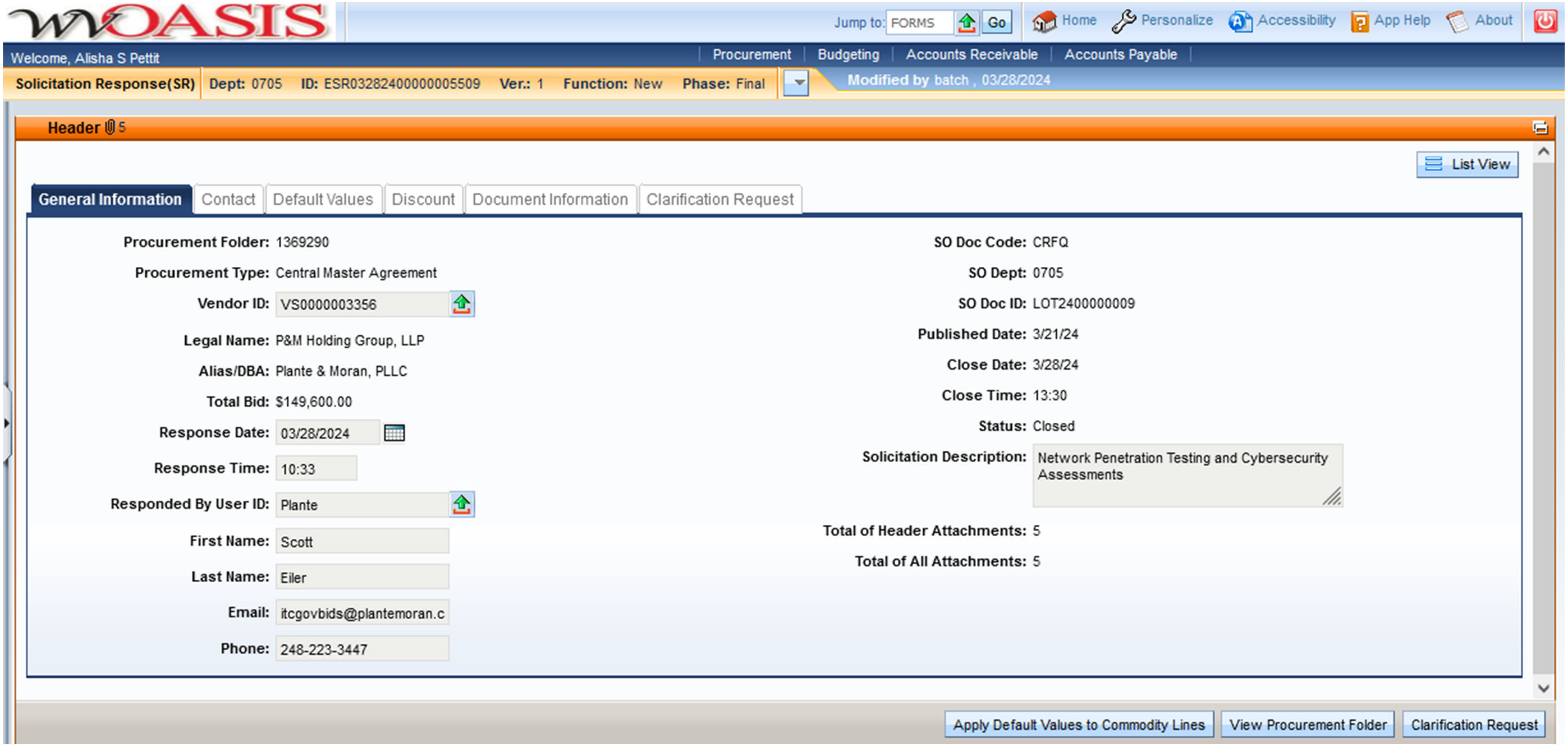
West Virginia
Purchasing Division

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

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



Welcome, Alisha S Pettit

Solicitation Response(SR) Dept: 0705 ID: ESR03282400000005509 Ver.: 1 Function: New Phase: Final

Modified by batch , 03/28/2024

| | |
|---|---|
| Procurement Folder: | 1369290 |
| Procurement Type: | Central Master Agreement |
| Vendor ID: | VS0000003356 |
| Legal Name: | P&M Holding Group, LLP |
| Alias/DBA: | Plante & Moran, PLLC |
| Total Bid: | $149,600.00 |
| Response Date: | 03/28/2024 |
| Response Time: | 10:33 |
| Responded By User ID: | Plante |
| First Name: | Scott |
| Last Name: | Eiler |
| Email: | itcgovbids@plantemoran.c |
| Phone: | 248-223-3447 |

| | |
|---|---|
| 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: | 5 |
| Total of All Attachments: | 5 |

| | |
|---|---|
| Department of Administration<br>Purchasing Division<br>2019 Washington Street East<br>Post Office Box 50130<br>Charleston, WV 25305-0130 | **State of West Virginia**<br>**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 ESR03282400000005509 | 1 |

**VENDOR**

VS0000003356
P&M Holding Group, LLP

**Solicitation Number:** CRFQ 0705 LOT2400000009

**Total Bid:** 149600 **Response Date:** 2024-03-28 **Response Time:** 10:33:19

**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 | | | | 5500.00 |

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

**Commodity Line Comments:** 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 | | | | 4500.00 |

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

**Commodity Line Comments:** 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 | | | | 120000.00 |

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

**Commodity Line Comments:** 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 | | | | 19600.00 |

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

**Commodity Line Comments:** Wireless Penetration Testing

**Extended Description:**

See Attached Specifications and
Exhibit - A Pricing Page

## EXHIBIT A - Pricing Page REVISED 1/25/2024

| Item # | Section | Description of Service | Unit Price per Assessment | Estimated Number of Assesments | Extended Amount |
|---|---|---|---|---|---|
| 1 | 4.1.1 | External Network Penetration Testing | 687.50 | 8 | $ 5,500.00 |
| 2 | 4.1.2 | Website and Web Application Penetration Testing | 562.50 | 8 | $ 4,500.00 |
| 3 | 4.1.3 | Internal Network Vulnerability Assessments | 17000.00 | 8 | $ 136,000.00 |
| 4 | 4.2.1 | Executive Summary Report | 150.00 | 8 | $ 1,200.00 |
| 5 | 4.2.2 | Technical Report | 150.00 | 8 | $ 1,200.00 |
| 6 | 4.2.3 | Findings Presentation | 150.00 | 8 | $ 1,200.00 |
| | | | | | $ 149,600.00 |

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

| | |
|---|---|
| **Vendor Name:** | Plante Moran |
| **Vendor Address:** | 3000 Town Center, Suite 100, Southfield, MI 48075 |
| **Email Address:** | joe.oleksak@plantemoran.com |
| **Phone Number:** | *847.628.8860* |
| **Fax Number:** | |
| **Signature and Date:** | 26-March-24 |

JANUARY 25, 2024

# STATE OF WEST VIRGINIA

## STATE LOTTERY

CRFQ 0705 LOT2400000005 - Network Penetration Testing and Cybersecurity Assessments Services Proposal

plante moran | Audit. Tax. Consulting.
Wealth Management.

plante moran

January 25, 2024

Mr. Brandon Barr
State of West Virginia
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Dear Mr. Barr,

Thank you for the opportunity to submit our proposal for network penetration testing and cybersecurity assessment services to the State of West Virginia (“State” or “Lottery”). Based on our understanding of your needs, you’re looking for a partner who can exceed your expectations and understand your organization’s unique needs.

As one of the top-ranked accounting and consulting firms in the nation, and with over 30 years of experience performing cybersecurity services for both public and private sector clients, we bring the expertise, perspective, and insight that the State needs. Our engagements identify and evaluate vulnerabilities, all while developing remediation recommendations to address deficiencies. Additionally, our recommendations will address identified weaknesses and their associated business risks. Our certified professionals, using industry-standard tools and tailored methodologies, will deliver a cost-effective and timely assessment with a workplan of practical recommendations to mitigate identified risks and leverage existing resources.

We’re guided by our “we care” philosophy of client service, which is based on upholding our core values of caring for our clients, caring for our work, and caring for each other. We believe that this simple, sincere philosophy is what makes our firm unique and is the key to our success. We’ve been awarded a place on Fortune magazine’s “100 Best Companies to Work For in America” list every year since 1998.

Thank you for the opportunity to serve you. I will follow up soon to answer any questions you might have. I look forward to it.

Sincerely,

**PLANTE & MORAN, PLLC**

Joe Oleksak
Engagement Partner
847-628-8860
joe.oleksak@plantemoran.com

# Table of contents

**Qualifications ... 1**
*Plante Moran in brief ... 2*
*Government experience ... 3*
*Cybersecurity ... 4*
*Staff certifications ... 4*
*Cybersecurity Services ... 6*
*Staff training ... 7*
*References ... 8*
*Project team overview ... 10*
*Team bios ... 11*
*Our methodology ... 14*
*Our proposed scope ... 16*
*Penetration testing approach and workplan phases ... 18*
*Security testing tools ... 24*
*Background checks ... 25*
*Non-Disclosure Agreement (NDA) ... 25*
*Addendum Acknowledgement ... 26*

**Appendix ... 27**
*Additional firm information ... 28*
*Customer service & client satisfaction- the Plante Moran way ... 29*
*Client satisfaction ... 30*
*Proposed contract exceptions ... 31*

# Qualifications

**3.1 Vendor must be in business at a minimum fifteen (15) years performing and delivering information technology cybersecurity assessments.**

**3.1.1 Vendor should provide with their bid, a general company overview that must include information regarding the number of years of qualification, experience, training, relevant professional education for each individual that will be assigned to the project team, professional services offered, and number of dedicated security staff resources.**

## Plante Moran in brief

We are the 15th largest certified public accounting and management consulting firm in the nation. With **a history spanning nearly 100 years**, our firm provides clients with financial, human capital, operations improvement, strategic planning, technology selection and implementation, and wealth management services.

### Fast facts

1924
Year founded

3,500+
Staff

360+
Partners

23
Offices worldwide

50
States with clients

150+
Countries where we've served clients

45+
Services available

25+
Industries served

### Our people are our most valuable differentiator.

Plante Moran's founders had a vision:
**"to create a people firm disguised as an accounting firm."**

In other words, our professional expertise is just one part of who we are. Our character is what sets us apart and allows us to build meaningful relationships with our clients and colleagues.

As we move into the future — and continue to use artificial intelligence, data analytics, and other technologies to empower our client service model in new ways — we'll hold steadfast to that philosophy.

