



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 2

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

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: VS0000045323 


Legal Name: Rapid Strategy, Inc

Alias/DBA: Rapid Strategy

Total Bid: \$226,912.00

Response Date: 03/28/2024 

Response Time: 8:34

Responded By User ID: rmeeting 

First Name: Ron

Last Name: Meeting

Email: meetingr@rapidstrategy.io

Phone: 9802240346

SO Doc Code: CRFQ

SO Dept: 0705

SO Doc ID: LOT2400000009

Published Date: 3/21/24

Close Date: 3/28/24

Close Time: 13:30

Status: Closed

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Total of Header Attachments: 2

Total of All Attachments: 2

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				36432.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: This line item outlines Item 1 Section 4.1 External Network Penetration Testing

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				55752.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: This line item outlines Item 2 Section 4.2 Website Penetration Testing

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				116952.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: This line item outlines Item 3 Section 4.3 Internal/Client-Side Network Penetration Testing

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				17776.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: This line item outlines Item 4 Section 4.4 Wireless Penetration Testing

Extended Description:

See Attached Specifications and Exhibit - A Pricing Page



**A
PROPOSAL RESPONSE
TO
REQUEST FOR QUOTATION FOR
NETWORK PENETRATION TESTING AND CYBERSECURITY
ASSESSMENTS
WEST VIRGINIA LOTTERY**



A Proposal Prepared By:
Rapid Strategy

Ron Meeting
Chief Executive Officer
9910 Ainslie Downs Street Charlotte, NC 28273
United States

Tel: +(980) 224-0346
Email: meetingr@rapidstrategy.io
Proposal validity: 120 days from due date

**A
PROPOSAL RESPONSE
TO
REQUEST FOR QUOTATION FOR NETWORK PENETRATION
TESTING AND CYBERSECURITY ASSESSMENTS
WEST VIRGINIA LOTTERY**



Due date: 28th, March 2024

Technical Proposal

Submitted to:
Brandon L. Barr
Contracting Officer

Department of Administration,
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

Submitted by:
Ron Meeting
Chief Executive Officer (CEO)
Rapid Strategy

9910 Ainslie Downs Street Charlotte,
Nc 28273
www.rapidstrategy.io
Email: meetingr@rapidstrategy.io
Phone: +(980) 224-0346

COVER LETTER

Rapid Strategy

9910 Ainslie Downs Street
Charlotte, NC 28273
United States

Friday, 22nd March 2024

Brandon L. Barr Contracting Officer

Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

Email: brandon.l.barr@wv.gov

RE: PROPOSAL RESPONSE TO THE STATE OF WEST VIRGINIA'S REQUEST FOR PROPALS FOR NETWORK PENETRATION TESTING AND CYBERSECURITY ASSESSMENTS - CRFQ 0705 LOT2400000009

Dear Brandon,

We are pleased to submit our proposal in response to the State of Virginia's Request for bids for Network Penetration Testing and Cybersecurity Assessments - Solicitation No CRFQ 0705 LOT2400000009.

We have carefully reviewed the requirements outlined in Solicitation No CRFQ 0705 LOT2400000009, and we firmly believe that our expertise and experience make us the ideal partner for this essential project.

We are a leading cybersecurity firm with a proven track record of delivering complex and multifaceted cybersecurity solutions to organizations across various sectors, such as the Small Business Administration, Federal Reserve Board, the Federal Trade Commission, ePlus Technology, Guidehouse, and PricewaterhouseCoopers. We were awarded the 2023 Charlotte's Best Small IT/Services Business, Fannie Mae's CIO Diverse Supplier Selection program, and were nominated by the NC Tech Association for one of the best providers of cyber solutions.

Rapid Strategy is an award-winning and certified HUB Zone minority-owned small business headquartered in Charlotte, North Carolina with satellite locations in the DMV area. We specialize in delivering innovative cybersecurity solutions for both public and private sector clients.

We have successfully executed Penetrating test across Internal, External, Web applications testing, Wireless, Red Team, Blue Team, and Purple Team (on site and remotely). These exercises were carried out across all tests black box, grey box, white box, social engineering through phishing and vishing. We have **successfully completed 52 penetration testing exercises** with clients across the federal government, state and local government, education, financial services, and healthcare giving us a unique capability with a blend of innovative techniques bad actors and state sponsored adversaries are using to compromise critical infrastructure and systems.

We proudly hold a position on the GSA MAS (Contract #47 QTCA23D0027) Vehicle for Highly Adaptive Cybersecurity Services, IT Professional Services, and Cloud Computing Professional Services, allowing us to offer state-of-the-art cybersecurity and IT support to federal agencies effortlessly.

We confirm our capability and willingness to carry out the commitments contained in this proposal. If you have any questions about our technical proposal response, please contact Ron Meeting, the CEO of Rapid Strategy. He can be reached at +(980) 224-0346, or via email at Meetingr@rapidstrategy.io.

Sincerely,



Ron Meeting
Chief Executive Officer
Rapid Strategy



Ron Meeting

Chief Executive Officer (CEO)
and Co-Founder of Rapid Strategy

A seasoned cyber professional and industry leader with nearly 20 years of experience in financial services and the federal government.

TABLE OF CONTENT

COVER LETTER	3
TABLE OF CONTENT.....	5
OUR UNDERSTANDING OF WEST VIRGINIA LOTTERY - CRFQ 0705 LOT2400000009	6
1. STATEMENT OF QUALIFICATIONS	7
2. BRIEF DESCRIPTION OF THE COMPANY	9
2.1. Principal Contact Details	9
2.2. Company Profile and Background.....	9
2.3. Our Strategic Partnership with ePlus technology.....	11
2.4. Offeror Litigation statement.....	11
2.5. Compliance to Confidentiality	11
3. MEET OUR TEAM.....	12
3.1. Project Governance	12
3.1.1. Project Manager	12
3.1.2. Project Management Office.....	12
3.1.3. Project Team	13
3.2. Meet Rapid Strategy’s - Management	15
4. APPROACH AND SCOPE OF WORK	16
4.1. Our Approach to scope of work.....	16
4.1.1. External Network Penetration Testing.....	16
4.1.2. Website Penetration Testing.....	17
4.1.3. Internal/Client-Side Network Penetration Testing	18
4.1.4. Wireless Penetration Testing.....	19
4.2. Penetrating testing stages	20
4.3. Schedules.....	21
5. PAST PERFORMANCE ON SIMILAR & SUCCESSFUL PROJECTS.....	23
6. TERMS AND CONDITIONS	26
7. NEXT STEPS.....	28
Appendix	29
Resumes, and Certificates	
Exhibit B - Non-Disclosure Agreement [signed -NDA]	

OUR UNDERSTANDING OF WEST VIRGINIA LOTTERY - CRFQ 0705 LOT2400000009.

We understand that West Virginia plan to lunch an award a contract limited to three (3) successive one (1) year period or multiple renewal periods less than one year. Further to that, West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery (Lottery) to establish a contract to perform and deliver information technology cybersecurity assessments, including external network, website, wireless, and internal/client-side penetration testing assessments. These assessments must follow the Center for Internet Security (CIS) methodology and employ techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide.

We understand that West Virginia Lottery operates technology assets in eight (8) locations:

- Main Office – 900 Pennsylvania Ave, Charleston, WV 25302
- Bridgeport – 64 Sterling Drive, Bridgeport, WV 26330
- Weirton – 100 Municipal Plaza Bldg. 34, Weirton, WV 26330
- Greenbrier – 101 W. Main Street, White Sulphur Springs, WV 24986
- Hollywood – 750 Hollywood Drive, Charles Town, WV 25414
- Mardi Gras – 1 Greyhound Drive, Cross Lanes, WV 25313
- Mountaineer – 1420 Mountaineer Circle, New Cumberland, WV 26047
- Wheeling Island – 1 Stone Street, Wheeling, WV 26003

Deliverables: We understand that we are required to perform the below listed tasks:

- Website Penetration Testing
- External Network Penetration Testing
- Internal/Client-Side Network Penetration Testing
- Wireless Penetration Testing

As per the terms of the Mission, we are to provide a detailed report that will include vulnerabilities that were discovered, an assessment of the potential impact if the vulnerability is exploited, recommendations for remediation, and references to the vulnerabilities. Additionally, the technical report must be submitted to the West Virginia Lottery electronically. Furthermore, the findings presentation should be delivered to the West Virginia Lottery, either in person or via a conference call, based on the Lottery's decision upon project completion.

1. STATEMENT OF QUALIFICATIONS

We hereby confirm that we, Rapid Strategy, have thoroughly reviewed solicitation No CRFQ 0705 LOT2400000009 and all relevant documents released.

