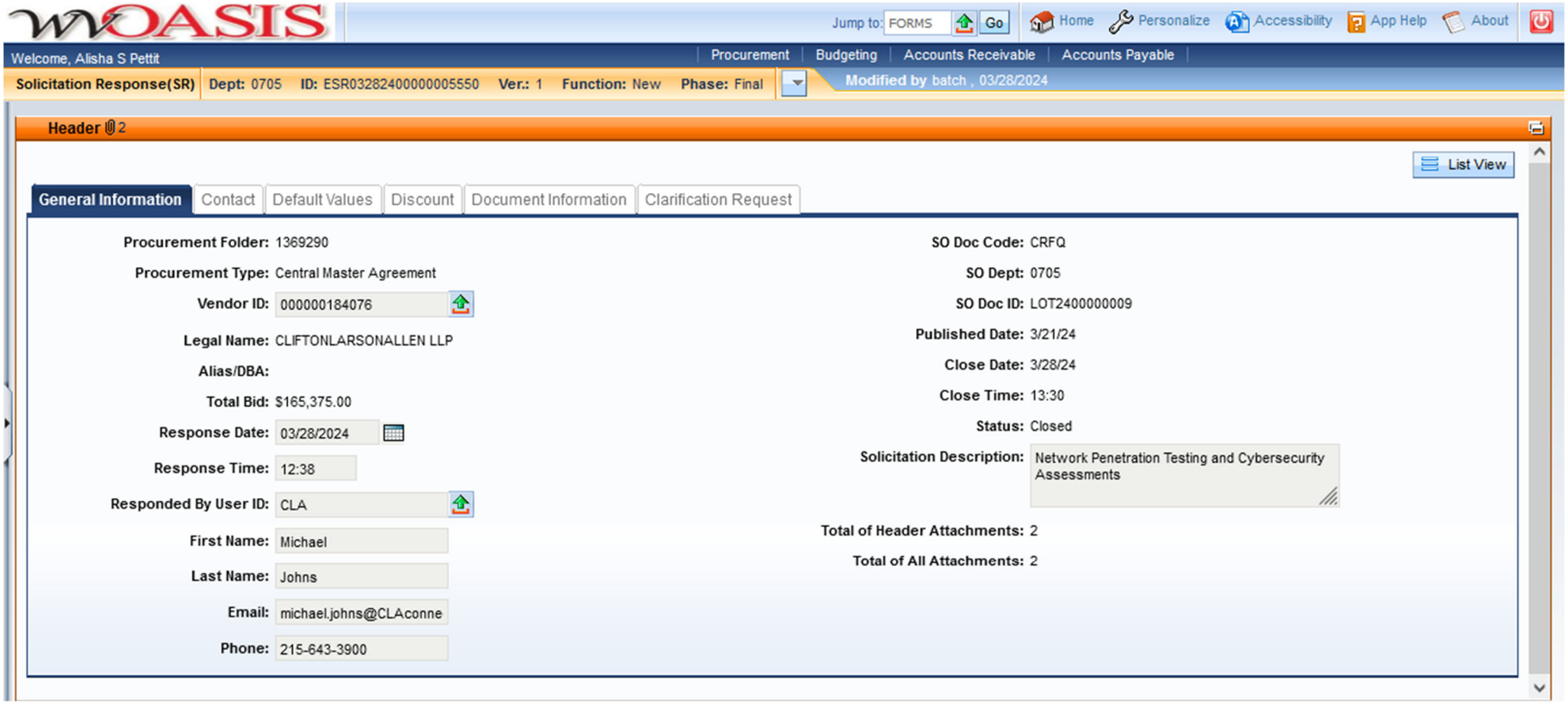
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency 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.


wvOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Alisha S Pettit
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0705 ID: ESR03282400000005550 Ver.: 1 Function: New Phase: Final
Modified by batch , 03/28/2024
Header 2
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 1369290
Procurement Type: Central Master Agreement
Vendor ID: 000000184076
Legal Name: CLIFTONLARSONALLEN LLP
Alias/DBA:
Total Bid: $165,375.00
Response Date: 03/28/2024
Response Time: 12:38
Responded By User ID: CLA
First Name: Michael
Last Name: Johns
Email: michael.johns@CLAconne
Phone: 215-643-3900
SO Doc Code: CRFQ
SO Dept: 0705
SO Doc ID: LOT2400000009
Published Date: 3/21/24
Close Date: 3/28/24
Close Time: 13:30
Status: Closed
Solicitation Description: Network Penetration Testing and Cybersecurity Assessments
Total of Header Attachments: 2
Total of All Attachments: 2

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

State of West Virginia
Solicitation Response

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

Solicitation Closes	Solicitation Response	Version
2024-03-28 13:30	SR 0705 ESR03282400000005550	1

VENDOR

000000184076
CLIFTONLARSONALLEN LLP

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 165375 **Response Date:** 2024-03-28 **Response Time:** 12:38:54

Comments: No discounts applicable

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				19950.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				19425.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				69300.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				56700.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

March 28, 2024

Proposal to provide professional cybersecurity services to:

West Virginia Lottery – RFP Solitation No. CRFQ LOT2400000009

Charleston, WV

Prepared by:

David Anderson, OSCP, Principal
David.Anderson@CLAconnect.com
612-376-4699 *Direct*

CliftonLarsonAllen LLP
227 West Trade Street, 8th Floor
Charlotte, NC 28202-1675

phone 704-998-5200 **fax** 704-998-5250
CLAconnect.com

March 28, 2024

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

RE: West Virginia Lottery, Solicitation No. CRFQ LOT 2400000009 – Network Penetration Testing and Cybersecurity Assessments

Dear Brandon:

Thank you for inviting us to propose our services to you. We gladly welcome the opportunity to share our approach to helping West Virgina Lottery (WV Lottery) meet its need for professional services. The enclosed RFP responds to your request for **Network Penetration Testing and Cybersecurity Assessments**.

Our security assessment services practice relies on a combination of tools that are developed internally by CLA security professionals, as well as open-source and commercially available software. While the core tools used by our practice remain the same, our professionals are constantly on the lookout for new tools and utilities to continually enhance their capabilities. Engagement projects can range from highly collaborative assessments of processes, infrastructure and controls to true Red Team/Black Box/breach simulation assessments designed to mimic true adversarial attack situations and measure and assess response capabilities. Specific scope, approach and desired outcomes are defined in collaboration with clients. Our assessment model includes a dedicated project management approach.

The penetration testing / cybersecurity engagements will be lead by David Anderson and David Nowacki. David Anderson leads the penetration testing practice at CLA. David Nowacki previously worked with the Oregon State Lottery as the Chief Audit Executive.

CLA is focused on delivering an exceptional level of knowledge, insight, and industry experience. As our clients' most trusted business advisor, we:

- Take a genuine interest in your opportunities and challenges
- Identify vulnerabilities and cybersecurity risks in your environment
- Proactively work with you to develop strategies to mitigate risk
- Continually strive to better your organization, the industry, the communities in which we work and live, the cybersecurity profession, and ourselves

We are eager to work with you and welcome the chance to present our proposal to WV Lottery's management team. If you have any questions about our offerings, please do not hesitate to contact me.

CLA (CliftonLarsonAllen LLP)

David Anderson, OSCP
Principal
612-376-4699
David.Anderson@CLAconnect.com

Table of Contents

Penetration Testing Services

External Network Penetration Testing

Overview

The External Network Penetration Test is designed to aggressively test your network perimeter to identify exposure to security breaches from outside your network. Completeness is a critical objective when securing the network perimeter, therefore our testing approach is designed to test your entire infrastructure to identify rogue gateway entry points, and test systems that interact with the outside including: Internet gateways, VPN, routers and firewalls, email infrastructure, remote access, and application interfaces.

Objective

Identify potential vulnerabilities outside the network that might be used to:

- Gain unauthorized access to sensitive confidential information.
- Modify or destroy data.
- Operate trusted business systems for non-business purposes.

Benchmarks

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

Approach

CLA Cybersecurity Services will use a variety of manual and automated tools to test the configuration of Internet-facing systems and services. The complete network penetration test occurs in four very distinct phases, including reconnaissance, mapping, discovery, and exploitation.

Phase 1 – Reconnaissance

- Perform WHOIS, ARIN, and DNS (public server) lookups
- OSINT - Public Searches/Dorks
- Build custom password lists
- DNS lookups (entities server)
- Gather information from entities network resources
- Analyze metadata

Phase 2 – Mapping

- Network Discovery (ICMP sweeps, traceroutes, bypass firewall restrictions, etc.)
- Port/Protocol Scanning (Scan for accepted IP protocols, open TCP/UDP ports)
- OS/Version Scanning (Identify underlying OS and software and their versions)

Phase 3 – Discovery

- Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner)
- Enumerating Network Services (Connect and interact with services to disclose information, gain access, identify misconfigurations, etc.)
- Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)

Phase 4 – Exploitation

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

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

The External Network Penetration Testing will also include social engineering in the form of **email phishing**. This will consist of a single phishing email scenario targeting approximately 200 active WV Lottery staff. The content will be verified and approved by WV Lottery.

Outcome

Our external penetration test and vulnerability assessment is designed to satisfy the following:

1. The HIPAA Security Rule Requirements for periodic technical validation testing: Evaluation (§ 164.308(a)(8)).
2. PCI-DSS requirement 11.3 for external penetration testing.
3. CIS Critical Controls
   - Control 17: Incident Response Management
   - Control 18: Penetration Testing
4. Open Source Security Testing Methodology Manual (OSSTMM)
5. Open Web Application Security Project (OWASP)
6. NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
7. GDPR (European Union General Data Protection Regulation): Article 32(d)

Our deliverable reports will provide your network administrators with detailed recommendations for how to address specific findings.

