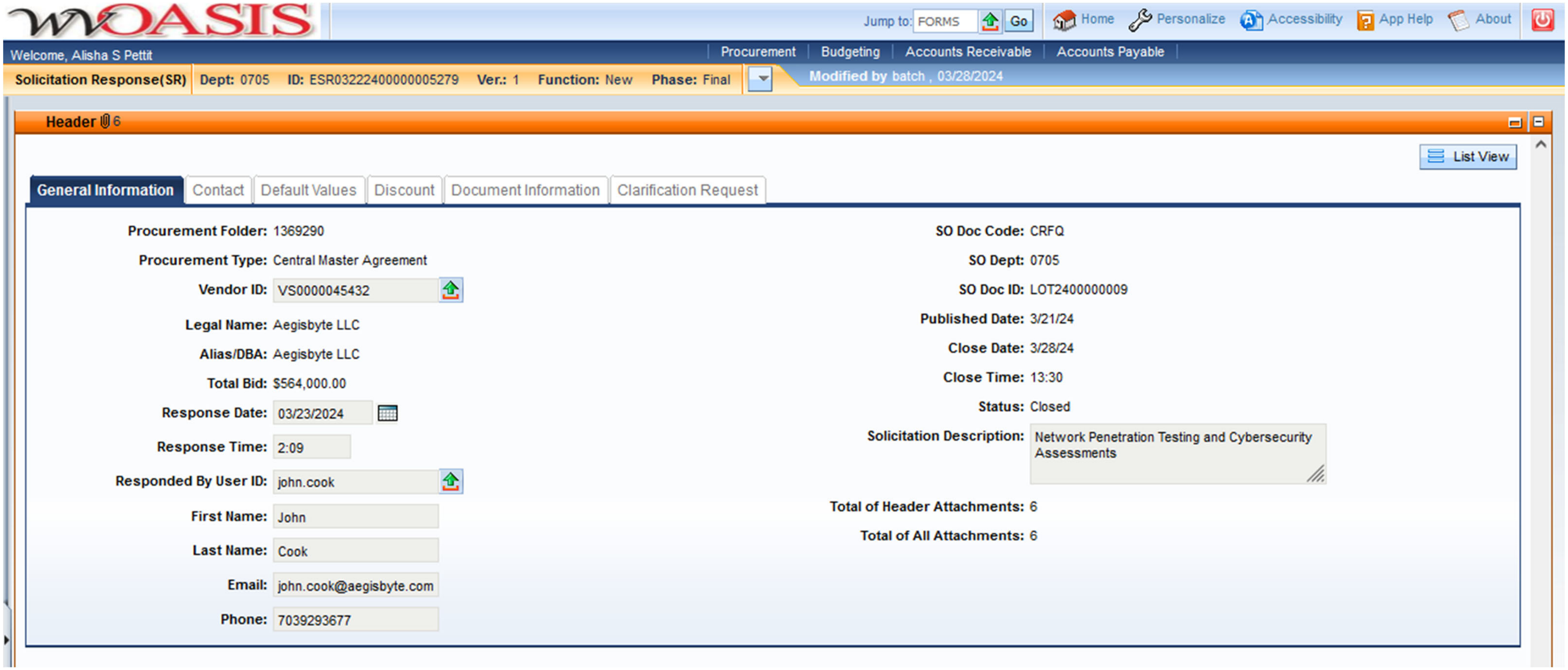
West Virginia
Purchasing Division

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

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



Welcome, Alisha S Pettit

Solicitation Response(SR) Dept: 0705 ID: ESR03222400000005279 Ver.: 1 Function: New Phase: Final

Modified by batch , 03/28/2024

Header 6

Procurement Folder:	1369290	SO Doc Code:	CRFQ
Procurement Type:	Central Master Agreement	SO Dept:	0705
Vendor ID:	VS0000045432	SO Doc ID:	LOT2400000009
Legal Name:	Aegisbyte LLC	Published Date:	3/21/24
Alias/DBA:	Aegisbyte LLC	Close Date:	3/28/24
Total Bid:	$564,000.00	Close Time:	13:30
Response Date:	03/23/2024	Status:	Closed
Response Time:	2:09	Solicitation Description:	Network Penetration Testing and Cybersecurity Assessments
Responded By User ID:	john.cook	Total of Header Attachments:	6
First Name:	John	Total of All Attachments:	6
Last Name:	Cook		
Email:	john.cook@aegisbyte.com		
Phone:	7039293677		

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 ESR03222400000005279	1

VENDOR

VS0000045432
Aegisbyte LLC

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 564000 **Response Date:** 2024-03-23 **Response Time:** 02:09:25

Comments:

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

Vendor Signature X **FEIN#** **DATE**

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	External Network Penetration Testing				200000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Cost includes travel and lodging.

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				39000.00

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				200000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Cost includes travel and lodging.

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				125000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Cost includes travel and lodging.

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

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	$25,000.00	$200,000.00
2	4.2	Website Penetration Testing	1	$39,000.00	$39,000.00
3	4.3	Internal/Client-Side Network Penetration Testing	8	$25,000.00	$200,000.00
4	4.4	Wireless Penetration Testing	10	$12,500.00	$125,000.00
				TOTAL BID AMOUNT	$564,000.00

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

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

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

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

Vendor Name:	Aegisbyte LLC
Vendor Address:	14894 Heather Bloom Dr Woodbridge, VA 22193
Email Address:	contact@aegisbyte.com
Phone Number:	(866) 422-5375 / 703-929-3673
Fax Number:	
Signature and Date:	03/22/2024

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

(Printed Name and Title) John W. Cook Jr

(Address) 5464 Lavender Lane Woodbridge, VA 22193

(Phone Number) / (Fax Number) 703-929-3677

(email address) john.cook@aegisbyte.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.

Aegisbyte LLC
(Company)

(Signature of Authorized Representative)

Felix Alcala - CEO
(Printed Name and Title of Authorized Representative) (Date)

(866) 422-5375 / 703-929-3673
(Phone Number) (Fax Number)

felix.alcala@aegisbyte.com
(Email Address)

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

State of West Virginia
Centralized Request for Quote
Service - Prof

Proc Folder: 1369290

Doc Description: Network Penetration Testing and Cybersecurity Assessments

Proc Type: Central Master Agreement

Reason for Modification:

Date Issued	Solicitation Closes	Solicitation No	Version
2024-03-08	2024-03-28 13:30	CRFQ 0705 LOT2400000009	1

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name : Aegisbyte LLC

Address : 14894 Heather Bloom Dr

Street :

City : Woodbridge

State : VA **Country :** USA **Zip :** 22193

Principal Contact : John Cook, Jr

Vendor Contact Phone: 703-929-3677 **Extension:**

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

Vendor Signature X **FEIN#** 92-0532707 **DATE** 03/22/2024

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

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

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	External Network Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

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

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Website Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

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

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

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

Comm Code	Manufacturer	Specification	Model #
81111801			

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

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Wireless Penetration Testing				

Comm Code	Manufacturer	Specification	Model #
81111801			

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

SCHEDULE OF EVENTS

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

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

MUTUAL NON-DISCLOSURE AGREEMENT

This Mutual Non-Disclosure Agreement ("Agreement") is entered into by and between the West Virginia Lottery, with its principal offices located at 900 Pennsylvania Avenue Charleston, WV 25302 ("Lottery"), and Aegisbyte LLC, with its principal offices located at 14894 Heather Bloom Dr, Woodbridge ("Party of the second part"), with an Effective Date of March 20th 2024. Lottery and Party of the second party also are referred to herein individually as a "party", or collectively as the "parties".