At Rapid Strategy, we are committed to delivering exceptional results ensuring strict adherence to the outlined scope of work without any deviations. Our team is dedicated to upholding the highest standards of professionalism including background checks, confidentiality, and random alcohol testing. As well, we will provide expertise that meets specific requirements of this project.

In addition, Rapid Strategy confirms to meet the minimum of Solicitation No CRFQ 0705 LOT2400000009:

Meeting the Minimum Requirements

We confirm to match the minimum requirements within Solicitation No CRFQ 0705 LOT2400000009, notably:

Certified Minority-Owned Small Business: We are a certified HUBZone minority-owned small business headquartered in Charlotte, North Carolina with satellite locations in the DMV area. We have a diverse workforce, and we strongly promote diversity and inclusiveness in our work culture.

Methodology and Compliance: Our approach aligns with the Center for Internet Security methodology, incorporating techniques and guidelines from reputable sources such as the Penetration Testing Execution Standards (**PTES**), Open Source Security Testing Methodology Manual (**OSSTMM**), Open Web Application Security Project (**OWASP**) Top 10 Project, and the NIST SP 800-115 Information Security Testing and Assessment technical guide.

Proven Track Record: We have successfully completed more than twenty penetration testing exercises similar projects in scope, scale, and complexity, underlining our expertise in delivering high-quality assessments. In accordance with the requirements of Solicitation No CRFQ 0705 LOT2400000009, we have provided three (3) references for projects of similar or greater size and scope, attesting to our capability and reliability.

Expert Project Lead and Team: Claude Bird, our proposed project lead/Contract Manager, brings 15 years of invaluable experience in cybersecurity consulting, holding both **PMP** and **CISSP** certifications. Furthermore, our project team members hold a range of certifications including Certified Penetration Testing Engineer (**CPTE**), Certified Information Systems Security Professional (**CISSP**), Certified Ethical Hacker (**CEH**), Certified Expert Penetration Tester (**CEPT**), Certified Wireless Security Professional (**CWSP**), and Certified Mobile and Web Application Penetration Tester (**CMWAPT**), demonstrating our commitment to maintaining the highest standards of expertise and proficiency.

We believe that our synergy of talent and experience proposed for this engagement brings unparalleled solutions with regards to Network Penetration Testing and Cybersecurity Assessments. Please find attached to the proposal as an annex the resumes of our staff with their respective certifications who have been assigned to this engagement.

Regular Check-ins with West Virginia Lottery or the designated Contracting officer: In our approach, we will work closely with project leadership and representatives from West Virginia Lottery to generate hypotheses, review the schedules, and valid the time lines to ensure the practicality of audit results and opportunities identified. Particularly given the quick timeline and breadth of areas covered in this scope of work, we believe that a strong governance process composed of steering committees toward the end of each phase should help to set priorities for where to focus on the following phase and in the creation of the Final Report. We will also have daily check-ins with the project team that will be critical to ensure alignment and removal of any barriers to progress.

2. BRIEF DESCRIPTION OF THE COMPANY

Rapid Strategy brings perspectives on best practices and approaches to Network Penetrating testing and Cybersecurity across the globe. Our 30 years' experience and our diverse skill set spans five core pillars: Cyber Strategy and Advisory, Cybersecurity Assessments, Technology Architecture and Implementation, Cloud Security, and Strategic Enablement.

2.1. Principal Contact Details

Name Ron Meeting
Address 9910 Ainslie Downs Street Charlotte, NC 28273
Telephone +(980) 224-0346
Email Meetingr@rapidstrategy.io
Web www.rapidstrategy.io

2.2. Company Profile and Background

Rapid Strategy is an award-winning and certified HUBZone minority-owned small business headquartered in Charlotte, North Carolina with satellite locations in the DMV area. With over 30 years of invaluable experience in the cybersecurity sector, we specialize in delivering innovative cybersecurity solutions for both public and private sector clients. As a certified member of the National Minority Supplier Development Council, we focus on providing cyber risk capabilities to help clients with our core competencies.

We have assisted federal government agencies in achieving and maintaining regulatory compliance, such as NIST, HIPAA, FISMA, and FedRAMP. Our compliance experts have extensive knowledge of relevant standards and regulations, and we provide guidance and support in implementing controls and processes to meet compliance requirements. We conduct regular assessments and audits to ensure ongoing compliance and address any identified gaps or vulnerabilities.

Five Core Pillars of Competencies

- Cyber Strategy and Advisory
- Cybersecurity Assessments
- Technology Architecture and Implementation
- Cloud Security
- Strategic Enablement

We proudly hold a position on the GSA MAS (**Contract #47 QTCA23D0027**) Vehicle for Highly Adaptive Cybersecurity Services, IT Professional Services, and Cloud Computing, allowing us to offer state-of-the-art cybersecurity and IT support to federal agencies effortlessly.



Our commitment to serving and supporting our partners effectively as a leading provider of cutting-edge cybersecurity and IT solutions is unparalleled.

Diversity

Our team brings a diverse array of backgrounds, perspectives, and languages, allowing us to break down barriers and communicate effectively in English, Spanish, or technical language. We ensure ease of interaction and collaboration, providing meaningful communication tailored to your needs.

Industry Certifications

Our team holds the following industry certifications:

- EC-Council Certified Chief Information Security Officer (CCISO)
- Certified Information Systems Security Professional (CISSP)
- ISACA Certified Information Security Manager (CISM)
- ISC2 Certified Cloud Security Professional (CCSP)
- Project Management Professional (PMP)
- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Certified Computer Network Defense Architect (CNDA)
- Microsoft Certified Azure Administrator
- CompTIA Security+

NAICS Codes

- 541512 - Computer Systems Design Services
- 541519 - Other Computer Related Services
- 518210 - Data Processing, Hosting & Related Services
- 519190 - All Other Information Services
- 541330 - Engineering Services
- 541690 - Other Scientific & Technical & Consulting

2.3. Our Strategic Partnership with ePlus Technology

Our unparalleled expertise has been refined with the strategic partnership we have with ePlus Technology with performed twelve penetration tests as a premier partner across state and local agency government, education, financial services, and healthcare. From Cloud and Data Center, Security, Collaboration, Networking and AI, to Digital Transformation, Managed and Professional Services or Financing, we bring a vast perspective that helps organizations design, orchestrate and seamlessly implement versatile technology solutions.

2.4. Offeror Litigation statement

Rapid Strategy confirm that it is not and has not been a party to any litigation in the last 5 years where it was alleged that Rapid Strategy breached a contract with a client/customer.

Rapid Strategy confirms that no government entity has debarred or otherwise prohibited Rapid Strategy from responding to its competitive solicitations within the last 5 years.

2.5. Compliance to Confidentiality

Rapid Strategy has thoroughly reviewed State of West Virginia's Statutes regarding the confidentiality Policies and Information Security Accountability Requirements, set forth in www.state.wv.us/admin/purchase/privacy.

We have enclosed to this proposal Exhibit B – Non-Disclosure Agreement (NDA) form completed and signed by the authorized personnel of Rapid Strategy.

3. MEET OUR TEAM

Our proposed team for the consulting mission - Network Penetration Testing and Cybersecurity Assessments will be a full and collaborative partner to the west Virginia lottery.

Rapid Strategy has assembled a multi-disciplinary team of professionals who have successfully provided similar Network Penetration Testing and Cybersecurity Assessments. Our professionals understand West Virginia's needs. Furthermore, these individuals understand and master the Cybersecurity assessments, and penetrating testing best practices.

We will work with West Virginia Lottery to achieve substantial, lasting results in the performance of this project. To deliver the right expertise to the needs of the project, we select the right people and the right team configuration for the unique problem.

We think of our teams as a collaborative and flexible resource that together creates the synergy required to deliver a unique solution to your problem. On this project, we would be including.

3.1. Project Governance

3.1.1. Project Manager

The overall client relationship will be overseen by **Claude Bird**. He will serve as the overall Director of Client Service and Project Manager for the West Virginia lottery. He will ensure the team is engaging with the right stakeholders in carrying out the Consulting mission. He will participate in executive leadership meetings with West Virginia Lottery team, provide ongoing guidance and direction, lead problem-solving with the team, draft documents, review analytics, and oversee the overall quality of deliverables.

3.1.2. Project Management Office

Rapid Strategy will utilize the Program Management Office (PMO) structure recommended by the PMBOK Guide to ensure that clearly defined goals, objectives and performance standards are mutually understood and agreed to. If there is no PMO, then Rapid Strategy will suggest a standard cadence of meetings, change management processes, approval gates, and metrics to be tracked and monitored.