**THE WHOLE PERSON**
**COMES TO WORK**

**We're more than the sum of our expertise. It's how we work collaboratively — with each other and with our clients — that sets us apart. Learn more by watching our video series "The Whole Person Comes to Work" at plantemoran.com/celebrate.**

# Government experience

When we serve governmental entities, ensuring compliance is just the first step. As the State's partner, we'll translate our expertise into solutions, helping you streamline operations, contain costs, and stay ahead of the curve. Why? It's simple: Investing in our clients means investing in the future of our communities.

## What our practice looks like

500+ Governmental clients, including:

- Airports
- Transportation organizations
- Authorities
- Local government
- Pension systems
- Special districts
- State agencies
- Utilities

1,500+ Public sector clients served

75 Years serving government entities

45 States with public sector clients

250+ Staff dedicated to serving governmental clients

25+ Partners dedicated to serving governmental clients

## How we stand apart from the competition

When it comes to serving municipalities and government entities, the Plante Moran difference can be boiled down to two key factors:

1

### Our governmental clients are served by professionals who have made the public sector a focus of their careers.

Because our firm is organized by industry (not by office or region), you'll always be served by specialists who have already served many governmental entities, including cities and counties, municipal operations, water and sewer authorities, transit authorities, state government agencies, and public library systems.

2

### Our firm is unmatched in the level of research we conduct on challenges facing governmental leaders.

Our active involvement in government associations — along with our firsthand experience serving a large, diverse client base — is at the heart of our technical expertise. We pass on what we learn to our staff in the form of internal training seminars and to our clients through our webinars, white papers, and toolkits.

# Cybersecurity

Establishing a strong cybersecurity program centered around defense should be a top priority for the State. Threats can come from anywhere, and the State needs to take a proactive approach to threat detection and response. That's where our team comes in. Our deep bench of cybersecurity professionals and government industry specialists offer relevant experience, insights, and technical expertise to fortify the State's defenses and maintain an effective cybersecurity program.

Our cybersecurity team can provide a variety of solutions to clients like State, including:

- IT risk and internal control assessments
- Baseline network security assessments (layered approach: internet, firewall, network, etc.)
- Business process/application security and control reviews
- Business continuity and disaster recovery planning
- Adherence to compliance-related issues, such as PCI Data Security Standards, HIPAA, GLBA, and Red Flag
- Network security assessment and penetration studies
- Security planning, including the development of security strategies and plans, policies, procedures, and training

## Practice profile and certifications

1,000+

cybersecurity assessments performed annually across all client industries

100+

staff dedicated to providing solutions to our clients' unique cybersecurity needs

1 of only 32

nationally approved HITRUST assessors also providing PCI and ISO services

# Staff certifications

Plante Moran's consulting team is highly recognized in the security community. Our team holds all necessary and relevant certifications to serve State with expert network penetration testing and cybersecurity assessment services. Additionally, we have a documented record of providing outstanding service to our clients — evidence that our core values are not just words on a page but standards we live by.

Our cybersecurity team averages more than 15 years of experience providing cybersecurity control evaluations, IT compliance testing, internal audit assistance, technical assessments, and internal control consulting services. Our team is comprised of individuals with one or more of the following certifications:

AWS Certified Security – Specialty Certification
Certified Ethical Hacker (CEH)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
Certified Information Systems Security Professional (CISSP)
Certified in Governance of Enterprise IT (CGEIT)
eLearn Security Certified Professional Penetration Tester (eCPPT)
eLearn Security Mobile Application Penetration Tester (eMAPT)
GIAC Penetration Tester (GPEN)
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

Certified Risk and Information Systems Control (CRISC)

Cisco Certified Network Associate (CCNA)

Cisco Certified Network Associate Security (CCNA Security)

CompTIA Security+

CompTIA Network+

CompTIA A+

CompTIA Linux+

EC-Council Certified Network Defense Architect (CNDA)

HIPAA HITRUST CSF Certified Assessor (CCFSP)

IACRB Certified Penetration Tester (CPT)

Microsoft Certified: Security, Compliance, and Identity Fundamentals

Offensive Security Certified Expert (OSCE)

Offensive Security Certified Professional (OSCP)

Offensive Security Wireless Professional (OSWP)

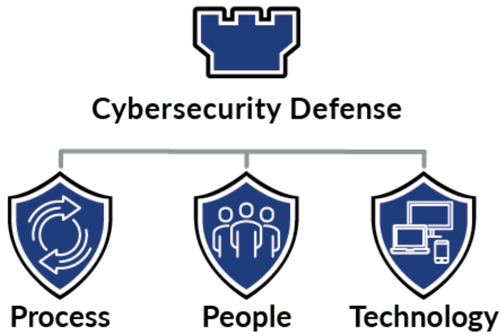
PCI DSS Qualified Security Assessor (QSA)

Project Management Professional (PMP)

Proofpoint Certified Phishing Specialist 2022

## Cybersecurity Services

By taking a holistic view of your organization — and your people, processes, and technology — we'll protect you not just from the threats you're aware of, but those you haven't even considered.



### How we can help State maintain a secure IT environment:

### Cyber assessment

- IT audits
- Risk assessment
- ERP security and controls
- Cloud security
- User access reviews
- Privacy compliance
- General controls review
- Application controls assessment

### Cyber advisory

- Seven-point cybersecurity assessment
- Cyber strategy
- Frameworks
- NIST, CIS Top 20
- Cyber PMO
- Risk analysis
- Business continuity plans (BCPs), disaster recovery plans (DRPs)
- Cyber incident response planning
- CyberKPi and dashboards

### Cyber assurance

- Readiness assessments
- SOC 1, SOC 2, and SOC 3
- SOC for cybersecurity
- SOC for supply chain
- PCI DSS certification
- HITRUST certification
- ISO27001 Security Standards certification

### Cyber solutions

- Solution selection and integrated custom dashboards
- GRC tools
- Identity management
- Threat intelligence
- Mobile/device management
- End-point security
- IDS/IPS
- SIEM tools

### Cyber lab

- Physical lab environment
- Network security assessments
- Vulnerability scans
- Web/mobile security
- Malware testing
- Red/blue team exercises

### Cyber forensics

- Identification, collection, analysis, and reporting
- Incident response and management

# Staff training

We know staff development is critical to our success as a firm. That's why we invest significant time and resources to staff training. We recruit and retain the best and the brightest professionals by offering both internal and external training to our staff, which increases their expertise and furthers their career.

Our internal training opportunities are offered at various levels in a staff member's professional development. These range from our library of on-demand, self-directed training and orientation presentations, up to in-person, instructor-led trainings that are customized by staff level. Our external training opportunities include attendance and presentations at specialized trainings that are offered by organizations such as the Institute of Internal Auditors. Combined, these opportunities keep our staff current and knowledgeable with the latest industry trends.

At a minimum, **all partners and professional staff are required to participate in 40 hours of continuing professional education (CPE) courses each year.** However, most staff and partners go above and beyond the minimum by participating in many more hours than required.

Our cybersecurity practice is specifically dedicated to going above and beyond when it comes to internal staff training and development. In addition to the 40 hours of continuing professional education, we annually conduct two weeks of formal training for our IT staff: one week in the spring and one in the fall. Our staff also participate in various professional organizations, where they obtain specific technical training and continue education that furthers their professional development. Plante Moran professionals also participate and speak at various national, regional, and local conferences to give back to our industries and professional communities while sharing our knowledge, technical expertise, and thought leadership.

Our other staff retention and development initiatives include our formal professional development and mentorship programs, our WorkFlex Committee which promotes work-life balance, our Diversity, Equity, and Inclusion (DEI) Council, our team partner system, and more. As a result of the culture we've created, Fortune magazine has recognized Plante Moran as one of the "100 Best Companies to Work For" every year since 1998.

## Recognition for training excellence

Our learning and development team has been recognized by The Association for Talent Development (ATD) as a BEST Award winner. The ATD BEST Award showcases organizations that exhibit firmwide success as a result of exceptional staff talent development. Award winners must have demonstrated that learning has value in the organization's culture, investments are made in talent development and performance initiatives, and learning links to individual and organizational performance.

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

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

## References

### Ohio Deferred Compensation Program

Jason Chang
IT Manager
257 E. Town Street, Suite 400
Columbus, OH 43215
614-466-7245
jchang@ohiodc.org

### Comprehensive IT Security Assessment

Plante Moran conducted a comprehensive security assessment that included external and internal network penetration testing, quarterly network vulnerability scanning, web application security assessment and penetration testing, and source code review of their participant portal to identify vulnerabilities and recommend appropriate safeguards to enhance Ohio Deferred Compensation's overall security controls.

Our services included the following:

- External (internet) network penetration testing
- Internal network penetration testing
- Network vulnerability assessment
- Web application security assessment (penetration testing)
- Source code security review
- Social engineering assessment
- Firewall security configuration review
- Security policies and procedures review
- Remote access security review

### Ohio Public Employees Retirement System (OPERS)

Caroline Stinziano
Director, Internal Audit
277 E. Town Street
Columbus, OH 43215
614-228-3303
cstinziano@opers.org

### Network Penetration Testing and Vulnerability Assessment

An information security assessment that included external network penetration testing, external network vulnerability assessment, web application security assessment, and wireless penetration testing to identify vulnerabilities and recommend appropriate safeguards to enhance OPERS' overall security controls.

Our services included the following:

- External (internet) network penetration testing
- External network vulnerability assessment
- Web application security assessment (penetration testing)
- Wireless penetration testing

## City of Roseville, CA

Mr. Hong Sae
Chief Information Officer
City of Roseville
316 Vernon Street,
Suite 300
Roseville, CA 95678
916 774-5152
hsae@roseville.ca.us

### IT Security Risk Assessment

Performed a review and assessment of the City's IT environment to evaluate security policies and procedures implemented to manage security, assess the overall level of security risk to the City, identify potential security vulnerabilities, and evaluate the design of security controls implemented. Scope of our work included the City's IT department, Public Safety division, and Utilities department.

The risk assessment based on NIST CSF Framework and included family categories as topical areas of inclusion for the assessment. We conducted department interviews, evaluated department policies and procedures, and review documentation to support IT security and technical operations. We also evaluated controls established to protect sensitive data maintained within the City's databases and applications.

We also conducted an information security assessment that included external and internal network penetration testing, external network vulnerability assessment, and wireless penetration testing to identify vulnerabilities and recommend appropriate safeguards to enhance the City's overall security controls.