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

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

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

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

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

II. **Disclosure Period and Term**. This Agreement protects against the disclosure of Confidential Information which is disclosed between the parties during each party's performance of its obligations associated with that certain CRFQ Agreement executed between the parties on March 20th 2024 (the "Effective Date") and 3 year(s) after the termination of such Agreement ("Disclosure Period"). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

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

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

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

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

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

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

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

EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

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

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

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

WEST VIRGINIA LOTTERY

By: ________________________________

Name: ________________________________

Title: ________________________________

Aegisbyte LLC **(VENDOR)**

By: ________________________________

Name: Felix Alcala

Title: Founder / CEO

MARCH 22ND, 2024

PROJECT PROPOSAL

WEST VIRGINIA - LOTTERY COMMISSION
(CRFQ-0705-LOT2400000009-1)

PRESENTED BY:

AEGISBYTE

Table of Contents

ABOUT AEGISBYTE

Aegisbyte is a Service-Disabled Veteran-Owned Business (SDVOB) and a Minority-Owned Enterprise that brings military expertise and business acumen to cybersecurity. With 90% of its security engineers and operations staff having military backgrounds, Aegisbyte is uniquely positioned to deliver unparalleled security solutions.

The founder of Aegisbyte has over two decades of deep cybersecurity experience, focusing on offensive security engineering. His broad experience covers systems and network administration, information assurance, and systems architecture. He has pivotal roles in high-intensity environments like SOCs, leading significant penetration testing projects. Aegisbyte has contributed to U.S. Navy programs like NAVAIR and the F35 initiative and held leadership positions for ARCYBER. It has managed penetration tests for federal entities like U.S. Customs and the CISA. Aegisbyte's roles often combined leading assessments with mentoring upcoming cybersecurity talents. Technically adept, Aegisbyte has developed tools and modules for platforms like Metasploit, Tenable, and Burp Suite. Its proficiency extends to real-time operating systems like VxWorks. Having been a part of the hacking community since the early '90s, Aegisbyte has contributed a wealth of exploits, underlining its dedication to cybersecurity. The founder's vision for Aegisbyte is clear: to deliver unmatched cybersecurity services. With its vast expertise, Aegisbyte pledges to provide tailored and formidable cybersecurity solutions for every client.

Aegisbyte has charted an impressive 20-year trajectory through the intricate landscapes of cybersecurity. Beginning with foundational experiences in the US Army Special Operations, specifically the 75th Ranger Regiment 2nd Ranger Battalion, Aegisbyte embraces rigorous disciplines and strategies over four transformative years. Transitioning from the military, Aegisbyte took on the mantle of security at a nuclear power plant. Responsibilities extended beyond the role to protect physical infrastructure and digital assets, showcasing a profound understanding of complex systems and a commitment to their defense. Aegisbyte engages with defensive and offensive cybersecurity operations and is imperative in identifying aviation. It has notable experience in malware and reverse engineering, blending an enthusiasm for technology with meticulous attention to security. Aegisbyte's mission is articulated with clarity and purpose to lead the nation's most innovative, efficient, and effective cybersecurity consulting firm. It creates tailored, next-level strategies for each client, building upon its unique strengths and veteran-owned heritage.

ORGANIZATION'S LEADERSHIP

FELIX ALCALA
CEO

JASON BREWER
CSO

JOHN COOK
COO

CERTIFIED
MINORITY
OWNED
BUSINESS

Service Disabled Veteran Owned Small Business
SDVOSB
CVE

MISSION AND VISION

Since opening our doors in 2022, Aegisbyte has not only carved its niche in the cybersecurity realm but also forged sterling partnerships with the crème de la crème of the corporate world. We're not just name-dropping here; we're talking about collaborations with giants like Cisco, Tenable, Experis, GSK, Amtrak, Lumen, and many more. Each association underscores our prowess in the offensive security domain.

Our specialty? Offering robust offensive security services that don't merely tick boxes but set industry benchmarks. Every partnership with these titans is a testament to our commitment, expertise, and ability to approach challenges. When corporations of such stature trust Aegisbyte for offensive security projects, it's evident we're not just in the game but leading it.

MISSION

Our process allows us to provide industry-leading protection for systems and apps across virtually any platform or industry. We also recognize that specific industries may have distinct data and systems security needs. We provide strategic security services focusing on the needs of the following sectors.

VISION

We offer a unique perspective and valuable insights into how an attacker could exploit vulnerabilities within an organization. Our team has the experience and knowledge to conduct comprehensive, real-world testing to help organizations identify and fix critical security issues before they can be exploited.

CUSTOMERS AND PARTNERS

tenable	Developed NASL and researched security vulnerabilities for Tenable.
cisco	Executed offensive security testing on Cisco networks and applications
gsk GlaxoSmithKline	Performed network penetration testing for GSK and custom Tenable code for their Tenable SecurityCenter and OT environments.
CLEARPATH	Partnered up with ClearPath to win more Tenable contracts in development and research.
Jefferson Wells™ ManpowerGroup	Partnered up with Experis and Jefferson Wells to execute offensive security projects and deliverables. Delivering over 100 web/API and network penetration tests since launch in September 2022

At Aegisbyte, our alliance with esteemed partners such as Tenable, Cisco, Experis, and others amplifies our commitment to excellence. We've meticulously curated a team that complements our clients' talented ranks and seamlessly integrates to provide robust security solutions.

While our approach is amiable and collaborative, our dedication to safeguarding our clients remains paramount. A glance at our clientele and accomplishments speaks volumes about our credentials. We aspire to become an integral, trusted pillar in your security infrastructure.

COVER LETTER

Aegisbyte is all set to provide cybersecurity and network penetration testing services to the West Virginia Lottery Commission. These services will cover a range of methods and evaluations customized to pinpoint, exploit, and suggest solutions for vulnerabilities in parts of the Commission's digital and physical network systems. The assessments will follow structured approaches across external networks, websites, internal/client-side networks, and wireless systems. This will ensure examination and detailed analysis of security threats.

The external and website penetration testing services will be conducted remotely, focusing on the defense mechanisms of networks and website security individually. These evaluations will stick to a timeline and list of exclusions agreed upon by both parties: Aegisbyte and the West Virginia Lottery Commission. The methodology for both types of assessments consists of four phases: reconnaissance (gathering data through WHOIS lookups, open source intelligence sources, and DNS queries), mapping (including scanning networks and ports), discovery (identifying vulnerabilities using tools like Nessus and Burp Suite), and exploitation (demonstrating possible breach techniques).
When conducting network tests, it's important to note that denial of service (DoS) attacks are not allowed. Both assessments involve a social engineering exercise mainly focusing on a phishing email scenario.

Internal and client-side wireless penetration testing must be conducted on-site at all Lottery locations to ensure a thorough evaluation of security measures from an insider's viewpoint and the integrity of wireless networks. These tests follow a four-phase approach and are customized to address the specific risks of internal networks and wireless communications. This involves testing against malware solutions' security restrictions and exploiting vulnerabilities to assess potential unauthorized access or data breaches. Particular emphasis is placed on identifying rogue access points and ensuring communications security encompassing Bluetooth and ZigBee technologies.

After each assessment, Aegisbyte provides reports and presentations to the Lottery Commission. These include an Executive Summary Report offering an overview of findings and recommendations, a Technical Report outlining identified vulnerabilities with risk ratings and remediation suggestions, and a Findings Presentation to discuss outcomes with Lottery management.

These items aim to provide the West Virginia Lottery Commission with information to enhance its cybersecurity defenses.