- Executive Summary Report - this report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
- Technical Report - this report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

The assessment will also include a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

Website Penetration Testing

Overview

Website Penetration Testing is designed to verify that websites are configured and operating in a secure manner. The test focuses on both anonymous access to validate appropriate Confidentiality, Integrity, and Availability are maintained. Application inputs, processing, and functionality are thoroughly reviewed.

Objective

Identify potential vulnerabilities within the application that might be used to:

- Gain unauthorized access to sensitive confidential information.
- Modify or destroy data.
- Operate trusted business systems for non-business purposes.

Benchmarks

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

Approach

The complete website penetration test occurs in four very distinct phases, including reconnaissance, mapping, discovery, and exploitation.

Phase 1 – Reconnaissance

- Perform WHOIS, ARIN, and DNS (public server) lookups
- OSINT - Public Searches/Dorks
- Build custom password lists
- DNS lookups (entities server)
- Gather information from entities network resources
- Analyze metadata

Phase 2 – Mapping

- SSL/TLS Analysis (Identify accepted SSL/TLS ciphers)
- Virtual Hosting & Load Balancer Analysis
- Software Configuration Discovery (Identify HTTP version, web services, scripting languages, third-party web applications, etc.)
- HTTP Options Discovery (Identify accepted HTTP methods)
- Web Application Spidering (gather/follow all links)
- Directory Browsing (Identify web directory listings, brute force common web directory names)
- Web Application Flow (Identify the business logic, flow, organization, and functionalities of the app)
- Session Analysis (Identify locations where session cookies are set and analyze predictability)

Phase 3 – Discovery

- Vulnerability Scanning (Identify vulnerabilities. Open source tools as well as Commercial: Nessus – network vulnerability scanner, Burp Suite – web application scanner)
- Username/Email Enumeration (Validate and guess usernames/emails using login forms, network services, etc.)
- Identify Web Application Specific/Web Service Specific Vulnerabilities (Command/XML/XXE/SQL Injection, File Inclusion, Directory Traversal, File Upload, XSS, CSRF, etc.)

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

Phase 4 – Exploitation

- Brute Force Logins (Using discovered username/email addresses, gain additional access through brute force)
- Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)
- Post-Exploitation and Pivot (Pillage the system to disclose information and additional vulnerabilities. Repeat the penetration test steps to attempt to gain privileged access. Use the compromised systems as a pivot point to attack other systems that are in scope).

The Website Penetration Testing will also include **Denial of Service (DoS) attacks,** which require notification to the Lottery and Lottery approval before the attack commences.

Outcome

Our website penetration test is designed to satisfy the following:

1. The HIPAA Security Rule Requirements for periodic technical validation testing: Evaluation (§ 164.308(a)(8)).
2. PCI-DSS requirements 6.5 for Develop Secure Applications
3. PCI-DSS requirements 6.6 for Secure Public Facing Websites
4. PCI-DSS requirement 11.3 for external penetration testing
5. CIS Critical Controls
   - Control 17: Incident Response Management
   - Control 18: Penetration Testing
6. Open Source Security Testing Methodology Manual (OSSTMM)
7. Open Web Application Security Project (OWASP)
8. NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment

Our deliverable reports will provide your network administrators with detailed recommendations for how to address specific findings.

- Executive Summary Report - this report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
- Technical Report - this report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

The assessment will also include a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

Internal/Client-Side Network Penetration Testing

Overview

The Internal/Client-Side Network Penetration Testing will be a technical evaluation of the devices (*file servers, mail servers, production servers, routers, switches, etc.*) that reside on your internal, trusted business network. Annual breach analysis reports conclude that the majority of breaches have root causes related to:

- Weak/default administrator and vendor credentials
- Unsecured network shares
- Vendor supplied/managed systems
- Weak or poor patch/update management – especially for non-operating system applications.

The Internal/Client-Side Network Penetration Testing is designed to confirm that your network is reasonably protected from these types of threats, which can be more disruptive and more expensive.

Objective

Identify potential vulnerabilities inside the network that might be used to:

- Gain unauthorized access to sensitive confidential information.
- Modify or destroy data.
- Operate trusted business systems for non-business purposes.

Benchmarks

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

Approach

The complete Internal/Client-Side Network Penetration Testing occurs in four very distinct phases, including reconnaissance, mapping, discovery, and exploitation.

Phase 1 – Reconnaissance

- Identify software versions along with potentially useful software configurations or settings
- Identify any anti-malware, firewall, and IDS products on the system
- Gather information about the network (i.e., domain user/group information, domain computers, password policy)
- Verify the ability to execute scripts or third-party programs

Phase 2 and 3 – Mapping and Disvoery

- Identify possible vulnerabilities affecting the provided host
- Determine the possibility of receiving and executing various malicious payloads

Phase 4 – Exploitation

- Attempt to bypass anti-malware solutions and security restrictions, escape restricted environments, and escalate privileges
- Exploitation (Using discovered vulnerability information, exploit vulnerabilities to gain additional access/disclose information)

The Internal/Client-Side Network Penetration Testing will be performed onsite at all eight (8) WV Lottery locations.

The Internal/Client-Side Network Penetration Testing will include two-part testing to assess the security of all networked assets, including but not limited to servers, desktops, firewalls, other network devices, and network monitoring & management.

- Part one simulates an attack by an untrusted outsider or an unauthenticated user without working knowledge of the Lottery's network.
- Part two will be performed with the low-level credentials of an authenticated user.

Outcome

Our Internal Penetration Test and Vulnerability Assessment is designed to satisfy the following:

1. The HIPAA Security Rule Requirements for periodic technical validation testing: Evaluation (§ 164.308(a)(8)).
2. PCI-DSS requirement 11.2.1 for internal vulnerability scanning.
3. PCI-DSS requirement 11.3 for internal penetration testing.
4. CIS Critical Controls
   - Control 17: Incident Response Management
   - Control 18: Penetration Teseting
5. Open Source Security Testing Methodology Manual (OSSTMM)
6. Open Web Application Security Project (OWASP)
7. NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
8. GDPR (European Union General Data Protection Regulation): Article 32(d)
9. The IVA is also a thorough validation review of configuration requirements documented throughout the rest of the PCI-DSS.

Our deliverable reports will provide your network administrators with detailed recommendations for how to address specific findings.

- Executive Summary Report - this report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
- Technical Report - this report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

The assessment will also include a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

Wireless Penetration Testing

Overview

Wireless Penetration Testing is designed to assess the configuration and security of existing wireless networks, evaluate segmentation controls to protect the internal, corporate network from less-secure wireless networks, and scan for rogue devices within your trusted infrastructure.

Objective

Identify potential vulnerabilities within the application that might be used to:

- Gain unauthorized access to sensitive confidential information.
- Modify or destroy data.
- Operate trusted business systems for non-business purposes.

Benchmarks

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

Approach

The complete wireless penetration test occurs in four very distinct phases, including reconnaissance, mapping, discovery, and exploitation.

Phase 1 – Reconnaissance

- Perform WHOIS, ARIN, and DNS (public server) lookups
- OSINT - Public Searches/Dorks
- Build custom password lists
- DNS lookups (entities server)
- Gather information from entities web applications
- Analyze metadata

Phase 2 – Mapping

- Sniffing (establish a baseline of traffic, sniff Wi-Fi, Bluetooth, Zigbee, and other RF)
- War Walk (map location of access points and their coverage, identify leakage)
- Identify Rogue Access Points* (Friendly, malicious, or unintended access points)
- Full access to the buildings will be granted to the testing team

Phase 3 – Discovery

- Identify Points of Attack (Identify WEP networks, capture WPA/WPA2 PSK key exchanges, identify clients for evil-twin and MiTM attacks
- Enumerating Services (Connect and interact with services on APs, Bluetooth Devices, and other RF devices to disclose misconfigurations
- Vulnerability Scanning (Identify vulnerabilities)

Phase 4 – Exploitation

- AP Attacks (Exploit hotspots, perform MiTM attacks, crack WEP, crack WPA/WPA2 PSK, etc.)
- Client Attacks (Perform Evil-Twin attacks, perform rogue AP attacks, MiTM, etc.)
- Denial of Service where applicable and with prior Lottery approval
- Bluetooth/Zigbee/SDR Attacks where applicable and with prior Lottery approval

The Wireless Penetration Testing will be performed onsite at all eight (8) WV Lottery locations.

Outcome

Our wireless penetration test is designed to satisfy the following:

1. The HIPAA Security Rule Requirements for periodic technical validation testing: Evaluation (§ 164.308(a)(8)).
2. PCI-DSS requirements related to wireless: 1.2.3, 2.1.1, and 4.1.1
3. CIS Critical Controls
   - Control 17: Incident Response Management
   - Control 18: Penetration Testing
4. Open Source Security Testing Methodology Manual (OSSTMM)
5. Open Web Application Security Project (OWASP)
6. NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment

Our deliverable reports will provide your network administrators with detailed recommendations for how to address specific findings.

- Executive Summary Report - this report is an overview of all testing results, including a summary report of the scope and approach, findings, key points of strength in the assessed infrastructure, and recommendations directed at senior management.
- Technical Report - this report details each vulnerability type discovered along with a critical, high, medium, or low risk rating.