Our services included the following:

- External (internet) network penetration testing
- Internal network penetration testing
- External network vulnerability assessment
- Wireless penetration testing

**3.3 Vendor should provide with their bid, documentation of current accreditations held by the project team assigned to Lottery cybersecurity assessments.**

**3.3.1 Documentation shall consist of an overview of the project team security assessments, resumes and documentation of certifications namely CISSP or SAN should be provided as stated below in section 3.4.**

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

## Project team overview

Our staffing approach is designed to assign personnel to areas of the project where their expertise is required. All the proposed team members have worked together on similar engagements for our clients. Specifically, our project-staffing plan is carefully tailored to assure that project team members are assigned tasks closely aligned to their experience and capabilities. All the proposed consultants are employees of Plante Moran. Additional staff will be assigned as needed.

Actual certificates are provided in appendix.

| Project team | Project role and responsibilities |
|---|---|
| **Joseph Oleksak \| CISSP, CRISC, QSA**<br>Partner | **Engagement Partner**<br>Will serve as an additional point of contact and will have the overall responsibility for engagement account management. Responsible for ensuring that all Plante Moran services are completed within schedule and budget. Will provide project quality control over Plante Moran deliverables and services. |
| **F. Alex Brown \| CPA, CHP,**<br>Principal | **Project Manager**<br>Will serve as Project Manager responsible for oversight of the workplan and day-to-day project activities. Works to ensure all project tasks are completed on schedule, within budget, and meet appropriate quality standards. Responsible for risk and issue management and regular project communications with the State. |
| **Saumil Shah \| CISA, CISSP, CEH, CCNA**<br>Senior Manager | **Penetration Testing Lead**<br>Will be responsible for managing the work plan and day-to-day project activities. Works to ensure all project tasks are completed on schedule, within budget and meet appropriate quality standards. Responsible for risk and issue management. |
| **Zachary Johnson \| OSCP, CEH, CPSA**<br>Manager<br>**DeShaun Ormond \| eJPT, eCPPT, OSCP**<br>Senior Consultant<br>**Shayna Harbecke**<br>Senior Consultant<br>**Harry Brennan**<br>Senior Consultant<br>**Mícheál Sheridan**<br>Consultant | **Penetration Testing Specialists**<br>These individuals have each participated in numerous Penetration Assessments as listed in our reference section. They bring hands-on experience from 1-5 years with assessing technical networks, performing penetration vulnerability assessments, and evaluating people, process and technologies associated with risk management and developing recommendations. |

| Project team | Project role and responsibilities |
|---|---|
| **Allen Allos \| CISA**<br>Manager | **Security Risk Consultants**<br>Will be responsible for evaluating technical security controls and identification of potential threats. Security Risk Consultant has participated in numerous cyber risk and control engagements, including risk assessments, incident response reviews, business continuity planning, compliance and regulatory reviews, IT Audits, and security access reviews. |

## Team bios

### Joseph Oleksak, CISSP, CRISC, QSA

**Partner**

Joe has more than 23 years of information systems security and information technology audit experience in multiple industries, including healthcare, state and local government, higher education, not-for-profit, and financial institutions including banks, credit unions, mortgage companies, and insurance companies. Joe's experience includes cybersecurity risk assessment, IT audit, penetration testing and network vulnerability assessment projects, web application vulnerability and security testing, PCI compliance, SSAE16 and SOC reviews, incident response planning and testing, business continuity, and disaster recovery management. Joe is a member of the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC)$^2$. He attends and presents at multiple security and industry conferences annually and is a member of both the Indiana Bankers Association Information Technology Committee and the Illinois Bankers Association Technology Committee. Joe is a Certified Information Systems Security Professional (CISSP) and Certified in Risk and Information System Controls (CRISC).

### F. Alex Brown, CPA, CHP

**Principal**

Alex has over 25 years of information technology audit, technology regulatory control compliance, and system integration project experience. Alex has extensive experience in the assessment of technology risk and evaluation of IT controls in support of IT security regulatory compliance engagements (e.g., HIPAA/HITECH, PCI). In addition, Alex has extensive experience in working with various IT security control frameworks (e.g., NIST 800, ISO 27001/27002, CSC). Alex has extensive industry experience including government, higher education, healthcare, and manufacturing. Alex's experience includes planning and performing engagements to evaluate and assess IT risk, evaluate the effectiveness of control measures implemented, identify IT control deficiencies, and develop remediation recommendations. Alex is a Certified HIPAA Security Professional (CHP), Certified Public Accountant, and is a member of the American Institute of Certified Public Accountants (AICPA). Alex holds a B.S. in accounting from North Carolina A&T State University.

## Saumil Shah, CISA, CISSP, CEH

**Senior Manager**

Saumil has over 17 years of information security, control, and IT audit experience in a number of industries, including financial institutions, insurance, and healthcare. Saumil's experience includes reviewing system configuration (router/switch/firewall/server settings etc.), conducting web and mobile application security, source code reviews, and social engineering assessments, as well as performing black-box/white-box network penetration testing on IT infrastructure components deployed and managed by the client infrastructure team. He has assisted with IT general control reviews, PCI-DSS, SSAE 16 reviews, and database security audits. Saumil holds a bachelor's degree in computer engineering from Mumbai University. Saumil is certified in Certified Information Systems Auditor (CISA), Cisco Certified Network Associate Security (CCNA-Security), Certified Ethical Hacker (CEH), EC-Council Certified Security Analyst (ECSA), and Provisional ISO 27001 Lead Auditor (ISO 27001 LA) & Certified Information Systems Security Professional (CISSP). Saumil regularly attends ISACA Chapter meetings and participates InfoSec discussions to identify challenges faced in security industry.

## Zachary Johnson, OSCP, CEH, CPSA

**Manager, Cybersecurity**

Zach has more than seven years of experience as an information security professional. Within Plante Moran's cybersecurity practice, Zach's areas of focus are penetration testing, vulnerability assessments, and social engineering. He has experience in penetration tests in several industries including financial services, higher education, real estate, K-12, marketing, and manufacturing/automotive. Zach holds a bachelor's degree in information assurance from Eastern Michigan University where he participated in State cybersecurity defense competitions. He attained the Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), and CREST Practitioner Security Analyst (CPSA) and CREST Registered Penetration Tester certifications.

## DeShaun Ormond, eJPT, eCPPT, OSCP

**Senior Consultant**

DeShaun is a cybersecurity professional with experience in education, financial industries, manufacturing, and the service industry, as well as with assisting clients with configuring their SIEM solution. Within Plante Moran's cybersecurity practice, DeShaun's area of focus is on penetration testing, vulnerability assessments, and social engineering. DeShaun holds a bachelor's degree in computer science from Coker College and a master's degree in computer networks and security from University of Essex. He has participated in various Capture the Flag (CTF) competitions, has obtained his eLearn Security Junior Penetration Tester, eLearn Security Certified Penetration Tester, and Offensive Security Certified Professional certification.

## Shayna Harbecke

### Senior Consultant

Shayna has almost 10 years of experience in various aspects of Information Technology ranging from hardware, software, networks, and administration to security. Her experience comes from the US Coast Guard where she held several different roles in the industry and has experience facing emerging security threats including the remediation processes required to mitigate them. Shayna earned her Master of Science in Cybersecurity Technology from the University of Maryland Global Campus, where she was able to supplement her experience with education on various policy management, procedure development, auditing, threat assessment, and hands-on security techniques. Her skills are now utilized for penetration testing, vulnerability assessments, and social engineering at Plante Moran. She is currently pursuing multiple Cybersecurity certifications and is committed to researching cybersecurity threats and vulnerabilities as they pose risks to various industries.

## Mícheál Sheridan

### Consultant

Mícheál joined the Plante Moran team in 2021 after receiving his B.S. in cybersecurity from Illinois State University and is currently pursuing multiple Cybersecurity certifications. While pursuing his degree, Mícheál worked in a network operations center at an internet service provider, gaining experience in tackling many of the networking and security issues that businesses face. Mícheál's area of focus at Plante Moran is on penetration testing, vulnerability assessments, and social engineering. He is committed to researching both existing and emerging cybersecurity threats and vulnerabilities that pose risks to various industries.

## Allen Allos, CISA

### Manager

Allen is a cybersecurity manager with over 9 years of experience in information security, IT compliance, and IT audit experience in several industries, including manufacturing and distribution, healthcare, private equity, and technology. Allen specializes in performing data mapping exercises for large organizations pertaining to privacy programs including GDPR and CPRA. Allen performs control assessments, drafts policies, performs security awareness trainings, and provides risk-based recommendations to assist clients in implementing cybersecurity best practices. Allen, He has experience performing information security audits to ensure clients fulfill compliance requirements, including SOC, PCI, ISO, SOX. Allen holds an M.S. in accounting, as well as a B.S. in aviation management and technology and a minor in general business from Eastern Michigan University. Allen is a Certified Information Systems Auditor (CISA).

**3.5 Vendor must comply with industry standards and compliance, namely the Penetration Testing Execution Standard (PTES), and follow a documented methodology to ensure consistent and thorough testing.**

**3.5.1 Vendor should provide with their bid, documentation of the industry standard and testing methodology leveraged and evidence of compliance.**

## Our methodology

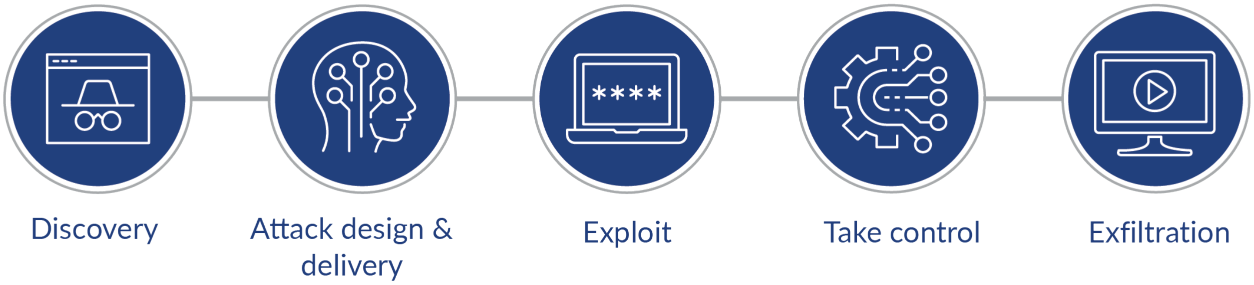
Our threat emulation methodology simulates various real-world threat scenarios against technical, physical, and social controls.

