for establishing the State’s Cybersecurity Program.</p>
	<p>vTech will also validate the effectiveness of the security measures implemented within the State’s Cybersecurity Program and ensure they meet the required standards.</p>
	<p>We will thoroughly examine the hardware and software configurations utilized in the State’s information systems. Evaluate their current state, settings, and potential vulnerabilities that may pose risks to the security of the systems and data.</p>
	<p>vTech will Gather valuable data and insights from the Vulnerability Assessment to inform the development and enhancement of the State’s Cybersecurity Program. This information will assist in prioritizing security measures and establishing a robust cybersecurity framework.</p>
<p>We will submit the retest report to the designated State representative responsible for overseeing cybersecurity. This individual will review the findings and recommendations presented in the report and take appropriate actions to address any remaining vulnerabilities and enhance the State’s security.</p>	

Task 5: Maintaining the State’s Cybersecurity Program

The Consultant will work with the county to establish a Cybersecurity Program. This program will consist of establishing schedules, checklists, and policies and procedures to maintain the integrity of the State’s Cybersecurity. These tools will be utilized to monitor and define the performance of the State’s I.T. Department or State’s I.T. Consultant. The program must consist of the following areas, but is not limited to, O.S. and software patches, antivirus, and device firmware updates. The program is to include general cybersecurity and system-specific recommendations

Understanding	Proposed Solution
<p>The Consultant will work with the county to establish a Cybersecurity Program. The program will consist of establishing schedules, checklists, policies, and procedures to maintain the</p>	<p>We will collaborate with the county to develop a comprehensive Cybersecurity Program tailored to their specific needs.</p> <p>vTech will develop schedules, checklists, policies, and procedures that outline the necessary steps and guidelines for maintaining a robust cybersecurity posture. These documents will provide a framework for the State’s IT department or IT consultant to follow, ensuring that cybersecurity measures are consistently implemented and maintained.</p>

integrity of the State’s Cybersecurity. The program will be used to monitor and define the performance of the County's IT department or IT consultant. The program must include areas such as O.S. and software patches, antivirus, and device firmware updates, along with general cybersecurity and system-specific recommendations.

We will implement monitoring mechanisms and performance indicators to evaluate the effectiveness of the State’s IT department or IT consultant in adhering to the established cybersecurity program. This will allow for ongoing assessment and improvement of their cybersecurity practices.

vTech will incorporate guidelines and best practices for O.S. and software patch management, antivirus solutions, device firmware updates, and other relevant areas into the Cybersecurity Program. Additionally, provide comprehensive recommendations for general cybersecurity practices that cover areas such as user awareness training, access controls, network security, incident response, and more, based on the specific systems and requirements of the State.

4.2 Executive Summary Report

External Network Penetration Testing

Scope and Approach: The External Network Penetration Testing conducted by vTech adhered to a comprehensive four-phased methodology, encompassing reconnaissance, mapping, discovery, and exploitation. Through meticulous analysis and utilization of industry-standard tools, our team scrutinized the Lottery's external network infrastructure to identify potential vulnerabilities and assess organizational impact.

Findings: Numerous vulnerabilities were uncovered during the assessment, ranging from critical to low risk. These vulnerabilities spanned various aspects of the network, including infrastructure, protocols, and services. Each vulnerability type was meticulously documented, providing clear insights into the potential risks posed to the Lottery's IT environment.

Key Points of Strength: Despite the identified vulnerabilities, several strengths were observed within the assessed infrastructure. These strengths include robust network architecture, effective access controls, and proactive security measures implemented by the Lottery.

Recommendations: To mitigate the identified vulnerabilities and enhance the overall security posture, vTech recommends immediate action on several fronts. These recommendations encompass patching known vulnerabilities, enhancing access controls, implementing network segmentation, and conducting regular security training and awareness programs for staff members.

Conclusion: In conclusion, the External Network Penetration Testing revealed both areas of improvement and commendable practices within the Lottery's IT environment. By addressing the identified vulnerabilities and implementing the recommended measures, the Lottery can strengthen its defenses against potential cyber threats and safeguard critical business processes and IT services.

Report Details: Each vulnerability discovered during the assessment is outlined in detail within this report. This includes information on how the vulnerability was discovered, its potential impact if exploited, recommendations for remediation, and references for further vulnerability analysis.

vTech's External Network Penetration Testing provides invaluable insights into the security posture of the Lottery's external network infrastructure, equipping senior management with actionable recommendations to enhance cybersecurity resilience and mitigate risks effectively.

Website Penetration Testing

Scope and Approach: vTech conducted a comprehensive Website Penetration Testing aimed at identifying vulnerabilities within the Lottery's web applications and associated environments. The assessment followed a meticulous four-phased methodology, encompassing reconnaissance, mapping, discovery, and exploitation. Each phase was executed with precision to ensure thorough coverage and accurate identification of potential risks.

Findings: Numerous vulnerabilities were uncovered throughout the testing process, ranging from common web application vulnerabilities to configuration issues and authentication bypasses. These findings provide critical insights into the security posture of the Lottery's web assets, enabling targeted remediation efforts to mitigate potential risks effectively.

Key Points of Strength: Despite the identified vulnerabilities, several strengths were observed within the assessed web infrastructure. These strengths include robust SSL/TLS configurations, effective session management practices, and proactive vulnerability scanning measures implemented by the Lottery.

Recommendations: To address the identified vulnerabilities and enhance the overall security resilience of the web applications, vTech recommends immediate action on several fronts. These recommendations include patching known vulnerabilities, implementing robust access controls, conducting thorough authentication and authorization checks, and enhancing security awareness among web developers.