The assessment will also include a Findings Presentation to the Lottery management team. This presentation shall provide an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

Project Management Approach

General Project Administration

We will assign a Principal and a Project Manager as your direct liaisons. These individuals will work with WV Lottery's designated project manager to oversee that the various components of the project are managed in a manner the meets everyone's expectations. We will work with your designated project manager to establish project timelines and deadlines, and communication protocols. These communication protocols will include formally scheduled project status meetings, as well as ongoing updates via phone and/or email. The exact timing and frequency for meetings and communication updates will be established as part of an initial kick off meeting between CLA and WV Lottery. We will keep you informed throughout all stages of the assessments. Any concerns or problems will be discussed with the client within 24 hours, and resolved within a reasonable time relative to the issue. We welcome job shadowing as a means of knowledge transfer, and are happy to openly share our processes and testing methodologies.

Quality Control Standards

We have undertaken an intensive internal quality control program to foster that professional standards are maintained in our work. This program is designed to provide reasonable assurance that our personnel will be competent and objective, and will exercise due professional care. Included in that program are the following:

- A quality control manual to dictate the quality control standards and policies of our firm. These standards often exceed requirements set forth by professional standards and governmental guidelines. To monitor the adherence to policies and procedures, and to oversee that the quality and accuracy of services provided meet our standards of client services, each office must have a regular internal examination performed by professionals from other firm offices.
- Quality control standards as prescribed by the American Institute of Certified Public Accountants (AICPA) are maintained. A principal-in-charge is involved in the planning, fieldwork and post-fieldwork review.

Our reports are issued promptly after the completion of our fieldwork. CLA's communication framework is set up to foster value-driven results. We require our auditors to prioritize their findings and discuss drafts of reports with the appropriate West Virgina Lottery and staff prior to issuance.

We believe this approach accomplishes the following:

- Confirms the information contained in the report.
- May foster a lesser reaction to significant findings.
- Encourages buy-in from the process owners.
- Increases likelihood of implementation of recommendations (if any).

We realize and appreciate that audit results and recommendations cannot be "textbook" responses. We work with our clients to assess and determine pragmatic recommendations based on cost-effectiveness, staffing and resource considerations, system limitations, and compliance considerations. This results in a collaborative effort to arrive at "real world" practical strategies and responses for executive management to consider and evaluate in managing IT risks.

Upon approval of the draft report, final reports will be issued to WV Lottery's senior management, and formally presented if requested. The final reports will consist of:

1) Executive Summary Report suitable for WV Lottery's senior management; summarizing the scope, approach, and findings; and

2) Detailed Report designed for WV Lottery's information technology staff which will include methodology employed, detailed information technology findings with a risk rating for each and detailed exhibit if appropriate, and detailed remediation steps.

Follow up calls after the completion of the final deliverable to discuss observations and recommendations are expected, and this is included in the fee quote – we believe it fosters a sound working relationship between our technical professionals and yours that leads to better outcomes.

A more detailed outline of our project management approach is set forth below.

Project Management Approach (Detailed Outline)

CLA will approach this project as a collaborative effort. CLA professionals will work closely with your team to achieve and satisfy the project objectives.

Project Planning Meeting

The major objectives of the initial meeting will be to validate the overall goals of the projects including definition of specific objectives and timelines. We will review the organization's organization structure, policies and procedures and any existing business and technology plans containing information that may impact the project.

Project Teams

Determine appropriate personnel who will participate in the project and have overall "ownership" from a strategic and day-to-day perspective.

Specific activities will vary but typical responsibilities include understanding the overall business and technology goals of the WV Lottery, defining and monitoring the project schedule, and keeping appropriate staff (and external business partners) informed on the status of the project.

Decision-Making Authority

Throughout the project various decisions will need to be made. CLA will work with you to determine who must be involved in various evaluation and selection activities and who must be involved in the approval process and decisions.

Communication Strategy

CLA and WV Lottery will jointly determine the best method for communicating project-related information including but not limited to:

- On-site Meetings
- Teleconferences
- Email communication
- Protocol for communicating audit findings
- Other

Project Plan

As a result of the information obtained during the project planning meeting, establish a project plan that will identify the following:

- Specific project tasks
- Anticipated start/completion date for tasks
- Individual(s) responsible for completion of tasks

Throughout the life of the project, CLA will facilitate periodic project status meetings to identify task status including those that need specific attention to maintain the project objectives and related schedule.

Advanced Preparation

CLA may request information to be provided in advance of any on-site or in-person interviews to conduct a thorough and effective assessment analysis. The information will be reviewed prior to any additional staff meetings. Specifically, the information that should be provided includes, but is not limited to, the following:

- Organization Structure (IT and Entity)
- Network Architecture Diagrams
- Application Inventory
- Information Security Policies and Procedures
- Key Vendor Relationships / Dependencies

This advanced preparation allows the audit professionals to more effectively use the time spent with your personnel. The CLA consulting team will review the information prior to the strategic planning meeting and summarize what factors are critical to the decision making process.

Project Timeline

We will work with WV Lottery's management team to formally establish project timelines and deadlines. Please see the chart below for a sample time frame relating to each segment of this engagement.

Engagement Activities	Weeks					
	1	2	3	4	5	6
Project Updates and Meetings						
Project Planning Meeting and Deliver Fieldwork Plan						
Complete Fieldwork						
Deliverables Preparation and Review						
Deliver Final Report(s)						

West Virgina Lottery Interaction

We can perform most of our testing in either an informed (white box) or uninformed (black box) manner. We prefer that most or all testing will be done in an informed manner. This allows us to:

- Be efficient with our time and your resources
- Focus our efforts on testing controls as opposed to discovering controls
- Work collaboratively with your IT administration and security staff to understand what is being observed, develop accurate observations, and meaningful recommendations

We will expect WV Lottery to provide documentation related to the testing that may include: network and application diagrams; system and asset inventories; policies, procedures, and standards; and previous assessment reports. This approach allows us to focus on thorough testing of controls as opposed to spending time on discovery of controls.

During assessments we will expect to be able to interact with WV Lottery staff to discuss the status of testing results in order to refine and focus our testing and collaborate on observations, issues and possible recommendations. We encourage WV Lottery staff to spend time with our testing professionals during the course of the assessments (i.e. job shadowing) as time allows.

For a successful engagement, support from WV Lottery resources is necessary. Our anticipated needs for support are approximated below:

1. Sponsors/Management: 4 - 8 hours for initial planning phase
2. Periodic meetings (15-30 minutes) throughout the engagement for project meetings and updates
3. Subject Matter Experts: 1-4 hours per week in support of testing

As part of the planning phase, it will be the responsibility of WV Lottery to specifically identify all sponsors / management and subject matter professionals who will be supporting this engagement.

Pricing

Assumptions. Onsite testing will be limited to the eight (8) facilities noted in the RFQ.

Schedule. CLA is prepared to begin the project within six (6) to ten (10) weeks of your notification to proceed. The duration of projects does not typically exceed six (6) weeks but is based on the availability of staff and cooperation in providing requested information in a timely manner.

Professional fees. Our professional fees for these services will be based on the time involved and the degree of responsibility and skills required, number of systems, system complexity, and asset size. The fees contained in this proposal are valid for ninety (90) days from the proposal date. Fees for each individual component are presented below:

EXHIBIT A - Pricing Page

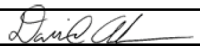
Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	$ 19,950 -	$ 159,600 -
2	4.2	Website Penetration Testing	8	$ 19,425 -	$ 155,400 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 69,300 -	$ 554,400 -
4	4.4	Wireless Penetration Testing	8	$ 56,700 -	$ 453,600 -
				TOTAL BID AMOUNT	$ 1,323,000 -

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

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

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

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

Vendor Name:	CliftonLarsonAllen, LLP
Vendor Address:	220 South Sixth Street, Sutie 300, Minneapolis, MN 55402-1436
Email Address:	David.Anderson@claconnect.com
Phone Number:	(612) 376-4699
Fax Number:	612-376-4850
Signature and Date:	

Our last word on fees – we are committed to serving you. Therefore, if fees are a deciding factor in your selection of a professional services firm, we would appreciate the opportunity to discuss with you the scope of our audit plan.

At CLA, it's more than just getting the job done…

Background - CLA Cybersecurity Services Group

General background and experience

CLA's Cybersecurity Services Group is the information security assessment and consulting arm of CLA's National Digital group, and is led by a team of six principals, ten directors and managers, and resources of over 55 professionals. We are a full-service consulting group with a depth of talent with specific experience with a number of enterprise data processing systems, operating systems and network protocols.

CLA has been performing a wide range of cybersecurity assessment services for over 25 years, including those requested by WV Lottery for this proposal. In this time we have performed more than 4,500 penetration tests, and thousands of IT audits and vulnerability assessments. Our core leadership team has been in place at CLA since the inception of the security services group as a standalone service line in 1999. Senior personnel have upwards of 25 years of experience in the information security and assessment field. We specialize in professional penetration testing, vulnerability assessment, IT and enterprise risk assessment, independent network security consulting, physical access controls and social engineering assessments, security incident response and computer forensics, and IT/security compliance against all major governance and compliance frameworks. We have client references for whom we have provided these services continuously for 10 or more years.

We have been providing PCI gap assessments and the underlying testing requirements (External and Internal Penetration Testing, Vulnerability Scanning and Assessment, Wireless Testing, and Social Engineering Assessments) for clients since the inception of the PCI DSS. Clients include financial institutions; non-profits and foundations; government agencies, counties, and municipalities; restaurant and retail; transportation; manufacturing; and higher education. CLA has been a certified QSA firm since 2011. CLA has developed a standard process/methodology that is mapped directly to the requirements set forth by the PCI Security Council.