3.1.3. Project Team

To provide the West Virginia Lottery with a clear picture of the level of support, experience, and caliber of staff it will receive for this effort, we have included the full list consultants assigned to the project:

Exhibit 3.2. Project team

Name/title	Key Qualifications
<p>Claude Bird Technical Project Manager</p>	<p>Claude brings over 15 years in cybersecurity consulting, specializing in assessing operational risks for assessor organizations. With a background as a Navy veteran, Claude brings a wealth of discipline and a strategic mindset to our team. His credentials include a Master’s Certificate in Penetration Testing & Ethical Hacking from the SANS Technology Institute, as well as a Bachelor of Science in Computer Information Systems from Stevenson University. Furthermore, Claude holds a range of industry-recognized certifications including PMP, CISSP, and CompTIA Security+, solidifying his status as a highly qualified and capable professional in the field.</p>
<p>Thomas Gilbert Senior Penetration Tester (Infrastructure)</p>	<p>Thomas, a cybersecurity consultant with over 10 years of experience, has a proven track record of delivering Security Testing services, including Penetration Testing and Ethical Hacking, across a wide range of enterprise-level assets, applications, systems, and software. He is equipped with a Bachelor of Science in Criminal Justice and has completed a Cyber Security Bootcamp at Indiana Wesleyan University. Additionally, Thomas holds several certifications, including CompTIA CNSP, CompTIA CySA+, CompTIA CNVP, CompTIA PenTest+, CompTIA Security+, and AWS Certified Cloud Practitioner.</p>
<p>Alec Romano Penetration Tester (WebApplication)</p>	<p>Alec, is a seasoned cybersecurity professional with 10+ years of experience across various domains within the cybersecurity industry. His proficiencies include DevOps, penetration testing, and red team assessments. Alec is academically distinguished, holding a Master’s Certificate in Penetration Testing & Ethical Hacking from the SANS Technology Institute (2019), and a Bachelor of Science in Computer Information Systems from Stevenson University (2017). Alec is fortified with an array of certifications, including the GIAC Penetration Tester (GPEN), GIAC Cloud Penetration Tester (GCPN), GIAC Certified Web Application Penetration Tester (GWAPT), GIAC Python Coder</p>

	(GPYC), GIAC Certified Incident Handler (GCIH), and CompTIA Security+
Mekhi Rhodie Junior Penetration Tester (Wireless)	Mekhi is a skilled penetration tester and web developer with expertise in identifying and addressing security vulnerabilities. Holding certifications in CompTIA Security+ (SY0-601) , and CompTIA CySA+ (CS0-002) , Mekhi is well-equipped to bolster your organization's security posture and ensure the integrity of your systems.

We recognize the importance of keeping up to date with the latest industry trends and developments in security policy development. To ensure our team's knowledge remains current, we regularly send our employees to attend: training opportunities, industry conferences, review whitepapers, and participate in speaking engagements. This enables our team to provide the most relevant and effective security policies and procedures to our clients.

3.2. Meet Rapid Strategy's - Management



Ron Meeting

Chief Executive Officer (CEO) and Co-Founder of Rapid Strategy

A seasoned cyber professional and industry leader with nearly 20 years of experience in financial services and the federal government.



Jesse Rhee

Chief Operating Officer (COO) and Co-Founder of Rapid Strategy.

Jesse comes from Fortune 100 companies specializing in IT management and solution delivery across the healthcare, finance, and defense space.

4. APPROACH AND SCOPE OF WORK

We will perform the Network Penetration Testing and Cybersecurity Assessments within the assets operated within the eight (8) locations of the West Virginia Lottery.

Our proposal is designed to meticulously address prioritized remediation needs, requirements, and associated risks in line with the scope of work of this engagement.

4.1. Our Approach to scope of work

4.1.1. External Network Penetration Testing

We will target the external-facing aspects of your network, focusing on a specified number of IP addresses associated with your organization. We employ a systematic approach to detect any security flaws, potential entry points for attackers, and areas of weakness within your network's perimeter. This process will be based on the four-phased assessment employing techniques and guidelines from the NIST SP 800-115 Information Security Testing and Assessment technical guide includes a detailed analysis of externally accessible IP addresses and the scrutiny of network endpoints at various organizational facilities. Our methodology ensures that all access points are adequately safeguarded, particularly emphasizing the importance of secure VPN connections for remote access.

Tools	External Network Penetration Testing
Nessus	Network discovery and vulnerability assessment tool by Tenable.
Netsparker	Web Application Vulnerability assessment tool.
Metasploit	Open-Source exploitation framework to compile and execute exploit code.
BurpSuite Pro	Web Application proxy and exploitation utility.
NMAP	Open-source utility for network exploration and security auditing.
Infection Monkey	Lateral movement across the AWS infrastructure.
Additional tools	Various other open source and commercial tools are utilized during testing according to the technology in use in the environment.

4.1.2. Website Penetration Testing

We undertake a focused security evaluation of critical web applications within your organization. This assessment is aimed at identifying vulnerabilities within application components and subsystems, with a special emphasis on areas critical to maintaining robust security, such as user authentication, access control, and data protection mechanisms. Our team rigorously tests for prevalent web application vulnerabilities, including SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF), following best practices outlined in both the Open Web Application Security Project (OWASP) Top 10 and MITRE ATT@CK sophisticated attack vectors.

Tools	Website Penetration Testing
Nessus	Network discovery and vulnerability assessment tool by Tenable.
Netsparker	Web Application Vulnerability assessment tool.
Metasploit	Open-Source exploitation framework to compile and executive exploit code.
BurpSuite Pro	Web Application proxy and exploitation utility.
Open Source	In addition to commercial products, Rapid Strategy may leverage open-source tools including Cain & Able, NMAP, Nikto/Wikto, Superscan, SSL Digger, MS Baseline Security Analyzer (MBSA) and Center for Internet Security (CIS) Benchmarks.

Our assessments will strictly adhere to the Center for Internet Security methodology and incorporate techniques and guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide.

4.1.3. Internal/Client-Side Network Penetration Testing

Leveraging iterative, four phased assessment employing techniques and guidelines from the NIST SP 800-115 Information Security Testing and Assessment technical guide, comprising activities to identify vulnerabilities at each operational layer of the target network. This includes two-part testing to assess the security of all networked assets, including but not limited to servers, desktops, firewalls, other network devices, and network monitoring & management. By applying methodologies aligned with NIST guidelines for human aspects of security, this assessment identifies potential vulnerabilities within your West Virginia’s Lottery's network 's social fabric, aiming to enhance the overall security culture and reduce the risk of information breaches through human error.

Tools	Internal/Client-Side Network Penetration Testing
Nessus	Network discovery and vulnerability assessment tool by Tenable.
Netsparker	Web Application Vulnerability assessment tool.
Metasploit	Open-Source exploitation framework to compile and execute exploit code.
BurpSuite Pro	Web Application proxy and exploitation utility.
NMAP	Open-source utility for network exploration and security auditing.
Infection Monkey	Lateral movement across the AWS infrastructure.
Additional tools	Various other open source and commercial tools are utilized during testing according to the technology in use in the environment.