Conclusion: In conclusion, the Website Penetration Testing conducted by vTech offers valuable insights into the security posture of the Lottery's web applications. By addressing the identified vulnerabilities and implementing the recommended measures, the Lottery can strengthen its defenses against potential cyber threats and safeguard critical web assets effectively.

Report Details: This report provides specific details for each vulnerability discovered during the assessment, including how the vulnerability was discovered, its potential impact if exploited, recommendations for remediation, and references for further vulnerability analysis. The Executive Summary Report offers a comprehensive overview of all testing results, empowering senior management with actionable insights to make informed decisions regarding cybersecurity posture and risk mitigation strategies.

Internal/Client-Side Network Penetration Testing

Scope and Approach: vTech conducted an exhaustive Internal/Client-Side Network Penetration Testing, focusing on assessing the security posture of all Lottery locations onsite. The assessment adhered to a meticulously structured four-phased methodology, encompassing reconnaissance, mapping, discovery, and exploitation. By conducting the assessment onsite, vTech ensured comprehensive coverage and accurate identification of potential vulnerabilities.

Findings: The assessment uncovered several critical vulnerabilities across networked assets, including servers, endpoints, firewalls, and network devices. These vulnerabilities ranged from software misconfigurations to weaknesses in security solutions, posing significant risks to the Lottery's infrastructure. Through thorough testing and analysis, vTech identified exploitable avenues and potential security gaps that require immediate attention.

Key Points of Strength: Despite the identified vulnerabilities, several strengths were observed within the assessed infrastructure. These strengths include robust network segmentation, effective endpoint protection measures, and proactive network monitoring capabilities. These strengths serve as foundational pillars for enhancing the overall security resilience of the Lottery's internal network environment.

Recommendations: To address the identified vulnerabilities and bolster the security posture of the internal network, vTech recommends immediate remediation actions. These recommendations include patching known vulnerabilities, strengthening access controls, enhancing network segmentation, and implementing robust intrusion detection and prevention mechanisms. Additionally, vTech advises ongoing security awareness training to empower Lottery staff in identifying and mitigating potential security risks.

Conclusion: In conclusion, the Internal/Client-Side Network Penetration Testing conducted by vTech provides valuable insights into the security landscape of the Lottery's internal network environment. By implementing the recommended remediation measures and leveraging the identified strengths, the Lottery can fortify its defenses against potential cyber threats and safeguard its critical assets effectively.

Report Details: This report offers specific details for each vulnerability discovered during the assessment, including how the vulnerability was discovered, its potential impact if exploited, recommendations for remediation, and references for further vulnerability analysis. The Executive Summary Report serves as a comprehensive overview of all testing results, empowering senior management with actionable insights to prioritize and address security concerns effectively.

Wireless Penetration Testing

Scope and Approach: vTech conducted comprehensive Wireless Penetration Testing at all Lottery locations onsite, adhering strictly to the prohibition of remote assessment. The testing followed a structured four-phased methodology, encompassing reconnaissance, mapping, discovery, and exploitation. By gaining full access to the buildings, vTech ensured thorough coverage and accurate assessment of wireless assets.

Findings: The assessment revealed critical vulnerabilities within the wireless infrastructure, including misconfigured access points, weak encryption protocols, and the presence of rogue access points. These vulnerabilities expose the Lottery's network to potential security breaches, unauthorized access, and data compromise. Through meticulous testing and analysis, vTech identified attack vectors and potential exploitation scenarios that necessitate immediate remediation.

Key Points of Strength: Despite the identified vulnerabilities, several strengths were observed within the wireless infrastructure. These strengths include robust encryption standards, effective access control mechanisms, and proactive detection of rogue access points. These strengths serve as essential foundations for enhancing the overall security posture of the Lottery's wireless environment.

Recommendations: To address the identified vulnerabilities and fortify the wireless infrastructure, vTech recommends prioritized remediation actions. These recommendations include implementing stronger encryption protocols, enhancing access point configurations, deploying intrusion detection systems for rogue AP detection, and conducting regular security audits. Additionally, vTech advises proactive monitoring and response measures to mitigate potential wireless threats effectively.

Conclusion: In conclusion, the Wireless Penetration Testing conducted by vTech provides valuable insights into the security resilience of the Lottery's wireless infrastructure. By implementing the recommended remediation measures and leveraging the identified strengths, the Lottery can strengthen its defenses against wireless attacks and safeguard sensitive data effectively.

Report Details: This report offers specific details for each vulnerability discovered during the assessment, including how the vulnerability was discovered, its potential impact if exploited, recommendations for remediation, and references for further vulnerability analysis. The Executive Summary Report serves as a comprehensive overview of all testing results, empowering senior management with actionable insights to address wireless security concerns proactively.

4.3 vTech meeting State’s Mandatory Requirements

vTech is fully prepared to meet the mandatory requirements set forth by the State of West Virginia for cybersecurity assessments for the West Virginia Lottery. With a focus on delivering exceptional service, vTech acknowledges the importance of adhering to industry-standard methodologies such as those outlined by the Center for Internet Security. Our team is dedicated to ensuring thorough compliance with each specification, utilizing our expertise to identify vulnerabilities and provide actionable recommendations. vTech's commitment to excellence and proficiency in cybersecurity assessment makes us the ideal partner to support the security needs of the West Virginia Lottery.