These threats range from external, non-knowledgeable “drive-by” attacks to targeted attacks by authorized, knowledgeable insiders. Using current threat intelligence, our cybersecurity specialists will work with State to identify specific targets and goals, and then launch controlled attacks from many common footholds, including:

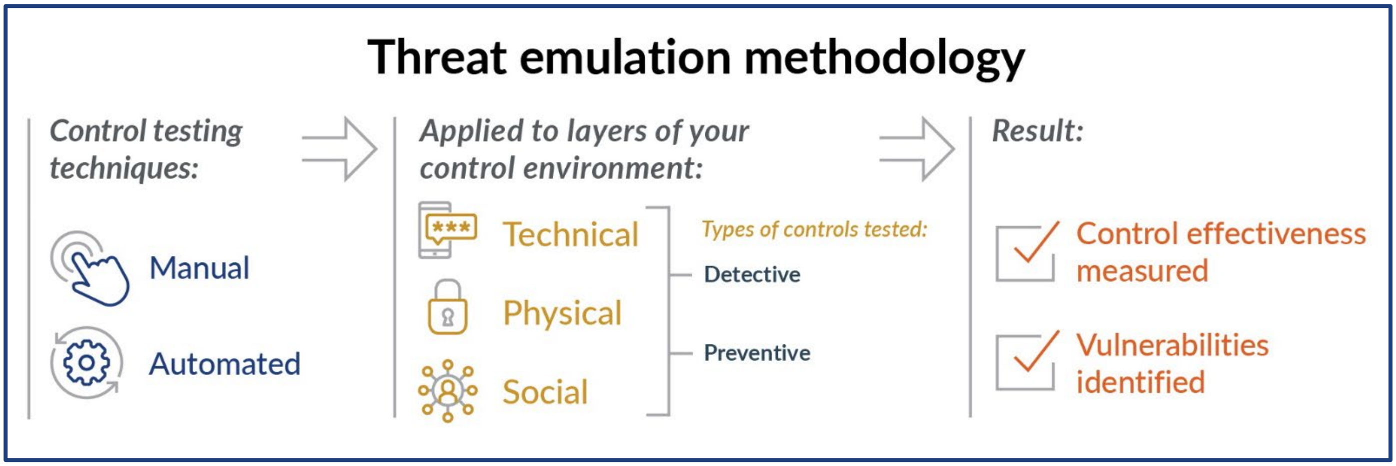
- network perimeter
- remote access
- unauthenticated and authenticated internal network access
- wireless access
- web-based applications
- physical access

### Testing your ability to identify and prevent attacks

Attackers approach organizations in their own unique way, yet all attacks consistently share the following five key components (otherwise known as the “attack chain”):



Using manual and automated techniques, our threat emulation methodology allows us to focus on testing not only your ability to prevent an attack, but also your ability to identify an attack during each of the five stages of the attack chain.


Threat emulation methodology
Control testing techniques:
Manual
Automated
Applied to layers of your control environment:
Technical
Physical
Social
Types of controls tested:
Detective
Preventive
Result:
Control effectiveness measured
Vulnerabilities identified

## Please note:

Our threat emulation methodology is modeled after the Penetration Testing Execution Standard (pentest-standard.org), and the Open Web Application Security Project (owasp.org). Both standards are designed to provide a common framework and scope for performing effective penetration testing and general security analysis. Our security testing uses these standards to provide repeatable quality of service based upon industry-leading standards and guidelines for our client base.

**3.6 Vendor should provide with their bid, an overview of the testing methodology with the proposed assessment plan and approach.**

**3.6.1 Vendors must meet or exceed the needs and expectations of the Lottery for each testing component.**

**3.6.2 Vendors must meet or exceed the general testing procedures that will be leveraged during each assessment.**

# Our proposed scope

When we perform a network penetration testing, we take a hands-on approach. Using information State provides via preliminary questionnaires and informal meetings with us, we'll develop a well-rounded understanding of the boundaries of your environment and the systems you already have in place. All of our work will include a prioritized list of remediation needs, requirements and associated risks.

## Network penetration testing and vulnerability assessments

- **External network penetration testing** simulates an attack from the internet using manual penetration techniques based on real-world threat intelligence. Testing will include reconnaissance (OSINT), foot-printing, enumeration, probing, and penetrating externally facing systems. Our objective is to identify and exploit vulnerabilities, gain control of targeted systems, escalate privileges, access sensitive data, and access the internal network from the internet. The timing of the assessment will be up to one (1) business week.
    - **Social Engineering Phishing Campaign:** The external network penetration testing includes a phishing exercise wherein Plante Moran will send emails that are designed to deceive the State's staff into clicking on a link or downloading a malicious document, and thereby (unintentionally and unknowingly) sharing sensitive data or passwords. Testing will then involve attempting to use such information to breach additional data and/or gain access to critical internal systems from the outside. The scope includes one (1) email scenario.
- **Internal network penetration testing** simulates an attack from inside the State (such as a rogue device) using manual penetration techniques based on real-world threat intelligence. Testing will include mapping out the network, enumerate systems and services/ports, attempt to obtain authenticated access, move laterally on the network, expand access, escalate privileges, and demonstrate exfiltrating data. Our objective is to identify and exploit vulnerabilities, gain control of targeted systems, obtain authenticated access, and escalate privileges to critical systems. Our testing can be performed remotely or onsite at all 8 locations including the main office location in 900 Pennsylvania Ave, Charleston, WV 25302. We estimate a total of 4 business days at each location to assess the State's internal network. This is assuming that networks from each of the 8 locations are only accessible from within those locations itself and there is no single point on the network with access to all network locations.

  Please note: The Internal Network Penetration Testing may be performed utilizing the following pre-determined network foothold assumptions:

    - Access from a physical network port without network credentials
    - Access from an authenticated workstation, simulating a trojan or successful phishing attack

  - Access or visibility of the entire network located throughout all 8 state locations from a single point within the network from where testing will be conducted.

- **Wireless penetration testing** simulates an attack on the wireless networks and infrastructure. Plante Moran will attempt to penetrate the State's in-scope wireless networks and devices, test the wireless signal pattern, physical installation of access points, rogue access point detection, system configuration, and wireless network segmentation. The wireless testing will be performed onsite within range of the Client's wireless networks at all 8 locations. We estimate a total of 2 business days at each location to assess the Client's wireless networks.
- **Website penetration testing** simulates an attack on in-scope web applications as an unauthenticated user. The purpose of this scenario is to identify if vulnerabilities exist within websites and web applications. This allows us to assess the security controls and secure coding in the web application itself as well as the host. The scope includes one (1) externally facing website. The timing of the assessment will be up to one (4) business days. In addition, we will perform automated vulnerability scans on both the web application and the hosts (e.g., WAF, web servers, databases etc.) for known flaws. At the completion of the automated scans, a review of all vulnerabilities detected will be validated to ensure that false positives are not included in the report.

  The Web Application Security Assessment primarily covers the OWASP Top Ten[1] vulnerability categories for web applications. Plante Moran's assessment also tests the Client's web application against portions of the CIS Critical Security Controls Top 20 list (formerly SANS). The assessment will include both manual and automated testing of the application and the host on which that application resides.
- **Network vulnerability assessments** involve performing vulnerability scans on the external and internal network including the wireless infrastructure to identify missing patches and common misconfigurations. Upon completion of the scanning, we analyze the results and summarize the critical and high vulnerabilities identified. Scanning will include the population of devices provided by management during our risk planning discussions at the beginning of our project.

## Project assumptions

- This is a point-in-time security assessment of State. It's possible for new vulnerabilities to arise daily, which could alter the state of State's vulnerability exposure. Monitoring and assessing information security should be processes that State performs on a proactive and ongoing basis. Prior to conducting the technical security assessment portion of this project, we will require management to sign and return an authorization letter on company letterhead permitting us to access its network, systems, and data.
- Any outsourced services or devices (outside the direct control of the State) will not be included in this engagement unless State obtains permission from these providers prior to our on-site review. We recommend management (as part of their vendor risk management process) contact any third-party providers responsible for hosting and/or managing these devices and obtain the results from their most recent penetration test and/or web application security assessment (if we are not granted permission to perform the testing).
- Our testing approach for each phase is time-based and can be performed remotely. To facilitate this testing, we will ship a small PC installed with our suite of penetration testing tools. This PC will be

[1] The Open Web Application Security Project (OWASP) is a worldwide open community focused on improving the security of application software. OWASP's mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. The OWASP Top Ten provides awareness for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

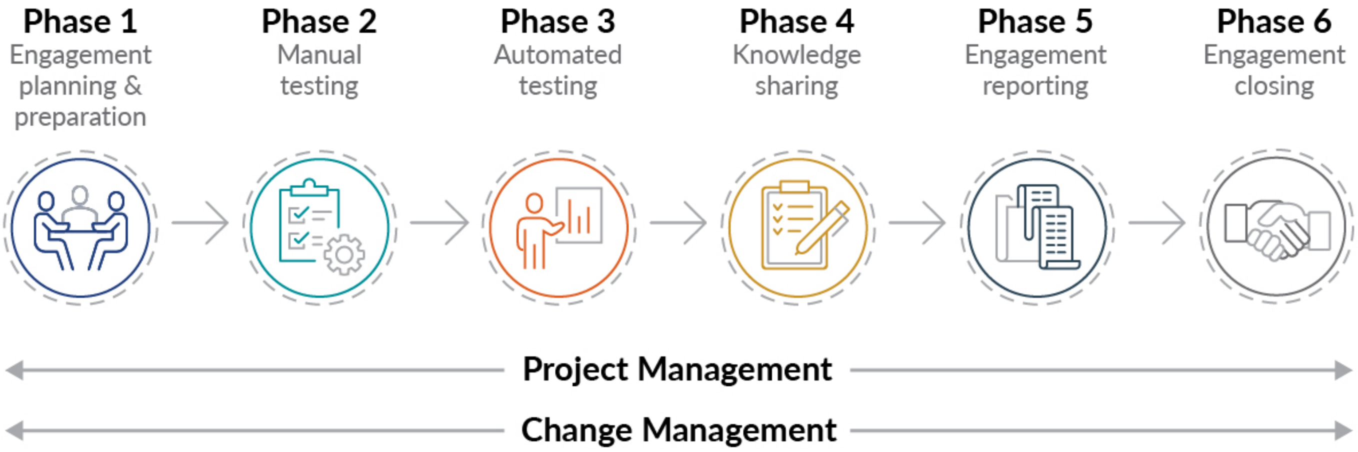
installed on State’s internal network with the help of the IT team. The device will connect to a server within our Cyber Lab that will be specifically configured for the engagement with applied access restrictions. At the completion of the engagement, the device will be sent back to us by State. Should the device not be returned or be returned damaged, State may be held responsible for the cost of replacement. Alternatively, we can configure a virtual machine to function in the same manner; this would require State to install a hypervisor of our choosing and run the virtual machine on the hypervisor.