4.1.4. Wireless Penetration Testing

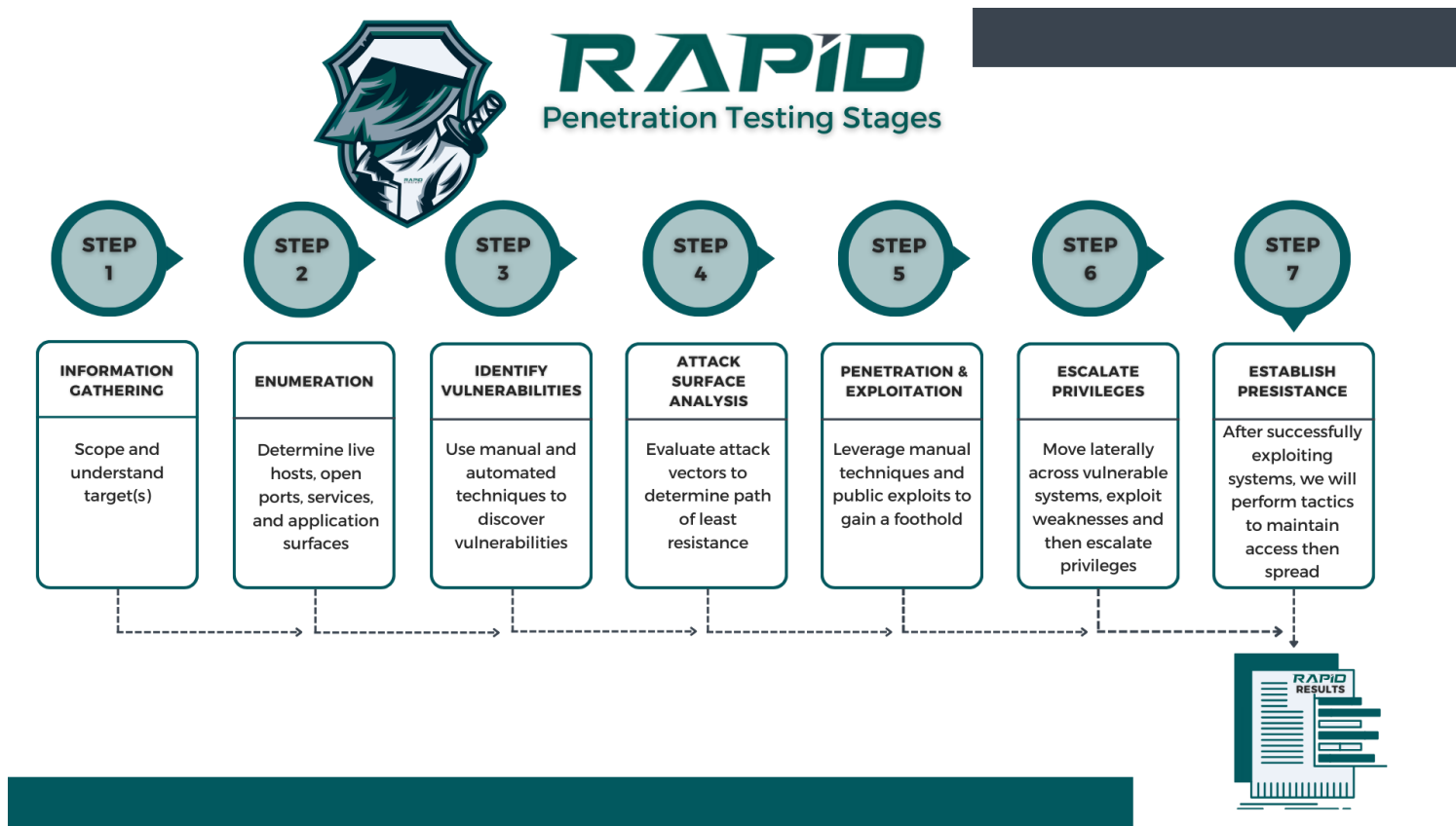
In performing the Penetrating Testing, we propose a complete assessment of the security of all wireless assets to ensure a thorough understanding of potential vulnerabilities.

Our wireless Penetrating Testing service is designed to assess the security of your wireless network infrastructure. We will conduct wireless penetrating testing onsite at all lottery locations. By examining the strength and implementation of encryption protocols, authentication procedures, and overall network security configurations, we aim to uncover any vulnerabilities that could be exploited by malicious actors. This assessment adheres to NIST recommendations for wireless security, focusing on identifying and mitigating risks associated with wireless networking to prevent unauthorized access and ensure the confidentiality and integrity of transmitted data.

4.2. Penetrating Testing Stages

As shown in Exhibit 4.1.2, our entire penetrating testing process is inclusive and offers the best in-market solution. Our Solution incorporates – testing tools capable of performing WHOIS, ARIN, and DNS (public server) lookups, OSINT - Public Searches/Dorks, DNS lookups (entities server), HTTP Options Discovery (Identify accepted HTTP methods), and etc.

Exhibit 4.1.2: Penetrating testing phases.



4.3. Schedules

Our project management approach is structured on the PMBOK, which defines five phases to the project management process: Initiating and Planning, Executing, Monitoring and Controlling, and Closure and Review.

We will utilize our project management expertise to ensure that every task is completed on time and within budget. The project milestone will be within 09 months.

Exhibit 4.3: Proposed Monthly schedule – CRFQ LOT2400000009

Task	Description	External Network Penetration Testing	Website Penetration Testing	Internal/Client-Side Network Penetration Testing	Wireless Penetration Testing
Pre-Assessment Preparation	Establish communication with the client to determine testing schedule, timeframes, and target completion dates. Define exclusions in conjunction with the client to align with the scope of work.	Week 1	Week 1	Week 1	Week 1
Reconnaissance	Perform WHOIS, ARIN, and DNS lookups. Conduct OSINT and public searches/dorks. Build custom password lists. Conduct DNS lookups and gather information from network resources. Analyze metadata.	Weeks 2 & 3	Weeks 2 & 3	Weeks 2 & 3	Weeks 2 & 3
Mapping and Discovery	Perform network discovery including ICMP sweeps, traceroutes, and bypass firewall restrictions. Conduct port/protocol scanning to identify open TCP/UDP ports. Identify underlying OS and software versions.	Weeks 2 & 3	Weeks 2 & 3	Weeks 2 & 3	Weeks 2 & 3
Vulnerability Scanning and Exploitation	Perform vulnerability scanning. Conduct brute force logins and exploitation based on discovered vulnerabilities. Post-exploitation and pivot to assess the impact on the system.	Weeks 2, 3 & 4	Weeks 2, 3 & 4	Weeks 2, 3 & 4	Weeks 2, 3 & 4

Reporting and Presentation	Prepare Executive Summary Report for senior management. Compile a Technical Report detailing each vulnerability type discovered. Conduct a Findings Presentation to the client's management team.	Week 4	Week 4	Week 4	Week 4
----------------------------	---	--------	--------	--------	--------

We excel in managing service level agreements (SLAs) to ensure the highest levels of service quality and customer satisfaction. Using dedicated SLA management modules within our ITSM tools, we define and negotiate SLA metrics and targets, monitor and report on performance, and conduct regular service reviews. Our deliverables encompass well-defined SLA frameworks, SLA agreements, SLA performance reports, service review meeting minutes, and improvement plans.

5. PAST PERFORMANCE ON SIMILAR & SUCCESSFUL PROJECTS

Detailed below are summaries of past Similar & Successful Projects, and Customer References.

Exhibit 5.1. ePlus Engagement- As the dedicated cybersecurity services provider for ePlus Technology. ePlus Technology is an established giant in the technology solutions sector, celebrated for its holistic offerings that cater to the multifaceted needs of contemporary businesses. As a publicly traded entity on NASDAQ (PLUS), ePlus's financial strength and market leadership are clear indicators of its capacity to invest in and drive forward the latest technological innovations and solutions. With a remarkable achievement in 2023, ePlus generated annual revenue of \$2.16 billion, highlighting its financial strength and dominant position in the market. This fiscal robustness allows ePlus to continually invest in cutting-edge technologies and pioneering solutions, making it the partner of choice for Rapid Strategy.

Offeror/Business Name	ePlus Technology
Offeror DUNS#	
Customer Name	Dease Moore
Contract Number	
(Either PRIME or Subcontractor)	Sub-contractor
Period of Performance	Jan 2023 – Present
Contract Award Amount	\$ 900k
Scope/Description of Services	Rapid Strategy successfully conducted internal/external penetration tests for clients in the healthcare, technology, and higher education spaces. We made use of tools such as Nessus, Netsparker, Metasploit BurpSuite Pro, and NMAP, which offer cutting edge External and Internal penetrating testing solutions. Our certified ethical hackers simulate real-world attack scenarios to identify weaknesses and potential entry points. Through comprehensive testing and analysis, we provide actionable recommendations to fortify defenses and improve overall security.
Key Deliverables	Enterprise penetration testing reports, weekly status reports, threat reports, security assessment reports

References:

Title	Name	Telephone	email
Contracting Officer	Dease Moore		DeMoore@eplus.com
Contracting Officer Technical Representative			
Program Manager			

Exhibit 5.2: Federal Trade Commission (FTC) - penetration testing, vulnerability assessments, and FISMA audit services.

Offeror/Business Name	RMA Associates
Offeror DUNS#	DNWVTJLMP5N3
Customer Name	Federal Trade Commission (FTC)
Contract Number	GS-23F-016AA/ FTC-0914-21-CA-0003
(Either PRIME or Subcontractor)	Subcontractor
Period of Performance	12/2021 - Present
Contract Award Amount	\$1000,000
Scope/Description of Services	Our work with the FTC entailed providing comprehensive penetration testing, vulnerability assessments, and FISMA audit services.
Key Deliverables	Our skilled team conducted rigorous penetration tests, identifying vulnerabilities in FTC OIG's information systems, while our vulnerability assessments evaluated the effectiveness of existing security controls. We delivered detailed reports with prioritized recommendations for remediation, empowering FTC OIG to enhance their cybersecurity posture. Our expertise, professionalism, and dedication were commended by the client, ensuring their satisfaction and continued trust in our services.

References:

Title	Name	Telephone	email
Contracting Officer	Jeff McGowan		j.mcgowan@rmafed.com
Contracting Officer Technical Representative			
Program Manager	Jeremy Goucher		j.goucher@rmafed.com

Exhibit 5.3. PwC Engagement- Conducted NIST CSF and data privacy maturity assessment.