EXECUTIVE SUMMARY

Aegisbyte LLC is pleased to submit our proposal in response to the State of West Virginia's solicitation CRFQ 0705 LOT2400000009 for Network Penetration Testing and Cybersecurity Assessments. As a Service-Disabled Veteran-Owned Business (SDVOB) and a Minority-Owned Enterprise with extensive experience providing cutting-edge cybersecurity solutions, Aegisbyte LLC is uniquely positioned to meet and exceed the State of West Virginia requirements. Our team of highly qualified professionals, led by founder Felix Alcala, combines military precision with advanced cybersecurity expertise to deliver comprehensive penetration testing and security assessments that safeguard critical infrastructure against evolving threats.

Company Overview:

Founded in 2022, Aegisbyte LLC has quickly established itself as a leader in cybersecurity, specializing in advanced penetration testing, ethical hacking, and threat simulations. Our services are designed to identify vulnerabilities before they can be exploited, ensuring the security and integrity of our clients' networks and systems. With over 1500 assessments conducted, including 350+ web and API application assessments and security enhancements for over 200 mobile applications, Aegisbyte's track record speaks to our commitment to excellence and our ability to deliver tailored solutions that meet the specific needs of our clients. In cybersecurity, specializing in advanced penetration testing, ethical hacking, and threat simulations. Our services are designed to identify vulnerabilities before they can be exploited, ensuring the security and integrity of our clients' networks and systems. With over 1500 assessments conducted, including 350+ web and API application assessments and security enhancements for over 200 mobile applications, Aegisbyte's track record speaks to our commitment to excellence and our ability to deliver tailored solutions that meet the specific needs of our clients.

Proposed Services:

In response to the RFP, Aegisbyte LLC proposes to provide the following services:

1. **External Network Penetration Testing -** Leveraging our advanced methodologies, Aegisbyte will conduct comprehensive testing of the State's external network infrastructure to identify and exploit vulnerabilities, providing detailed reporting and recommendations for remediation.

2. **Website Penetration Testing -** Utilizing techniques from the OWASP Top 10 Project, our team will assess the security of the sState'sweb presence, identify potential risks, and provide actionable insights to enhance website secure actionable insights to enhance website security.

3. **Internal/Client-Side Network Penetration Testing -** Through rigorous assessment of internal network components, Aegisbyte will identify potential internal threats and provide strategies for strengthening the State's internal defenses.

4. **Wireless Penetration Testing -** Aegisbyte will assess the security of the State's wireless networks, identify vulnerabilities, and provide recommendations for securing wireless communication channels against unauthorized access.

Compliance and Methodology

Aegisbyte LLC's services are aligned with industry best practices and compliance standards, including HIPAA, PCI DSS, FedRAMP, ISO27001, and SOC2. Our methodology, inspired by our military background and adherence to the Center for Internet Security (CIS) and the NIST SP 800-115 guidelines, ensures a comprehensive and systematic approach to cybersecurity assessments.

Qualifications and Experience

Our team's unparalleled qualifications include CISSP, GPEN, OSCP, CEH, and more. Our founder, Felix Alcala, brings over two decades of cybersecurity experience, contributing to significant projects for the U.S. Navy, ARCYBER, and other federal entities. Aegisbyte's commitment to excellence is further demonstrated by our active engagement in the cybersecurity community and our development of proprietary tools and methodologies.

Conclusion

Aegisbyte LLC is fully committed to partnering with the State of West Virginia to enhance its cybersecurity posture. Our unique blend of military discipline, advanced cybersecurity expertise, and commitment to tailored solutions makes us the ideal partner for this critical initiative. We look forward to discussing our proposal further and contributing to the security and resilience of the State of West Virginia's digital infrastructure.

PROJECT MANAGEMENT

Aegisbyte LLC is dedicated to providing the State of West Virginia with a comprehensive and detailed penetration testing service to uphold the utmost security and compliance standards. Our methodology is designed to meet the specific requirements set forth by the State of West Virginia, ensuring a tailored and practical approach to enhancing the state's cybersecurity defenses.

Post-Remediation Reviews

Aegisbyte will provide comprehensive post-remediation reviews to discuss the outcomes of remediation efforts. These sessions will include reassessing previously identified vulnerabilities to ensure that all security issues have been effectively addressed and mitigated.

Methodology for Network and Asset Assessment

Our methodology encompasses a multi-layered approach, starting with reconnaissance to gather intelligence about the target environment. This is followed by vulnerability scanning using industry-leading tools and techniques, exploitation where feasible to understand the depth of potential breaches, and reporting and providing strategic remediation guidance. Throughout the process, we focus on technical vulnerabilities and potential human-factor weaknesses.

Data Management

After finalizing the testing activities, Aegisbyte LLC will ensure a comprehensive clean-up process for the State of West Virginia, which includes:

- Deletion of all accounts explicitly established for testing activities.
- Remove any tools or software deployed on the State of West Virginia’s systems during the penetration tests.
- Secure eradication of confidential information obtained during the testing phase, following industry-standard protocols for data destruction.

Data Storage and Confidentiality

Aegisbyte LLC will not retain any data collected during the penetration testing, guaranteeing the confidentiality and security of the State of West Virginia's information. To formalize this commitment, a non-disclosure agreement (NDA) will be executed, with the State of West Virginia keeping a copy for its records.

PROJECT MANAGEMENT

Aegisbyte LLC is committed to offering the State of West Virginia a thorough and precise penetration testing service customized to comply with the security and compliance requirements of the solicitation **CRFQ 0705 LOT2400000009**. Our project management plan outlines the systematic approach we will utilize to ensure the penetration testing process adheres to the highest security and efficiency standards.

Post-Remediation Reviews

Upon completing the remediation efforts, Aegisbyte will conduct detailed post-remediation reviews with the State of West Virginia. These sessions are designed to evaluate the effectiveness of the remediation actions taken, with a re-assessment of the vulnerabilities to confirm that all identified security issues have been fully resolved and appropriately mitigated.

Methodology for Network and Asset Assessment

Our methodology follows a structured multi-phased approach, ensuring a thorough assessment of the State's network and assets:

- **Reconnaissance** - The initial phase involves gathering intelligence on the target environment to identify potential entry points and valuable assets.
- **Vulnerability Scanning** - Using leading-edge tools and techniques to scan for vulnerabilities, identifying potential security weaknesses within the network and systems.
- **Exploitation**—Simulated attacks on identified vulnerabilities, where feasible, to assess the depth of potential breaches and understand their real-world impact.
- **Reporting and Remediation Guidance** - Comprehensive reporting on findings with strategic remediation guidance, focusing on technical vulnerabilities and human-factor weaknesses.

Data Management and Clean-up Process

Following the completion of penetration testing activities, Aegisbyte ensures a thorough clean-up process to maintain the integrity and security of the State's systems:

- **Removal of Testing Footprint** - All accounts created for testing purposes will be deleted, and any tools or software introduced during the penetration testing process will be uninstalled.
- **Secure Data Disposal** - All confidential data obtained during the penetration tests will be disposed of securely, in accordance with best data destruction practices, ensuring that no residual data remains. Following the customer's directions, the data will be deleted from repositories 30 days after the assessment is completed.

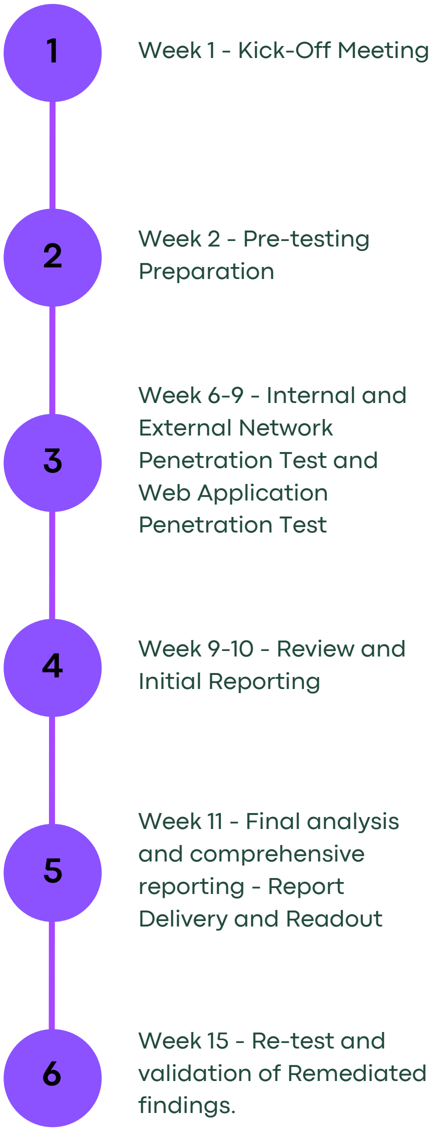
Data Storage and Confidentiality

Aegisbyte will maintain the highest standards of data confidentiality and security throughout the project:

- **No Data Storage Policy** - Aegisbyte will not store data obtained during the penetration tests, ensuring the complete confidentiality and security of the State of West Virginia's information.
- **Non-Disclosure Agreement (NDA)** - An NDA will be signed between Aegisbyte and the State of West Virginia, with the State retaining a copy for its records to ensure the confidentiality of the project details and findings legally.

PROPOSED TIMELINE

1. **Kick-off Meeting**
   - Within one week of contract signing, establish the project scope, objectives, and initial coordination with the State's IT team.
2. **Pre-Testing Preparation**
   - Two weeks after kick-off: Finalize testing methodologies, tools, and target environments based on initial assessments and discussions.
3. **Internal and External Penetration Testing**
   - Conduct external penetration tests to ensure alignment with the state's external network environment and security policies.
   - Execute internal penetration tests across designated locations (8), coordinating closely with on-site IT personnel.
   - Wireless Assessment of each facility (8).
4. **Review and Initial Reporting**
   - Present the initial findings to the State's IT team for preliminary review and discussion.
5. **Final analysis and comprehensive reporting - Report Delivery and Readout**
   - Complete a detailed analysis of all external, internal, web application, and wireless test findings and prepare comprehensive reports.
   - Present the final findings, recommendations, and remediation strategies to the State's management and IT teams.
6. **Post-Remediation Review and Finalization**
   - **Optional** - Conduct post-remediation assessments, if applicable, and finalize all documentation and reporting.



1 Week 1 - Kick-Off Meeting

2 Week 2 - Pre-testing Preparation

3 Week 6-9 - Internal and External Network Penetration Test and Web Application Penetration Test

4 Week 9-10 - Review and Initial Reporting

5 Week 11 - Final analysis and comprehensive reporting - Report Delivery and Readout

6 Week 15 - Re-test and validation of Remediated findings.

This timeline provides a structured approach to the penetration testing project. It allows for thorough planning, execution, and reporting while also accommodating the state of West Virginia's operational needs and feedback.

Proposal for Section 4.1 - External Network Penetration Testing

External Network Penetration Testing (Section 4.1)

- Aegisbyte LLC acknowledges that it is securing the State of West Virginia Lottery's external network against potential cyber threats. Our proposed approach for External Network Penetration Testing encompasses the following structured methodology, aligning closely with the RFP's specifications:

Remote Testing Capability (Section 4.1.1)

- Aegisbyte is fully equipped to perform External Network Penetration Testing remotely, employing secure and efficient methods to simulate external cyber threats without needing physical presence at the Lottery's facilities.

Coordination of Timeframes and Schedules (Section 4.1.2)

- We commit to working closely with the Lottery to establish clear timeframes, testing schedules, target completion dates, and any necessary exclusions, ensuring a seamless and minimally disruptive testing process.

Four-Phased Structure Methodology (Section 4.1.3)

Our testing methodology is divided into four critical phases: reconnaissance, mapping, discovery, and exploitation, each incorporating specific activities aligned with the RFP's requirements:

- **Reconnaissance (Section 4.1.3.1)**
  - Perform WHOIS, ARIN, and DNS lookups.
  - Conduct Open Source Intelligence (OSINT) gathering using public searches and Google Dorks.
  - Build custom password lists tailored to the Lottery's external network environment.
  - Execute DNS lookups for entities' servers and gather information from the entities' network resources.
  - Analyze metadata for initial vulnerability indicators.

- **Mapping (Section 4.1.3.2)**
  - Network Discovery using ICMP sweeps, traceroutes, and methods to bypass firewall restrictions.
  - Port/Protocol Scanning to identify open TCP/UDP ports and accepted IP protocols.
  - OS/Version Scanning to determine underlying operating systems and software versions.

- **Discovery (Section 4.1.3.3)**
  - Utilize open-source and commercial tools like Nessus and Burp Suite for Vulnerability Scanning.
  - Enumerate Network Services to disclose information, gain access, and identify misconfigurations.
  - Conduct Username/Email Enumeration to validate and guess credentials using various methods.

- **Exploitation (Section 4.1.3.4)**
  - Implement Brute Force Logins using discovered credentials to gain additional access.
  - Exploit identified vulnerabilities to gain further access and disclose information.
  - Perform Post-Exploitation and Pivot actions to uncover additional vulnerabilities and leverage compromised systems to explore the network further.

Identification of Exploitable Vulnerabilities (Section 4.1.4)

- Our testing will identify exploitable vulnerabilities and assess their potential impact on the Lottery's organizational security, providing critical insights for remediation.

Prohibition of DoS Attacks (Section 4.1.5)

- In line with the RFP, Aegisbyte ensures that Denial of Service (DoS) attacks will not be part of our testing strategy to maintain the integrity and availability of the Lottery's services.

Proposal for Section 4.1 - External Network Penetration Testing (cont.)

Inclusion of a Social Engineering Exercise (Section 4.1.6)

- A carefully designed phishing email scenario will be included to target approximately 200 active Lottery staff, with content and target addresses developed in collaboration with the Lottery for approval before execution.

Approval for Heavy Load and Brute Force Attacks (Section 4.1.7)

- Any heavy load brute force or automated attacks will be conducted only with prior approval from the Lottery, ensuring transparency and consent.

Notification of Service Disruption (Section 4.1.8)

- Immediate notification will be provided to the Lottery for any assessment activities resulting in unexpected service disruption.

Immediate Reporting of Critical Vulnerabilities (Section 4.1.9)

- Any discovered security vulnerabilities posing immediate threats to critical business processes or IT services will be promptly reported to the Lottery.

Deliverables (Section 4.1.10)

Upon assessment conclusion, Aegisbyte will provide:

- An **Executive Summary Report** and a **Technical Report** detailing the scope, approach, findings, and recommendations, with samples available upon request.

- A **Findings Presentation** to the Lottery management team, offering a comprehensive overview of the assessment's outcomes. The presentation format (in-person or conference call) will be determined in collaboration with the Lottery.

Proposal for Section 4.2 - Website Penetration Testing Requirements

Remote Performance Capability (Section 4.2)

Aegisbyte LLC is equipped to perform comprehensive website penetration testing remotely, aligning with modern cybersecurity best practices and the flexibility required by the State of West Virginia.

Coordination of Timeframes and Schedules (Section 4.2.2)

We will work closely with the State of West Virginia to establish clear timeframes, testing schedules, target completion dates, and any exclusions, ensuring our operations are seamlessly integrated with state requirements and timelines.

Assessment of Web Environment Complexity (Section 4.2.3)

Aegisbyte will meticulously determine the count of static and dynamic pages within each web environment, including production, development, and quality assurance, conducting assessments tailored to each unique environment.

Four-Phased Structure Methodology (Section 4.2.4)

Our comprehensive methodology, meticulously designed to uncover vulnerabilities and bolster web application security, encompasses reconnaissance, mapping, discovery, and exploitation phases.

Reconnaissance Phase (Section 4.2.5.1)

- **WHOIS, ARIN, and DNS Lookups -** Initial steps to gather intelligence on domain ownership, IP range allocation, and DNS configurations.
- **OSINT Techniques -** Utilizing open-source intelligence to uncover publicly available information via search engines and specialized tools.
- **Password List Creation -** Custom password lists are built, leveraging information gathered during reconnaissance to enhance brute force and credential stuffing attacks.
- **Network Resource Information Gathering -** Aggregating data from the entity's network resources to map the digital landscape.
- **Metadata Analysis -** Examining files and web elements to extract metadata that may reveal internal paths, software versions, or sensitive information.

Mapping Phase (Section 4.2.5.2)

- **SSL/TLS and Network Discovery -** Analysis of security certificates, virtual hosting environments, and network topography.
- **Software Configuration and HTTP Options Discovery -** Identifying web server configurations, services, and HTTP methods enabled.
- **Web Application Spidering -** Automated crawling of web applications to enumerate links, directories, and functionalities.
- **Session Analysis -** Investigation of how and where session cookies are set and their attributes and predictability.

Proposal for Section 4.2 - Website Penetration Testing Requirements (cont.)

Discovery Phase (Section 4.2.5.3)

- **Vulnerability and Service Enumeration -** This involves using open-source and commercial tools to scan for vulnerabilities and manually enumerating services to uncover misconfigurations or insecure protocols.

- **Web Application Specific Vulnerabilities -** Identification and testing for OWASP Top 10 vulnerabilities and beyond, including business logic errors and session management flaws.

Exploitation Phase (Section 4.2.5.4)

- **Credential Attack and System Exploitation -** Applying brute force techniques and exploiting identified vulnerabilities to gain unauthorized access.

- **Post-Exploitation Analysis -** Further exploiting the compromised system to discover additional vulnerabilities and sensitive data, employing pivoting techniques for broader access.

Prioritization of Remediation (Section 4.2.6)

Our findings will highlight vulnerabilities with prioritized remediation strategies, ensuring that the State of West Virginia can effectively mitigate risks based on their impact and exploitability.

Comprehensive Testing (Section 4.2.7)

Each component of the website's ecosystem, from server OS to application platforms and databases, will be rigorously tested to ensure no vulnerability is overlooked.

Denial of Service (DoS) Policy (Section 4.2.8)

Aegisbyte understands the critical nature of DoS attacks and will undertake such testing only with explicit approval from the State, ensuring no disruption to services.

Controlled Attack Simulation (Section 4.2.9)

Heavy load and brute force attacks will be conducted under controlled environments and only with prior approval, ensuring the integrity of the web applications.

Reporting and Communication (Section 4.2.10)

Upon assessment conclusion, Aegisbyte will provide an Executive Summary Report and a Technical Report detailing our methodology, findings, and recommendations. A Findings Presentation will complement these reports, facilitating a comprehensive security posture review and actionable insights.

- **Executive Summary Report** - This report provides an overview of the testing scope, approach, key findings, and recommendations for senior management.

- **Technical Report** - Detailed analysis of each identified vulnerability, including discovery methods, potential impacts, and remediation strategies.

- **Findings Presentation** - An interactive session with the Lottery management team to discuss the assessment's outcomes, highlight critical vulnerabilities, and recommend the next steps.

Aegisbyte LLC is committed to ensuring the highest level of web application security for the State of West Virginia, aligning our advanced testing methodologies with the state's specific requirements to safeguard against evolving cyber threats.

Proposal for Section 4.2 - Website Penetration Testing Requirements (cont.)

Aegisbyte presents a strategy that combines various industry-standard tools and technologies. They utilize Burp Suite Professional for analyzing and exploiting security vulnerabilities and Invicti for automated detection of common threats like SQL Injection and Cross-site Scripting. Their approach focuses on reducing positives through Proof-Based Scanning™. Additionally, they incorporate open-source tools specific to cybersecurity to target vulnerability detection based on the web applications' threat landscape.

In addition to tools, Aegisbyte introduces its internally developed tools, which stem from extensive offensive security expertise and innovative cybersecurity research. These exclusive tools tackle security issues and are integrated into a comprehensive testing process covering reconnaissance, vulnerability assessment, exploitation, post-exploitation activities, and detailed reporting. This thorough methodology does not only identify vulnerabilities but also offers insights for effective remediation by leveraging Aegisbyte's cybersecurity knowledge and custom technological solutions to bolster the web applications' security posture.

Proposal for Section 4.3 - Internal / Client-Side Network Penetration Testing Requirements

On-site Testing Requirement (Section 4.3.1)

Aegisbyte LLC acknowledges the requirement for on-site internal/client-side network penetration testing at all Lottery locations. Our experienced team is prepared to conduct these assessments in person, ensuring comprehensive coverage and adherence to the specific security environments of each location.

Coordination of Testing Schedule (Section 4.3.2)

We will closely collaborate with the Lottery to define testing schedules, completion dates, and any necessary exclusions, tailoring our approach to meet operational needs and minimize disruptions.

Four-Phased Methodology (Section 4.3.3)

Our methodology encompasses four critical phases: reconnaissance, mapping, discovery, and exploitation, ensuring a thorough assessment of the internal network's security posture.

Reconnaissance Phase (Section 4.3.3.1)

- **Software and Configuration Analysis -** Identify software versions and configurations to uncover potential security weaknesses.

- **Security Product Identification -** Examine anti-malware, firewall, and IDS/IPS solutions for misconfigurations or bypass opportunities.

- **Network Information Gathering -** Compilation of network details such as domain user/group information, domain computers, and password policies.

- **Execution Rights Verification -** Assessing the network's controls over script and third-party program execution to identify potential avenues for exploitation.

Mapping and Discovery Phase (Section 4.3.3.2)

- **Vulnerability Identification -** Use of manual techniques and automated tools to identify vulnerabilities that could be exploited.

- **Payload Feasibility -** Evaluation of the network's defenses against various malicious payloads, assessing the potential for successful exploitation.

Exploitation Phase (Section 4.3.3.3)

- **Security Bypass and Privilege Escalation -** Attempts to circumvent security measures, escape restricted environments, and gain elevated privileges.

- **In-depth Exploitation -** Utilization of discovered vulnerabilities to extract sensitive information, further compromising the network's integrity.

Prioritization of Remediation (Section 4.3.4)

Following our assessment, we will prioritize remediation efforts based on the severity and potential impact of identified vulnerabilities, offering tailored recommendations to mitigate risks effectively.

Proposal for Section 4.3 - Internal / Client-Side Network Penetration Testing Requirements (cont.)

Comprehensive Network Assessment (Section 4.3.5)

Our testing extends to all networked assets, including servers, endpoints, firewalls, and network devices, ensuring a holistic security evaluation.

Executive Summary Report (Section 4.3.6)

Upon completing the assessment, Aegisbyte will provide an Executive Summary Report, offering a high-level overview of the findings, key strengths, vulnerabilities, and actionable recommendations for senior management. A sample of this report is available upon request and will be submitted electronically for Lottery review.

Technical Report (Section 4.3.7)

The Technical Report will detail each discovered vulnerability, classified by risk rating, and include:

- Methods of discovery
- Potential impacts of exploitation
- Remediation recommendations
- References for further reading

A sample of the Technical Report will be provided with our bid response and submitted electronically for comprehensive review.

Reports' Detailed Requirements (Section 4.3.8)

Each report will encompass detailed analyses of vulnerabilities, including discovery methods, exploitation impacts, and remediation strategies, ensuring the Lottery has all the necessary information to address identified security concerns effectively.

Findings Presentation (Section 4.3.9)

Concluding the assessment, Aegisbyte will deliver a Findings Presentation to the Lottery management team, highlighting the assessment's strengths, weaknesses, and vulnerabilities. This presentation will be tailored to the Lottery's preference for an in-person meeting or a conference call.

Aegisbyte LLC is committed to partnering with the Lottery to enhance its internal network security. Our in-depth, on-site assessments and collaborative approach to scheduling and reporting ensure that the Lottery's internal networks are thoroughly evaluated and strengthened against current and emerging threats.

Proposal for Section 4.4 - Wireless Penetration Testing Requirements

On-site Testing Requirement (Section 4.4.1)

Aegisbyte LLC fully recognizes the necessity of conducting wireless penetration testing on-site at all Lottery locations. Our dedicated team will deploy to each specified location to ensure thorough and accurate assessments, adhering to the requirement for on-site analysis without reliance on remote assessments or centralized testing from one location.

Coordination of Testing Framework (Section 4.4.2)

Aegisbyte will work in close partnership with the Lottery POCs to establish a detailed schedule for the testing process, including timeframes, target completion dates, and any specific exclusions, ensuring our testing protocols align with operational requirements and minimize potential disruptions.

Four-Phased Testing Methodology (Section 4.4.3)

Our comprehensive methodology for wireless penetration testing includes the following four critical phases: reconnaissance, mapping, discovery, and exploitation, designed to identify and address vulnerabilities within the wireless network environment.

Reconnaissance Phase (Section 4.4.3.1)

- Information Gathering - We will conduct WHOIS, ARIN, and DNS lookups, engage in OSINT techniques, build custom password lists, and perform DNS lookups on entity servers to compile a robust data set.
- Metadata Analysis - Examination of metadata from web applications and network resources to identify potential vulnerabilities or informational leaks.

Mapping Phase (Section 4.4.3.2)

- Network Analysis - Techniques such as sniffing for traffic and War Walking will be employed to map out wireless networks, identify rogue access points, and assess wireless access points' coverage and security configurations.

Discovery Phase (Section 4.4.3.3)

- **Vulnerability Identification—**We will identify potential security flaws and misconfigurations within the wireless network by actively engaging with network services and using both open-source and commercial vulnerability scanning tools.

- **Attack Vector Analysis -** Identifying potential attack points, including weak encryption methods and vulnerabilities that could allow for evil-twin and man-in-the-middle (MiTM) attacks.

Exploitation Phase (Section 4.4.3.4)

- **Active Exploitation -** With prior approval, we will simulate attack scenarios against identified vulnerabilities, including AP and client attacks, to understand their real-world implications.

- **Risk Evaluation -** Evaluation of the impact of exploitation efforts to determine the vulnerability of the wireless network to potential attackers.

Proposal for Section 4.4 - Wireless Penetration Testing Requirements (cont.)

Remediation and Risk Prioritization (Section 4.4.4)

Following the assessment, Aegisbyte will prioritize remediation strategies based on the severity and potential impact of identified vulnerabilities, offering actionable recommendations to mitigate these risks effectively.

Comprehensive Wireless Security Assessment (Section 4.4.5)

Our assessment will encompass all wireless assets within the Lottery's environment, ensuring a holistic evaluation of wireless networks' security posture.

Executive Summary Report (Section 4.4.6)

Upon completion of the assessment, Aegisbyte will compile an Executive Summary Report detailing the assessed infrastructure's scope, approach, findings, key strengths, and strategic recommendations. A sample report will be provided with our bid response and submitted electronically for Lottery review.

Technical Report (Section 4.4.7)

The Technical Report will provide an in-depth analysis of each discovered vulnerability, categorized by risk rating, and details on discovery methods, potential impacts, and remediation recommendations. A sample of this report will accompany our bid response and be submitted electronically.

Detailed Reporting Requirements (Section 4.4.8)

Each report will detail the vulnerabilities' discovery process, potential impacts, and specific remediation strategies, ensuring the Lottery comprehensively understands its wireless network's security posture.

Findings Presentation (Section 4.4.9)

Aegisbyte will conclude the assessment with a Findings Presentation, delivered in person or via a conference call, as the Lottery prefers, to provide an overview of the strengths, weaknesses, and vulnerabilities identified throughout the assessment process.

Aegisbyte LLC is committed to delivering an exhaustive and insightful wireless penetration testing service for the Lottery, encompassing detailed analysis, actionable recommendations, and strategic guidance to enhance the wireless network's security and resilience against potential cyber threats.

METHODOLOGIES

Aegisbyte LLC is committed to conducting thorough and effective penetration testing for the State of West Virginia, aligning with the solicitation CRFQ 0705 LOT2400000009. We integrate recognized industry standards and frameworks to assess vulnerabilities and security controls within the state's digital infrastructure.

Our methodology is grounded in the Open Source Security Testing Methodology Manual (OSSTMM), guiding our comprehensive vulnerability testing and security assessments to align with established best practices. This approach ensures a thorough security review, focusing on identifying, evaluating, and mitigating potential risks.

In compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Special Publication 800-53A Revision 5, Aegisbyte will employ rigorous penetration testing and security assessment methods. These standards provide robust guidance for managing cybersecurity risks effectively, ensuring a structured and comprehensive evaluation process.

Implementing the Penetration Testing Execution Standard (PTES) allows Aegisbyte to plan, conduct, and conclude penetration testing activities systematically. Following the PTES lifecycle guarantees a meticulous and consistent approach to identifying and addressing security vulnerabilities, enhancing the overall security posture of the State of West Virginia.

Our penetration tests also adhere to the Open Web Application Security Project (OWASP) standards. They utilize the OWASP Testing Guide, Web Security Testing Guide (WSTG), and Mobile Security Testing Guide (MSTG) for thorough web and mobile application security assessments. These resources facilitate the identification of vulnerabilities in applications, ensuring robust security measures for the State's online and mobile platforms.

The OWASP Application Security Verification Standard (ASVS) provides a framework for securing web applications, outlining essential security requirements and controls. Aegisbyte will leverage the ASVS to assess and improve the security of the State’s web applications, ensuring they meet high-security benchmarks.

Aegisbyte will utilize the Common Vulnerability Scoring System (CVSS) versions 3.1 and 4.0 for vulnerability assessment and prioritization. This will standardize the evaluation of vulnerability severity and assist the State of West Virginia in prioritizing remediation efforts based on the potential impact and exploitability of identified vulnerabilities.

By integrating these comprehensive standards and methodologies, Aegisbyte LLC is poised to deliver an in-depth security evaluation for the State of West Virginia. Our approach aims to uncover and mitigate vulnerabilities effectively, thereby enhancing the cybersecurity framework and resilience of the State's digital infrastructure.

CERTIFICATIONS AND CREDENTIALS

OSCP
OffSec

OSWE
OffSec

OSEP
OffSec

OSED
OffSec

GPEN
SANS GIAC

GXPN
SANS GIAC

GMOB
SANS GIAC

GWAPT
SANS GIAC

GCIH
SANS GIAC

GSEC
SANS GIAC

and more!

FELIX ALCALA RESUME

Contact Information

Email: felix.alcala@aegisbyte.com
Phone: (703) 929-3673
GitHub: github.com/dethlocker
LinkedIn: linkedin.com/in/felixalcala

Professional Summary

With over 20 years of extensive experience in cybersecurity, particularly in offensive security engineering, I bring a wealth of knowledge and a robust track record in identifying and exploiting software vulnerabilities. My career spans a significant breadth of the Information Technology field, focusing on systems administration, network administration, systems engineering, architecture, and information assurance analysis. My expertise lies in leading security operations centers (SOCs), penetration testing, and contributing to significant security architecture in SOC environments. My work supports key government agencies, including the Department of Defense, Homeland Security, and the U.S. Navy, demonstrating my capability in high-stakes, fast-paced environments.

Experience

Principal Engineer - Sr Penetration Tester, DHS/CISA

- Spearheaded penetration testing for DHS CISA, producing critical security access reports and recommendations for GOTS applications, frameworks and networks.

Senior Penetration Tester, CBP

- Led offensive security and red team engagements for over 10,000 DHS and CBP assets, streamlining cybersecurity measures.

Senior Offensive Security Engineer, ARCYBER

- Conducted red team operations along with advanced network hunting and analysis, identifying significant cyber threats for the Army Cyber network.

Cyber Security Architect, US Census

- Developed incident response processes and conducted cyber security assessments for the U.S. Census 2020 project.

Senior Penetration Tester, NAVAIR/NAWCAD

- Evaluated the Navy's enterprise infrastructure from a red team perspective, enhancing security protocols for mission-critical systems.

Education & Certifications

- Certified Red Team Operator (CRTO), ZeroPointSecurity
- Offensive Security Certified Professional (OSCP)
- Offensive Security Web Expert (OSWE)
- Offensive Security Experienced Penetration Tester (OSEP)
- GIAC Certified Incident Handler (GCIH)
- GIAC Penetration Tester (GPEN)
- Extensive certifications in cybersecurity domains, including penetration testing, web application security, and exploit development.

Skills

- Expertise in Web App & Network Penetration Testing
- Advanced Red Team Engagements & Reverse Engineering
- Proficient in Research and Development for Security Solutions
- Skilled in Mobile App Security Testing & Threat Modeling

JOHN COOK JR. RESUME

Contact Information

Email: john.cook@aegisbyte.com
Mobile: (703) 929-3677
LinkedIn: linkedin.com/in/johnwcookjr

Professional Summary

Accomplished Information Technology Project Manager with extensive experience leading high-impact projects within the Defense Information Systems Agency (DISA) and the U.S. Army, now serving at Aegisbyte. Proven track record in strategic project leadership, operational management excellence, security compliance oversight, and cross-functional team coordination. Spearheaded significant initiatives, including enterprise-wide cybersecurity frameworks and cloud migrations, demonstrating leadership in technology innovation and operational improvement.

Experience

Chief Operations Officer, Aegisbyte LLC

- Spearheaded the strategic direction and operational execution of cybersecurity initiatives within State, Local, and Education (SLED) contracts, enhancing Aegisbyte's market footprint in public sector cybersecurity solutions.
- Managed budget allocation, financial forecasting, and resource planning for the cybersecurity division optimizing investment in technologies and human capital to maximize ROI on SLED contracts. Advocated for cybersecurity awareness and education among SLED entities, organizing workshops and training sessions emphasizing cyber hygiene and proactive defense strategies.

Information Technology Project Manager, DISA

- Directed the enterprise-wide deployment of Microsoft Defender for Endpoints, enhancing cybersecurity for 44,000 endpoints. Managed the successful OneDrive NIPR Migration, transitioning over 10,000 personnel to cloud-based solutions with a 95% success rate.
- Implemented Virtualization-based Security with Credential Guard and developed secure SFTP solutions, significantly boosting system security. Coordinated multi-disciplinary teams, ensuring project milestones were met efficiently by developing comprehensive RACI documents. Engaged with senior leadership to align IT projects with organizational goals, supervising diverse IT teams to foster innovation and operational excellence.

Operations Officer, U.S. Army Reserves, United States Special Operations Command

- Led actions within the Countering Weapons of Mass Destruction Fusion Cell, providing IT, logistics, and exercise coordination expertise.
- Supervised senior commissioned officers during multinational exercises, enhancing DoD's CWMD mission readiness.

IT Specialist - Network, Information Technology Agency

- Oversaw Change and Configuration Management and Incident Management, maintaining high network performance and security standards.

Education

- Master's Degree in Cybersecurity: Intelligence/Forensics, Utica College, NY
- Bachelor's Degree in Computer Technology, Bowie State University, MD
- Technical Certifications, including Security+ and U.S. Army Signal Center training in communications and IT management

Skills

- Strategic IT Project Management
- Cybersecurity Framework Implementation
- Cloud Migration & Virtualization
- Cross-functional Team Leadership
- Stakeholder Engagement & Supervision
- Security Compliance & Risk Management

JASON BREWER RESUME

Contact Information

Email: jason.brewer@aegisbyte.com
Phone: (703) 929-3674
LinkedIn: linkedin.com/in/jasonbrewer

Professional Summary

A highly experienced Senior Principal IT Security Specialist with over 15 years of expertise in systems engineering, penetration testing, exploit development, and reverse engineering across a variety of platforms, including web applications, networks, Active Directory, and mobile applications. My career encompasses significant contributions to incident response activities on NAVAIR avionics platforms and traditional networks. At Aegisbyte, I leverage my comprehensive background in cybersecurity to develop innovative solutions that enhance organizational security posture, automate incident response processes, and implement effective security measures across diverse IT environments.

Experience

Senior Principal IT Security Specialist, DHS/CISA

- Lead penetration testing activities across Windows Active Directory environments and proprietary web applications.
- Develop custom Python and Bash scripts to automate penetration testing processes.
- Provide expert guidance to junior team members and contribute to the design and implementation of team TTPs.
- Execute targeted phishing campaigns and develop secure network architecture for testing environments.

Co-Founder and CSO, Aegisbyte LLC

- Consult on network architecture design, threat hunting, threat analysis, risk mitigation, and overall security posture for a variety of clients.
- Conduct penetration testing on networks and standalone systems, including mobile devices, to enhance security measures and awareness.

Senior Cyber Security Engineer, Department of Defense

- Specialize in patch diffing on binaries, creating custom zero-days, and automating binary examination processes.
- Perform extensive analysis and testing on endpoint security devices and conduct penetration testing on AWS cloud environments.

Education & Certifications

- M.S. in Information Security Engineering, SANS Technology Institute, 2022
- Numerous GIAC certifications, including GDSA, GCCC, GCPM, GCIA, GSEC, GXPN, and GPEN
- Graduate Certificates in Pen Testing and Ethical Hacking, SANS Technology Institute, and International Security, Stanford University

Skills

- Incident Response & Web Application Testing
- Network Penetration Testing & Security Research
- Reverse Engineering & Exploit Development
- Static Code Analysis & Custom Tool Development

Languages & Tools

- Proficient in Python, Bash, C, C++, PowerShell
- Expertise in VMWare, Docker, IDA, Ghidra, Wireshark, Kali Linux suite of tools

BUSINESS REFFERENCES

For your review and consideration, Aegisbyte LLC presents its distinguished portfolio of cybersecurity services, underscored by our exemplary track record in enhancing the security posture of various esteemed organizations across the government and private sectors. Below, we outline our engagements with key clients, demonstrating our comprehensive capabilities and commitment to excellence in cybersecurity.

Steve Pruskowski - Department of Homeland Security, Office of the Chief Information Officer

- **Contact: Mobile:** (571) 550-1396, **Email:** steven.pruskowski@cisa.dhs.gov
- **Engagement Overview:** Aegisbyte LLC spearheaded establishing and leadership a specialized team at the Cybersecurity and Infrastructure Security Agency (CISA), which is dedicated to advanced offensive security operations. Our focus spanned network security, cloud environments, web and API security, and rigorous application security within the DevSecOps lifecycle. Our efforts were pivotal in fortifying the cyber defenses of CISA, DHS, and other affiliated government entities. Recognition through various awards since 2019 underscores our significant contributions to national cybersecurity initiatives.

Rick Jacobs - Duggal Visual Solutions, Director of Information Technology

- **Contact: Phone:** (646) 638-7236, **Email:** rjacobs@duggal.com
- **Engagement Overview:** Aegisbyte LLC conducted extensive penetration testing and red team operations across all Duggal Visual Solutions locations, scrutinizing over 72,000 assets. Our comprehensive web application assessments encompassed seven major web applications and numerous APIs. These efforts were instrumental in identifying and mitigating potential security vulnerabilities and safeguarding critical digital infrastructure.

David Williams - The Conservation Fund, Vice President of Technology, CIO

- **Contact: Phone:** (703) 908-5835, **Email:** dwilliams@conservationfund.org
- **Engagement Overview:** Aegisbyte LLC executed specialized Wireless Penetration Testing at The Conservation Fund's headquarters. We provided a detailed assessment report outlining all attack vectors against their wireless access points, showcasing our methodical approach to identifying and rectifying security vulnerabilities. Our exemplary service and results have cemented a strong relationship with The Conservation Fund, which intends to continue leveraging our cybersecurity services.

Gunny Hundertmark, Ph.D. - Sustainable Aquatics Food Exports LLC, Executive Vice President - COO/CTO

- **Contact: Phone:** (772) 212-2486, **Email:** gunny@semaquatics.com
- **Engagement Overview:** Aegisbyte LLC supported SAFE LLC with a suite of cybersecurity services, including Mobile Threat Defense (MTD), Mobile Application Security Testing, comprehensive Penetration Testing, integrated Endpoint Detection and Response (EDR), Managed Detection and Response (MDR) within a Security Operations Center (SOC) environment. Our multidimensional approach to cybersecurity has significantly bolstered SAFE LLC's resilience against cyber threats.

Aegisbyte LLC prides itself on delivering state-of-the-art cybersecurity solutions tailored to meet each client's unique needs. Our commitment to excellence and our proven track record position us as the ideal partner for the West Virginia Lottery Commission in achieving unparalleled cybersecurity readiness and resilience.

For inquiries, contact us.

www.aegisbyte.com

contact@aegisbyte.com

(866) HACKER-5

Service Disabled Veteran Owned Small Business

SDVOSB

CVE

Aegisbyte LLC
14894 Heather Bloom Dr
Woodbridge, VA 22193

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 03/16/2024

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

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

PRODUCER
BIBERK
P.O. Box 113247
Stamford, CT 06911

CONTACT NAME:
PHONE (A/C, No, Ext): 844-472-0967 FAX (A/C, No): 203-654-3613
E-MAIL ADDRESS: customerservice@biBERK.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : Berkshire Hathaway Direct Insurance Company	10391
INSURER B :	
INSURER C :	
INSURER D :	
INSURER E :	
INSURER F :	

INSURED
Aegisbyte LLC

14894 Heather Bloom Dr
Woodbridge, VA 22193

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

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

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	☒ COMMERCIAL GENERAL LIABILITY ☐ CLAIMS-MADE ☒ OCCUR ☐ ☐ GEN'L AGGREGATE LIMIT APPLIES PER: ☐ POLICY ☐ PRO-JECT ☐ LOC ☒ OTHER:			N9BP859603	03/17/2024	03/17/2025	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$ 1,000,000 $ 50,000 $ 5,000 $ Included $ 2,000,000 $ 2,000,000 $
	AUTOMOBILE LIABILITY ☐ ANY AUTO ☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS ☐ HIRED AUTOS ONLY ☐ NON-OWNED AUTOS ONLY ☐ ☐						COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$ $ $ $ $
	☐ UMBRELLA LIAB ☐ OCCUR ☐ EXCESS LIAB ☐ CLAIMS-MADE ☐ DED ☐ RETENTION $						EACH OCCURRENCE AGGREGATE	$ $ $
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? ☐ (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N / A					☐ PER STATUTE ☐ OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ $ $
	Professional Liability (Errors & Omissions): Claims-Made						Per Occurrence/ Aggregate	

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

CERTIFICATE HOLDER

Aegisbyte LLC
14894 Heather Bloom Dr
Woodbridge, VA 22193

CANCELLATION

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

AUTHORIZED REPRESENTATIVE Rakesh Gupta

Aegisbyte LLC
14894 Heather Bloom Dr
Woodbridge, VA 22193

CERTIFICATE OF PROPERTY INSURANCE

DATE (MM/DD/YYYY) 03/16/2024

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

PRODUCER

BIBERK
P.O. Box 113247
Stamford, CT 06911

CONTACT NAME:	
PHONE (A/C, No, Ext):	(844) 472-0967
FAX (A/C, No):	(203) 654-3613
E-MAIL ADDRESS:	salessupport@biberk.com
PRODUCER CUSTOMER ID:	

INSURED

Aegisbyte LLC
14894 Heather Bloom Dr
Woodbridge, VA 22193

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A :	Berkshire Hathaway Direct Insurance Compa	541611
INSURER B :		
INSURER C :		
INSURER D :		
INSURER E :		
INSURER F :		

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

LOCATION OF PREMISES / DESCRIPTION OF PROPERTY (Attach ACORD 101, Additional Remarks Schedule, if more space is required)

Location: 14894 Heather Bloom DrWoodbridge, VA 22193
Bldg #001: Consultants - All Other - 4167702

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

INSR LTR	TYPE OF INSURANCE			POLICY NUMBER	POLICY EFFECTIVE DATE (MM/DD/YYYY)	POLICY EXPIRATION DATE (MM/DD/YYYY)	COVERED PROPERTY		LIMITS
	☒	PROPERTY		N9BP859603	03/17/2024	03/17/2025	□	BUILDING	$ 0
	CAUSES OF LOSS		DEDUCTIBLES				□	PERSONAL PROPERTY	$ 0
	□	BASIC	BUILDING 250				□	BUSINESS INCOME	$ *
	□	BROAD					□	EXTRA EXPENSE	$ *
	☒	SPECIAL	CONTENTS				□	RENTAL VALUE	$
	□	EARTHQUAKE					□	BLANKET BUILDING	$ n/a
	□	WIND					□	BLANKET PERS PROP	$ n/a
	□	FLOOD					□	BLANKET BLDG & PP	$ n/a
	□						□		$
	□						□		$
	□	INLAND MARINE		TYPE OF POLICY			□		$
	CAUSES OF LOSS						□		$
	□	NAMED PERILS		POLICY NUMBER			□		$
	□						□		$
	□	CRIME					□		$
	TYPE OF POLICY						□		$
							□		$
	□	BOILER & MACHINERY / EQUIPMENT BREAKDOWN					□		$
							□		$
							□		$
							□		$

SPECIAL CONDITIONS / OTHER COVERAGES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

* ALS up to 12 months.

CERTIFICATE HOLDER

Aegisbyte LLC
14894 Heather Bloom Dr
Woodbridge, VA 22193

CANCELLATION

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

AUTHORIZED REPRESENTATIVE

Rakesh