- Plante Moran reserves the right to reschedule any phase of the scope if the requested items are not provided by the Client in the appropriate amount of time before the engagement is scheduled to begin.

## Penetration testing approach and workplan phases

Our technical information security projects are governed by a standard workplan that facilitates client communication, coordination, and collaboration throughout each phase of the engagement. This phased workplan controls the overall progression of the project, allowing us to build momentum and synergy into each project phase. We’ve combined this workplan with our threat emulation methodology to create a framework that delivers valuable results, customized to State, void of false positives, with both executive and technical messaging supported by practical recommendations for remediation.

**Our proposed project for State will be organized into the following six project phases:**



**Phase 1** Engagement planning & preparation

**Phase 2** Manual testing

**Phase 3** Automated testing

**Phase 4** Knowledge sharing

**Phase 5** Engagement reporting

**Phase 6** Engagement closing

**Project Management**

**Change Management**

### Benefits that differentiate Plante Moran’s approach

Our main area of focus is on manual testing techniques (Phase 2), where we tend to find significant issues that typically go unnoticed/unreported by firms that rely too heavily on tool output to drive the focus of their reviews. Other unique advantages of our phased approach include knowledge-sharing throughout each phase of our review, coupled with ongoing advice, training, and year-round availability for each of the entities under review. We are not limited by project timelines; our team-oriented goal is to provide ongoing support and open relationships.

## **Phase 1:** Engagement planning and preparation

### 1.1 Project initiation and planning

Project initiation is key to the overall success of the engagement. Our activities will include the following:

- Reconfirm engagement assessment goals and objectives, scope, logistics, and timing
- Introduce our Plante Moran team
- Confirm project sponsor(s) and identify key project stakeholders
- Establish project collaboration portal for securely sharing documents and deliverables
- Discuss and validate the format for project deliverables
- Conduct kickoff meeting

### 1.2 Identify areas for testing

Working with State, we will perform a preliminary risk analysis and identify areas for penetration testing. We will also ask to review any prior testing results, policies, procedures, and other documentation that will assist in our testing efforts.

### 1.3 Develop project plan and organizational structure

Our approach is flexible to provide the services and level of professional support required to meet your individual needs for this engagement. We will work jointly with your project manager to develop and finalize a plan to meet the objectives and established timelines. During the early stages of the project, we suggest creating a cross-functional group of representatives from essential departments to be involved in the project and provide overall governance. We find that this collaborative approach creates a high probability of success.

### 1.4 Develop rules of engagement

We will develop a “rules of engagement” document, including detailed guidelines and constraints regarding the penetration testing execution. This document will define the scope, guidelines, and constraints for each engagement, and will be approved by State. This document will be approved prior to any testing.

### 1.5 Status reporting/communication

Throughout the testing process, we will provide frequent updates on the results and findings. If critical findings are uncovered, we will immediately communicate them to State. Formal status reporting will be provided on a weekly basis during the testing activity.

Open communication is key to a successful implementation, as it allows problems to be addressed early on or avoided entirely. This minimizes wasted effort and keeps the project on track. We will schedule weekly meetings and/or conference calls with you to:

- Report on the status of the project workplan and timeline
- Reschedule tasks as necessary
- Discuss major open issues/risks and develop strategies to address them
- Review next steps

## Phase 2: Manual testing

During this project phase, we will test the ability to prevent and/or identify an ongoing attack. This is accomplished through a targeted attack simulation initiated from specific attack vectors. Our objectives are to help State:

- Test existing controls and processes to identify a targeted attack. We will work with State to define attack vectors against the IT infrastructure.
- Obtain an understanding of your ability to detect and effectively respond to an attack.
- Obtain an understanding of State's ability to hinder an attacker from obtaining confidential or sensitive data (PII, financial, member/partner, employee, cardholder, etc.).
- Understand the effectiveness of attack scenarios modeled after real-world threat intelligence.

As part of our activities, we will perform penetration testing of your networks and systems. Our penetration testing follows industry-standard approaches, including CREST, PTES, ISSAF, MITRE, NIST, and OWASP.

At the conclusion of this phase, you'll have a fuller picture of the existing weaknesses in State's current network architecture and implemented technologies.

## Phase 3: Automated testing

The purpose of this project phase is to test the effectiveness of your vulnerability and patch management programs against known vulnerabilities. Our overall objective is to help State:

- Identify known vulnerabilities currently present within your environment
- Obtain an understanding of the implications of the vulnerabilities identified
- Where possible, without causing disruption, validate scan results
- Provide a filtered end-product, which helps management prioritize their remediation efforts
- Assess State's current patch management levels

### 3.1 Vulnerability scanning

We'll help you identify known and detectible vulnerabilities present in both the external and internal network infrastructure. Vulnerability scanning is performed on servers, workstations, web-based applications, and other general devices to provide management with an understanding of the exposure to preventable security flaws.

We will use various automated vulnerability scanners. These tools are configured to not cause system disruptions or degradation of service. However, we cannot control how your information systems are affected by the scans. We will discuss the specific tools we will use and the timing for running the tests to minimize any potential impact with your technology department.

### 3.2 Validation and prioritization of results

This phase will include an assessment of the vulnerability scanning results. We will assist State with validating, filtering, and prioritizing the scan output, as well as eliminating false positives.

Raw vulnerability scan output often contains superfluous levels of detail; we'll help you cut through any unnecessary or redundant data to present a clear picture of the results that are relevant to State. Management will receive details on any known vulnerabilities that we believe pose a significant risk to the selected systems; these vulnerabilities will be candidates for focused remediation.

While the output of our review will be filtered to highlight critical, high, and moderate issues, we will also provide the exhaustive raw scan output, in the event management would like to review all issues identified by our vulnerability scanning tools during our assessment.

## Phase 4: Knowledge-sharing

The purpose of this project phase is to provide State's technical team with a detailed step-by-step dissection of our attack methodology, key learning points, and live demonstrations of select activities and exploitation performed during project execution.

This phase will provide a non-threatening environment for State's staff to engage in open and honest technical discussions about the issues identified in our assessment. Our goal is to build a clear understanding of the constraints and current strategies that led to the results of our assessment. We'll also confirm our own understanding of the potential impact of issues identified and provide strategies for remediation. At the end of the engagement, we'll provide a separate, executive-level meeting to discuss the results of the technical exit and other phases of our assessment.

We will clean up after the testing is completed and ensure that the State environment is not impacted. Clean-up activities can include, but are not limited to (where applicable):

- Update and/or remove test accounts added or modified during testing
- Update and/or remove database entries added or modified during testing

- Uninstall test tools or other artifacts (if applicable)
- Restore security controls that have been altered for testing (if applicable)
- Provide State with necessary information and/or guidance on how to verify that environments have been restored
- Provide State with confirmation that the environments have been cleaned and restored

## **Phase 5:** Engagement reporting

We will provide a written report to management containing our recommendations. This report will be discussed in draft with management, and we will incorporate your feedback into the final report.

### 5.1 Compile recommendations and prepare draft report

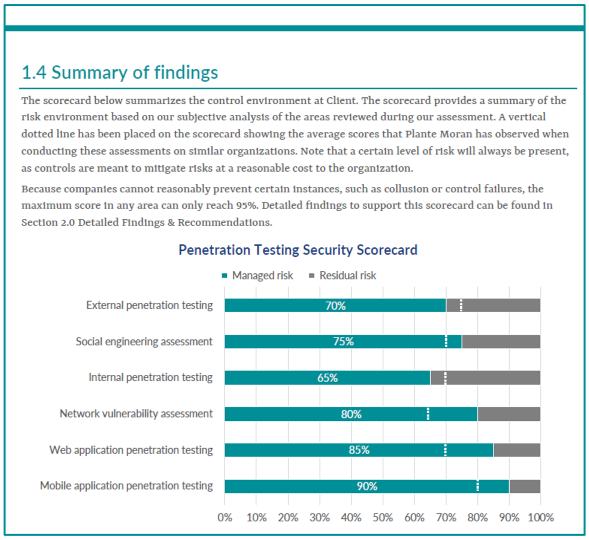
Based on testing performed, we will compile our recommendations to be considered for remediation. However, please note that we will also communicate our observations throughout the course of the engagement, to ensure there are no late-breaking surprises or any misunderstandings related to discussions or documentation.

The observations and recommendations discussed previously will be translated into a draft report that will include the following:

- Executive summary, with clear, concise, and easy-to-understand descriptions of managed and residual risks
- Scope (including limitations/constraints), objectives, and goals
- Detailed and repeatable description of each attack vector with a risk ranking for severity
- Proof-of-concept screenshots of vulnerabilities and exploits identified
- Recommendations and opportunities for improvement and remediation
- Supporting appendices (methodology, tools used, etc.)

Our deliverable will also include a prioritized list of risk items for management’s consideration of risk administration (i.e., risk transfer, avoidance, acceptance, or remediation).

Sample screenshots from our deliverables are included below:



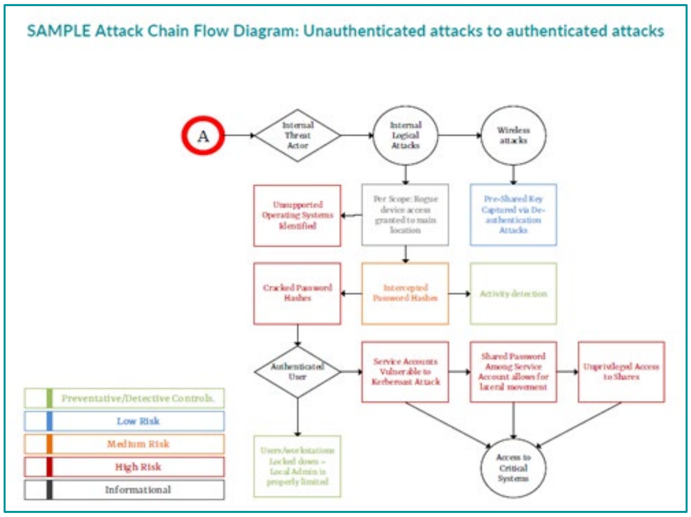
## 1.4 Summary of findings

The scorecard below summarizes the control environment at Client. The scorecard provides a summary of the risk environment based on our subjective analysis of the areas reviewed during our assessment. A vertical dotted line has been placed on the scorecard showing the average scores that Plante Moran has observed when conducting these assessments on similar organizations. Note that a certain level of risk will always be present, as controls are meant to mitigate risks at a reasonable cost to the organization.