Offeror/Business Name	PWC
Offeror DUNS#	
Customer Name	
Contract Number	
(Either PRIME or Subcontractor)	Sub-contractor
Period of Performance	Jan 2022 – Jan 2023
Contract Award Amount	\$ 250k
Scope/Description of Services	We conducted a NIST CSF and data privacy maturity assessment for PwC. Our methodology involved a gap analysis, review of existing policies, and alignment with the latest privacy regulations.
Key Deliverables	The outcomes included enhanced data governance and strengthened compliance posture, leading to positive feedback on our strategic insights and actionable recommendations.

References:

Title	Name	Telephone	email
Contracting Officer	Kevin Simmonds	90442.47261	Kevin.simmonds@pwc.com
Contracting Officer Technical Representative			
Program Manager			

6. TERMS AND CONDITIONS

Certifications and Licenses

Rapid Strategy will provide copies of all certifications and resumes of key staff assigned to the project.

Validity of the proposal

This proposal is valid for acceptance for 120 days from the date of submission, except if a contract is signed between both parties before the expiration of the proposal. The validity of 120 days includes the terms and conditions herein, pricing, and delivery conditions stated in the terms and conditions.

Confidentiality

Rapid Strategy agrees that any confidential Information received from the other party shall be used only for this Contract. The Confidential Information may be disclosed to our respective employees involved in the Project. These restrictions will not apply to any information which:

- (a) is or becomes generally available to the public other than because of a breach of an obligation under this clause;
- or (b) is acquired from a third party who owes no obligation of confidence to the disclosing party in respect of the information;
- or (c) is or has been independently developed by the recipient without recourse to the Confidential Information of the other party;
- or (d) the recipient can show was known to it before receipt.

Insurance

Rapid Strategy confirms to have procured insurance policy number ESM0239815442, which matches the requirements outlined in solicitation No CRFQ LOT2400000009. The insurance policy is enclosed to the proposal.



CERTIFICATE OF LIABILITY INSURANCE

DATE (MMDD/YYYY)
03/08/2024

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.		
IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).		
PRODUCER USAA INSURANCE AGENCY INC/PHS 65812845 The Hartford Business Service Center 3600 Wiseman Blvd San Antonio, TX 78251	CONTACT NAME: PHONE (A/C, No, Ext): (866) 467-8730 FAX (A/C, No): E-MAIL ADDRESS: INSURER(S) AFFORDING COVERAGE NAIC#	
INSURED Rapid Strategy, Inc 3123 N DAVIDSON ST STE 210 CHARLOTTE NC 28205-1162	INSURER A: Nutmeg Insurance Company 39608 INSURER B: Lloyds, Underwriters at Lloyds 15792 INSURER C: INSURER D: INSURER E: INSURER F:	

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MMDD/YYYY)	POLICY EXP (MMDD/Y YYY)	LIMITS
B	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC <input type="checkbox"/> OTHER:			ESM0239815442	11/22/2023	11/22/2024	EACH OCCURRENCE \$1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$250,000 MED EXP (Any one person) \$10,000 PERSONAL & ADV INJURY \$1,000,000 GENERAL AGGREGATE \$2,000,000 PRODUCTS - COMPROP AGG \$2,000,000
	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> HIRED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS						COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)
	UMBRELLA LIAB EXCESS LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> CLAIMS-MADE DED: RETENTION \$						EACH OCCURRENCE AGGREGATE
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A		65 WBC AP2DZN	11/22/2023	11/22/2024	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTHER E.L. EACH ACCIDENT \$1,000,000 E.L. DISEASE -EA EMPLOYEE \$1,000,000 E.L. DISEASE - POLICY LIMIT \$1,000,000
B	Professional Liability Cyber Liability			ESM0239815442	11/22/2023	11/22/2024	Each Claim \$1,000,000 Aggregate \$1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required) Those usual to the Insured's Operations.	
CERTIFICATE HOLDER For Informational Purposes 3123 N DAVIDSON ST STE 210 CHARLOTTE NC 28205-1162	CANCELLATION SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE <i>Susan S. Castaneda</i>

© 1988-2015 ACORD CORPORATION. All rights reserved.

7. NEXT STEPS

We would be pleased to collaborate with West Virginia Lottery to undertake the Network Penetration Testing and Cybersecurity Assessments. We have the expertise, Experience and commitment to delivery this engagement at the most competitive price.

Ron Meeting

Ron Meeting
Chief Executive Officer
9910 Ainslie Downs Street Charlotte, Nc 28273

Email: meetingr@rapidstrategy.io
Phone: +(980) 224-0346
Respectfully submitted.



Appendix A – Resumes

CLAUDE BIRD SR. CISSP, PMP

Senior Information Security Analyst

EXECUTIVE SUMMARY

US Navy Veteran with a comprehensive background in spearheading and successfully delivering mission-critical initiatives, bring a wealth of ability in applying Cyber Security Principles and Practices alongside a robust foundation in IT Governance and Compliance. Proven history of process improvement, and process mapping. Utilizes PMI and Lean/Six Sigma methodologies, enabling a holistically sound method to assess personnel, workflows, and technology to enhance security, stability, efficiency, and resiliency. Eagerly embraces innovation and keeps a flexible mindset and willingness to swiftly adapt to evolving technological landscapes. Assimilates novel technologies and swiftly adjusts to dynamic priorities. As a seasoned servant leader, consistently proven ability for fostering excellence within teams, facilitating the creation of high-performing units that deliver exceptional results.

ACCREDITATION

- CISSP
- PMP Certified
- Lean Six Sigma Black Belt Certified
- Security+ CE
- COBIT (GRC)
- PSM (Scrum Agile)
- ITIL
- CNNA
- ISO9001 Lead Auditor

SKILLS

- 3+ years of GDPR experience working with HP as a Cybersecurity Program Manager in the Information Risk Management organization.
- Background in ISO 270001 requirements and NIST Framework to include but limited to Cybersecurity Framework (CSF) and Risk Management Framework (RFM) as outlined in NIST Pub 800-37 and PCI.
- Demonstrated experience delivering on-site and remote projects Delivery.
- Working knowledge of enterprise PPM tools (Planview, Microsoft Project Online, Clarity, Daptiv)
- Proficient in Microsoft SharePoint, Excel, and PowerPoint
- Excellent communication skills, proactive, and able to work in a fast-paced environment



EXPERIENCE**Columbia Advisory Group (CAG)****Mar 2022 – Jul 2023****Director Project Management Office (PMO) Practice**

- Developed an expert knowledge of cybersecurity as it relates to cloud, applications, and IOT embedded devices.
- Directed project management leadership across a diverse portfolio of Cybersecurity initiatives, critical in safeguarding multiple core business functions.
- Led end-to-end cybersecurity projects for diverse initiatives, ensuring alignment of business and technology goals.
- Oversaw the successful delivery of critical project components, including business requirements, technical and user interface designs, comprehensive testing, and comprehensive project planning.
- Established and upheld rigorous compliance standards, industry best practices, and a structured method for ongoing enhancements.

IT Governance Leader

- Directed the strategic development of comprehensive IT Governance Frameworks, Regulatory Compliance strategies, Risk Management protocols, and Information Security initiatives.
- Designed and executed IT Policies and Procedures, resulting in a remarkable 20% enhancement in service delivery efficiency, simultaneous risk reduction, and a more robust alignment with business aims.
- Led internal ISO9001 audits, meticulously naming areas for improvement, and effectively implementing changes, resulting in a flawless record with no findings during external audits.

IT Vendor Management/Sales

- Performed and championed quarterly business reviews with multiple clients, driving significant increases in the company's market share.
- Strategically oversaw and managed vendor/client engagement plans, meticulously highlighting critical priorities, essential business needs, and financial goals.
- Pioneered, managed, and bolstered a structured meeting cadence, resulting in the cultivation of robust executive relationships among CAG, its clients, and key vendors.
- Played a pivotal role as an information clearinghouse for vendor and client relationships, delivering transparent and uniform partnership reporting.
- Collaborated closely with the Sales and Marketing team to develop a tailored marketing plan aligned with key business goals.

PWC/USAA**Oct 2021 – Mar 2022****Business Continuity Planning – Advisor**

- Actively contributed to the facilitation of Business Impact Assessment questionnaires across various Bank product lines and business support functions, a critical part of the Bank's robust Business Continuity Planning program.
- Supplied expert guidance to product owners on the fundamental principles of Business Impact Assessments, encompassing fiscal, reputational, and operational impact analysis.
- Led discussions concerning the influence of third-party relationships on business continuity, the regulatory implications of Business Continuity Planning (BCP), and the strategic aspects of risk management within BCP.
- Thoroughly documented the outcomes of the BIA assessment and delivered strategic recommendations to leadership for effective risk mitigation within the BCP/DRP framework which led to overall business risk reduction.