We have been providing HIPAA Security readiness and compliance assessments and the underlying testing requirements (External and Internal Penetration Testing, Vulnerability Scanning and Assessment, Wireless Testing, and Social Engineering Assessments) for clients since the Security Rule was announced in 2005. Clients include nearly all the sub-industries within health care, as well as public agencies, and private companies required to be in compliance. CLA has developed a standard process/methodology that is mapped directly to the requirements set forth by the HIPAA Security Rule and the underlying NIST standards framework.

On an annual basis, CLA's cybersecurity professionals present at seminars and teach hands on classes focused on IT audit techniques, vulnerability assessment, and penetration testing. These seminars are offered through CLA directly several times per year, as well as our teaming with national, regional, state and local associations such as ISACA, the Minnesota Government IT Symposium, the Florida Government Finance Officers Association, the Independent Community Bankers of America, and many others. Our professionals are active in a variety of associations, and we actively sponsor Cyber Collegiate Defense competitions and Cyber Security training institutes in conjunction with the Minnesota Cyber Security Careers Consortium (*mnc3.advanceitmn.org)*. They are actively sought out as instructors for the services we provide, including penetration testing, IT auditing, SSAE16 assessments and PCI-DSS.

Our professionals are people with character who invest their emotional capital in a vision they understand and adopt as their own to provide CLA's competitive advantage—emotional ownership. They want to succeed personally, they want our Firm to succeed, and above all, they want those they are serving to succeed.

Technical qualifications

Following is a listing of the information management systems and security tools that CLA has experience with as a result of previous projects.

Security Tools: Our security assessment services rely on a combination of tools that are developed internally by CLA security professionals, as well as open-source and commercially available software. While the core tools used by our practice remain the same, our professionals are constantly on the lookout for new tools and utilities to continually enhance their capabilities.

- **Internally developed tools to perform the following:**
  - *Audit scripts for various database applications*
  - *Automated drive mapping utility*
  - *Keystroke loggers for remote monitoring*
  - *Password changing utility*
  - *Remote access command prompt management tool*
  - *Remote host configuration auditing tool*
  - *Various wireless attack programs and scripts*

- **Free / Open Source Tools:**
  - Aircrack Suite
  - AirSnort
  - Autopsy Forensic Browser
  - CAIN
  - CIS software & benchmarks:
    - RAT
    - OS benchmarks
  - Dictgen
  - DumpACL
  - Hydra
  - John the Ripper
  - Kismet
  - Metasploit Framework
  - Zed Attack Proxy
  - Visual Studio
  - MBSA
  - BeEF
  - W3af
  - Nikto
  - SET
  - Dsniff
  - Wireshark
  - VirtualBox
  - SQLmap
  - Medusa
  - THCSSLCheck
  - NBTEnum
  - Netcat
  - Netstumbler
  - Nmap
  - pwdump2
  - Sleuthkit
  - VNC
  - SQLPing3
  - Mana Toolkit
  - libesedb
  - rcracki
  - DNSenum
  - DirBuster
  - DNSRecon
  - IKEScan
  - RAWR
  - Sysinternals Suite
  - LdapAdmin
  - Maltego
  - Recon-ng
  - Impacket
  - Responder
  - Mimikatz
  - OllyDbg
  - PowerSploit
  - PowerShell Empire
  - Veil Framework
  - Windows Credential Editor

- **Commercial Tools:**
  - EnCase Forensic Edition
  - LC5
  - Microsoft OS & apps
    - Resource kits
    - Enterprise Manager
    - Query Analyzer
  - Nessus
  - pcAnywhere
  - Sandstorm PhoneSweep
  - Silent Watch
  - SolarWinds
  - SpyTech
  - VMware Fusion
  - Burp Suite
  - IDA Pro
  - Hyena
  - SAINT
  - Qualys Guard

Engagement team

An experienced engagement team has been aligned to provide the most value to your organization. The team consists of personnel with technical and business credentials, including CBA, CCSE, CCSFP, CEH, CFE, CHPS, CIA, CICA, CISA, CISM, CISSP, CITP, CPA, CPT, CRISC, CRMA, CTGA, FCSP, GCFA, GCIH, GSEC, GWAPT, HCISPP, ITIL, MCNE, MCP, MCSE-Security, OSCP, OSWP, PCI-QSA, PMP, WCNA and others. The team members have performed numerous engagements of this nature and will commit the resources necessary to provide top quality service throughout the engagement.

The most important resource any business has is people — the right people.

The core proposed management team members are listed below and will be supported by additional business, process, and technology professionals as needed.

Resource	*Title*	*Role/Emphasis*
David Anderson	*Principal*	*Service Leadership – Cybersecurity/IT*
David Nowacki	*Director*	*Service Leadership – Cybersecurity/IT*
Sedric Louissaint	*Director*	*Technical Analyst – IT Audits, Cybersecurity and Vulnerability Assmts.*
Zoran Jovic	*Manager*	*Technical Analyst – IT Audits, Cybersecurity and Vulnerability Assmts.*
Andrew Petro	*Senior*	*Technical Analyst – IT Audits, Cybersecurity and Vulnerability Assmts.*
Daniel Printke	*Senior*	*Technical Analyst – IT Audits, Cybersecurity and Vulnerability Assmts.*
RJ Stallkamp	*Senior*	*Technical Analyst – IT Audits, Cybersecurity and Vulnerability Assmts.*

Resumes

Detailed biographies are available beginning on the next page.

David Anderson, OSCP

CLA (CliftonLarsonAllen LLP)

Principal
Minneapolis, Minnesota

612-376-4699
David.Anderson@CLAconnect.com

Profile

David is a Principal and Cybersecurity Consultant in the CLA National Digital group with a strong focus on Offensive Cybersecurity. He has over 11 years of experience in the field, performing penetration testing, vulnerability assessments, and social engineering engagements. David's expertise also includes project management for cybersecurity engagements across a diverse range of industries.

Technical experience

David has firsthand knowledge and experience using leading edge hacking/testing methods:

- External and internal network penetration designed to gain access to high value targets
- Social engineering techniques designed to assess security related to the human element
- Techniques for email phishing that result in remote access to company networks, bypassing improperly configured firewalls and proxy systems
- Domain and network management

Education and professional involvement

- Bachelor of art, information technology with focus on networking and security, Minnesota State University – Mankato (MNSU)
- Offensive Security Certified Professional (OSCP)

Speaking engagements

David has been a featured speaker at national conferences and training sessions related to cybersecurity including topics related to:

- Penetration testing and vulnerability assessments
- Corporate account takeovers
- Email phishing
- Social engineering
- Network security

David Nowacki, CISA, CIA

CLA (CliftonLarsonAllen LLP)

Director
West Hartford, Connecticut

860-561-6811
david.nowacki@CLAconnect.com

Profile

Dave is a Director with the CLA Cybersecurity team, a part of the National Digital group. He has more than 21 years of combined experience in cybersecurity, IT controls, enterprise risk management, internal audit, and management consulting. He has worked with government entities, financial services, and various other private businesses in setting strategies, reviewing, and assessing operations, governance and enterprise risk management practices, project and program management practices; information security programs, and identifying process improvement opportunities. David previously worked with the Oregon State Lottery as the Chief Audit Executive.

Technical experience

- Cybersecurity Program Development
- Department of Defense (DFARs) Cybersecurity Compliance (CMMC)
- NIST Cybersecurity Framework and NIST SP800-171
- GLBA and FFIEC Cybersecurity Frameworks
- MUSL Security Rules
- IT General Controls
- IT Audit and Information Security
- Enterprise Risk Management
- Process Improvement
- Strategic Planning
- Organizational Transformation

Education and professional involvement

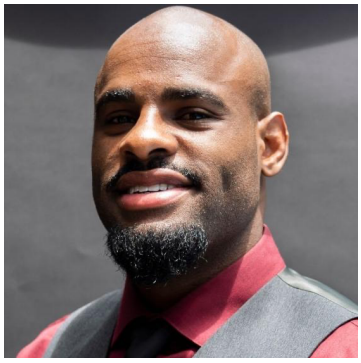
- Bachelor of Science, Information Systems from the University of Montana
- Certified Information Security Auditor (CISA) (ISACA)
- Certified Internal Auditor (CIA) (TheIIA)

Lottery Experience

David has extensive experience in the Lottery industry; as a consultant, auditor, and executive employee of a lottery. Below in a sample of his experience:

- SOC-1 Reporting for State Lotteries and Gaming Management System Providers
- Internal Audit and Enterprise Risk Management
- Lottery Systems Security Reviews
- IT General Controls
- Instant Ticket Printing Security
- Operational / Compliance Auditing for Outsourced Lottery Operations
- Retail Contracting and Adminsitration and Enforcement
- Video and Traditional System SDLC
- Lean Transformation
- Business Continuity / Disaster Recovery

Sedric Louissaint, CISSP, CySA+, PenTest+, Net+, Sec+, CCNA



CLA (CliftonLarsonAllen LLP)

Director
Orlando, FL

386-450-1293
sed.louissant@CLAconnect.com

Profile

Sedric is a Director in Cybersecurity Penetration Testing in the CLA National Digital group. Sedric currently performs and manages IT and Cybersecurity testing and assessments within the healthcare and other industries served by CLA. Sedric has technical and management experience in providing IT solutions, security, customer service, and project management.