Because companies cannot reasonably prevent certain instances, such as collusion or control failures, the maximum score in any area can only reach 95%. Detailed findings to support this scorecard can be found in Section 2.0 Detailed Findings & Recommendations.

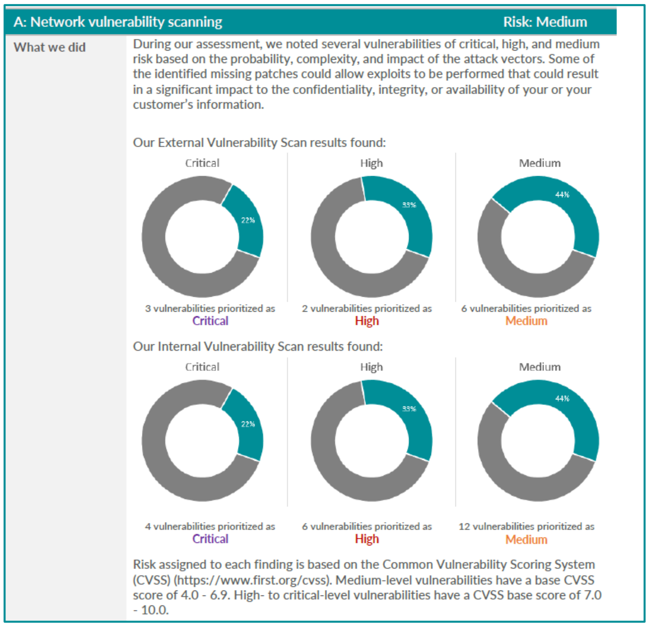
Penetration Testing Security Scorecard

■ Managed risk
■ Residual risk
External penetration testing
70%
Social engineering assessment
75%
Internal penetration testing
65%
Network vulnerability assessment
80%
Web application penetration testing
85%
Mobile application penetration testing
90%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

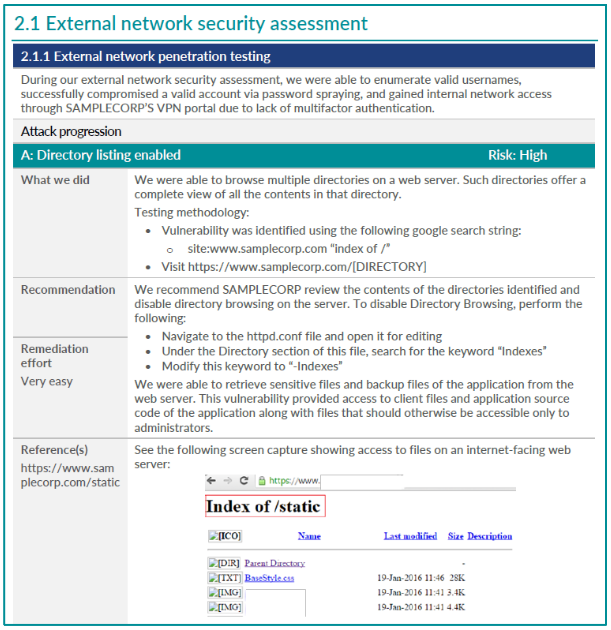


SAMPLE Attack Chain Flow Diagram: Unauthenticated attacks to authenticated attacks

A
Internal Threat Actor
Internal Logical Attacks
Wireless attacks
Unsupported Operating Systems Identified
Per Scope: Rogue device access granted to main location
Pre-Shared Key Captured via De-authentication Attacks
Cracked Password Hashes
Intercepted Password Hashes
Activity detection
Authenticated User
Service Accounts Vulnerable to Kerberoast Attack
Shared Password Among Service Account allows for lateral movement
Unprivileged Access to Shares
Users/workstations Locked down – Local Admin is properly limited
Access to Critical Systems
Preventative/Detective Controls
Low Risk
Medium Risk
High Risk
Informational



| A: Network vulnerability scanning | Risk: Medium |
|---|---|
| What we did | During our assessment, we noted several vulnerabilities of critical, high, and medium risk based on the probability, complexity, and impact of the attack vectors. Some of the identified missing patches could allow exploits to be performed that could result in a significant impact to the confidentiality, integrity, or availability of your or your customer's information.<br>Our External Vulnerability Scan results found:<br>3 vulnerabilities prioritized as Critical · 2 vulnerabilities prioritized as High · 6 vulnerabilities prioritized as Medium<br>Our Internal Vulnerability Scan results found:<br>4 vulnerabilities prioritized as Critical · 6 vulnerabilities prioritized as High · 12 vulnerabilities prioritized as Medium<br>Risk assigned to each finding is based on the Common Vulnerability Scoring System (CVSS) (https://www.first.org/cvss). Medium-level vulnerabilities have a base CVSS score of 4.0 - 6.9. High- to critical-level vulnerabilities have a CVSS base score of 7.0 - 10.0. |



## 2.1 External network security assessment

### 2.1.1 External network penetration testing

During our external network security assessment, we were able to enumerate valid usernames, successfully compromised a valid account via password spraying, and gained internal network access through SAMPLECORP'S VPN portal due to lack of multifactor authentication.

Attack progression

| A: Directory listing enabled | Risk: High |
|---|---|
| What we did | We were able to browse multiple directories on a web server. Such directories offer a complete view of all the contents in that directory.<br>Testing methodology:<br>• Vulnerability was identified using the following google search string:<br>○ site:www.samplecorp.com "index of /"<br>• Visit https://www.samplecorp.com/[DIRECTORY] |
| Recommendation | We recommend SAMPLECORP review the contents of the directories identified and disable directory browsing on the server. To disable Directory Browsing, perform the following:<br>• Navigate to the httpd.conf file and open it for editing<br>• Under the Directory section of this file, search for the keyword "Indexes"<br>• Modify this keyword to "-Indexes" |
| Remediation effort<br>Very easy | We were able to retrieve sensitive files and backup files of the application from the web server. This vulnerability provided access to client files and application source code of the application along with files that should otherwise be accessible only to administrators. |
| Reference(s)<br>https://www.samplecorp.com/static | See the following screen capture showing access to files on an internet-facing web server: |

https://www.

**Index of /static**

```
[ICO]   Name              Last modified      Size  Description
[DIR]   Parent Directory                      -
[TXT]   BaseStyle.css     19-Jan-2016 11:46  28K
[IMG]                     19-Jan-2016 11:41  3.4K
[IMG]                     19-Jan-2016 11:41  4.4K
```

### 5.2 Prepare final information security assessment deliverable

After receiving your feedback on the draft report, we will update the reports and share them as a final deliverable. In addition to delivering the final reports in electronic and hard copies, we will also be available to present the reports via teleconference/webinar to any applicable management or committee member(s).

## Phase 6: Engagement closing

At the conclusion of the project, we will officially close out the engagement with the sponsor, prepare final billings, discuss document return and retention, terminate the SharePoint portal access, and request your feedback via our client satisfaction survey.

# Security testing tools

The use of automated tools allows us to provide a consistent and efficient execution of security tests. These tools have been widely recognized and proven to be effective in the information security industry. Our vendor-based toolkit includes a large compilation of automated tools and applications. Our tools are updated regularly and represent the most current technologies available.

We deploy tools either on Windows operating systems or using the Kali Linux penetration testing platform.

| PURPOSE / CATEGORY | TOOLS USED | | | |
|---|---|---|---|---|
| **Information gathering** | DumpSec<br>enum4linux | fierce<br>Masscan | Nmap<br>Sublist3r | theHarvester |
| **Vulnerability analysis** | Nessus | | | |
| **Exploitation tools** | Armitage<br>BeEF<br>Cobalt Strike | CrackMapExec<br>Empire<br>ExploitDB | Impacket<br>Metasploit Framework | SET<br>Snarf |
| **Maintaining access** | Ncat<br>PowerSploit | PsExec | Weevely | winexe |
| **Sniffing and spoofing** | bettercap<br>Cain and Abel | mitmproxy<br>ngrep | NetworkMiner<br>Responder | tcpdump<br>Wireshark |
| **Password attacks** | gpp-decrypt<br>hash-identifier | hashcat<br>HexorBase | Mimikatz<br>THC-Hydra | John the Ripper<br>wordlists |
| **Wireless attacks** | aircrack-ng package | hostapd-wpe<br>Reaver | Wifiphisher | Wifite |
| **Web applications** | Burp Suite<br>DirBuster | DotDotPwn<br>Gobuster | Nikto<br>sqlmap | W3A<br>WebScarab |

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

## Background checks

Plante Moran will comply with fingerprint and background check verification of staff working on the project.  For your information, Plante Moran performs rigorous background checks on new staff. The following practices are used:

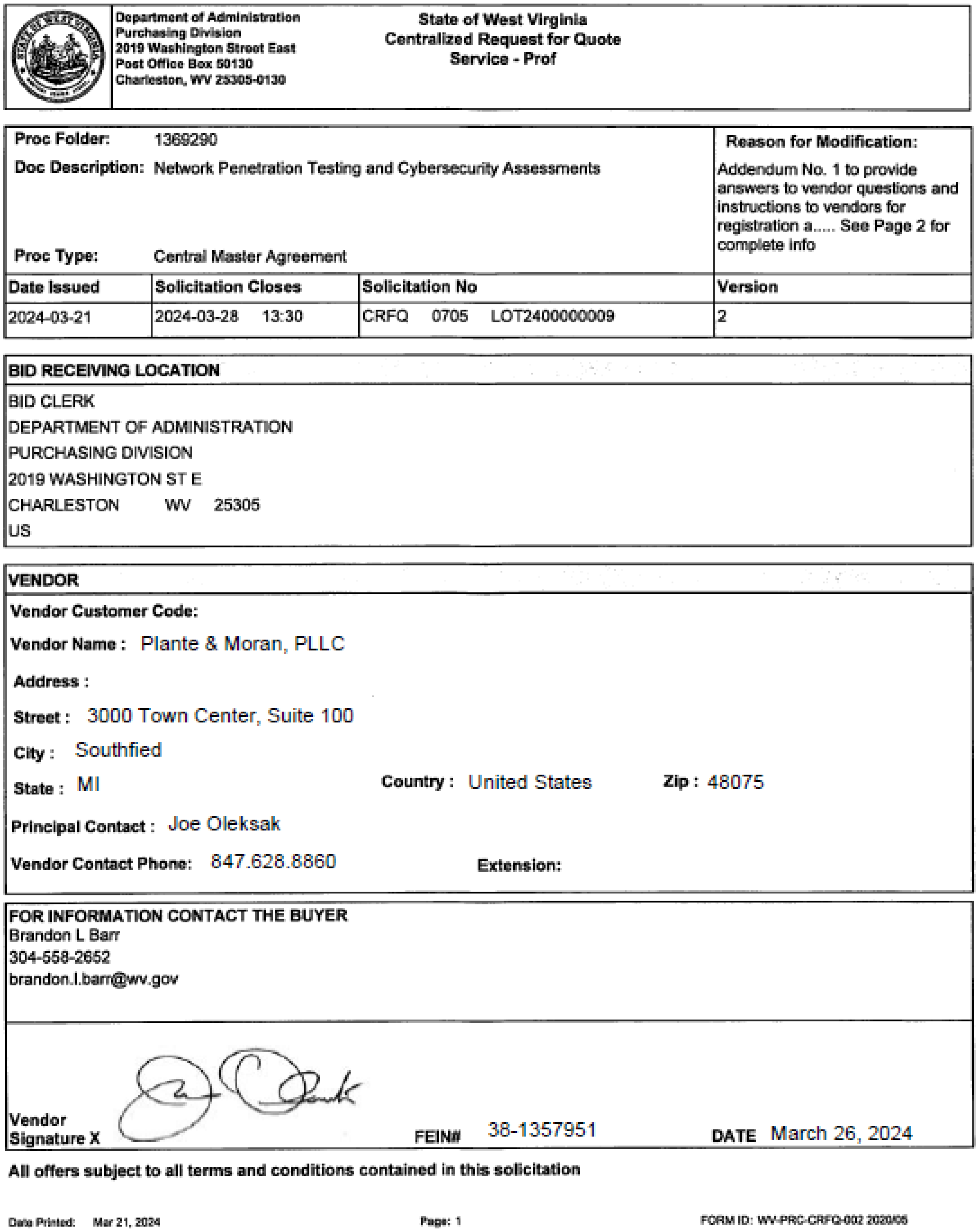
- County Criminal Felony and Misdemeanor – all counties lived & worked
- County Civil Upper – all counties lived & worked
- National Federal Criminal Search
- Pre-Employment Credit History
- Employment Verification – In-Depth or Professional
- Education Verification
- Driver’s History Report
- Professional License Verification
- Multi-Jurisdictional Index Search
- Social Security Trace Report

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

## Non-Disclosure Agreement (NDA)

Plante Moran will comply with executing the NDA if selected as the preferred vendor and prior to contract engagement.

# Addendum Acknowledgement



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

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

**Proc Folder:** 1369290

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

**Proc Type:** Central Master Agreement

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

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

**BID RECEIVING LOCATION**

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

**VENDOR**

**Vendor Customer Code:**

**Vendor Name :** Plante & Moran, PLLC

**Address :**

**Street :** 3000 Town Center, Suite 100

**City :** Southfied

**State :** MI **Country :** United States **Zip :** 48075

**Principal Contact :** Joe Oleksak

**Vendor Contact Phone:** 847.628.8860 **Extension:**

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

**Vendor Signature X** **FEIN#** 38-1357951 **DATE** March 26, 2024

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

Date Printed: Mar 21, 2024 Page: 1 FORM ID: WV-PRC-CRFQ-002 2020/05

# Appendix

# Additional firm information

## Structured differently — to serve you differently

Our “one-firm” firm philosophy is a unifying structure that prioritizes client service over maximizing profits. Unlike other accounting firms, we don’t have office-level profit centers, meaning our offices don’t compete. What does that mean for you? It means you receive the collective power of the firm and the expertise you need regardless of location. The result: seamless service, a personal touch, and future-focused thinking.

### Seamless service

One touchpoint with us will give you unfiltered access to the right experts, at the right time.

### Personal touch

The better we know you, the better we can serve you. We build lasting relationships to foster a client-focused, collaborative culture.

### Future-focused

Your future is our priority. We partner with you to ensure you to achieve your goals today and beyond.

## Plante Moran benefits and strengths

The following table provides an overview of the benefits you will experience by working with Plante Moran:

| State’s needs | Benefits you will experience |
|---|---|
| Industry experience | • Help meeting your information security goals and objectives by discussing industry risks and solutions<br>• Hand-picked team members who are best equipped with the skillsets suitable for serving government clients<br>• Year-round thought leadership on cybersecurity risk management and compliance via seminars, webinars, publications, podcasts, legislative updates, and alerts |
| Efficient approach | • Tailored processes based on a strong understanding of the unique cyber risks facing government clients<br>• Proactive communication, planning, technical expertise, and significant senior-level involvement to ensure your engagement is delivered on time and within the scope |

| | |
|---|---|
| Client-focused service | • Service orientation that places your needs ahead of our own<br>• Diverse, expert, and well-rounded thinking to solve your challenges and complex issues<br>• Superior client satisfaction according to the scoring methodology of the American Customer Satisfaction Index (ACSI) and your peers, who rate Plante Moran above the world's best client service companies, including Apple and Amazon |
| Flexible, proactive solutions | • Direct access to our firm's best resources for your specific needs regardless of geographic location, because we operate without office-level profit centers (i.e., "one-firm" firm approach)<br>• Forward-thinking perspective that keeps you abreast of upcoming developments<br>• Wide range of in-house capabilities with an ability to consult on large and small projects and scale our approach to your specific needs |

## Customer service & client satisfaction- the Plante Moran way

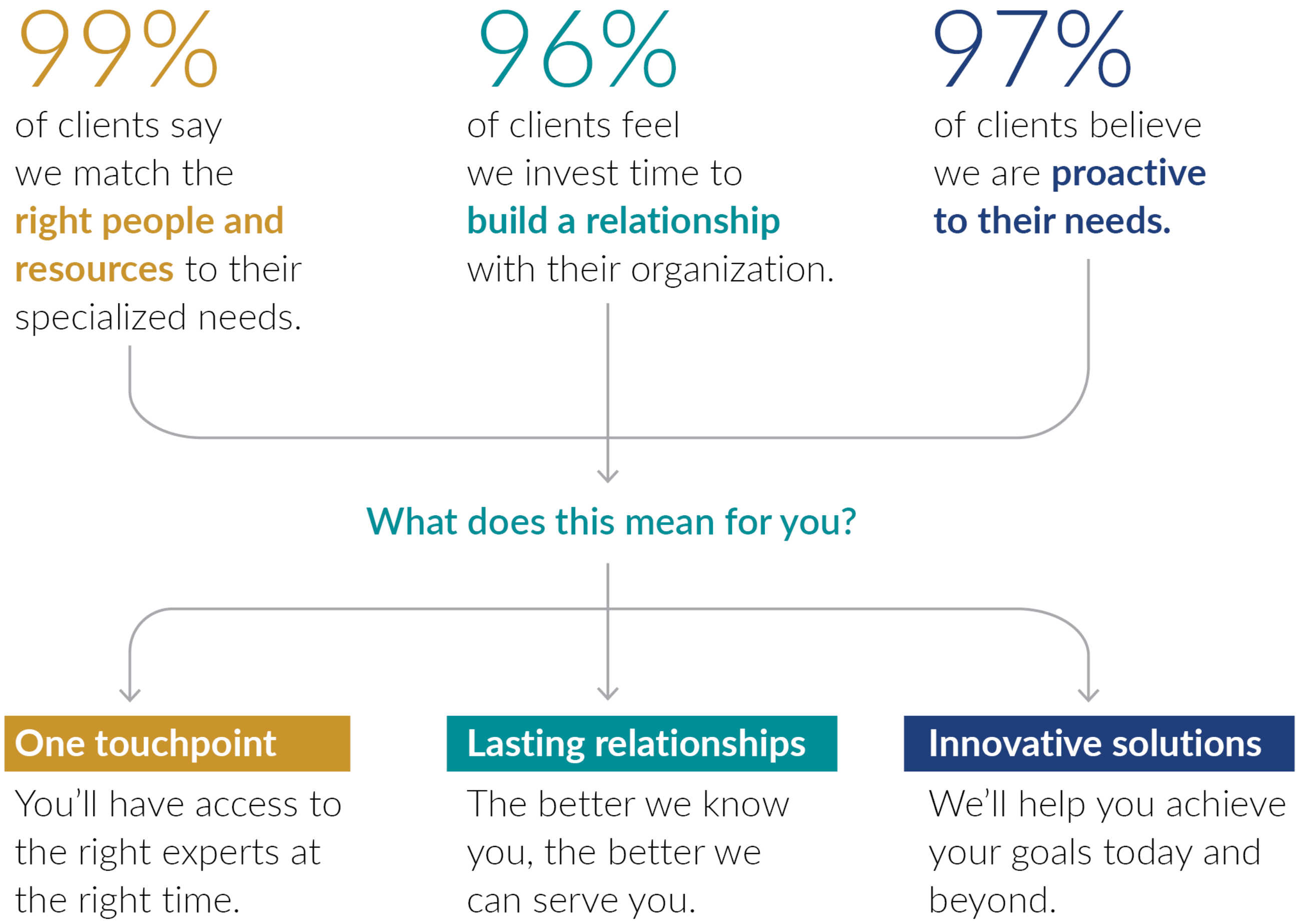
When clients engage Plante Moran as their advisor, they say they can feel the difference almost immediately. Whether it is an innovative approach to problem-solving, our collaborative culture, or solutions borne out of deep industry expertise, our clients benefit from an attentive advisor who brings a caring approach to each engagement.

Here are a few considerations that make Plante Moran different and help assure that we provide responsive service to our clients:

- **Low staff turnover**: We have the lowest staff turnover rate of any major accounting firm in the United States. By minimizing turnover, we can provide better staff continuity, which in turn makes sure that our teams are organized, prepared, and not slowed down by on-the-job learning.
- **More senior-level involvement**: Our staffing mix involves a high degree of partner and senior manager-level involvement in our engagements who are knowledgeable about different disciplines. This provides you with diverse, expert, and well-rounded thinking to solve your increasingly difficult day-to-day challenges and complex issues.
- **Flexibility and experience**: Our deep experience in working with clients of all sizes and ownership structures allows us to acclimate to your organizational environment quickly.
- **Communication**: We consider communication is the key to a successful relationship. Our clients tell us that we regularly exceed their expectations because we take ownership of that requirement. Regular communication avoids surprises, keeps projects on track, and promotes a healthy relationship.
- **Commitment**: We listen upfront to what you need, and we deliver. On-time and what you requested. We meet the promises we make. This is the number one thing that business executives tell us they want when we ask them what is important when hiring a professional service company, and we aim to meet their needs.

## Client satisfaction

At Plante Moran, we know we haven't done our job unless you're confident in our value. We enlist an independent third party to conduct an ongoing survey program that collects feedback from our clients. This tool allows us to identify areas of satisfaction or dissatisfaction so we can reinforce the good and quickly correct any areas of concern. The results of each client satisfaction survey are reviewed by firm management. We're gratified that our clients love us, and we work hard to keep it that way, but, as a prospective client, you deserve to see the numbers for yourself.



99%

of clients say we match the **right people and resources** to their specialized needs.

96%

of clients feel we invest time to **build a relationship** with their organization.

97%

of clients believe we are **proactive to their needs.**

What does this mean for you?

**One touchpoint**

You'll have access to the right experts at the right time.

**Lasting relationships**

The better we know you, the better we can serve you.

**Innovative solutions**

We'll help you achieve your goals today and beyond.

## Proposed contract exceptions

| Page | Section/reference | Proposed exception | Rationale |
|---|---|---|---|
| 11 | 1 | ***Please Modify as Follows:***<br>Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract, subject to the exceptions in the Vendor's bid. | Plante Moran can agree that its signature signifies its agreement to be bound subject to the exceptions in its bid. |
| 16 | 12 | ***Please Modify as Follows:***<br>**ACCEPTANCE:** Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated by the exceptions in its bid. | Plante Moran can agree that its signature signifies its agreement to be bound subject to the exceptions in its bid. |
| 19 | 12 | ***Please Modify as Follows:***<br>**CANCELLATION:** The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Vendor may cancel this Contract, if the State does not comply with any of its obligations under this Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules§ 148-1-5.2.b. | Plante Moran would like the cancellation rights to be reciprocal. |
| 17 | 22, first paragraph | ***Please Modify as Follows:***<br>**COMPLIANCE WITH LAWS:** Vendor shall comply with ~~all applicable~~ federal, state, and local laws, regulations and ordinances, in each case that apply to Vendor. ~~By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.~~ | |
| 28 | 30 | ***Please Modify as Follows:***<br>**PRIVACY, SECURITY, AND CONFIDENTIALITY:** The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or | Plante Moran would like to clarify that this section applies to such information that is disclosed by the Agency to the Vendor for the performance of |

| Page | Section/reference | Proposed exception | Rationale |
|---|---|---|---|
|  |  | other confidential information ~~gained from~~ disclosed by the Agency to the Vendor for the performance of the services under this Contract, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. ~~Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in www .state. wv. us/admin/purchase/privacy.~~ Confidential information does not include information that is publicly available at the time of disclosure or becomes publicly available after disclosure; information that is already known to Vendor; information received from a third party not known by Vendor to owe a duty of confidentiality to the Agency as to that information; or information that is independently developed by Vendor without using information disclosed by the Agency for the performance of services under this Contract. | the services under this contract.<br>Plante Moran does not agree to comply with client policies.<br>Plante Moran would like to include the indicated exceptions to what is considered confidential information. |
| 19 | 34 | ***Please Modify as Follows:***<br>**VENDOR NON-CONFLICT:** ~~Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which~~ Vendor will not enter into any professional services relationships with other clients that would ~~compromise~~ materially and adversely impact its objectivity in the performance of its services hereunder. ~~Any such interests shall be promptly presented in detail to the Agency.~~ | The conflict language as written is too broad. |
| 20 | 35, second paragraph | ***Please Modify as Follows:***<br>Delete this section in its entirety. | Plante Moran does not agree to this indemnification. |
| 20 | 36 | ***Please Modify as Follows:***<br>**INDEMNIFICATION:** The Vendor agrees to indemnify~~, defend, and hold harmless~~ the<br>State and the Agency, their officers, and employees from and against~~: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data~~ | Plante Moran can agree to indemnify the Agency in proportion to Plante Moran's fault, if any. |

| Page | Section/reference | Proposed exception | Rationale |
|---|---|---|---|
| | | ~~used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe; State and Federal laws including, but not limited to, labor and wage and hour laws~~ liability, damages, losses, and costs incurred, in each case to the extent caused by the gross negligence or willful misconduct of the Vendor in the performance of the services under this Contract. | |
| 20 | 38 | ***Please Modify as Follows:***<br>**CONFLICT OF INTEREST:** Vendor~~, its officers or members or employees,~~ shall not ~~presently have or acquire an interest, direct or indirect, which~~ enter into any professional services relationship with other clients that would ~~conflict with or compromise~~ materially and adversely impact its objectivity in the performance of its obligations hereunder. ~~Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.~~ | The conflict language as written is to broad. |
| 21 | 39, first checked box | ***Please Modify as Follows:***<br>Such reasonable reports as the Agency and/or the Purchasing Division may reasonably request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc. | Plante Moran would like to add reasonableness qualifiers. |
| 21-22 | 41 and 42 | ***Please Modify as Follows:***<br>Delete these sections in their entirety. | These sections do not apply given the nature of the professional services to be provided. |
| 24 | Certification and Signature | ***Please Modify as Follows:***<br>**CERTIFICATION AND SIGNATURE:** By signing below, or submitting documentation through wvOASIS, I, on behalf of the Vendor, certify that: I, on behalf of the Vendor, have reviewed this Solicitation/Contract in its entirety; that ~~I~~the Vendor understands 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 | This certification should be on behalf of the Vendor. |

| Page | Section/reference | Proposed exception | Rationale |
|---|---|---|---|
| | | 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~~ in the exceptions noted in its bid, offer, or proposal; that ~~I am~~ the Vendor 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~~ the individual signing on behalf of the Vendor is 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~~ and is authorized to bind the ~~v~~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. | |
| 34 | 10.1.3 | ***Please Modify as Follows:***<br>Failure to comply with any laws, rules, and ordinances applicable to the ~~Contract Services provided under this Contract~~ Vendor. | Plante Moran can agree that an event of default can be its failure to comply with laws applicable to it. |
| | Exhibit B, first "Whereas" clause | ***Please Modify as Follows:***<br>WHEREAS, the parties to this Agreement may wish to exchange certain information related to the provision of certain ~~information or communication technology~~ professional services by one party of interest to the other party; and | Plante Moran would be providing professional services. |
| 36 | Fourth paragraph | ***Please Modify as Follows:***<br>NOW THEREFORE, in order to protect certain Confidential Information that may be disclosed between the parties, Lottery and ~~Alpha~~ party of the second part agree to maintain the confidentiality of the Confidential Information as follows: | "Alpha" is not a defined term. |
| 36 | Exhibit B, I, opening clause | ***Please Modify as Follows:*** | Plante Moran would like to clarify that the information covered by this definition is that which is disclosed for the |

| Page | Section/reference | Proposed exception | Rationale |
|---|---|---|---|
| | | **Definition of Confidential Information.** The term "Confidential Information" ~~disclosed under~~ as used in this Agreement is defined as follows:<br>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 by the disclosing party to the receiving party for the performance of the services under the Contract to which this Exhibit B is attached, including, but not limited to: | performance of the services under the underlying contract to which this exhibit is attached. |
| 36 | Exhibit B, I | ***Please Modify as Follows:***<br>Add the following text after the end of the section:<br>Confidential information does not include information that is publicly available at the time of disclosure or becomes publicly available after disclosure; information that is already known to Vendor; information received from a third party not known by Vendor to owe a duty of confidentiality to the Agency as to that information; or information that is independently developed by Vendor without using information disclosed by the Agency for the performance of services under the contract to which this Exhibit B is attached. | Plante Moran would like to add the indicated exceptions to the definition of "Confidential Information". |
| 37 | Exhibit B, III | ***Please Modify as Follows:***<br>**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.~~ providing or receiving the professional services under the contract to which this Exhibit B is attached. | Plante Moran would like to clarify that the use of Confidential Information is for the providing or receiving of its professional services. |
| 37 | Exhibit B, V, (b) | ***Please Modify as Follows:***<br>(b) is a matter of public knowledge at the time of disclosure; or becomes a matter of public knowledge after disclosure other than through ~~no fault of~~ disclosure in violation of this Agreement by the recipient; | |
| 37 | Exhibit B, VII | ***Please Modify as Follows:***<br>**Export Administration.** Each party to this Agreement agrees to comply fully with ~~all~~ | Plante Moran would like to clarify that this obligation is for each party to comply with |

| Page | Section/reference | Proposed exception | Rationale |
|---|---|---|---|
| | | ~~relevant~~ export laws and regulations of the United States and other countries, in each case that are applicable to that party ~~to assure that no Confidential Information or any portion thereof is exported, directly or indirectly, in violation of such laws~~. | export laws and regulations that apply to the applicable party. |
| 38 | Exhibit B, IX, last sentence | ***Please Modify as Follows:***<br>~~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.~~ | The purpose and meaning of this sentence are not clear. |

We look forward to working with you.
Please contact us with any questions.

Joe Oleksak
Engagement Partner
847-628-8860
joe.oleksak@plantemoran.com

According to our recent client satisfaction survey,

**98%**

of clients say they **would recommend Plante Moran.**

plante moran | Audit. Tax. Consulting.
Wealth Management.

**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:** Furney Brown
**Telephone Number:** 248.223.3396
**Fax Number:** 248.223.7533
**Email Address:** furney.brown@plantemoran.com

**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) Joe Oleksak, Partner

(Address) 3000 Town Center, Suite 100, Southfield, MI 48075

(Phone Number) / (Fax Number) 847.268.8860

(email address) joe.oleksak@plantemoran.com

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

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

Plante & Moran, PLLC
(Company)

(Signature of Authorized Representative)

Joe Oleksak, Partner March 26, 2024
(Printed Name and Title of Authorized Representative) (Date)

847.628.8860
(Phone Number) (Fax Number)

joe.oleksak@plantemoran.com
(Email Address)

# 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 _Plante & Moran, PLLC_______________, with its principal offices located at _3000 Town Center, Southfield, MI 48075_______ (“Party of the second part”), with an Effective Date of _~March 26,2024_________. 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

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

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

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

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

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

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

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

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

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

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

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

**WEST VIRGINIA LOTTERY**

By: ________________________________

Name: ______________________________

Title: _______________________________

______________________________ **(VENDOR)**

By:_________________________________

Name: Joe Oleksak_____________________

Title: _March 26, 2024___________________