FromHereOn**Apr 2021 – Oct 2021****Senior Program Manager Information Security (GRC)**

- Championed and guided working sessions, workshops, and interviews involving IT staff, IT leadership, and business stakeholders to name assumptions, risks, and constraints in the complex remediation of 400+ non-supported servers and applications, collectively valued at over \$7 Million.
- Formulated comprehensive Rough Order of Magnitude (ROM) assessments, encompassing application remediation strategies, cost estimations, resource allocation, and precise timelines for completion of server remediation project.
- Took the helm in collaborating with IT and business owners to pinpoint Program and Project risks, conflicts, and dependencies, then devised and executed strategies to mitigate constraints and enhance organizational efficiency and constructive collaboration by 10 percent.
- Orchestrated the development of a compelling business case, a meticulous migration plan, and actively championed their adoption among IT leadership, senior executives, and key business leaders.

PWC/PepsiCo**Apr 2020 - Apr 2021****Senior Manager Information Security**

- Supplied strategic leadership, governance, and direction for Manufacturing/Operational Technology (MFG/OT) cybersecurity programs.
- Cultivated strong working partnerships and strategic alliances with key stakeholders, encompassing business and technology leaders, to seamlessly align implementation and operational strategies.



- Forged strong partnerships and strategic alliances with key stakeholders, including business and technology leaders, ensuring seamless alignment of implementation and operational strategies.
- Took on a global leadership role, supplying oversight and direction for Site Isolation and Site Resiliency cybersecurity programs.
- Assumed a pivotal role in cybersecurity audits, enforcing strict adherence to set up governance, and supplying expert guidance to resolve identified findings.
- Led the design, promotion, and successful implementation of streamlined processes for risk and issue management in MFG/OT cybersecurity programs.
- Led the development of security standards and procedures to enhance resiliency, business continuity, and disaster recovery.
- Chaired regular status meetings with senior management and business owners, delivering critical insights into the cybersecurity program's influence on their lines of business.

Macy's Technology**2017 – 2020****Senior Infrastructure and Implementation Project Manager (Macy's, Inc / Bloomingdales)**

- Led comprehensive project management activities, including planning, execution, reporting, and initiative-taking resolution of issues and risks for more than fifty projects.
- Forge close collaborations with Business and IT leadership on large multi-site projects to precisely define and communicate systems' vision and direction.
- Led initiatives aimed at boosting efficiency and removing roadblocks that previously hindered the successful execution of high-priority projects, resulting in elevated customer and employee engagement and an enhanced overall experience.
- Cultivated impactful working relationships and played a pivotal role in achieving outstanding results: a remarkable 20% cost reduction, a substantial 25% improvement in efficiency, and elevated delivery quality.
- Efficiently led cross-functional project teams with over twenty resources, consistently ensuring on-time, within-budget project delivery of the highest quality.
- Managed the complete end-to-end process, encompassing RFP requests, vendor evaluation, selection, and the ongoing management of chosen vendor relationships.

Hewlett Packard Plano, TX**Mar 2014 – Apr 2017****Cyber Security Program Manager, Information Risk Management (GDPR)**

- Managed and spearheaded the European Union General Data Protection Regulation (GDPR) Compliance Program for Hewlett Packard Enterprise (HPE) Services, significantly reducing the company's risk exposure to potential multimillion-dollar fines.
- Effectively managed cross-functional, matrix teams of twenty-four engineers and support professionals, including both onshore and offshore resources, to support fifty thousand endpoints while keeping service level agreements with over 99% uptime.



- Directed cybersecurity response activities, including identification, response, elimination, and user/management education on root cause and prevention.
- Initiated efforts to show and keep robust relationships with the customer's risk management, security, and audit organizations, resulting in a significant 20% reduction in compliance findings.
- Took the lead in championing a continuous improvement program aligned with the principles outlined in the Account Security Plan.
- Oversaw project financials and conducted strategic analysis for P&L ranging from \$1M to \$20M.
- Led initiatives to understand and communicate regulatory compliance requirements for the Canadian Imperial Bank of Commerce (CIBC) account, and actively contributed to audits, audit findings, and remediation efforts.

BELK**Nov 2011 – Mar 2014****IT Infrastructure Project Management Office (PMO) Leader**

- Effectively managed cross-functional teams of seventeen resources, spanning both onshore and offshore support for twenty thousand endpoints, while consistently keeping a service level agreement of over 99% uptime.
- Led the delivery of Infrastructure Projects for over three hundred nationwide locations, consistently surpassing scope, cost, and quality expectations.
- Took the lead in developing and supporting cybersecurity playbooks and related documents.
- Managed client relationships with senior executive (C-suite) client management, proactively addressing issues and risks to drive the achievement of strategic goals.

OTHER EXPERIENCE

- Managed and led the adoption and migration of new and emerging technologies with a focus on innovation.
- Managed project budgets exceeding \$30 Million, including the Airport Renewal Project and other infrastructure projects.
- Developed and mentored a team of highly skilled technologists, project managers, business analysts, quality assurance, and developers, to successfully achieve business goals.
- Conducted in-depth analysis of the impact of new software applications on business operations.
- Chief of Staff, Virgin Islands 26th Legislature (1 Year)
- Advisor to Senator of the 26th law-making body of the U.S. Virgin Islands government
- Avionic Technician /Midshipman, US NAVY
- Honorable Discharge (8 years, Active and in-active)



EDUCATION

- Bachelor of Science in Electrical Engineering Technology – Southern Polytechnic State University
- Associates of Applied Science of Electronics - DeVry Institute of Technology
- Information Technology Senior Management Forum (ITSMF) – Mgmt. Academy



Claude Bird: Certifications and credentials

CISSP

active: 1/1/2022 thru 12/31/2024

Cert# [REDACTED]

SECURITY+ ce

Active: 8/26/2011 thru 8/26/2026

Cert# [REDACTED]

CCNA (Inactive)

PMP

Active: 3/2/2016 thru 3/1/2025

Cert# [REDACTED]

ITIL4

Active: 9/24/2020 thru 1/1/9999

Cert# [REDACTED]

COBIT (GRC)

Active: 8/26/2020 thru 1/1/9999

Cert# [REDACTED]

SCRUM (AGILE) PSM

Active: 10/10/2020 thru 1/1/9999

Cert# [REDACTED]

ALEC ROMANO

Penetration Tester

Career Focus

Lifelong learner looking to apply skills in network security, while continuing professional certifications, going to security conferences and participating in capture the flag tournaments. Currently holds a clearance, multiple DOD 8570 certifications.

Skill Highlights

- ACAS/Nessus
- Python Programming
- Red Hat/CentOS
- Penetration Testing
- BASH Scripting
- Vulnerability Assessment
- Virtualization
- Automation

Experience Summary

Senior Penetration Tester, 12/2021 - Current

ECS / IronVine – Maryland

- Conducted and participated in Red Team exercises.
- Conducted IT audit assessments for systems or applications to recommend solutions to mitigate risks.
- Designed tests and tools to break into security-protected applications and networks to probe for vulnerabilities.
- Discovered OWASP Top 10 vulnerabilities such as XSS, SQLi, RCE and more.

Penetration Tester, 06/2021 - 10/2021

M9 Solutions

- Conducted IT audit assessments for systems or applications to recommend solutions to mitigate risks.
- Discovered, documented and reported vulnerabilities such as SQLi, XSS, XXE, IDOR and open redirects.
- Performed network audits that led to RCE and the obtaining AWS access

Penetration Tester (mid), 03/2019 - 06/2021

XOR Security

- Conducted black box and grey box testing



- Performed Web Application assessments daily
- Utilized tools such as Nmap, Nessus, Acunetix, Burp, Kali Linux, Metasploit, ZAP and sqlmap
- Discovered and documented OWASP top 10, including but not limited to SQL injections, XSS, CSRF,
- XXE, command injections, code injections and open redirects
- Delivered technical reports documenting the discovery process and explaining the possible impact and how to remediate
- Used open source intelligence and passive reconnaissance to enumerate targets
- Wrote Python and BASH scripts to automate tests and exploit vulnerabilities
- Recommended IT security improvements to achieve system confidentiality, integrity and availability.

System Administrator, 10/2018 - 11/2018**Onyx Point, Inc.**

- Utilized troubleshooting and scripting abilities to fix scripts to automate cluster deployment in an Azure environment
- Deployed resources to the cloud using HashiCorp stack tools such as Terraform and Vagrant
- Installed and imaged System Integrity Management Platform (SIMP) for Azure which led to a marketplace item

System Administrator, 11/2017 - 10/2018**Enlighten IT Consulting**

- As a member of the Devops team, wrote code, ensured cluster up-time and collaborated with colleagues
- Designed and implemented customized Nagios checks to alert for unwanted behavior
- Worked with Puppet and SIMP to configure host settings
- Utilized Python to automate processes
- Parsed JSON, YAML and other data formats
- Troubleshot issues on clusters running cloud services
- Used ZAP and Nikto to scan Big Data clusters for web vulnerabilities
- Used Python libraries to interface with APIs from applications such as Apache Spark, Hadoop, Nagios and AWS

System Administrator, 01/2016 - 11/2017**BAE Systems**

- Used Wireshark and tcpdump to interpret packet captures for diagnosing network issues
- Automated repetitive tasks by creating scripts using Perl, Python and Bash
- Researched attack methodologies through open-source references to identify new threats



- Configured and performed vulnerability scans, analyzed scan results, and remediated issues to ensure continuous compliance with DoD requirements
- Troubleshoot Cisco IDS/IPS, router and switches to fix issues and ensure network up time
- Troubleshoot network, firewall and security issues to track incidents and resolve network issues
- Inspected and monitored network traffic for malicious activity
- Installed, updated and managed Checkpoint Firewalls to ensure network security
- Utilized Nmap to map networks and identify network vulnerabilities
- Utilized Nessus/ACAS scanners to find and document application vulnerabilities
- Configured and troubleshoot Unix services including SSHD, bind, Postfix, Sendmail, HTTPD and NGINX
- Established network specifications and analyzed workflow, access, information and security requirements.
- Designed proactive preventative maintenance schedules to prevent unnecessary downtime and hardware faults.
- Created patches and solutions to fix bugs in existing applications.
- Kept software licenses current for all computers and mobile devices.
- Oversaw file system, storage and other digital asset upgrades while safeguarding data integrity and redundancy.

System Administration Intern, 06/2015 - 01/2016

BAE Systems

- Installed and configured Linux servers
- Secured Linux servers to DoD specifications (DoD 8500.2) by applying DISA STIGs.
- Installed and configured client software such McAfee Antivirus and Symantec NetBackup
- Installed and configured a pfSense firewall to segment a network
- Installed and configured Nagios for service and host monitoring

Specialist, 12/2008 - 12/2014

Army National Guard

EDUCATION

Masters Certificate: Penetration Testing & Ethical Hacking, 2019
SANS Technology Institute - Bethesda, MD

Bachelor of Science: Computer Information Systems, 2017
Stevenson University - Baltimore, MD
3.55 GPA
Dean's List

Associate of Applied Science: Information Systems Security, 2014



The Community College of Baltimore County - Baltimore, MD

3.26 GPA

Dean's List

Member of the Cyber Security Computer Club

CERTIFICATIONS

- GPEN: GIAC Penetration Tester
- GCPN: GIAC Cloud Penetration Tester
- GWAPT: GIAC Certified Web Application Penetration Tester
- GPYC: GIAC Python Coder
- GCIH: GIAC Certified Incident Handler
- CompTIA Security+
- LPI Linux Essentials



THOMAS GILBERT

Cyber Security Analyst | Penetration Tester

Summary

Experienced cyber security professional with strong desire and passion to continue to grow within the Information Security field. Dependable and hardworking with a commitment to respect, integrity, and service to others.

8+ years of experience within the Information Security field. Additional expertise includes 5+ years of personnel and operations management, with strengths in structuring a positive work environment while mentoring and developing team-members.

Profile and Highlights

Security is a critical component to the success of any organization. I've had the opportunity to interact with hundreds of clients and deeply assess their IT infrastructure, security architecture, and general security policies. Through this I've formed a strong understanding of organizational security risks and vulnerabilities, and how to mitigate and manage those risks.

I have developed a communication style that allows me to articulate the meaning and importance of risk to organizational leadership while also creating concrete, actionable mitigation steps for the organization to implement. This enables the businesses I work with to effectively enact real change that provides genuine improvements to secure their business, guard client data, and stay in compliance. My degree in Criminal Justice motivates me to actively work against threat actors who wish to harm the clients that I work with. My time as a manager of Chick-fil-A formed a leadership style in me that helps me to encourage and mentor the team around me. My dedication to ongoing self-improvement and growth continues to sharpen and refine the value that I bring to organizations.

Skills and Abilities

- Project Management and Delivery
- Threat and Exploit Research
- Vulnerability and Risk Assessments
- Penetration Testing / Ethical Hacking
- Technical Writing and Documentation
- Process Improvement
- Team Collaboration

Experience Summary

Sr. Security Consultant

Pondurance, LLC.

Launched my security-focused career with an entry-level position in September, 2015. After two years I was promoted to a Senior-level position. During this time I



worked with clients in various industries including: Government; Hospitals; Energy Cooperatives; Universities; Retail; etc., and formulated strategic remediation strategies for those different environments. In 2020 Pondurance went through a Merger and Acquisition and has experienced significant growth since then.

- Proactive and Direct Communication with Clients on a Daily Basis Including Project Status, Critical Findings, and Potential Remediation Steps
- Manage, Update, and Develop Methodologies for Security Testing, Incorporating Standards Such as NIST and Other Industry Best Practices
- Perform Security Testing (Penetration Testing / Ethical Hacking) Against a Variety of Enterprise-level Assets, Applications, Systems, and Software
- Utilize a Broad Range of Open-source and Commercial Tools Including: Nessus, BurpSuite, Nikto, WiFite, SQLmap, Metasploit, CrackMapExec, BloodHound, etc.
- Exhibit Strong Attention to Detail in Regards to Project Scoping, Management, Execution, Documentation, and Delivery
- Prepare and Present Summary of Findings to Executives and GRC Committees
- Peer Review and Quality Assurance of Security Testing Processes and Deliverables
- Balance Multiple Projects as the Lead Consultant

Inventory Coordinator / IT Support

LaCrosse Footwear, Inc.

Began this role as a Distribution Associate in February, 2013 and was promoted to the lead role in the "Returns" department.

- Provided IT Support for Customers and Departments within Organization
- Quality Control/Assurance for Company Products
- Inventory/Database Management and Tracking

EDUCATION

Masters Certificate: Penetration Testing & Ethical Hacking, 2019
SANS Technology Institute - Bethesda, MD

Bachelor of Science: Computer Information Systems, 2017
Stevenson University - Baltimore, MD
3.55 GPA
Dean's List

Associate of Applied Science: Information Systems Security, 2014
The Community College of Baltimore County - Baltimore, MD



3.26 GPA
Dean's List
Member of the Cyber Security Computer Club

AFFILIATIONS / ORGANIZATIONS

The Order of the Sword and Shield

Member, from 2014 - present

National academic and professional honor society dedicated exclusively to Homeland Security, Intelligence, Emergency Management, and all protective security disciplines.

InfraGard, Indiana Members Alliance

Member, from 2016 - present

Organization with partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.A.

CERTIFICATIONS

- CompTIA - CNSP
- CompTIA – CySA+
- CompTIA – CNVP
- CompTIA – PenTest+
- CompTIA – Security+
- AWS – Certified Cloud Practitioner
- Autopsy Digital Forensics Training
- Microsoft – Networking Fundamentals
- Microsoft – Security Fundamentals



MEKHI RHODIE

Junior Penetration Tester

Executive Summary

Experienced penetration and web developer proficient in discovering and rectifying security vulnerabilities. Demonstrated expertise in API security testing, secure coding practices, code reviews, and employing DevSecOps strategies. Adept in SAST and DAST methodologies, excelling in identifying issues in alignment with the OWASP Top 10. Skilled in web server configuration, with a deep understanding of HTTP/HTTPS, TCP/IP, and WebSockets. Proficient in using an array of security-oriented tools including, Docker, Kali Linux, Metasploit, Burp Suite, OWASP ZAP, Nmap, cURL, and Bash scripting. Praised for robust communication and active listening skills, demonstrating adaptability in dynamic environments. Recognized for meticulous attention to detail, superior problem-solving abilities, and an unwavering commitment to maintaining the highest level of web application security. Devoted to staying current with emerging technology trends and sharpening industry knowledge.

Experience Summary

Full-stack Web Developer, MakeMine 08/2020 – 02/2021 | Charlotte, United States

- Designed and developed interactive, user-friendly web applications using HTML, CSS, JavaScript, and TypeScript, ensuring high performance on both front-end and back-end functionalities.
- Managed databases using GraphQL and SQL, creating, maintaining, and optimizing data storage and retrieval for complex application needs.
- Implemented secure coding practices to prevent common security vulnerabilities, ensuring the safety and integrity of user data and application functionalities.
- Utilized problem-solving skills to identify, analyze, and address software issues, leading to more reliable and effective web applications.

Desktop Support Analyst, Barings 08/2021 – 12/2021 | Charlotte, United States

- Troubleshooting both hardware and software-related issues both in-person and on-call.
- Communicate clearly when walking customers through troubleshooting steps.
- Documented IT support procedures and system configurations, enhancing clarity and efficiency.

Computer Systems Analyst, Charter Communications 12/2022 – 12/2023 | Charlotte, United States

- Provided technical support to end-users, troubleshooting software issues to maintain business continuity.



- Performed routine audits of the software, ensuring the usage of up-to-date and secure applications.
- Assisted in the implementation and monitoring of security measures for the protection of computer systems, networks, and information.
- Installed, maintained, and troubleshoot various software applications, identifying compatibility issues and making recommendations for optimal performance.
- Trained staff in software applications, improving overall cybersecurity awareness and competency.

Bug Bounty Hunter, Self-Employed 01/2024 – present | Charlotte, United States

- Conduct thorough security assessments and penetration testing on various web applications to identify vulnerabilities and security flaws.
- Participated in bug bounty platforms and forums, engaging with the cybersecurity community, contributing to the responsible disclosure of security findings, and employing creative methods to discover and exploit security issues.
- Maintain up-to-date knowledge of the latest security trends, vulnerabilities, and exploitation techniques to stay ahead of emerging threats to adapt to evolving web application security landscapes.
- Proven ability to work independently and efficiently manage time and resources to maximize the identification of critical vulnerabilities.
- Use penetration testing tools, such as but not limited to, nmap, cURL, OWASP ZAP, Burp Suite, Metasploit, Sqlmap, and Nikto to aid in the process of discovering vulnerabilities in web applications.

Junior Penetration Tester, Rapid Strategy 02/2024 – present | Charlotte, United States

- Assist in performing penetration testing on web applications, networks, and infrastructure.
- Perform project management activities such as scheduling and coordinating "Stand-up" meetings.
- Conduct vulnerability assessments and penetration tests using various tools and methodologies.
- Collaborate with senior team members to analyze findings and prioritize remediation efforts.
- Document and report security vulnerabilities, findings, and recommendations to stakeholders.
- Participate in security research and stay updated on the latest threats and attack techniques.
- Work closely with clients to understand their security requirements and provide appropriate recommendations.

EDUCATION

Full-Stack Web Development, University of North Carolina at Charlotte 07/2019 - 01/2020 |
Charlotte, United States

CERTIFICATIONS

- **CompTIA Security+ SY0-601**
████████████████████
- **CompTIA CySA+ CS0-002**
████████████████████



Mekhi Rhodie

has successfully completed the requirements to be recognized as



CANDIDATE ID

November 01, 2022

CERTIFICATION DATE

EXP DATE: 11/01/2025

TODD THIBODEAUX, PRESIDENT & CEO

Code: R752PCKS1EVQ1WSH

Verify at: <http://verify.CompTIA.org>

Mekhi Rhodie

has successfully completed the requirements to be recognized as



CANDIDATE ID

February 28, 2022

CERTIFICATION DATE

EXP DATE: 02/28/2025

A handwritten signature in black ink, appearing to read "TThibodeaux".

TODD THIBODEAUX, PRESIDENT & CEO

Code: WJP3L9PP4CEQ1PC3

Verify at: <http://verify.CompTIA.org>

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) John J. Bird

(Address) 282 < //), rp I Ho/1 ad . rX ?kov

(Phone Number)/ (Fax Number) 472 - 816 - 2711

(email address) bbird@rapidstrategy.io

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, 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 § SA-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code SA-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Rapid Strategy
(Company)
John J. Bird - Advisor
(Signature of Authorized Representative)
John J. Bird 3/27/2024
(Printed Name and Title of Authorized Representative) (Date)
472-816-2711
(Phone Number) (Fax Number)
bbird@rapidstrategy.io
(Email Address)



THE HARTFORD
BUSINESS SERVICE CENTER
3600 WISEMAN BLVD
SAN ANTONIO TX 78251

March 8, 2024

For Informational Purposes
3123 N DAVIDSON ST STE 210
CHARLOTTE NC 28205-1162

Account Information:

Policy Holder Details :	Rapid Strategy, Inc
--------------------------------	----------------------------

Contact Us

Need Help?

Chat online or call us at
(866) 467-8730.

We're here Monday - Friday.

Enclosed please find a Certificate Of Insurance for the above referenced Policyholder. Please contact us if you have any questions or concerns.

Sincerely,

Your Hartford Service Team



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
03/08/2024

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER USAA INSURANCE AGENCY INC/PHS 65812845 The Hartford Business Service Center 3600 Wiseman Blvd San Antonio, TX 78251	CONTACT NAME:		
	PHONE (A/C, No, Ext): (866) 467-8730	FAX (A/C, No):	
	E-MAIL ADDRESS:		
INSURER(S) AFFORDING COVERAGE		NAIC#	
INSURED Rapid Strategy, Inc 3123 N DAVIDSON ST STE 210 CHARLOTTE NC 28205-1162	INSURER A : Nutmeg Insurance Company		39608
	INSURER B : Lloyds, Underwriters at Lloyds		15792
	INSURER C :		
	INSURER D :		
	INSURER E :		
	INSURER F :		

COVERAGES**CERTIFICATE NUMBER:****REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/Y YYY)	LIMITS	
B	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY			ESM0239815442	11/22/2023	11/22/2024	EACH OCCURRENCE	\$1,000,000
	<input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	\$250,000
							MED EXP (Any one person)	\$10,000
							PERSONAL & ADV INJURY	\$1,000,000
GEN'L AGGREGATE LIMIT APPLIES PER:							GENERAL AGGREGATE	\$2,000,000
	POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC <input type="checkbox"/>						PRODUCTS - COMP/OP AGG	\$2,000,000
	OTHER:							
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	
	<input type="checkbox"/> ANY AUTO						BODILY INJURY (Per person)	
	<input type="checkbox"/> ALL OWNED AUTOS	<input type="checkbox"/> SCHEDULED AUTOS					BODILY INJURY (Per accident)	
	<input type="checkbox"/> HIRED AUTOS	<input type="checkbox"/> NON-OWNED AUTOS					PROPERTY DAMAGE (Per accident)	
	<input type="checkbox"/> AUTOS							
	UMBRELLA LIAB EXCESS LIAB						EACH OCCURRENCE	
	<input type="checkbox"/> OCCUR CLAIMS-MADE						AGGREGATE	
	DED: <input type="checkbox"/> RETENTION \$							
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY			65 WBC AP2DZN	11/22/2023	11/22/2024	<input checked="" type="checkbox"/> PER STATUTE	<input type="checkbox"/> OTHER
	PROF/NEO/FA/INE/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH)	<input type="checkbox"/> Y/N	N/A				E.L. EACH ACCIDENT	\$1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE -EA EMPLOYEE	\$1,000,000
							E.L. DISEASE - POLICY LIMIT	\$1,000,000
B	Professional Liability			ESM0239815442	11/22/2023	11/22/2024	Each Claim	\$1,000,000
	Cyber Liability						Aggregate	\$1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Those usual to the Insured's Operations.

CERTIFICATE HOLDER**CANCELLATION**
 For Informational Purposes
 3123 N DAVIDSON ST STE 210
 CHARLOTTE NC 28205-1162

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Suzan L. Castaneda

© 1988-2015 ACORD CORPORATION. All rights reserved.

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 Rapid Strategy _____, with its principal offices located at 9910 Ainslie Downs Street Charlotte, NC 28273 (“Party of the second part”), with an Effective Date of 27th March 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 _____ (the “Effective Date”) and 3 year(s) after the termination of such Agreement (“Disclosure Period”). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

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

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

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

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

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

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

WEST VIRGINIA LOTTERY

By: _____

Name: _____

Title: _____

_____(VENDOR)

By: Rapid Strategy

Name: Ron Meeting

Title: Chef Executive Officer

Ron Meeting

EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	\$ 4,554 -	\$ 36,432 -
2	4.2	Website Penetration Testing	8	\$ 6,897 -	\$ 55,752 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$ 9746 -	\$ 116,952 -
4	4.4	Wireless Penetration Testing	8	\$ 2,222 -	\$ 17,776 -
TOTAL BID AMOUNT					\$226,912 -

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:	Rapid Strategy
Vendor Address:	9910 Ainslie Downs Street Charlotte, NC 28273
Email Address:	meetingr@rapidstrategy.io
Phone Number:	(980) 224-0346
Fax Number:	
Signature and Date:	27th March 2024 <i>Ron Meeting</i>