Technical Experience

- External and Internal Network Penetration Testing and Vulnerability Assessments
- Web and Mobile Application Penetration Testing
- Risk Assessments
- Assist with planning, managing and executing on premise infrastructure and cloud infrastructure projects using AWS/Azure
- Consulting on Governance, Risk Management, and Compliance using frameworks such as NIST-SP 800 & CSF, HIPAA, HITRUST, GDPR, and PCI-DSS

Education and Professional Involvement

- Bachelor of Science in Information Systems Technology (Specialization in Cybersecurity), Seminole State College
- Associate of Science in Information Systems Technology (Specialization in Cybersecurity), Seminole State College
- Technical Certificate in Information Technology Client Specialist, Seminole State College
- CompTIA Network+/Security+/CySA+/PenTest+/CSAP/CNSP/CNVP
- ISC_2 CISSP
- Cisco CCNA-RS
- DoD IAT/IAM Level I, II, III
- DoD IASAE level I, II
- DoD CSSP Analyst/Auditor/Incident Responder/Infrastructure Support
- Fortinet NSE 1, 2, 3

Zoran Jovic, GPEN

CLA (CliftonLarsonAllen LLP)

Manager
Tampa, Florida

813-384-2728
zoran.jovic@CLAconnect.com

Profile

Zoran is a Cybersecurity Penetration Testing Manager in the National Digital group, focusing on Technical Assessments. Zoran currently performs network penetration testing, internal and external vulnerability assessments, social engineering assessments, and wireless network security assessments. Prior to joining the firm, Zoran worked with a wide range of organizations, ranging from start-up, small businesses to Fortune 10 organizations. Zoran's experience includes technical assessments, project management and consulting. Zoran is also a United States Army Veteran.

Technical Experience

- Internal/External Network Penetration Testing
- Remote/On-Site Social Engineering
- Wireless Network Security Assessments

Education and Professional Involvement

- Bachelor of Science in Cybersecurity from Bellevue University - Bellevue, Nebraska
- Associates of Science in Computer Science from Onondaga Community College - Syracuse, New York
- GIAC Network Penetration Tester (GPEN)

Andrew Petro, OSCP

CLA (CliftonLarsonAllen LLP)

Senior
Oak Brook, IL

312-343-3162
Andrew.Petro@CLAconnect.com

Profile

Andrew Petro is a Senior Cybersecurity Penetration Testing in CLA's National Digital group focused on Technical Assessments. Prior to CLA, Andrew worked as an Enterprise Networking and Security consultant for Sirius Computer Solutions. He has a B.A. in Mathematics and a M.S. in computer security.

Technical Experience

- Enterprise Networking and Security
- Internal Penetration Testing
- External Penetration Testing
- Firewall Reviews
- VMware Virtualization
- Software Defined Networking

Education and Professional Involvement

- Bachelor of Science in Mathematics from Illinois Wesleyan University
- Master's in Computer Security from DePaul University
- Offensive Security Certified Professional (OSCP)

Daniel Printke, OSCP

CLA (CliftonLarsonAllen LLP)

Senior
Minneapolis, MN

612-256-8314
Daniel.Printke@CLAconnect.com

Profile

Daniel is a Senior Cybersecurity Penetration Tester in CLA's National Digital group.
Daniel currently performs penetration tests to identify cybersecurity risks on a client's production environment and their external perimeter. Daniel also performs social engineering engagements both remote and on location to evaluate a client's employees. Testing their ability to not fall victim to specially crafted phishing emails, deceitful phone calls, and in-person masquerading attempts to gain unauthorized access. Daniel has performed engagements for financial, government, healthcare, education, automotive, and non-profit institutions to identify and present recommendations to executive management. Daniel develops custom exploitation tools to improve the internal toolset that can be leveraged by other CLA team members.

Technical experience

- Conduct internal and external penetration testing and vulnerability assessments in client production environments, including collaborative purple team testing.
- Perform remote and on-site social engineering engagements including email phishing, phone calls, and in-person masquerading from both a white box and black-box approach.
- Evaluate physical security using various tools and techniques in order to gain unauthorized access to locations and facilities.
- Evaluate physical security using various tools and techniques in order to gain unauthorized access to locations and facilities.
- Laterally move, escalate privileges, and identify access to confidential information within Active Directory environments utilizing discovered misconfigurations, and vulnerabilities.
- Develop and leverage custom exploitation tools to further improve the team's internal toolset.

Education and professional involvement

- Bachelor of Information Technology and Security, Cyber Defense from Baker College of Flint
- Offensive Security Certified Professional (OSCP)

RJ Stallkamp, OSCP

CLA (CliftonLarsonAllen LLP)

Senior
Minneapolis, MN

615-939-4723
rick.stallkamp@CLAconnect.com

Profile

RJ is a Senior Cybersecurity Penetration Tester in CLA's National Digital group. RJ currently performs cybersecurity and social engineering assessments within a wide range of industries including financial, manufacturing and distribution, healthcare, non-profit, insurance and government agencies.

Prior to working for CLA, RJ gained experience as a Department of Defense contractor, which allowed him to assist active-duty military with a multitude of technological issues. RJ's passion for security is made known in every engagement by ensuring that each client is equipped with the knowledge necessary to take on the ever-growing landscape of malicious attacks.

Technical experience

- Internal/external network penetration testing
- Remote/on-site social engineering
- Web application penetration testing
- Wireless network security assessments

Education and professional involvement

- Offensive Security Certified Professional (OSCP)

References

We are pleased to provide you with the following references, who have used our cybersecurity assessment and consulting services. Please do not hesitate to contact any of the individuals listed regarding the value provided by CLA's Cybersecurity Services Group.

Client	Contact Name	Contact Telephone/Email
City of Phoenix, AZ *Phoenix, AZ*	Shannon Lawson CISO / ACIO	480/536-3018 shannon.lawson@phoenix.gov
Services performed: PCI readiness, remediation, and compliance; external and internal penetration testing; internal vulnerability assessment; and IT risk assessments.		
Lake County *Lake County, FL*	Terri Freeman Inspector General	352/253-4937 tfreeman@lakecountycleak.org
Services performed: Data governance and HIPAA security risk assessment, general controls review, vendor management assessment, external and internal network penetration testing, internal vulnerability assessment, web application testing, and wireless assessment.		
Otter Tail Corp / Otter Tail Power (and subsidiaries)	Craig Brye Internal Audit Manager IT	701/451-3584 cbrye@ottrertail.com
Services Provided: CLA has served the cybersecurity needs of Otter Tail Corporation and subsidiaries for over ten years. During that time, CLA has performed External Penetration Testing, Internal Penetration Testing, Social engineering (email phishing), Onsite / in-person / physical security testing and social engineering, Wireless Network Security Assessments, NERC CIP active and paper vulnerability assessments, Custom penetration testing to evaluate specific security controls implemented by the organizations.		
Polk County Florida BOCC *Bartow, FL*	Phil Lambert Security Administrator	863/534-7564 phillambert@polk-county.net
Services performed: External Penetration Testing, Web Application Penetration Testing, Internal Vulnerability Assessment, Wireless Assessment, Social Engineering Assessments, and IT General Controls Reviews.		
Sarasota County *Sarasota, FL*	Scott Gibbs Enterprise Systems Architect	941/861-2130 sgibbs@scgov.net
Services performed: External and internal network penetration testing, internal vulnerability assessment, web application testing, wireless assessment, PCI gap assessment and vulnerability scanning, other audit and accounting services		

Quality control procedures and peer review report

In the most recent peer review report, dated November 2022, we received a rating of ***pass***, which is the most positive report a firm can receive. We are proud of this accomplishment and its strong evidence of our commitment to technical excellence and quality service.

In addition to an external peer review, we have implemented an intensive internal quality control system to provide reasonable assurance that the firm and our personnel comply with professional standards and applicable legal and regulatory requirements. Our quality control system includes the following:

- A quality control document that dictates the quality control policies of our firm. In many cases, these policies exceed the requirements of standard setters and regulatory bodies. Firm leadership promotes and demonstrates a culture of quality that is pervasive throughout the firm's operations. To monitor our adherence to our policies and procedures, and to foster quality and accuracy in our services, internal inspections are performed annually.
- Quality control standards as prescribed by the AICPA. The engagement principal is involved in the planning, fieldwork, and post-fieldwork review. In addition, an appropriately experienced professional performs a risk-based second review of the engagement prior to issuance of the reports.
- Hiring decisions and professional development programs designed so personnel possess the competence, capabilities, and commitment to ethical principles, including independence, integrity, and objectivity, to perform our services with due professional care.
- An annual internal inspection program to monitor compliance with CLA's quality control policies. Workpapers from a representative sample of engagements are reviewed and improvements to our practices and processes are made, if necessary, based on the results of the internal inspection.
- Strict adherence to the AICPA's rules of professional conduct, which specifically require maintaining the confidentiality of client records and information. Privacy and trust are implicit in the accounting profession, and CLA strives to act in a way that will honor the public trust.
- A requirement that all single audit engagements be reviewed by a designated single audit reviewer, thereby confirming we are in compliance with the standards set forth in the *Uniform Guidance*.

Cherry Bekaert LLP
Your Guide Forward

Report on the Firm's System of Quality Control

To the Principals of CliftonLarsonAllen LLP
and the National Peer Review Committee

We have reviewed the system of quality control for the accounting and auditing practice of CliftonLarsonAllen LLP (the "Firm") applicable to engagements not subject to PCAOB permanent inspection in effect for the year ended May 31, 2022. Our peer review was conducted in accordance with the Standards for Performing and Reporting on Peer Reviews established by the Peer Review Board of the American Institute of Certified Public Accountants ("Standards").

A summary of the nature, objectives, scope, limitations of, and the procedures performed in a System Review as described in the Standards, may be found at www.aicpa.org/prsummary. The summary also includes an explanation of how engagements identified as not performed or reported on in conformity with applicable professional standards, if any, are evaluated by a peer reviewer to determine a peer review rating.