State of West Virginia Requirement	vTech’s Comments
4.1. External Network Penetration Testing	
4.1.1. External Network Penetration Testing may be performed remotely.	vTech is equipped to conduct External Network Penetration Testing remotely, ensuring flexibility and accessibility in the assessment process.
4.1.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.	We commit to collaborating closely with the Lottery to establish appropriate timeframes, testing schedules, and target completion dates. Exclusions will be determined in conjunction with the successful vendor to ensure a comprehensive testing approach.
4.1.3. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.	Our methodology for External Network Penetration Testing adheres to a four-phased structure, covering reconnaissance, mapping, discovery, and exploitation. This comprehensive approach ensures thorough assessment and identification of vulnerabilities.
4.1.3.1.Reconnaissance should include:	
4.1.3.1.1. Perform WHOIS, ARIN, and DNS (public server) lookups	For reconnaissance in External Network Penetration Testing, vTech will: <ul style="list-style-type: none"> • Perform WHOIS, ARIN, and DNS lookups to gather domain registration and network information. • Conduct OSINT (Open Source Intelligence) searches and utilize public search tools for additional data gathering. • Create custom password lists to aid in potential credential-based attacks. • Perform DNS lookups on entity servers to identify potential vulnerabilities. • Gather information from entity network resources to assess network infrastructure and topology. • Analyze metadata associated with network resources to uncover hidden information and potential vulnerabilities.
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:	

<p>4.1.3.2.1. Network Discovery (ICMP sweeps, traceroutes, bypass firewall restrictions, etc.)</p> <p>4.1.3.2.2. Port/Protocol Scanning (Scan for accepted IP protocols, open TCP/UDP ports)</p> <p>4.1.3.2.3. OS/Version Scanning (Identify underlying OS and software and their versions)</p>	<p>For mapping in External Network Penetration Testing, vTech will:</p> <ul style="list-style-type: none"> • Conduct Network Discovery using ICMP sweeps, traceroutes, and methods to bypass firewall restrictions, ensuring comprehensive coverage of the network. • Perform Port/Protocol Scanning to identify accepted IP protocols and open TCP/UDP ports, revealing potential entry points for attackers. • Utilize OS/Version Scanning techniques to identify the underlying operating systems and software versions running on network devices, aiding in vulnerability assessment and exploitation.
<p>4.1.3.3. Discovery should include:</p>	
<p>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)</p>	<p>During External Network Penetration Testing, vTech will employ industry-standard tools like Nessus and Burp Suite for comprehensive vulnerability scanning. These tools will help identify and assess vulnerabilities in network devices and web applications, enabling us to deliver detailed insights and recommendations for enhancing security.</p>
<p>4.1.3.3.2. Enumerating Network Services (Connect and interact with services to disclose information, gain access, identify misconfigurations, etc.)</p>	<p>During network penetration testing, vTech will thoroughly enumerate network services by connecting and interacting with them to uncover valuable information, detect potential misconfigurations, and gain insights into system vulnerabilities. This process involves probing various network services to identify any weaknesses that could be exploited by attackers. By meticulously examining these services, we can provide actionable recommendations to strengthen the security posture and mitigate risks effectively.</p>
<p>4.1.3.3.3. Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)</p>	<p>As part of our network penetration testing approach, vTech will conduct username/email enumeration by validating and attempting to guess usernames/emails using login forms, network services, and other available resources. This process helps identify potential entry points for unauthorized access and highlights any weaknesses in authentication mechanisms. By thoroughly assessing username/email enumeration, we can provide recommendations to enhance security measures and prevent unauthorized access to sensitive information.</p>
<p>4.1.3.4. Exploitation should include:</p>	
<p>4.1.3.4.1. Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force)</p>	<p>In our network penetration testing methodology, vTech will include brute force login attempts using discovered username/email addresses to gain unauthorized access through repeated login attempts. By simulating these attacks, we can identify vulnerabilities in password security measures and provide recommendations for strengthening authentication protocols. This proactive approach helps mitigate the risk of unauthorized access to critical systems and data.</p>
<p>4.1.3.4.2. Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)</p>	<p>As part of our network penetration testing process, vTech will engage in exploitation activities to simulate real-world cyber threats. This involves leveraging discovered vulnerabilities to gain unauthorized access or disclose sensitive information. By exploiting weaknesses in the network infrastructure or applications, we can assess the potential impact of a successful attack and provide actionable recommendations for remediation. Our goal is to help our clients strengthen their defenses and minimize the risk of exploitation by malicious actors.</p>

<p>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).</p>	<p>After successful exploitation, vTech conducts post-exploitation activities to uncover additional vulnerabilities and extract sensitive information. We iterate through penetration testing steps to gain privileged access and assess potential damage, using compromised systems as pivot points for subsequent attacks. This approach strengthens defense mechanisms against cyber threats.</p>
<p>4.1.4. Must identify exploitable vulnerabilities and demonstrate organizational impact.</p>	<p>vTech meticulously identifies exploitable vulnerabilities and demonstrates their organizational impact, providing a clear understanding of the potential risks to the client's infrastructure and operations. This comprehensive approach ensures effective mitigation strategies can be implemented to bolster cybersecurity defenses.</p>
<p>4.1.5. Denial of service (DoS) attacks are prohibited for External Network Penetration Testing services</p>	<p>External Network Penetration Testing services provided by vTech strictly adhere to the prohibition of Denial of Service (DoS) attacks, ensuring the integrity and availability of the client's network resources without disruption.</p>
<p>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.</p>	<p>As per the requirement, vTech will conduct a social engineering exercise as part of the External Network Penetration Testing. This exercise will involve creating a phishing email scenario meticulously crafted to target approximately 200 active Lottery staff. The content of the email will be designed to maximize successful phishing attempts. Additionally, both the email content and target addresses will be thoroughly verified and approved by the Lottery before execution.</p>
<p>4.1.7. Heavy load brute force or automated attacks will only be performed with prior Lottery approval.</p>	<p>Heavy load brute force or automated attacks will be conducted only upon obtaining prior approval from the Lottery, as per the specified requirement for External Network Penetration Testing.</p>
<p>4.1.8. Must notify Lottery of any portion or portions of the assessment resulting in service disruption.</p>	<p>vTech will promptly notify the Lottery of any portion or portions of the assessment that result in service disruption, ensuring transparency and collaboration throughout the testing process as required.</p>
<p>4.1.9. The Lottery must be notified immediately upon identifying any security vulnerability threatening critical business processes or IT services.</p>	<p>vTech acknowledges and agrees to promptly notify the Lottery upon identifying any security vulnerability that poses a threat to critical business processes or IT services. This commitment ensures timely communication and collaboration to address and mitigate potential risks effectively.</p>
<p>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.</p>	<p>Upon completing the assessment, vTech will deliver a comprehensive Executive Summary Report to the Lottery. This report will offer an overarching view of the assessment's outcomes, encompassing details on the scope and methodology employed, key findings, notable strengths within the assessed infrastructure, and targeted recommendations tailored for senior management.</p>
<p>4.1.10.1. The vendor shall provide a sample of the executive summary report with their bid response.</p>	<p>As per the requirement, vTech will include a sample of the Executive Summary Report along with our bid response. This sample will offer insight into the structure, content, and quality of the reports we deliver upon the conclusion of assessments.</p>
<p>4.1.10.2. The report must be submitted to the Lottery electronically for review.</p>	<p>Following the assessment's conclusion, vTech will ensure that the Executive Summary Report is submitted electronically to the Lottery for thorough review and evaluation. This electronic submission process will facilitate efficient communication and</p>

	ensure prompt access to the assessment findings and recommendations.
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.	vTech will furnish a comprehensive Technical Report to the Lottery. This report will meticulously outline each identified vulnerability type, accompanied by a clear categorization of its risk level—ranging from critical to low. By providing detailed insights into the nature and severity of vulnerabilities, this report aims to equip the Lottery with the necessary information to prioritize and address security concerns effectively.
4.1.12. Reports must include specific details for each vulnerability found, including:	
4.1.12.1. How the vulnerability was discovered	In compliance with the stipulated requirements, vTech's technical reports will meticulously document each discovered vulnerability, providing a comprehensive overview for the Lottery's review. This documentation includes detailed insights into the discovery process, elucidating how each vulnerability was identified. Furthermore, the reports will outline the potential impact of exploitation, enabling the Lottery to gauge the severity and implications of each vulnerability on their systems. Moreover, the reports will offer clear and actionable recommendations for remediation, empowering the Lottery to address identified weaknesses effectively. Each vulnerability will be referenced with pertinent information, ensuring clarity and traceability. Additionally, vTech will include a sample of the technical report with our bid response, allowing the Lottery to assess the depth and quality of our reporting. Finally, to facilitate efficient review and collaboration, all reports will be submitted electronically to the Lottery.
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.	Following the conclusion of the assessment, vTech commits to delivering a comprehensive Findings Presentation to the Lottery management team. This presentation will serve as a platform to provide a holistic overview of the strengths, weaknesses, and vulnerabilities identified during the assessment process. Through engaging visuals and clear communication, vTech will highlight key findings, elucidate vulnerabilities, and underscore areas of strength within the assessed infrastructure. The presentation will offer actionable insights, enabling the Lottery management team to make informed decisions regarding cybersecurity posture and risk mitigation strategies. vTech is dedicated to ensuring that the Findings Presentation serves as a valuable resource for the Lottery, facilitating collaborative discussions and fostering a shared understanding of the assessment outcomes.
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.	The findings presentation shall be flexible in its delivery method, accommodating the preferences of the Lottery. vTech is committed to ensuring that the presentation is accessible and convenient for the Lottery management team. Whether conducted in person or via a conference call, the presentation will be tailored to meet the needs and scheduling requirements of the Lottery. By offering flexibility in presentation format, vTech aims to facilitate seamless collaboration and communication, ensuring that the assessment findings are effectively conveyed and discussed with key stakeholders.
4.2. Website Penetration Testing	
4.2.1. Website Penetration Testing may be performed remotely.	Read, Understood & Acknowledged.
4.2.2. Timeframes, testing schedule, target completion dates and exclusions will be	The timeline, schedule, and target completion dates for Website Penetration Testing will be collaboratively established between

determined in conjunction with the successful vendor.	vTech and the Lottery to ensure alignment with project goals and deadlines.
4.2.3. The successful vendor must determine static and dynamic page counts.	The determination of static and dynamic page counts will be the responsibility of vTech, leveraging our expertise to accurately assess the scope and complexity of the website.
4.2.4. Any environment, such as production, development, quality assurance, etc., may be tested. Each environment will be assessed separately.	Website Penetration Testing may encompass various environments, including production, development, and quality assurance, with each environment evaluated separately to capture specific vulnerabilities and risks.
4.2.5. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.	vTech will employ a comprehensive four-phased methodology for Website Penetration Testing, comprising reconnaissance, mapping, discovery, and exploitation, to systematically identify and address potential security threats and weaknesses.
4.2.5.1.Reconnaissance should include:	
4.2.5.1.1. Perform WHOIS, ARIN, and DNS (public server) lookups	vTech will conduct WHOIS, ARIN, and DNS lookups to gather comprehensive domain information during the website penetration testing. These lookups will provide details about domain registration, ownership, IP address allocation, and DNS records, helping to identify potential attack vectors and vulnerabilities.
4.2.5.1.2. OSINT - Public Searches/Dorks	vTech will utilize OSINT techniques, including public searches and dorks, to gather valuable information about the target website for effective reconnaissance.
4.2.5.1.3. Build custom password lists	vTech will craft customized password lists to enhance the reconnaissance phase, ensuring thorough coverage and exploration of potential vulnerabilities.
4.2.5.1.4. DNS lookups (entities server)	vTech will conduct DNS lookups on the entities' servers to gather essential information during the reconnaissance phase of the website penetration testing process.
4.2.5.1.5. Gather information from entities web applications	During the reconnaissance phase of website penetration testing, vTech will collect pertinent information from the entities' web applications to assess their security posture and identify potential vulnerabilities.
4.2.5.1.6. Analyze metadata	As part of the reconnaissance phase in website penetration testing, vTech will analyze metadata to extract valuable information about the target web applications, helping to identify potential vulnerabilities and weaknesses.
4.2.5.2.Mapping should include:	
4.2.5.2.1. SSL/TLS Analysis (Identify accepted SSL/TLS ciphers)	During the mapping phase of website penetration testing, vTech will conduct SSL/TLS analysis to identify the SSL/TLS ciphers accepted by the target web applications. This analysis helps to assess the security configuration of the SSL/TLS protocols and identify potential vulnerabilities related to encryption and data protection.
4.2.5.2.2. Virtual Hosting & Load Balancer Analysis	As part of the website penetration testing mapping phase, vTech will conduct virtual hosting and load balancer analysis. This involves identifying the virtual hosting configurations and load balancer setups used by the target web applications. Understanding how virtual hosting and load balancing are implemented helps assess the resilience and scalability of the web infrastructure and identifies potential points of failure or misconfigurations that could be exploited by attackers.
4.2.5.2.3. Software Configuration Discovery (Identify HTTP version, web services, scripting languages, third-party web applications, etc.)	During the mapping phase of website penetration testing, vTech will perform software configuration discovery to identify various aspects of the web server setup. This includes determining the HTTP version being used, identifying active web services,

	detecting scripting languages employed in web development, and recognizing any third-party web applications integrated into the system. Understanding the software configuration is crucial for assessing security vulnerabilities and ensuring the robustness of the web infrastructure.
4.2.5.2.4. HTTP Options Discovery (Identify accepted HTTP methods)	As part of the website penetration testing process, vTech will conduct HTTP Options Discovery to identify the accepted HTTP methods supported by the web server. This involves examining the server's response to various HTTP requests to determine which methods it allows. Understanding the accepted HTTP methods is essential for assessing the security posture of the web application and identifying potential vulnerabilities related to improper method handling or configuration.
4.2.5.2.5. Web Application Spidering (gather/follow all links)	During web application penetration testing, vTech will conduct web application spidering to systematically explore the application by following all accessible links. This automated process enables the identification of hidden pages, directories, and endpoints, providing a comprehensive mapping of the application's structure, content, and functionality.
4.2.5.2.6. Directory Browsing (Identify web directory listings, brute force common web directory names)	During web app penetration testing, vTech will conduct directory browsing to identify web directory listings and brute force common directory names, aiming to uncover sensitive information or hidden resources.
4.2.5.2.7. Web Application Flow (Identify the business logic, flow, organization, and functionalities of the app)	vTech will analyze the web application flow to discern its business logic, organization, and functionalities, providing insights into how data and processes are structured and interact within the application.
4.2.5.2.8. Session Analysis (Identify locations where session cookies are set and analyze predictability)	vTech will conduct session analysis to identify the locations where session cookies are set within the web application and analyze their predictability, enhancing the understanding of session management and potential security vulnerabilities.
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)	vTech will conduct vulnerability scanning using open-source tools like Nessus and commercial tools like Burp Suite to identify potential vulnerabilities.
4.2.5.3.2. Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)	vTech will validate and attempt to guess usernames/emails using login forms, network services, etc., to uncover potential security risks.
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.)	vTech will identify and address specific vulnerabilities such as Command/XML/XXE/SQL Injection, File Inclusion, Directory Traversal, File Upload, XSS, CSRF, etc., to enhance web application security.
4.2.5.3.4. Identify Authentication/Authorization Issues/Bypasses (Weak access control, weak password policy, session management, etc.)	vTech will identify and address issues related to weak access control, weak password policies, and session management to mitigate authentication and authorization vulnerabilities.
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)	vTech will attempt to gain additional access through brute force using discovered username/email addresses, adhering to security protocols and obtaining necessary permissions from the Lottery.
4.2.5.4.2. Exploitation (Using	

<p>discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)</p>	
<p>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).</p>	<p>vTech will exploit discovered vulnerabilities to gain additional access or disclose information, ensuring compliance with ethical standards and obtaining appropriate approvals from the Lottery before proceeding. After gaining initial access, vTech will conduct post-exploitation activities to disclose information and identify additional vulnerabilities. The team will repeat penetration testing steps to attempt to gain privileged access and use compromised systems as a pivot point to attack other systems within scope, with Lottery approval.</p>
<p>4.2.6. Must provide identification of prioritized remediation needs, requirements, and associated risks.</p>	<p>vTech will prioritize and identify remediation needs, requirements, and associated risks based on the assessment findings, ensuring clear communication and understanding of security vulnerabilities to facilitate effective remediation efforts.</p>
<p>4.2.7. Testing shall determine if website vulnerabilities exist by testing each website, including server operating systems, application platforms, and databases.</p>	<p>vTech will comprehensively test each website, including server operating systems, application platforms, and databases, to identify and address any existing vulnerabilities, ensuring thorough evaluation and mitigation of potential security risks.</p>
<p>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.</p>	<p>vTech will conduct Denial of Service (DoS) attacks as required for Website Penetration Testing, adhering to Lottery regulations and obtaining necessary approvals and permissions before commencing the attack.</p>
<p>4.2.9. Heavy load brute force or automated attacks will only be performed with prior Lottery approval.</p>	<p>vTech will seek prior approval from the Lottery before conducting heavy load brute force or automated attacks, ensuring compliance with regulations and ethical standards to protect the integrity and security of the assessment process.</p>
<p>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.</p>	<p>vTech will provide an Executive Summary Report upon concluding the assessment, offering an overview of all testing results, including scope, approach, findings, strengths, weaknesses, and recommendations directed at senior management, delivered in accordance with Lottery requirements and guidelines.</p>
<p>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.</p>	<p>vTech will deliver a comprehensive Technical Report detailing each discovered vulnerability type along with a critical, high, medium, or low risk rating, ensuring clear documentation and understanding of security risks for effective remediation efforts.</p>
<p>4.2.12. Reports must include specific details for each vulnerability found, including:</p>	
<p>4.2.12.1. How the vulnerability was discovered</p>	<p>vTech will meticulously document how each vulnerability was discovered, providing transparency and insight into the testing methodology and ensuring clarity regarding the origin and nature of identified vulnerabilities.</p>
<p>4.2.12.2. The potential impact of its exploitation.</p>	<p>vTech's reports will outline the potential impact of exploiting each vulnerability, including potential consequences for the system, data, and operations, facilitating informed decision-making and prioritization of remediation efforts by the Lottery.</p>
<p>4.2.12.3. Recommendations for remediation.</p>	<p>vTech will offer clear and actionable recommendations for remediating each vulnerability, tailored to the specific context and</p>

	requirements of the Lottery, to support effective mitigation strategies and enhance the overall security posture of the assessed infrastructure.
4.2.12.4. Vulnerability references	vTech will include vulnerability references in the reports, ensuring traceability and facilitating further investigation or verification by the Lottery or relevant stakeholders, contributing to transparency and accountability in the assessment process.
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.	vTech acknowledges the requirement for onsite testing at all Lottery locations to conduct Internal/Client Side Network Penetration Testing, ensuring direct access to internal networks and systems for comprehensive assessment and accurate results.
4.3.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.	vTech commits to collaborating with the Lottery to establish appropriate timeframes, testing schedules, and target completion dates, ensuring alignment with project goals and accommodating any exclusions or specific requirements identified during planning.
4.3.3. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.	vTech will implement a structured four-phased methodology encompassing reconnaissance, mapping, discovery, and exploitation to systematically identify vulnerabilities and assess internal/client-side network security posture, ensuring thorough and effective testing processes.
4.3.3.1. Reconnaissance should include:	
4.3.3.1.1. Identify software versions along with potentially useful software configurations or settings	vTech will meticulously identify software versions and assess configurations/settings for potential vulnerabilities or weaknesses, ensuring thorough scrutiny of all installed software within the internal/client-side network environments.
4.3.3.1.2. Identify any anti-malware, firewall, and IDS products on the system	vTech will identify and document the presence of anti-malware, firewall, and intrusion detection system (IDS) products deployed within the internal/client-side network, analyzing their configurations and effectiveness in protecting against malicious activities and intrusions.
4.3.3.1.3. Gather information about the network (i.e., domain user/group information, domain computers, password policy)	vTech will gather comprehensive information about the internal/client-side network, including domain user/group details, domain computers, and password policies, facilitating a deeper understanding of network architecture and potential security vulnerabilities.
4.3.3.1.4. Verify the ability to execute scripts or third-party programs	vTech will verify the ability to execute scripts or third-party programs within the internal/client-side network environments, assessing the potential risk posed by unauthorized or malicious scripts/programs and identifying any security weaknesses related to execution permissions.
4.3.3.2. Mapping and Discovery should include:	
4.3.3.2.1. Identify possible vulnerabilities affecting the provided host	vTech will diligently identify possible vulnerabilities affecting the provided hosts within the internal/client-side network, conducting thorough vulnerability assessments to detect weaknesses and potential entry points for unauthorized access or exploitation by malicious actors.
4.3.3.2.2. Determine the possibility of receiving and executing various malicious payloads	vTech will assess the possibility of receiving and executing various malicious payloads within the internal/client-side network environments, evaluating the security posture against different attack vectors and ensuring robust defenses against potential malware threats.
4.3.3.3. Exploitation should include:	

<p>4.3.3.3.1. Attempt to bypass anti-malware solutions and security restrictions, escape restricted environments, and escalate privileges</p>	<p>vTech will conduct thorough testing to attempt bypassing anti-malware solutions and security restrictions, aiming to identify vulnerabilities that could allow unauthorized privilege escalation or escape from restricted environments, ensuring robust security measures are in place.</p>
<p>4.3.3.3.2. Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)</p>	<p>vTech will exploit discovered vulnerabilities within the internal/client-side network environments to gain additional access or disclose sensitive information, ensuring all weaknesses are thoroughly tested and potential risks are identified for appropriate remediation.</p>
<p>4.3.4. Must identify prioritized remediation needs, requirements, and associated risks.</p>	<p>vTech will prioritize remediation needs based on the severity of identified vulnerabilities, outlining clear requirements and associated risks to guide the Lottery in effectively addressing security weaknesses within the internal/client-side network environments.</p>
<p>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.</p>	<p>vTech will comprehensively assess the security of all networked assets, including servers, endpoints, firewalls, network devices, and monitoring and management systems, ensuring no vulnerabilities are overlooked and the entire network infrastructure is evaluated.</p>
<p>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.</p>	<p>vTech will provide an Executive Summary Report summarizing all testing results, including scope, approach, findings, strengths, and recommendations for senior management, ensuring clear insights into the security posture of the internal/client-side network environments are provided.</p>
<p>4.3.6.1. Vendor shall provide a sample of the executive summary report with their bid response.</p>	<p>vTech will include a sample of the executive summary report with the bid response, offering the Lottery a preview of the reporting format and content to ensure alignment with their expectations and requirements.</p>
<p>4.3.6.2. Report must be submitted to Lottery electronically for review.</p>	<p>vTech will submit the Executive Summary Report electronically to the Lottery for review, ensuring efficient communication and easy access to assessment findings for timely decision-making and remediation planning.</p>
<p>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.</p>	<p>vTech will deliver a detailed Technical Report documenting each discovered vulnerability, categorizing them based on risk severity, and providing comprehensive details on discovery, potential impact, recommendations, and references for further information.</p>
<p>4.3.8. Reports must include specific details for each vulnerability found, including:</p>	
<p>4.3.8.1. How the vulnerability was discovered.</p>	<p>vTech will detail the discovery method for each vulnerability, providing insights into the testing process and techniques used to identify weaknesses within the internal/client-side network environments.</p>
<p>4.3.8.2. The potential impact of its exploitation.</p>	<p>vTech will assess the potential impact of exploiting each vulnerability, highlighting the risks associated with successful exploitation to emphasize the importance of timely remediation and mitigation efforts.</p>
<p>4.3.8.3. Recommendations for remediation.</p>	<p>vTech will provide clear and actionable recommendations for remediating each vulnerability, offering guidance on how to address identified weaknesses effectively to enhance the security posture of the internal/client-side network environments.</p>

<p>4.3.8.4. Vulnerability references.</p>	<p>vTech will include references for each vulnerability found, allowing the Lottery to access additional information or resources for a deeper understanding of the identified security risks and potential mitigation strategies.</p>
<p>4.4. Wireless Penetration Testing</p>	
<p>4.4.1. Wireless Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited.</p>	<p>vTech will conduct Wireless Penetration Testing onsite at all Lottery locations to ensure accurate assessment of wireless networks and associated vulnerabilities, adhering to the requirement to assess locations locally rather than remotely or from a central location, ensuring thorough evaluation of the wireless infrastructure's security posture.</p>
<p>4.4.2. Timeframes, testing schedule, target completion dates and exclusions will be determined in conjunction with the successful vendor.</p>	<p>vTech will collaborate with the Lottery to establish appropriate timeframes, testing schedules, target completion dates, and exclusions, ensuring alignment with project requirements and accommodating any specific needs or constraints identified during the planning phase to facilitate efficient and effective Wireless Penetration Testing.</p>
<p>4.4.3. Must provide a four-phased structure methodology, including reconnaissance, mapping, discovery, and exploitation.</p>	<p>vTech will employ a four-phased methodology for Wireless Penetration Testing, encompassing reconnaissance, mapping, discovery, and exploitation stages to systematically identify and assess vulnerabilities within the wireless network environment, ensuring comprehensive coverage of testing activities and enabling the identification of potential security weaknesses from initial reconnaissance through to exploitation and impact assessment.</p>
<p>4.4.3.1. Reconnaissance should include:</p>	
<p>4.4.3.1.1. Perform WHOIS, ARIN, and DNS (public server) lookups</p>	<p>vTech will conduct WHOIS, ARIN, and DNS lookups to gather relevant information about the wireless network infrastructure, including ownership details, IP address allocations, and domain name information, facilitating the identification of potential attack vectors and informing subsequent testing activities for thorough Wireless Penetration Testing.</p>
<p>4.4.3.1.2. OSINT - Public Searches/Dorks</p>	<p>vTech will leverage Open Source Intelligence (OSINT) techniques, including public searches and dorks, to gather additional information about the wireless network environment, such as publicly available data, vulnerabilities, or configuration details, enhancing reconnaissance efforts and enabling comprehensive assessment of potential security risks within the wireless infrastructure.</p>
<p>4.4.3.1.3. Build custom password lists</p>	<p>vTech will create custom password lists tailored to the wireless network environment, including common or default passwords, known vulnerabilities, or leaked credentials, to facilitate password-based attacks during Wireless Penetration Testing, ensuring comprehensive coverage of potential attack vectors and enabling the identification of weak or compromised authentication mechanisms within the wireless infrastructure.</p>
<p>4.4.3.1.4. DNS lookups (entities server)</p>	<p>vTech will perform DNS lookups on entities' servers to gather information about the wireless network infrastructure, including domain name resolution details, hostnames, and IP address assignments, aiding in the identification of network assets and potential security vulnerabilities within the wireless environment, ensuring thorough reconnaissance and effective testing coverage during Wireless Penetration Testing.</p>
<p>4.4.3.1.5. Gather information from entities web applications</p>	<p>vTech will collect information from entities' web applications, if applicable to the wireless network environment, to identify potential vulnerabilities or misconfigurations that may impact the</p>

	security of the wireless infrastructure, ensuring comprehensive reconnaissance efforts and enabling thorough assessment of web-related attack vectors during Wireless Penetration Testing.
4.4.3.1.6. Analyze metadata	vTech will analyze metadata associated with wireless network assets and communications to extract valuable information about file attributes, timestamps, or document properties, aiding in the identification of potential security risks or data leakage within the wireless environment, ensuring thorough reconnaissance and enabling comprehensive assessment of metadata-related vulnerabilities during Wireless Penetration Testing.
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)	vTech will conduct sniffing activities to establish a baseline of network traffic, capturing Wi-Fi, Bluetooth, Zigbee, and other RF signals to analyze network behavior and identify potential vulnerabilities or security weaknesses within the wireless network infrastructure.
4.4.3.2.2. War Walk (map location of access points and their coverage, identify leakage)	vTech will perform war walking to map the locations of access points and their coverage areas, identifying signal leakage and potential gaps in wireless network coverage to ensure comprehensive wireless network security and address any areas of vulnerability or potential unauthorized access.
4.4.3.2.3. Identify Rogue Access Points* (Friendly, malicious, or unintended access points)	vTech will identify and categorize rogue access points, including friendly, malicious, or unintended ones, to assess the security risks associated with unauthorized access points and take appropriate measures to mitigate potential threats and ensure the integrity and confidentiality of the wireless network
4.4.3.2.4. Full access to the buildings will be granted to the testing team	vTech will be granted full access to the buildings during the wireless penetration testing to ensure thorough assessment of the wireless network infrastructure, enabling the testing team to identify vulnerabilities and security weaknesses effectively and provide comprehensive recommendations for remediation.
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 misconfigurations)	vTech will identify potential points of attack within the wireless network, including WEP networks, capturing WPA/WPA2 PSK key exchanges, and identifying clients vulnerable to evil-twin and Man-in-the-Middle (MiTM) attacks, misconfigurations, or other security weaknesses. This comprehensive approach ensures thorough assessment and mitigation of security risks.
4.4.3.3.3. Vulnerability Scanning (Identify vulnerabilities)	vTech will conduct vulnerability scanning to identify weaknesses and vulnerabilities within the wireless network infrastructure, leveraging both open-source tools and commercial solutions to comprehensively assess the security posture of the network and provide recommendations for remediation to enhance overall security and mitigate potential risks.
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.)	vTech will exploit access points (APs), perform MiTM attacks, and attempt to crack encryption to assess vulnerabilities. Recommendations will be provided based on attack scenarios.
4.4.3.4.2. Client Attacks (Perform Evil-Twin attacks, perform rogue AP attacks, MiTM, etc.)	vTech will execute client-side attacks like Evil-Twin and rogue AP attacks to assess device vulnerabilities. Remediation recommendations will be provided.
4.4.3.4.3. Denial of Service where applicable and with prior Lottery approval	With Lottery approval, vTech will test network resilience against DoS attacks, adhering to ethical standards. Disruptions will be minimized.

4.4.3.4.4. Bluetooth/Zigbee/SDR Attacks where applicable and with prior Lottery approval	vTech will perform attacks on other wireless technologies with Lottery approval, identifying vulnerabilities and suggesting remedies.
4.4.4. Must identify prioritized remediation needs, requirements, and associated risks.	vTech will prioritize remediation based on findings, outlining requirements to address vulnerabilities effectively.
4.4.5. Testing shall assess the security of all wireless assets.	vTech will comprehensively evaluate all wireless components for vulnerabilities, including access points and client devices. Recommendations will aim to enhance overall wireless security.
4.4.8. Reports must include specific details for each vulnerability found, including:	
4.4.8.1. How the vulnerability was discovered.	vTech will detail the methodology used to uncover each vulnerability, providing insights into the testing process.
4.4.8.2. The potential impact of its exploitation.	For each vulnerability, vTech will outline the potential consequences if exploited, including data breaches, service disruptions, and other security risks.
4.4.8.3. Recommendations for remediation.	vTech will offer actionable recommendations to mitigate identified vulnerabilities effectively, tailored to the Lottery's environment and security needs.
4.4.8.4. Vulnerability references.	Each vulnerability will be referenced with industry-standard identifiers and references for further investigation and understanding.
4.4.8.5. The vendor shall provide a sample of the technical report with their bid response.	A sample technical report showcasing vTech's reporting style and depth will be included with the bid response, offering insight into the thoroughness and clarity of the final deliverable.
4.4.8.6. The report must be submitted to the Lottery electronically for review.	The comprehensive technical report will be submitted electronically to facilitate efficient review by Lottery stakeholders, ensuring timely access to critical security findings and recommendations.
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.	vTech will deliver a comprehensive findings presentation to the Lottery management team, highlighting strengths, weaknesses, and vulnerabilities identified during 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.	The presentation format, whether in person or via conference call, will be determined by Lottery preferences, ensuring effective communication and understanding of assessment results.

5.0 Exhibit A – Pricing Page

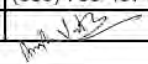
EXHIBIT A - Pricing Page					
Item #	Section	Description of Service	*Estimated Number of Assessments*	Unit Cost per Assessment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	\$ 42,570.00 -	\$ 340,560.00 -
2	4.2	Website Penetration Testing	8	\$ 12,500.00 -	\$ 100,000.00 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$ 18,920.00 -	\$ 151,360.00 -
4	4.4	Wireless Penetration Testing	8	\$ 14,770.00 -	\$ 118,160.00 -
TOTAL BID AMOUNT					\$ 710,080.00 -

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:	vTech Solution, Inc
Vendor Address:	1100 H Street NW Suite 750 Washington DC 20005
Email Address:	rfp.vtech@vtechsolution.com
Phone Number:	(202) 644-9774
Fax Number:	(866) 733-4974
Signature and Date:	 3/25/2024

6.0 Appendix: Forms

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) Anisha Vataliya

(Address) 1100 H Street NW Suite 750 Washington DC 20005

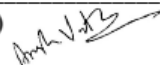
(Phone Number) / (Fax Number) Phone Number: (202) 644-9774 | Fax: (866) 733-4974

(email address) rfp.vtech@vtechsolution.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through vOASIS, 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.

vTech Solution, Inc

(Company) 

(Signature of Authorized Representative)
Anisha Vataliya, President

(Printed Name and Title of Authorized Representative) (Date)
Phone Number: (202) 644-9774 | Fax: (866) 733-4974

(Phone Number) (Fax Number)
rfp.vtech@vtechsolution.com

(Email Address)

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: Kartik Hirpara
Telephone Number: 202 644 9774 x 133
Fax Number: (866) 733-4974
Email Address: kartik.h@vtechsolution.com