Firm's Responsibility

The Firm is responsible for designing and complying with a system of quality control to provide the Firm with reasonable assurance of performing and reporting in conformity with the requirements of applicable professional standards in all material respects. The Firm is also responsible for evaluating actions to promptly remediate engagements deemed as not performed or reported on in conformity with the requirements of applicable professional standards, when appropriate, and for remediating weaknesses in its system of quality control, if any.

Peer Reviewer's Responsibility

Our responsibility is to express an opinion on the design of and compliance with the Firm's system of quality control based on our review.

Required Selections and Considerations

Engagements selected for review included engagements performed under *Government Auditing Standards*, including compliance audits under the Single Audit Act; audits of employee benefit plans; audits performed under FDICIA; and examinations of service organizations (SOC 1® and SOC 2® engagements).

As a part of our peer review, we considered reviews by regulatory entities as communicated by the Firm, if applicable, in determining the nature and extent of our procedures.

Opinion

In our opinion, the system of quality control for the accounting and auditing practice of CliftonLarsonAllen LLP applicable to engagements not subject to PCAOB permanent inspection in effect for the year ended May 31, 2022, has been suitably designed and complied with to provide the Firm with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. Firms can receive a rating of *pass*, *pass with deficiency(ies)* or *fail*. CliftonLarsonAllen LLP has received a peer review rating of *pass*.

Cherry Bekaert LLP

Cherry Bekaert LLP
Charlotte, North Carolina
November 18, 2022

cbh.com

Appendix

License to practice

CLA is a limited liability partnership and is duly licensed to practice in the state of West Virginia. A copy of our state license is provided below:

State of West Virginia
West Virginia Board of Accountancy
405 Capitol Street, Suite 908
Charleston, WV 25301-1744
(304) 558-3557

The entity listed below was issued a
FIRM PERMIT
for the period beginning
JULY 1, 2023 THROUGH JUNE 30, 2024

F0347A
CLIFTONLARSONALLEN LLP
220 S 6TH ST STE 300
MINNEAPOLIS MN 55402

Board President Executive Director

State of West Virginia
West Virginia Board of Accountancy
405 Capitol Street, Suite 908
Charleston, WV 25301-1744
(304) 558-3557

The entity listed below was issued a
FIRM PERMIT
for the period beginning
JULY 1, 2023 THROUGH JUNE 30, 2024

F0347A
CLIFTONLARSONALLEN LLP
220 S 6TH ST STE 300
MINNEAPOLIS MN 55402

Board President Executive Director

To use license as a Wall License, cut off excess paper and affix the above to wall for display.

To use the license as a Pocket Card, cut right column to the size of a business card or driver's license and laminate if desired.

State of West Virginia
West Virginia Board of Accountancy
405 Capitol Street, Suite 908
Charleston, WV 25301-1744
(304) 558-3557

The entity listed below was issued an
Authorization to Perform
Attest and/or Compilation Services
for the period beginning
JULY 1, 2023 THROUGH JUNE 30, 2024

F0347A
CLIFTONLARSONALLEN LLP
220 S 6TH ST STE 300
MINNEAPOLIS MN 55402

Board President Executive Director

State of West Virginia
West Virginia Board of Accountancy
405 Capitol Street, Suite 908
Charleston, WV 25301-1744
(304) 558-3557

The entity listed below was issued an
Authorization to Perform
Attest and/or Compilation Services
for the period beginning
JULY 1, 2023 THROUGH JUNE 30, 2024

F0347A
CLIFTONLARSONALLEN LLP
220 S 6TH ST STE 300
MINNEAPOLIS MN 55402

Board President Executive Director

To use license as a Wall License, cut off excess paper and affix the above to wall for display.

To use the license as a Pocket Card, cut right column to the size of a business card or driver's license and laminate if desired.

Sample Executive Summary Report & Technical Report

The following pages show samples from an Executive Summary Report and a Technical Report.

ABC Company

External Penetration Test

Executive Summary

March 17, 2023

The following files are part of the entire report:
DetailedFindings-ABC-EPT-2023.xlsx
AppendixA-ExploitationEvidence-ABC-EPT-2023.pdf
ExecutiveSummary-ABC-EPT-2023.pdf (This Report)

Please note the observations below are for discussion purposes only and do not necessarily contain all the findings that will appear in the final report.

External Penetration Test Objective

The objective of the External Penetration Test (EPT) is to identify potential vulnerabilities on the external network perimeter that could be exploited to gain unauthorized access to confidential information, modify or destroy data, or operate trusted business systems for non-business purposes.

Scope

The scope of the External Penetration Test included the following systems.

Table 1: Technical Scope

Asset	Description
scope item 1	description 1
scope item 2	description 2
scope item 3	description 3
scope item 4	description 4

Executive Summary

Based on the observations during the External Penetration Test, multiple critical and high-risk vulnerabilities were discovered. Multiple web applications were vulnerable to SQL injection, which allowed CLA to gain unauthorized access to these applications. In addition, it was possible to use SQL injection to compromise the service account that the SQL database was running as, which is an administrative account. This was possible due to insecure firewall filtering and because the database user account had a weak password. With access to this user account, it was possible to take advantage of a vulnerability in the Exchange email server that allowed CLA to gain full control of the email server, providing unauthorized access to the internal network. CLA was able to use this access to gain full control of the internal network, allowing access to any systems or files on the network.

Other high risk vulnerabilities were discovered related to missing security patches on ABC's websites and one of the firewalls. In addition, remote access services, like webmail and VPN, were not protected with multi-factor authentication. If an attacker gains access to an employee account, it would be possible to gain unauthorized access to these services from the Internet.

To summarize these issues:

- Web applications on an Extranet server were vulnerable to SQL injection, among other issues
- The Exchange server was missing a security patch that made it vulnerable to remote exploit
- Insecure filtering on the firewall allowed CLA to extract the password from the database server
- The database service account was an administrator and had a weak password
- Remote access services (VPN and webmail) did not require multi-factor authentication
- Other ABC websites were missing several patches or had insecure configurations

CLA recommends that ABC ensure all web applications are configured in a secure manner to mitigate web application attacks. The database user account should not have administrator rights and should be configured

with a stronger password. Input sanitization will mitigate the risk of SQL injection, along with other types of web-based vulnerabilities. The Exchange server and ABC websites should have the latest security patches applied. In addition, remote access services should be configured require multi-factor authentication. See Appendix A for more details.

Unauthorized Access Summary

The following table lists any data or elevated access CLA obtained during the assessment, as well as the associated findings CLA exploited. This may include gaining administrative access to systems or gaining unauthorized access to data in order to demonstrate the risk associated with identified findings.

Was CLA able to gain access to sensitive information?
YES **Notes** CLA was able to access sensitive information through 3 method(s). Sensitive Information Obtained: • Unauthorized access to extranet database server • Credentials for the database user account • Unauthorized access to email server and file transfer server **Exploited Findings** • SQL Injection (See finding #5). Affected 3 assets. • Insufficient Egress Filtering (See finding #41). Affected 1 asset. • Unauthorized access to online service (See finding #1). Affected 1 asset.

Was CLA able to obtain administrator privileges?
YES **Notes** CLA was able to gain local administrator privileges. CLA was able to gain domain administrator privileges. **Exploited Findings** • Security Updates for Exchange (See finding #18). Affected 1 asset.

<TRIMMED FOR BREVITY>

ABC Company

External Penetration Test

Appendix A - Exploitation Evidence

March 17, 2023

Please note the observations below are for discussion purposes only and do not necessarily contain all the findings that will appear in the final report.

Overview

This document demonstrates the risks associated with exploitable vulnerabilities discovered by CliftonLarsonAllen (CLA) during the engagement. Details and evidence for each exploitable vulnerability are included in the following page(s). Detailed information for the associated findings are located in the accompanying Excel spreadsheet:

DetailedFindings-ABC-EPT-2023.xlsx

Summary Table

The following table lists the vulnerabilities exploited along with the severity level and the number of assets affected by the vulnerability.

Table 1: Exploitation Evidence

Exploit	Exploited Vulnerability	Associated Finding #
1	SQL Injection	5
2	Insufficient Egress Filtering	41
3	Unauthorized access to online service	1
4	Exchange Deserialization Remote Code Execution	18
5	Insecure client-side access controls in web application	7
6	Cross-Site Scripting - Reflected	6

Exploit 1: SQL Injection

Description
SQL injection is a vulnerability in which an application takes user supplied input without properly sanitizing it and submits it within a SQL query. An attacker can abuse this to inject their own SQL commands that would get executed by the database server. This could allow an attacker to read sensitive data from the database, modify database data, execute administration operations on the database, and in some cases issue commands to the underlying operating system.

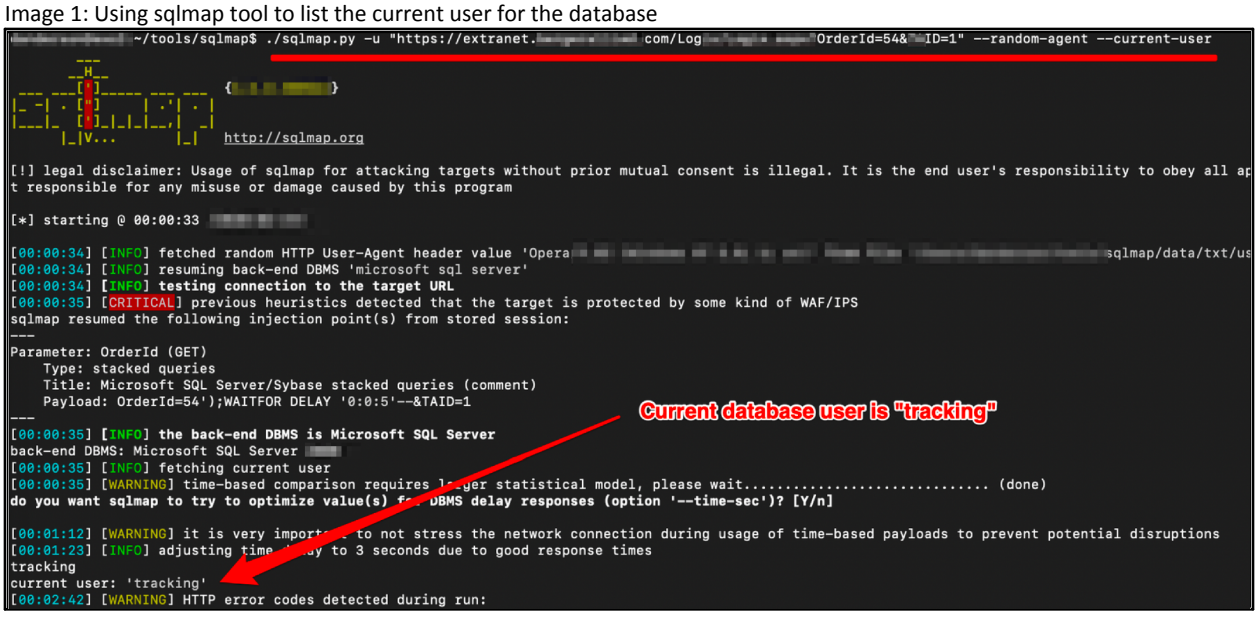
Associated finding
Finding #5: SQL Injection

Associated assets
extranet.website.com:443/tcp (https://extranet.website.com/Log.aspx),
extranet.website.com:443/tcp (https://extranet.website.com/Test/),
extranet.website.com:443/tcp (https://extranet.website.com/Winner/site.asp)

CLA was able to insert SQL statements into parameters on the Extranet website and have the database commands executed by the backend database system. This allowed CLA to perform SQL injection and gain control of the underlying database. Any data stored in the database was accessible by CLA.

There were multiple websites on the Extranet server that were affected by this vulnerability: Log, Winner, and Test.

Image 1: Using sqlmap tool to list the current user for the database



Exploit 2: Insufficient Egress Filtering

Description
Egress filtering is a control where the firewall restricts what ports and services internal employees are able to access on the Internet. Typically, only necessary traffic should be permitted, such as web browsing. The network allowed unnecessary network protocols to pass from the internal network to untrusted hosts on the Internet.

Associated finding
Finding #41: Insufficient Egress Filtering

Associated asset
[redacted]

CLA used the SQL injection vulnerability and executed the "xp_dirtree" stored procedure to cause the SQL database server to attempt to list the directory contents of a file share hosted by CLA on the Internet. This occurs over TCP port 445, which is commonly used for file and print sharing. This port should not be allowed from the internal network to the Internet.

CLA configured their system to capture authentication attempts and, since Windows systems automatically authenticate to file shares due to single sign-on, it was possible to capture the username and hashed password for the user account that the database was running as (**SQLService**).

CLA was able to crack the password for the SQLService account due to it having a weak password.

Image 2: Performing SQL injection to cause database sever to authenticate to CLA's server on the Internet over TCP 445

Image 3: Decoded SQL command

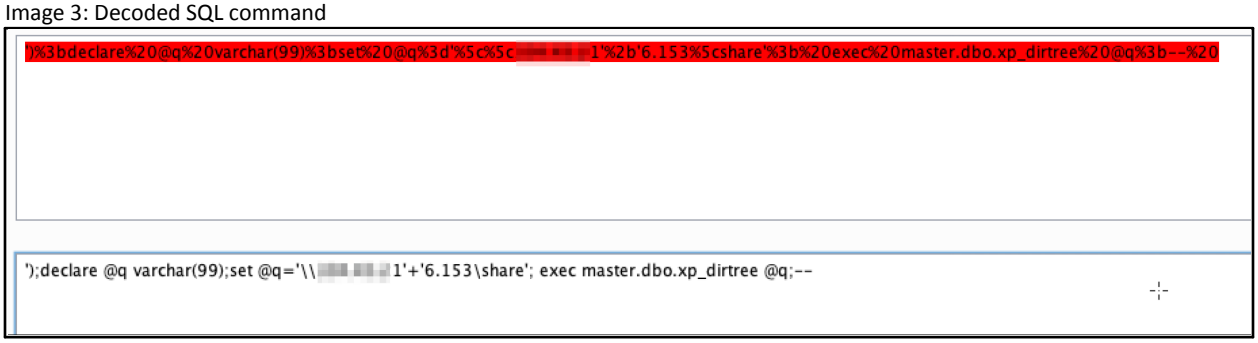


Image 4: Captured password hash for SQLService account

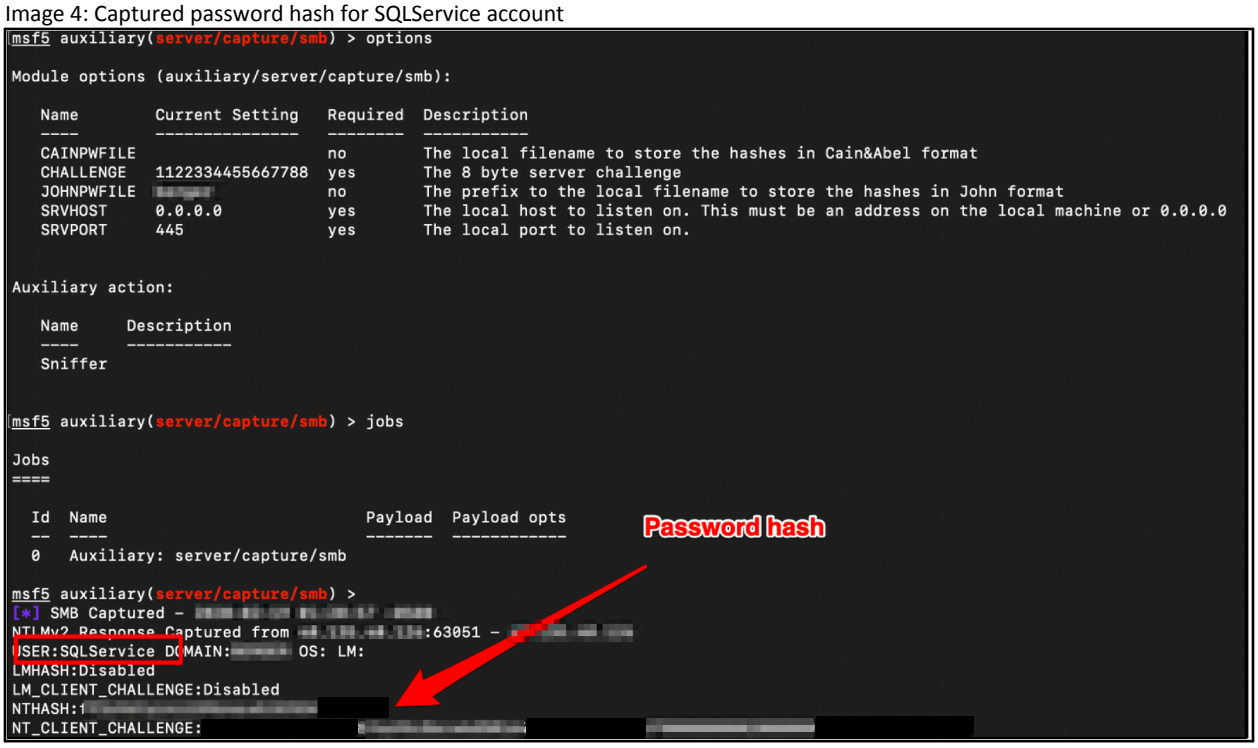


Image 5: Cracked password for SQLService account

<TRIMMED FOR BREVITY>

Detailed Findings - Excel Spreadsheet

Finding	Severity	CVSS	Classification	Description	Detail	Remediation	Category	Asset
1	Critical	n/a	Awareness, Monitoring and Alerting	Unauthorized access to online service	Unauthorized access to this online service was achieved using credentials harvested through email phishing or through a brute force login attack.	If this service is not needed to be accessible from the Internet, it should be blocked by the firewall.	User Awareness	device 1
2	Critical	10.0	Patch Management	Cisco ASA / IOS IKE Fragmentation Vulnerability	The remote Cisco Adaptive Security Appliance (ASA) or device running IOS / IOS XE is affected by one of the following vulnerabilities in the Internet Key Exchange (IKE)	Upgrade to the relevant fixed version referenced in Cisco Security Advisories cisco-sa-20160210-asa-ike and cisco-sa-20160323-ios-ikev2.	Network Device Patches	device 2
3	Critical	10.0	Patch Management	PHP Unsupported Version Detection	According to its version, the installation of PHP on the remote host is no longer supported, which implies that no new security patches for the product will be released by the	Upgrade to a version of PHP that is currently supported.	Web Application Vulnerabilities	device 3
3	Critical	10.0	Patch Management	PHP Unsupported Version Detection	According to its version, the installation of PHP on the remote host is no longer supported, which implies that no new security patches for the product will be released by the	Upgrade to a version of PHP that is currently supported.	Web Application Vulnerabilities	device 4
4	Critical	10.0	Patch Management	WordPress Unsupported Version Detection	According to its self-reported version number, the installation of WordPress running on the remote host is no longer supported.	Upgrade to a version of WordPress that is currently supported.	Web Application Vulnerabilities	device 5
5	Critical	7.5	Configuration Management	SQL Injection	SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out	The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two	Web Application Vulnerabilities	device 6
5	Critical	7.5	Configuration Management	SQL Injection	SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out	The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two	Web Application Vulnerabilities	device 7
5	Critical	7.5	Configuration Management	SQL Injection	SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out	The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two	Web Application Vulnerabilities	device 8
6	High	n/a	Configuration Management	Cross-site scripting (reflected)	Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the applications immediate response in an unsafe way. An attacker can use	In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:	Web Application Vulnerabilities	device 9
6	High	n/a	Configuration Management	Cross-site scripting (reflected)	Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the applications immediate response in an unsafe way. An attacker can use	In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:	Web Application Vulnerabilities	device 10
7	High	n/a	Authentication	Insecure client-side access controls in web application	The application relied upon client-side access controls to restrict access to features or pages within the application. Attackers can manipulate the client-side code to bypass	Ensure that all authentication and authorization is handled by the server so there is not a reliance upon client-side code.	Web Application Vulnerabilities	device 11
8	High	n/a	Configuration Management	Multi-factor authentication not required for remote access service	The service allows remote access to company resources and is not configured to require multi-factor authentication. If an attacker is able to guess a user's password or gain access	Configure the service to require multi-factor authentication.	Insecure or Misconfigured Services	device 12
8	High	n/a	Configuration Management	Multi-factor authentication not required for remote access service	The service allows remote access to company resources and is not configured to require multi-factor authentication. If an attacker is able to guess a user's password or gain access	Configure the service to require multi-factor authentication.	Insecure or Misconfigured Services	device 13
8	High	n/a	Configuration Management	Multi-factor authentication not required for remote access service	The service allows remote access to company resources and is not configured to require multi-factor authentication. If an attacker is able to guess a user's password or gain access	Configure the service to require multi-factor authentication.	Insecure or Misconfigured Services	device 14

<TRIMMED FOR BREVITY>

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

State of West Virginia
Centralized Request for Quote
Service - Prof

Proc Folder:	1369290		**Reason for Modification:**
Doc Description:	Network Penetration Testing and Cybersecurity Assessments		
Proc Type:	Central Master Agreement		
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2024-03-08	2024-03-28 13:30	CRFQ 0705 LOT2400000009	1

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: **000000184076**
Vendor Name : **CliftonLarsonAllen LLP**
Address : **220 South 6th St.**
Street : **Suite 300**
City : **Minneapolis**
State : **MN** **Country :** **Hennepin** **Zip :** **55402**
Principal Contact : **David Anderson**
Vendor Contact Phone: **612-376-4699** **Extension:** **N/A**

FOR INFORMATION CONTACT THE BUYER

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

Vendor Signature X  **FEIN#** 41-0746749 **DATE** March 28, 2024

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

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

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	External Network Penetration Testing			$19,950	

Comm Code	Manufacturer	Specification	Model #
81111801			

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

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Website Penetration Testing			$19,425	

Comm Code	Manufacturer	Specification	Model #
81111801			

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

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Internal/Client-Side Network Penetration Testing			$69,300	

Comm Code	Manufacturer	Specification	Model #
81111801			

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

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Wireless Penetration Testing			$56,700	

Comm Code	Manufacturer	Specification	Model #
81111801			

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

SCHEDULE OF EVENTS

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

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

GENERAL TERMS AND CONDITIONS:

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

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

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

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

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

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

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

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

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

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

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

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

☑ **Term Contract**

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

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

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

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

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

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

☐ the contract will continue for _____ years;

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

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

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

☐ **Other:** Contract Term specified in _____

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

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

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

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

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

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

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

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

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

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

☑ See Section 3. QUALIFICATIONS of the Specifications

☐

☐

☐

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

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

Vendor must maintain:

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

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

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

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

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

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

☐ **Pollution Insurance** in an amount of: _____ per occurrence.

☐ **Aircraft Liability** in an amount of: _____ per occurrence.

☐

☐

☐

☐

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

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

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

☐ _____ for _____.

☐ Liquidated Damages Contained in the Specifications.

☑ Liquidated Damages Are Not Included in this Contract.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(Printed Name and Title) David Anderson, Principal

(Address) 220 South Sixth Street, Suite 300, Minneapolis, MN 55402-1436

(Phone Number) / (Fax Number) 612-376-4699/612-376-4850

(email address) David.Anderson@CLAconnect.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.

CliftonLarsonAllen, LLP
(Company)

(Signature of Authorized Representative)

David Anderson, Principal 3/25/2024
(Printed Name and Title of Authorized Representative) (Date)

612-376-4699/612-376-4850
(Phone Number) (Fax Number)

David.Anderson@CLAconnect.com
(Email Address)

SPECIFICATIONS

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

   BACKGROUND INFORMATION:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.4.10.1 This certification is only applicable to Wireless Penetration Testing Services

3.4.11 Certified Mobile and Web Application Penetration Tester (CMWAPT)

3.4.11.1 This certification is only applicable to Website Penetration Services

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

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

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

4. MANDATORY REQUIREMENTS:

4.1. External Network Penetration Testing

4.1.1. External Network Penetration Testing may be performed remotely.

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

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

4.1.3.1. Reconnaissance should include:

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

4.1.3.1.2. OSINT - Public Searches/Dorks

4.1.3.1.3. Build custom password lists

4.1.3.1.4. DNS lookups (entities server)

4.1.3.1.5. Gather information from entities network resources

4.1.3.1.6. Analyze metadata

4.1.3.2. Mapping should include:

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

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

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

4.1.3.3. Discovery should include:

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

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

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

4.1.3.4. Exploitation should include:

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

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

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

4.1.4. Must identify exploitable vulnerabilities and demonstrate organizational impact.

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

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

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

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

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

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

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

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

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

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

4.1.12.1. How the vulnerability was discovered

4.1.12.2. The potential impact of its exploitation.

4.1.12.3. Recommendations for remediation.

4.1.12.4. Vulnerability references

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

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

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

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

4.2. Website Penetration Testing

4.2.1. Website Penetration Testing may be performed remotely.

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

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

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

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

4.2.5.1. Reconnaissance should include:

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

4.2.5.1.2. OSINT - Public Searches/Dorks

4.2.5.1.3. Build custom password lists

4.2.5.1.4. DNS lookups (entities server)

4.2.5.1.5. Gather information from entities web applications

4.2.5.1.6. Analyze metadata

4.2.5.2. Mapping should include:

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

4.2.5.2.2. Virtual Hosting & Load Balancer Analysis

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

4.2.5.2.4. HTTP Options Discovery (Identify accepted HTTP methods)

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

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

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

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

4.2.5.3. Discovery should include:

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

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

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

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

4.2.5.4. Exploitation should include:

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

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

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

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

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

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

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

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

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

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

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

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

4.2.12.1. How the vulnerability was discovered

4.2.12.2. The potential impact of its exploitation.

4.2.12.3. Recommendations for remediation.

4.2.12.4. Vulnerability references

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

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

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

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

4.3. Internal/Client-Side Network Penetration Testing

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

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

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

4.3.3.1. Reconnaissance should include:

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

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

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

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

4.3.3.2. Mapping and Discovery should include:

4.3.3.2.1. Identify possible vulnerabilities affecting the provided host

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

4.3.3.3. Exploitation should include:

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

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

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

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

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

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

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

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

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

4.3.8.1. How the vulnerability was discovered.

4.3.8.2. The potential impact of its exploitation.

4.3.8.3. Recommendations for remediation.

4.3.8.4. Vulnerability references.

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

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

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

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

4.4. Wireless Penetration Testing

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

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

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

4.4.3.1. Reconnaissance should include:

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

4.4.3.1.2. OSINT - Public Searches/Dorks

4.4.3.1.3. Build custom password lists

4.4.3.1.4. DNS lookups (entities server)

4.4.3.1.5. Gather information from entities web applications

4.4.3.1.6. Analyze metadata

4.4.3.2. Mapping should include:

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

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

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

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

4.4.3.3. Discovery should include:

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

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

4.4.3.3.3. Vulnerability Scanning (Identify vulnerabilities)

4.4.3.4. Exploitation should include:

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

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

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

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

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

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

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

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

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

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

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

4.4.8.1. How the vulnerability was discovered.

4.4.8.2. The potential impact of its exploitation.

4.4.8.3. Recommendations for remediation.

4.4.8.4. Vulnerability references.

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

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

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

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

5. CONTRACT AWARD:

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

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

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

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

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

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

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

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

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

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

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

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

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

10. VENDOR DEFAULT:

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

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

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

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

10.1.4. Failure to remedy deficient performance upon request.

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

10.2.1. Immediate cancellation of the Contract.

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

10.2.3. Any other remedies available in law or equity.

11. MISCELLANEOUS:

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

Contract Manager: David Anderson
Telephone Number: (612) 376-4699
Fax Number: 612-376-4850
Email Address: David.Anderson@CLAconnect.com

EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	$ 19,950 -	$ 159,600 -
2	4.2	Website Penetration Testing	8	$ 19,425 -	$ 155,400 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 69,300 -	$ 554,400 -
4	4.4	Wireless Penetration Testing	8	$ 56,700 -	$ 453,600 -
				TOTAL BID AMOUNT	$ 1,323,000 -

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

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

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

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

Vendor Name:	CliftonLarsonAllen, LLP
Vendor Address:	220 South Sixth Street, Sutie 300, Minneapolis, MN 55402-1436
Email Address:	David.Anderson@claconnect.com
Phone Number:	(612) 376-4699
Fax Number:	612-376-4850
Signature and Date: