




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

## Header 2

 List View

## General Information | Contact | Default Values | Discount | Document Information | Clarification Request

Procurement Folder: 1369290

Procurement Type: Central Master Agreement

Vendor ID: VS0000039706 


Legal Name: Bulletproof Solutions, Inc.

Alias/DBA:

Total Bid: \$24,420.00

Response Date: 03/28/2024 

Response Time: 12:22

Responded By User ID: BPprocurement 

First Name: Kristin

Last Name: Biser

Email: kristin.biser@bulletproofsi.

Phone: 7032069383

SO Doc Code: CRFQ

SO Dept: 0705

SO Doc ID: LOT240000009

Published Date: 3/21/24

Close Date: 3/28/24

Close Time: 13:30

Status: Closed

Solicitation Description: Network Penetration Testing and Cybersecurity Assessments

Total of Header Attachments: 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 ESR03282400000005542	1

**VENDOR**  
 VS0000039706  
 Bulletproof Solutions, Inc.

**Solicitation Number:** CRFQ 0705 LOT2400000009  
**Total Bid:** 24420  
**Response Date:** 2024-03-28  
**Response Time:** 12:22:48  
**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				4255.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:** Cost above is the Unit Cost per Assessment & Reports for the External Network Penetration Testing task.

**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				7585.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:** Cost above is the Unit Cost per Assessment & Reports for the Website Penetration Testing task.

**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				9065.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:** Cost above is the Unit Cost per Assessment & Reports for the Internal/Client-Side Network Penetration Testing task.

**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				3515.00

Comm Code	Manufacturer	Specification	Model #
81111801			

**Commodity Line Comments:** Cost above is the Unit Cost per Assessment & Reports for the Wireless Penetration Testing task.

**Extended Description:**

See Attached Specifications and Exhibit - A Pricing Page



**BULLETPROOF**

a GLI company

**Contact Person:**

**Pat Costaregni**

Account Executive

Pat.Costaregni@bulletproofsi.com

**Phone: (401) 241-9262**

**Bulletproof Solutions**

3040 Williams Drive, Suite 510

Fairfax, VA 22031

(703) 206-9383

www.bulletproofsi.com

**Response to Request for  
Centralized Quote for  
Network Penetration Testing and  
Cybersecurity Assessments**

**Prepared for  
West Virginia Lottery**

**RFP #CRFQ 0705 Lot 2400000009**

**Pricing Response**

Closing Date and Time:

**March 28, 2024 at 1:30 PM EST**

## Table of Contents

*Pricing*..... 1

## Pricing

---

**EXHIBIT A - Pricing Page**


Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	\$ 4,255 -	\$ 34,040 -
2	4.2	Website Penetration Testing	8	\$ 7,585 -	\$ 60,680 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	\$ 9,065 -	\$ 72,520 -
4	4.4	Wireless Penetration Testing	8	\$ 3,515 -	\$ 28,120 -
<b>TOTAL BID AMOUNT</b>					\$ 195,360 -

**\*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.

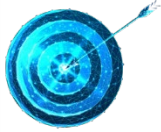
Any product or service not on the Agency provided Pricing Page will not be allowable.

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

<b>Vendor Name:</b>	Bulletproof Solutions, Inc.
<b>Vendor Address:</b>	3040 Williams Drive, Suite 510, Fairfax, VA 22031
<b>Email Address:</b>	Pat.Costaregni@bulletproofsi.com
<b>Phone Number:</b>	(401) 241-9262
<b>Fax Number:</b>	(703) 206-9666
<b>Signature and Date:</b>	 March 27, 2024
	<small>TELETYPE BURNS (Mar 27, 2024 23:19 EDT)</small>



## *Bulletproof's Why, Vision, & Values*



### OUR **WHY**

We believe everyone has the right to feel safe and secure. Our mission is to serve and protect organizations to ensure their success.



### OUR **VISION**

To serve, secure, and empower the world through people and technology; one customer at a time.

### OUR **VALUES**



**People First:** We take care of our people, so they can take care of our customers.

**Customer Obsessed:** We have a “first responder” mentality and a serving spirit.

**Respect Always:** We value and respect everyone equally.

**Trustworthy:** We seek what’s right, not who’s right. Do the right thing.

**Authentic Communication:** We are committed to responsive and thoughtful communication.



**BULLETPROOF**

a GLI company



**BULLETPROOF**

a GLI company

**Contact Person:**

**Pat Costaregni**

Account Executive

Pat.Costaregni@bulletproofsi.com

**Phone: (401) 241-9262**

**Bulletproof Solutions**

3040 Williams Drive, Suite 510

Fairfax, VA 22031

(703) 206-9383

www.bulletproofsi.com

**Response to Request for  
Centralized Request for Quote  
for**

**Network Penetration Testing and  
Cybersecurity Assessments**

**Prepared for  
West Virginia Lottery**

**RFP #CRFQ 0705 Lot 2400000009**

Closing Date and Time:

**March 28, 2024 at 1:30 PM EST**

## Table of Contents

<i>Cover Letter</i> .....	1
<i>Executive Summary</i> .....	3
<i>Qualifications</i> .....	4
<i>References</i> .....	8
<i>Project Team Experience</i> .....	11
<i>Compliance with Industry Standards</i> .....	13
<i>Testing Approach</i> .....	14
Management Approach.....	14
Internal Infrastructure Vulnerability Assessment .....	17
External Infrastructure Vulnerability Assessment.....	17
Internal & External Penetration Tests.....	19
Web Application Security Assessment.....	19
Wireless Penetration Testing .....	22
Deliverables.....	23
Virtual Machine (VM) Drone .....	26
<i>Background Checks</i> .....	28
<i>Non-Disclosure Agreements</i> .....	29
<i>Signed Forms</i> .....	30
CRFQ Cover Page .....	30
CRFQ Page 23.....	31
CRFQ Page 39.....	32
Addendum #1.....	33
<i>Appendix A: Resumes</i> .....	34

## List of Tables

Table 1: Bulletproof’s Relevant Past Performance ..... 6  
Table 2: Proposed Project Team Members ..... 12  
Table 3: Overview of Bulletproof’s Project Management Process ..... 16

## Cover Letter

---

March 28, 2024

Department of Administration  
Purchasing Division  
2019 Washington Street East  
Post Office Box 50130  
Charleston, WV 25305-0130  
Brandon L. Barr, Buyer

### **RE: West Virginia Lottery RFQ 0705 Lot 240000009 for Network Penetration Testing and Cybersecurity Assessments**

Dear Mr. Barr,

Bulletproof Solutions, Inc. is pleased to provide the following response to the West Virginia Purchasing Division on behalf of the West Virginia Lottery (the Lottery) Request for Quote (RFQ) to provide Network Penetration Testing and Cybersecurity Assessment services.

Bulletproof is gaming security and with the unique knowledge and experience we have gained partnering with our parent company, Gaming Laboratories International (GLI), we are uniquely qualified to support the Lottery's security and integrity. Bulletproof's cybersecurity resources have been providing security services to the gaming and lottery industry for over 20 years – and many come from world class gaming and lottery organizations. This direct lottery security experience, coupled with decades of global gaming knowledge, means unmatched added value for the Lottery, resulting in more cost effective, efficient and thorough security services.

Our security services are tailored directly to our gaming and lottery clients and, importantly, address your unique threat landscape and most common vulnerabilities. This diverse and current experience means we do not provide off the shelf services, which given the unique challenges the West Virginia Lottery faces, is essential protecting your revenue. At Bulletproof, our priority is to satisfy every customer, every time, through outstanding personalized, ethical and protocol-conscious service.

We commit to maintaining a focus on your objectives and striving to exceed your expectations and minimize the workload of your valuable staff. We take pride in our ability to bring value, stability and superior service to our customers.



a G.L.I. company

**West Virginia Lottery  
Network Penetration Testing and Cybersecurity  
Assessments**

**CRFQ # 0705 Lot 240000009  
Technical Response**

Should you have any questions or require additional information regarding this submission, please contact Pat Costaregni, Account Executive, at (401) 241-9262 or via email at [Pat.Costaregni@bulletproofsi.com](mailto:Pat.Costaregni@bulletproofsi.com). Thank you for your time and consideration of our proposal.

Sincerely,

A handwritten signature in black ink, appearing to read 'S Burns', positioned above a horizontal line.

STEVEN BURNS (Mar 27, 2024 15:37 EDT)

Steven Burns  
President & Chief Operating Officer

## Executive Summary

---

We offer extensive lottery security experience including successful and comprehensive security studies for the Multi-State Lottery Association, North Carolina Education Lottery, the Wisconsin Lottery, the Florida Lottery, Illinois State Lottery, Kansas Lottery, and Hoosier Lottery, among others. We have also conducted World Lottery Association-Security Control Standard (WLA-SCS) assessments worldwide, including partnering with Missouri and California to enable them to attain WLA Security certification.

Bulletproof's expertise spans the full spectrum of the lottery and gaming industry: lottery and gaming industry operations, devices, systems, partners, retailers, and suppliers. Further, our knowledge of gaming suppliers is unparalleled. Our decades of independently auditing and working with suppliers such as Scientific Games and IGT enable us to offer the Lottery an informed perspective and assess risk to operations efficiently and effectively.

Additionally, our security expertise has been requested by several State Attorney's General and Lotteries to provide expert testimony in prominent lottery fraud cases and key staff have conducted security training to gaming companies alongside US Homeland Security and other local and national law enforcement agencies.

Bulletproof's Security Experts are just that – experts. They hold certifications from and follow the industry leading frameworks of world-renowned organizations like ISO/IEC, NIST, SANS Institute, ISACA, CERT, and WLA. These certifications are backed by 100s of engagements for large, complex clients worldwide – including upwards of 500 similar assessments and audits for lottery and gaming clients.

Further, many of our security resources have developed and managed security programs themselves within the lottery industry, providing added value to the Lottery beyond just security consulting – at Bulletproof we understand the unique considerations and complexities of operating and managing security programs within a lottery organization.

Our combination of direct lottery risk assessment, coupled with decades of global gaming knowledge, provides unmatched added value, resulting in a more cost effective, efficient and thorough security study. This direct experience has enabled us to truly understand the greatest risks and vulnerabilities present within a lottery's operations, which will help us provide a fresh perspective and a more efficient audit, focusing on the key risks lotteries are presently facing.

The cornerstones of every lottery operation are security and integrity. The Lottery's reputation is one of its biggest assets. Many risks exist in all aspects of a lottery's operation, some obvious and others often hidden. The Lottery is well aware that good risk management practice is to conduct regular assessment of the risks that could adversely affect it in achieving its objectives and accordingly applies measures to mitigate these risks to acceptable levels.

We commit to maintaining a focus on your objectives and we strive to exceed your expectations. We take pride in our ability to bring value, stability and superior service to our customers.



## Qualifications

---

Bulletproof is an innovative leader in IT services, specializing in networking and information systems security consulting for State and Federal agencies, as well as commercial entities. As previously detailed in this proposal, our experience and qualification in lottery and gaming security is unrivalled.

Bulletproof focuses on helping clients meet their network infrastructure and information security goals by establishing close working relationships and by mapping clients' goals and mission requirements to proven solutions. At all times, Bulletproof maintains an awareness of clients' established policies and procedures and ensures that all of our work efforts are compliant with government regulations and corporate industry best practices.

Bulletproof has been in business since 2000 assisting more than 1,200 public and private-sector and lottery and gaming clients in improving their information security. The services we provide include:

- Information security audits
- Information vulnerability assessments and penetration testing
- Information security program development and planning
- Information security architecture design and implementation
- Information security operations
- Compliance verification, among others

Bulletproof's proposed team members are IT industry, lottery, and gaming veterans who possess both subject matter technical expertise as well as extensive experience in managing large-scale projects.

Information security covers a wide range of topics and issues. Bulletproof has gained substantial experience and expertise over the years, ranging from simple system security reviews to ground-up information security system deployments. We offer this experience and expertise through a range of services that are specifically tailored to our clients' individual needs and are backed by our continuing commitment to excellence.

Unique to Bulletproof, we have a dedicated security research division with a core focus on extensively researching evolving online gaming threats and security. Our teams regularly present at lottery and gaming industry conferences on this subject and provide informative articles for both print and online publications. Based on these efforts, Bulletproof has established a line of business focusing on this emerging and growing area.

### **We live and breathe in your threat landscape day in and day out.**

Our comprehensive security auditing practice not only offers all the rigor and diligence of a Big 4 firm, and the deep expertise in security program best practice, but as a managed security provider to the gaming industry, we understand – up to the minute – the threats you face and the protections you need to put in place to properly protect your organization.

Our managed security services, delivered through our state-of-the-art Security Operations Center (SOC) affords us a deep 24/7/365 operational security expertise that other professional services firms cannot provide. Through proactive threat hunting, event monitoring and incident management – and access to the latest threat intelligence sources and trends – our 24/7/365 work identifying and protecting against security threats means we bring the Lottery an informed and up to the minute perspective in assessing and improving information security, financial controls, and operational processes. We support the networks of clients all over the world in various industries, including gaming, giving us an informed, unique, and current risk perspective.

Recognized as Microsoft’s Global Security Partner of the Year for 2021, we are at the forefront of security innovation, helping organizations navigate the evolving cloud-based enterprise and the increased threats this presents to organizations.

Bulletproof has amassed significant experience in all areas of Information Assurance. Specifically, as it relates to this RFQ, Bulletproof has helped multiple lotteries assess the level of their security through testing and other compliance related activities against threats and risks. Our superior performance has not gone unnoticed. Bulletproof and its staff have earned multiple awards and certifications for technical competence and outstanding performance. Our earned awards are a credit to our satisfied customers and our staff’s perseverance and ability to get the job done right the first time.

### **Ability to conduct a comprehensive study of all aspects of lottery security**

The reputation we have earned is built upon being a trusted partner and advisor to the lottery industry. Bulletproof has a strong track record of delivering value and successful projects, and our vast experience within the lottery industry continues to grow rapidly as we complete more and more security audits. A testament to the quality of services that Bulletproof has delivered is evident in the number of recurring engagements with the same clients.

As demonstrated in this proposal, Bulletproof is uniquely qualified to perform this network security assessment for the Lottery. To date, Bulletproof has supported more than 1,200 clients across multiple industry sectors and business lines to achieve their security objectives and has performed more than 500 similar security studies for lottery and gaming organizations around the globe. The breadth of our support specifically related to our gaming and lottery clients is presented in **Table 1**.

**TABLE 1: BULLETPROOF’S RELEVANT PAST PERFORMANCE**

Client	Information Services Provided (Abbreviated List)					
	Penetration Testing	RNG Forensics and Security	Security Audit	Compliance Review	Web Application Testing	Security Architecture Review
Michigan Lottery		✓				
Massachusetts Lottery				✓		
California Lottery			✓			
Illinois Lottery		✓	✓	✓		
North Carolina Lottery	✓		✓	✓	✓	✓
Wisconsin Lottery		✓	✓	✓		
MUSL	✓	✓	✓	✓	✓	✓
Iowa Lottery	✓	✓	✓			✓
Florida Lottery			✓	✓		
Arizona Lottery			✓	✓		
Connecticut Lottery	✓	✓				
Indiana Lottery		✓	✓			
Arkansas Lottery		✓				
Colorado Lottery	✓	✓		✓		
Missouri Lottery	✓					
Virginia Lottery	✓		✓	✓		✓
Oregon State Lottery	✓		✓	✓	✓	✓
Alberta Gaming Liquor and Cannabis (AGLC)	✓		✓			✓
Western Canada Lottery				✓		

Information Services Provided (Abbreviated List)						
Client	Penetration Testing	RNG Forensics and Security	Security Audit	Compliance Review	Web Application Testing	Security Architecture Review
Corporation (WCLC)						
Atlantic Lottery Corporation (ALC)	✓					
South African Lottery		✓				
Costa Rica Lottery		✓				

*Remainder of page intentionally left blank*

## References

The following references have been included to show Bulletproof's experience performing similar services for other lotteries.

North Carolina Education Lottery	
<b>Contact Name</b>	Kim Thomas
<b>Title</b>	Director of Internal Audit
<b>Phone</b>	(919) 301-3571
<b>Email</b>	<a href="mailto:Kimberly.Thomas@lotterync.net">Kimberly.Thomas@lotterync.net</a>
<b>Address</b>	2728 Capital Blvd., Suite 144, Raleigh, NC 27604
<b>Services Performed</b>	<p>Bulletproof performed an independent security assessment and audit of North Carolina Education Lottery (NCEL) systems and gaming operations. We worked with and reported directly to the internal audit team at NCEL. Our review focused on both gaming systems (i.e., RNG, ICS) as well as the supporting IT infrastructure. Bulletproof utilized NIST 800-53 "Security and Privacy Controls of Federal Information Systems and Organizations" revision 4 as the baseline for the audit.</p> <p>In addition to performing interviews and examinations, technical vulnerability assessment scans were also conducted on the NCEL network and systems. Vulnerability scans were conducted both from external and internal perspectives. A limited web application security assessment was also conducted on mission critical applications identified by NCEL. A physical security review was performed on the headquarters in Raleigh and a field office in Greensboro.</p> <p>Bulletproof also performed the 2019 required security audit for NCEL.</p>

Colorado Lottery	
<b>Contact Name</b>	Tara Stosek
<b>Title</b>	Senior Security Analyst
<b>Phone</b>	(719) 924-0115
<b>Email</b>	<a href="mailto:Tara.Stosek@state.co.us">Tara.Stosek@state.co.us</a>
<b>Address</b>	225 N. Main Street, Pueblo, CO 81003

<b>Colorado Lottery</b>	
<b>Services Performed</b>	<p>Over the past several years, we have provided numerous security project services for the Colorado Lottery including:</p> <ul style="list-style-type: none"> <li>SSAE-16 Audit – provided technical expertise in evaluating the security controls in place for the lottery and their gaming operator, IGT. These results were included in the official report that was issued by our CPA partner.</li> <li>RNG Review- performed our established digital draw integrity assurance program for Colorado’s new RNG systems. The following year, we performed a follow-up review.</li> <li>IGT Penetration test – at the request of the Lottery, we performed a penetration test of the IGT gaming platform. This consisted of connecting to various retailer locations and assessing the risk and identifying vulnerabilities.</li> </ul> <p>Lottery Security Assessment – performed a security assessment of Colorado’s IT infrastructure. This involved internal and external vulnerability scans along with a wireless security assessment.</p>

<b>Wisconsin Lottery</b>	
<b>Contact Name</b>	Chris Heitmann
<b>Title</b>	IS Security Officer
<b>Phone</b>	(608) 444-0273
<b>Email</b>	Chris.Heitmann@wisconsin.gov
<b>Address</b>	2135 Rimrock Road, Madison, WI 53713
<b>Services Performed</b>	<p>Bulletproof performed an independent Security Assessment and Computer Security System Assessment of the following for the Wisconsin Lottery:</p> <ul style="list-style-type: none"> <li>Security of Lottery Locations</li> <li>Security Operations</li> <li>Ticket Claim Processing Procedures</li> <li>Distribution Security</li> <li>Mailroom Security</li> <li>Computer Security</li> <li>Retailer Background Checks</li> <li>Security of Lottery Tickets and Validation Files</li> <li>Disaster Recovery Plans</li> </ul>

**Wisconsin Lottery**

- Compliance with State Law and Administrative Rules, and include
  - Compliance with Internal Lottery Policy and Procedures
  - Compliance with MUSL requirements
  - Any irregularities indicated by the audit
  - Equipment problems
  - Personnel or vendor/contractor issues

Bulletproof prepared a report with findings and recommendations including details regarding the nature and significance of the findings and recommendations for improvement.

*Remainder of page intentionally left blank*

## Project Team Experience

Bulletproof’s highly experienced Program Manager will be Gus Fritschie, the company’s Vice President, Information Security Services. Gus has been involved in the field of information security for more than 20 years. He began his career in information technology (IT) as a system administrator for a growing financial company. It was there that he gained a fundamental understanding of all aspects of IT, including network security. Gus then joined the information security consulting practices of both KPMG and Deloitte and Touche. He led and performed numerous vulnerability assessments and penetration tests in support of FISCAM, FISMA, HIPAA and other compliance related efforts. Clients included Fortune 500 companies, civilian agencies, and the DoD.

**All proposed technical personnel have relevant security certifications, such as CISSP, Security+, CEH, and experience assessing the cybersecurity of gaming organizations.**

Over the past decade, Gus has specialized in security for lottery, online, and traditional gaming. Taking his information security knowledge and years of experience, Gus has performed research into the security of online gaming and has presented his findings at security conferences such as DefCon, HackerCon, DerbyCon, iGaming North America, and NASPL.

He has also presented at numerous government agencies on a wide variety of information security topics and has written articles discussing the need for security in online gaming for publications like *Global Gaming Business*.

Gus will be supported by a team of highly qualified security personnel who not only carry the industry’s highest level of certification, but have performed multiple security studies for lotteries worldwide.

**Table 2** below displays a list of proposed personnel that includes Bulletproof’s Project Manager and staff. All staff members hold certifications appropriate for their assigned project task areas. The information provided in this table is intended to demonstrate in a concise format the depth and breadth of relevant experience and expertise our highly experienced staff brings to this project. Complete resumes are provided below in **Appendix A**.



**TABLE 2: PROPOSED PROJECT TEAM MEMBERS**

Name/Proposed Position	Lottery Security Experience	Experience	Skills	Qualifications
Gus Fritschie, Project Manager, Technical Lead	NCEL Colorado Wisconsin Florida Connecticut Virginia Oregon MUSL Missouri Indiana Idaho Arkansas	Vice President, Information Security Services (2019-Present) CTO (2003— 2019) Senior Security Engineer (2000— 2003) System Administrator (1999—2000)	Penetration Testing Vulnerability Assessments Program Management Technical Implementation Architecture Experience	Certified CISSP High Level Federal Program Development Management and Leadership Experience Managed large-scale multi-million-dollar tasks and programs
Rizwan Ahmed, Senior Security Engineer	Multi-State Lottery Association Florida Lottery	Sr. Security Engineer (2009— Present) Help Desk (2005—2009)	Penetration Testing Network Design Security Architecture Incident Response	CISSP CISM Access Data Certified Examiner v6 CEH CompTIA Security + MCDST MSCE 4.0 A+ Certified
Nicholas Rosasco, Senior Security Engineer	Colorado Lottery	Senior Security Engineer (2017- Present) Managed Solutions Engineer (2014- 2017)	Web Application Penetration Testing Internal/External Penetration Test & Vulnerability Assessments	Certified Ethical Hacker (CEH) Offensive Security Certified Professional (OSCP) Offensive Security Web Expert (OSWE)

## Compliance with Industry Standards

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.

As noted in the following Technical Approach section, Bulletproof's methodologies comply and employ guidelines from the Open Web Application Security Project (OWASP) Top 10 Project and NIST 800-115 Information Security Testing and Assessment technical guide.

## Testing Approach

---

### *Management Approach*

Bulletproof will use its streamlined management oversight methodology to ensure the success of this effort—from the executive level to the program/project level and down to the individual task assignments. An executive corporate official will be assigned as Program Manager with overall responsibility for this contract. Reporting directly to this official will be the Bulletproof assigned Project Manager. This experienced individual will be charged with overseeing the completion of all tasks under this effort. The Program Manager will create and maintain the project plan; work breakdown schedule and action plan for each task and will be responsible for all deliverables.

The Project Manager will serve as a single point of contact (POC) for the Lottery. Bulletproof will establish reporting procedures to ensure coordination at all levels. Bulletproof will utilize automated tools to track progress and produce reports detailing each activity under this contract in terms of milestones achieved, expended level of effort and unplanned dependencies (if any).

Bulletproof will submit weekly progress reports identifying status of ongoing work, accomplishment of the past week and planned work for the week ahead. A log of interaction with the Lottery's staff will also be included as well as request for interviews and documentation.

Bulletproof will submit meeting minutes for all progress and status meetings held with the Lottery's officials. Meeting notes will highlight any decision reached, agreements made, or actions to be taken.

Throughout this effort, Bulletproof will maintain continuous interaction with the Lottery's personnel at multiple levels.

As an IT consulting firm, Bulletproof believes that professional consulting services must be viewed in terms of project execution life cycles. A complete life cycle consists of a range of technical and management services that are executed over allocated time and are focused at the granular level necessary to meet specific contract objectives. Such services may be broadly grouped and viewed as technical phases and management phases that constitute our integrated approach—allowing Bulletproof to coordinate key project resources and serve as a single point-of-contact for all of our clients' needs. This approach has been successfully implemented for previous tasks in similar engagements and we believe it will be instrumental in meeting the objectives of this effort.

Conducting a successful assessment effort on the scale and scope required by the Lottery relies not only on the skills and expertise level of the practitioners, but also on meticulous planning and oversight throughout the project.

Over the years, Bulletproof has developed a comprehensive management approach. This approach relies on the following cornerstones:

- Understanding of the client's expectations;

- Detailed planning;
- Strong team leadership;
- Close coordination with the client;
- Oversight by Bulletproof's executive management; and
- Progress reviews and solicitation of feedback from the client.

Bulletproof recognizes the value of continuous interaction with the Lottery's staff on all matters related to the project. Bulletproof assigns priority to all aspects of the Lottery's project and elevates the project's visibility to the top executive level. The Lottery's IT Director, Network/IT Operations Lead, or other designated personnel will have the ability to directly address Bulletproof's management team any time there is a need for an executive decision. Bulletproof also would appreciate periodic feedback concerning our team's performance. We recommend scheduling periodic face-to-face meetings or teleconferences at this level.

Below the executive level, Bulletproof will assign a Project Manager who will be the point of contact for all day-to-day activities covering contractual, staffing, management, and administration issues.

Upon award notification and prior to the commencement of the audit, Bulletproof's Program Manager will prepare materials for the kick-off meeting. We will create a "Day Zero Checklist" that will combine the meeting agenda with the initial request for actions and materials. Typical action items may include the introduction of key project participants on both sides; logistics, such as access to facilities, networks and systems; worksite needs; and signing Non-Disclosure Agreements. A very important item that needs to be discussed is what we call the "Assessment Rules of Engagements" (ROE), which should include responsibility of all involved parties and the "boundaries" for testing (e.g., whether exploits are allowed and to what extent, what type of evidence will be sufficient, etc.).

The Checklist will also include a request for detailed information directly related to the assessment.

Based on the information obtained following the kick-off meeting discussions, Bulletproof will create a Project Plan and submit it to the Lottery for approval. The approved plan will then be distributed to all stakeholders involved.

Concurrently, we will work on the development of an assessment plan (when applicable) and request for information from various City departments involved in the review. These two documents will be submitted for approval, then further customized for each department and distributed to their points of contact.

**Table 3** below is an overview of Bulletproof’s standard Project Management Process.

**TABLE 3: OVERVIEW OF BULLETPROOF’S PROJECT MANAGEMENT PROCESS**

Overview of Bulletproof’s Project Management Process	
Project Management Activity	Principal Objective
<b>Project Initiation</b>	
<b>Initiation</b>	Initiation involves starting up the project.
<b>Project Planning</b>	
<b>Project Mandate / Charter Development</b>	Communicates and obtains stakeholders’ sign off on the project scope, objectives, deliverables, cost, milestones and schedule.
<b>Milestone Management</b>	Provides measurements of the project’s progress and allows re-assessment of the project’s ability to meet critical path project timelines early in the project.
<b>Budget Estimation</b>	Establishes baseline figures for work effort, capital and expense for the project to use as input into project funding.
<b>Risk Planning</b>	Allows early identification of risk and establishes the mitigation and contingency plans needed to address the identified risks.
<b>Schedule Development and Management</b>	Identifies and monitors specific activities, deliverables, milestones, associated resources, time frames and dependencies.
<b>Project Execution</b>	
<b>Issue Management</b>	Ensures the identification, escalation and resolution of issues in a time efficient manner to minimize impacts to the project.
<b>Change Management</b>	Provides a mechanism for requesting, evaluating, tracking, resolving and reporting changes occurring to a project throughout its lifecycle.
<b>Project Reporting</b>	Establishes regular communications between project managers and executive management regarding project status.
<b>Risk Management</b>	Allows early identification of risks and the subsequent tracking and monitoring in order to respond to any associated impacts.
<b>Quality Control</b>	Provides metrics for measuring projects against established targets, standards and guidelines to ensure the creation of quality deliverables and work products.
<b>Financial Management</b>	Assesses and determines fund allocation for projects and monitors the financials to ensure that projects are executed within budgetary limits.
<b>Resource Management</b>	Provides planning and allocation of resources to ensure that projects are staffed efficiently with limited strain on existing staff.
<b>Communication</b>	Identifies organizational change impacts and the requirement for communication and training.
<b>Vendor / Procurement Management</b>	Guides the selection, monitoring and provisioning of third-party vendors with responsibility for project execution.
<b>Project Close</b>	
<b>Closure</b>	Closure involves winding-down the project by releasing staff, handing over deliverables to the customer and completing a post-implementation review.

Bulletproof’s experience has shown that the only reliable way to deliver high quality services is through continuous interaction between all stake holders throughout the duration of the

project. Direct communication channels should be established at multiple hierarchical levels. This allows early identification, mitigation, and prevention of potential problems, including scope and requirements misunderstandings.

Informal daily interaction will be augmented with periodic status reports, conference calls, meetings, and reviews of deliverables as specified in the RFP. The Program Manager is responsible for compiling a schedule that is included in the status report. In addition, he will compile and sign a weekly timesheet showing hours worked, tasks performed, and any other information deemed appropriate by the Lottery.

### ***Internal Infrastructure Vulnerability Assessment***

The security of your systems is paramount, and with an internal vulnerability scan you can be assured that you are informed of any vulnerability that exist on your systems. Vulnerability scanning will significantly reduce the risk of internal infrastructure and application vulnerabilities going undetected.

As part of the service, we provide analysis, verification, reporting, and advisory services – notifying you of infrastructure vulnerabilities, and giving you advice on how to mitigate them. All results are verified to ensure that you are only informed where an issue exists.

We will draw on our expertise in order to scan the internal infrastructure for potential attack vectors. A typical internal vulnerability scan will include:

- Network surveying;
- Port scanning;
- System identification (enumeration);
- Services identification;
- Network infrastructure vulnerability identification;
- Network vulnerability verification (exploit verification where possible); and
- Firewall testing.

An internal vulnerability scan will give you freedom from doubt that your systems are free from common exploitable vulnerabilities, giving the assurance your organization needs that your infrastructure estate is truly secure.

### ***External Infrastructure Vulnerability Assessment***

This remote phase of testing will focus on retrieving as much publicly available data as possible about the hosting environment. After this passive research, various tools will be used to actively gather information about the systems under review and their topology. Information such as OS identification and software type or version information, along with associated potential vulnerabilities, will be collated and researched.

Where appropriate, attempts will be made to exploit the systems.

This phase plans on:

- Conducting an external, black-box security assessment on hosts associated with the infrastructure, identifying devices and potential vulnerabilities. This will give a hacker's-eye view of the site.
- Attempting to attack visible servers with no valid user credentials or trust.
- Circumventing the firewall or router perimeter security to directly access and exploit other components of the system.

Profiling of the corporate Internet-facing infrastructure using non-invasive techniques includes:

- Domain-based discovery;
- Viewing customer website (if available);
- Web interface to Network Solutions and RIPE databases;
- DNS zone transfer attempts to listed DNS servers;
- Bounce email messages to determine location of mail servers and IP block; and
- Open-source vulnerability checks.

We will use a variety of scanning tools and techniques to locate live hosts and services within target IP range and perform a comprehensive assessment against all these IP addresses in scope, including:

- UDP / TCP Port Scanning – commonly done using industry standard port-scanning tools;
- Operating system fingerprint;
- Service Identification – service identification tools are used to analyze all live systems;
- User enumeration – dependent on what services are offered; and
- Network Mapping – Hping, traceroute, IP fingerprinting.

Once the automated discovery is completed, manual testing will investigate the results to identify possible attack vectors. Manual assessment of all live hosts and the exposed services focuses on the following areas:

- Host and service configuration – mis-configurations and poor build process can leave insecure services available. These often allow a trivial route to achieve system compromise.
- Patching vulnerabilities – lack of a stringent patching strategy can leave hosts vulnerable; efforts will be made to locate out-of-date services and operating system-wide missing patches.
- Use of insecure protocols or credentials - such as Telnet and FTP may increase risk of compromise, any usage will be highlighted. Default and easy-to-guess passwords will be attempted.

We use all information gathered in this assessment to attack the services exposed in penetration testing.

## ***Internal & External Penetration Tests***

Our team will perform internal and/or external penetration tests to validate the vulnerabilities found during our infrastructure vulnerability assessments.

The penetration test is a method of evaluating the security of your computer systems and/or network by simulating an attacker. This process involves an active analysis of your system for any weaknesses, flaws, or vulnerabilities. The analysis is performed as from a potential attacker's position and can involve active exploitation of the security vulnerabilities discovered during the vulnerability scans.

Unlike the vulnerability scans, penetration testing is mainly a manual process. Bulletproof will manually probe the target host for common misconfigurations or flaws because a vulnerability scanner can fail to identify certain vulnerabilities.

Attack scenarios will use a combination of exploits including, where agreed with the client, memory corruptions vulnerabilities and system mis-configuration. All exploitation is done in strict accordance with agreed rules of engagement: it should be noted that exploitation is highly dependent on the circumstances.

Authentication processes are attacked directly and indirectly using a combination of brute-force and password guessing techniques. Where there is a risk of account lockout brute-force attacks are not used.

Once exploits have been successful any access and privileges gained are then used to attempt to escalate access rights to the highest level possible. Detailed records are kept of all data recovered and copies are taken before changes are made to any files. All exploits are risk-assessed to minimize disruption to live systems.

## ***Web Application Security Assessment***

The purpose of the web application test will be to identify security vulnerabilities that may be exploited to compromise either the server-side application or the application or data of end users of the application.

During the assessment the consultants will use proven non-invasive testing techniques to quickly identify any weaknesses. While our techniques are non-invasive, certain testing will need to save data within the application. The application will be viewed and manipulated from several perspectives – applying no credentials, standard end user credentials, privileged user credentials, etc. Our methodology covers all of the [OWASP top 10 Web Application Security risks](#) where, in 2021, the following top 10 was considered:

- A01:2021 Broken Access Control
- A02:2021 Cryptographic Failures
- A03:2021 Injection
- A04:2021 Insecure Design
- A05:2021 Security Misconfiguration



- A06:2021 Vulnerable and Outdated Components
- A07:2021 Identification and Authentication Failures
- A08:2021 Software and Data Integrity Failures
- A09:2021 Security Logging and Monitoring Failures
- A10:2021 Server-Side Request Forgery (SSRF)

Our consultants will perform testing including but not are not limited to the Top 10, within the limits of any explicitly defined testing restrictions. Testing will cover all areas defined in the [OWASP Web Security Testing Guide](#). The following categories are followed:

- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Business Logic Testing
- Client-side Testing
- API Testing

We will perform an in depth and thorough test of in scope web applications while ensuring that correct configuration and recommended practices are followed to minimize client exposure. The following is a sample of common tests that are performed when carrying out an application test. The specific tests performed will vary depending on the technology and protocols that have been implemented:

## Web Server Specific

- Identify known vulnerabilities related to the web server version.
- Assess configuration issues such as potential issues with allowed HTTP methods.
- Search for default web server content and for information leakage.
- Examine information contained in banners and error messages.

## Identification & Authentication

- Test for default, weak, or well-known passwords, such as "Password1" or "admin/admin".
- Ensure a lockout policy for failed attempts is implemented and assess if a lockout time-out is in place.
- Ensure other controls are in place to prevent brute force or other automated attacks.
- Test for weak or ineffective credential recovery and lost password recovery processes, such as "knowledge-based answers"
- Attempt to bypass authentication with spoofed tokens and with replayed authentication information.
- Ensure the password is sent over a secure channel (adequate TLS version and valid certificate required) and not using plain text, weak encryption, or a weak hashing algorithm.
- Check for missing or ineffective multi-factor authentication.
- Check use of generic authentication error messages, preventing username enumeration.
- Determine the application logic to maintain authentication sessions and login time outs.

## Authorization Control

- Examine unauthorized directory/file access with path/directory traversal and check for Insecure direct object references (IDOR).
- Attempt to bypass access control checks by modifying the URL, internal application state, or the HTML page, or simply using a custom API attack tool.
- Check for vertical and horizontal segregation in the authorization schema:
  - Can a user A access/edit information of user B?
    - Ex. By providing/manipulating the user's unique identifier.
  - Can a user perform an elevation of privilege?
    - Ex.: Acting as a user without being logged in or acting as an admin when logged in as a user.
    - Ex.: Attempting metadata manipulation, such as replaying or tampering with a JSON Web Token (JWT) access control token, or a cookie or hidden field manipulated to elevate privileges or abusing JWT invalidation.

- Check for CORS misconfiguration that could allow API access from unauthorized/untrusted origins.
- Access API through vulnerabilities in access control configurations for POST, PUT and DELETE.

### **Session Management**

- Determine session management information – number of concurrent sessions allowed, IP-based authentication, role-based authentication, identity-based authentication, cookie usage, and session ID in hidden HTML field variables.
- Check the session identifier (cookie) attributes.
- Check for exposed session identifier in the URL.
- Manipulate session information (cookie) and check for persistent cookie usage.
- Check session identifier renewal after a successful login.
- Check for correct session ID invalidation. User sessions or authentication tokens (mainly single sign-on (SSO) tokens) should be properly invalidated during logout or after a period of inactivity.
- Evaluate session ID sequence and format.
- Check application for Cross Site Request Forgery (CSRF) vulnerabilities.

### **Input validation**

- Find limitations of defined variables and protocol payload, data length and type, construct format.
- Check validation adequacy, ensuring strong type, length and data format input.
- Use exceptionally long character-strings to find buffer overflow vulnerabilities in applications.
- Examine “Cross-Site Scripting” feasibility in the web application.
- Inject SQL language in the input strings of database-tied web-applications.
- Concatenate commands in the input strings of the applications.
- Manipulate hidden field variables in the HTML forms.
- Execute remote commands through “Server Side Includes.”
- Force the application to generate errors (where possible) and analyze any error/debug messages in the application output and program behaviors to detect injection points.

### **Wireless Penetration Testing**

This assessment will completely map all wireless access points that are on the property at the time of the assessment, enabling Bulletproof to identify authorized access. We will identify the

encryption levels and their respective risks and identify how far the wireless bleeds outside the property to prevent possible hackers from being outside the property and attempting to hack the system. The Wireless Network Assessment will include the following:

- Scanning of the wireless system and all access points (APs);
- Identification of un-authorized APs on the system, if any;
- Identification of encryption and notification of the risks involved in the encryption levels found to the property;
- Bleed test to identify the wireless access outside the outlined build;
- Identification of vulnerabilities against a published vulnerabilities database; and
- Identification of areas that a potential hacker can gain access to.

All areas of vulnerabilities that are identified will be described in an in-depth report to help clear the issues.

## ***Deliverables***

This effort will likely generate a significant amount of work products and deliverables. Bulletproof will collate the results of various tasks and deliver reports as required. Our final reports are meticulously detailed. Because all assessments are documented as they are performed, we accumulate a wealth of information, which we try to convey in the most concise and clear form possible in our report. Raw assessment and test results are normally delivered on a separate CD due to the large volume of data. The following sections describe additional deliverables under this effort.

### Weekly Report

Bulletproof will provide weekly status reports to the Lottery's POC. These reports will provide status updates in key measurement areas such as schedule, cost, etc. They will also outline important events that occurred during the past week, plans for the next week, and any project concerns. An updated version of the project plan is also provided at this time.

### Test Plan

The Test plan will be developed following the kick-off meeting and a review of relevant documentation provided by the Lottery. Its purpose is twofold—it serves as a working document for Bulletproof to utilize while engaged in this activity and also as a specific description for the Lottery's stakeholders of the planned testing activities. The plan sample below, will contain the following information:

- Background, goals, and objectives;
- Scope and methodology for each identified area;
- Tools and utilities to be used during the testing;
- Rules of engagement;

- Logistical issues;
- Responsible POCs for Bulletproof and the Lottery;
- Schedules; and
- Reporting and coordination procedures.

### Penetration Test Assessment Report

The Penetration Test Report is the main outcome of this effort. Bulletproof will provide the final report within 15 business days of completion of the assessments. All highly sensitive information such as passwords, encryption keys, financial, or personally identifiable information will be redacted or removed from the report. The Final Assessment Report will include the following:

1. An Executive Summary providing a high-level review of the effort and main findings as well as synopsis of the report. This section of the report will contain an overview of the assessment and assessment results, and highlight significant findings, including things the Lottery is performing well and recommended improvement areas. The Executive Summary will be prepared in a format appropriate for upper management. This section of the report will also detail the Lottery's Cybersecurity position and will include a comparative scorecard of findings; the results of vulnerability assessments performed; identify cybersecurity vulnerabilities, gaps, and mitigation plans; and include a prioritized road map of activities. This will all be developed in conjunction with the Lottery's staff to enhance their future cybersecurity position. This document will be first provided in a draft format for review and requested changes prior to final publication.
2. An overview of the findings grouped by category of assessments such as:
  - Vulnerabilities detected
  - Inventory of systems assessed
  - Hostname / IP address
  - System function (web server, email server, etc.)
  - Risk level for the particular system as determined and confirmed by the assessment results
  - Detailed vulnerability description
  - Description of the vulnerability
  - Description of mitigating factors in place
  - Level of risk as it applies to the specific case
  - System(s) affected
  - Ramification of exploitation
  - Remediation recommendations
  - Detailed timeline of the assessment identifying each step of the assessment. Included for each step:
    - Date/time stamp
    - Vulnerability / issue explored

- System(s) affected
  - Method(s) employed
  - Tool(s) employed
  - Expected results
  - Actual results
  - Screen shots where appropriate
  - Evidence of system access
  - Screen shots of non-public information, or showing administrative access (redact any sensitive or confidential information)
  - Plain-text flag files using readily identifiable names and contents.
  - Other non-destructive, non-disruptive methods.
  - Observations and recommendations
  - Validation of assessment
  - Test Scripts
  - Tools Utilized
- Remediation Requirements
  - Management response to recommendations
  - Findings
3. A step-by-step description of each assessment conducted.
  4. A table of findings titled "Findings and Recommendations" listing all identified notable information concerning assessed areas, an overall risk rating, and recommended corrective action with applicable pointers. Each area is assigned a "severity level" based on the following definitions:
    - **CRITICAL:** If uncorrected, this area would yield complete control of the subject system or give hackers access to extremely sensitive data. It could severely disrupt system operations and integrity.
    - **HIGH:** If uncorrected, this area would give over at least partial control of the system; allow access to sensitive data, and compromise system controls or system integrity.
    - **MEDIUM:** While not directly leading to a system security breach, exploiting this area may play a significant role in degrading a system if combined with other vulnerabilities or pertinent system information available to an attacker.
    - **LOW:** An area which is unlikely in itself to lead directly to a system compromise, but it can in some way aid an attacker indirectly in mounting attacks against the subject system.
  5. Conclusions and detailed recommendations for remediation actions along with estimated level of effort required for implementation. The Recommendations section is divided into subsections addressing each of the assessment areas requested by the Lottery.
  6. An appendix will contain any relevant screen captures and results referenced in the report. Results will be provided on a separate CD-ROM.

The Report will be provided first in a draft form to allow your officials to review and comment on its findings. Bulletproof will make necessary updates as identified in the Lottery's feedback and deliver a final version.

Our final reports are meticulously detailed and will help the Lottery meet the established, industry-standard assessment frameworks and guidelines, including the NIST security compliance standard requirements.

The final report will also include projected costs with an estimated range, based upon Bulletproof's previous experience, of the total services costs to implement the proposed recommendations for mitigating any identified risks.

### **Knowledge Transfer**

Bulletproof believes knowledge transfer is an important objective of our engagements and are committed to working with your IT Team throughout the project to provide the appropriate level of on-the-job training. Some of the methods we will utilize to achieve this will be full documentation of test results accompanied by formal presentations, informal work meetings, and discussions between your IT team and the Bulletproof audit team.

### ***Virtual Machine (VM) Drone***

Other than the requested assessment of physical access security and protocols, Bulletproof can complete this project remotely utilizing our Virtual Machine (VM) drone.

The VM Drone contains identical software as our physical drone and can be downloaded via our Secure File Transfer Protocol (SFTP) site. The SFTP site will be provided to you by the tester ahead of the assessment date. The VM image is made for VMware and is provided as a VMDK but can also be provided as an OVF file that can be imported into other virtual technologies such as AWS, Google Cloud, and Azure. VMDK can also be converted to VirtualBox, a free VM environment from Oracle.

### **Drone Deployment**

The VM Drone contains identical software as our physical drone and can be downloaded via our SFTP site. The SFTP site will be provided to you by the tester ahead of the assessment date. The VM image is made for VMware and is provided as a VMDK but can also be provided as an OVF file that can be imported into other virtual technologies such as AWS, Google Cloud, and Azure. VMDK can also be converted to VirtualBox, a free VM environment from Oracle.

### **Drone Decommissioning**

At the end of each engagement, the security engineer will sanitize the data on the drone once they have downloaded all the information they need. If there is a physical drone, a return shipping label will be provided. In the case of a VM, the security engineer will sanitize the data, disable the VPN permanently, and shutdown the VM. If needed, the engineer can preserve the image, VPN connection, and data for future assessments. The VM will need to be shut off until such time when it is needed again.

*Remainder of page intentionally left blank*



## Background Checks

---

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

Bulletproof agrees to provide the names, addresses, and fingerprint information for a law enforcement background check for any staff working on the Lottery's project team.

## Non-Disclosure Agreements

---

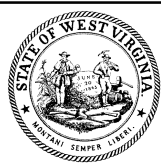
Prior to award both parties, the Vendor and Lottery must sign a mutual Non-Disclosure Agreement (NDA), attached as Exhibit - B, to ensure the confidentiality of the information exposed and proprietary tools and techniques used during these assessments.

Bulletproof understands and agrees that we will be required to sign a mutual Non-Disclosure Agreement (Exhibit B) to ensure the confidentiality of the information exposed and proprietary tools and techniques used during the assessments.

## Signed Forms

---

*CRFQ Cover Page*



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

<b>Proc Folder:</b> 1369290			<b>Reason for Modification:</b>
<b>Doc Description:</b> Network Penetration Testing and Cybersecurity Assessments			
<b>Proc Type:</b> Central Master Agreement			
<b>Date Issued</b>	<b>Solicitation Closes</b>	<b>Solicitation No</b>	<b>Version</b>
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:** VS0000039706  
**Vendor Name :** Bulletproof Solutions, Inc.  
**Address :**  
**Street :** 3040 Williams Drive, Suite 510  
**City** Fairfax  
**State :** Virginia **Country :** United States **Zip :** 22031  
**Principal Contact :** Pat Costaregni  
**Vendor Contact Phone:** (401) 241-9262 **Extension:**

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

**Vendor Signature X**  **FEIN#** 81-2643879 **DATE** March 27, 2024  
STEVEN BURNS (Mar 27, 2024 15:37 EDT)

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



**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) Pat Costaregni, Account Executive

(Address) 3040 Williams Drive, Suite 510, Fairfax, VA 22031

(Phone Number) / (Fax Number) T: (401) 241-9262 | F: (703) 206-9666

(email address) Pat.Costaregni@bulletproofsi.com

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

*By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 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.*

Bulletproof Solutions, Inc.

(Company)   
STEVEN BURNS (Mar 27, 2024 15:37 EDT)

(Signature of Authorized Representative)  
Steven Burns, President & COO

(Printed Name and Title of Authorized Representative) (Date)  
T: (703) 206-9383 | F: (703) 206-9666

(Phone Number) (Fax Number)  
Steven.Burns@bulletproofsi.com

(Email Address)



REQUEST FOR QUOTATION  
West Virginia Lottery  
Network Penetration Testing and Cybersecurity Assessments

---

**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:** Pat Costaregni  
**Telephone Number:** (401) 241-9262  
**Fax Number:** (703) 206-9666  
**Email Address:** Pat.Costaregni@bulletproofsi.com



*Addendum #1*



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

<b>Proc Folder:</b> 1369290			<b>Reason for Modification:</b> Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration a..... See Page 2 for complete info
<b>Doc Description:</b> Network Penetration Testing and Cybersecurity Assessments			
<b>Proc Type:</b> Central Master Agreement			
<b>Date Issued</b>	<b>Solicitation Closes</b>	<b>Solicitation No</b>	<b>Version</b>
2024-03-21	2024-03-28 13:30	CRFQ 0705 LOT2400000009	2


**BID RECEIVING LOCATION**

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

**VENDOR**

**Vendor Customer Code:** VS0000039706  
**Vendor Name :** Bulletproof Solutions, Inc.  
**Address :**  
**Street :** 3040 Williams Drive, Suite 510  
**City :** Fairfax  
**State :** Virginia **Country :** United States **Zip :** 22031  
**Principal Contact :** Pat Costaregni  
**Vendor Contact Phone:** (401) 241-9262 **Extension:**

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

**Vendor Signature X**  **FEIN#** 81-2643879 **DATE** March 27, 2024  
STEVEN BURNS (Mar 27, 2024 15:37 EDT)

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

**ADDENDUM ACKNOWLEDGEMENT FORM**  
**SOLICITATION NO.: LOT240000009**

**Instructions:** Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

**Acknowledgment:** I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

**Addendum Numbers Received:**

(Check the box next to each addendum received)

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6  |
| <input type="checkbox"/> Addendum No. 2            | <input type="checkbox"/> Addendum No. 7  |
| <input type="checkbox"/> Addendum No. 3            | <input type="checkbox"/> Addendum No. 8  |
| <input type="checkbox"/> Addendum No. 4            | <input type="checkbox"/> Addendum No. 9  |
| <input type="checkbox"/> Addendum No. 5            | <input type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Bulletproof Solutions, Inc.

\_\_\_\_\_  
Company

  
\_\_\_\_\_  
STEVEN BURNS (Mar 27, 2024 15:37 EDT)

\_\_\_\_\_  
Authorized Signature

March 27, 2024

\_\_\_\_\_  
Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.

Revised 6/8/2012

## Appendix A: Resumes

---

# Gus Fritschie, CISSP, CAP, CEH

V i c e P r e s i d e n t , S e c u r i t y  
S e r v i c e s



(703) 206-9383



Gus.Fritschie@bulletproofsi.com



Fairfax, VA

## EDUCATION

B.A. Geography, Mary Washington College

## Certifications

Certified Information Systems  
Security Professional

Certification and Accreditation  
Professional

NSA INFOSEC Assessment  
Methodology

CompTIA Security+

Solaris Certified Security  
Administrator

System Administration in  
INFOSEC, NSTI No. [REDACTED]

Certified Cisco Network  
Administrator

Cisco Secure PIX Firewall  
Administrator

## PROFESSIONAL PROFILE

Gus has been involved in the field of information security for 20 years. In 2010, he transitioned a significant portion of his practice into the gaming sector. Since then he has established himself and Bulletproof as the IT security leader in in gaming. He has supported a number of clients across the gaming spectrum from iGaming operators, land-based casinos, gaming manufacturer, lotteries, tribal gaming, and daily fantasy sports. Gus has performed research into the security of online gaming and has presented his findings at security conferences such as DefCon, HackerCon, DerbyCon, iGaming North America, and NASPL.

## WORK EXPERIENCE

### Vice President

#### Bulletproof Solutions, Inc. | Fairfax, VA | 2003 – Present

Gus manages and leads security teams performing vulnerability assessments for government and commercial agencies. The assessments involve performing wireless, network, and mainframe vulnerability and penetration testing. He provides C&A testing and conducts testing on web applications during the development, pre-production, and production phases. Gus develops vulnerability/penetration testing methodologies. He conducts security reviews and risk assessments using Federal guidelines set forth in the Federal Information System Controls Audit Manual (FISCAM), Federal Information Processing Standard (FIPS) publications, Office of Management and Budget (OMB) guidelines (127 and 130), and FISMA.

He's worked for such lotteries as North Carolina Education Lottery, Colorado, Virginia, Oregon, Wisconsin, MUSL, Florida, Missouri, Connecticut, Hoosier, Idaho, and Arkansas to name a few. Select project descriptions are as follows.

#### **Multi-State Lottery Association (MUSL):**

In response to the Eddie Tipton RNG fraud, a comprehensive security audit was overseen by the MUSL Security Task Force. The task force selected our Team and another vendor to perform an enterprise security audit of MUSL's management, operational, and technical controls. Gus served as the project lead and served as the primary security engineer. He conducted multiple site visits and testing at MUSL headquarters and was responsible for delivering a report detailing the findings and providing recommendations on improvements that needed to be implemented. He then provided a formal presentation to the MUSL board. As a result of this work, plans were developed and mitigations made based on the work our Team and Gus performed.

#### **Wisconsin Lottery:**

As part of the required Lottery security audit Gus performed a technical review of the Lottery's security controls. This involved conducting interviews, examination artifacts/evidence, and interfacing with IT staff from the Department of Revenue. Issues were documented and summarized in the overall audit report.

#### **Colorado Lottery:**

For the past three years Gus has led the security testing services for the Colorado Lottery. This involved a variety of tasks including:

- SSAE 16 Audit Support
- Lottery Security Testing
- IGT Penetration Testing
- RNG Security Audits

#### **Oregon Lottery:**

For the past two audit cycle Gus was the technical lead for the required security audit. This involved hands-on technical penetration testing and a review of operational and management security controls. He also reviewed IGT's security controls in order to verify the correct level of protection was in-place. In 2018 he led an additional task where he assessed their current and planned security controls and created a security roadmap.

# Gus Fritschie, CISSP, CAP, CEH

---

## Certifications *continued*

---

Check Point Certified Systems  
Engineer

Check Point Certified Security  
Administrator

Microsoft Certified Systems  
Engineer

Certified Ethical Hacker

## Clearances

OPM Public Trust

## EXPERIENCE *CONTINUED*

---

### *North Carolina Educational Lottery (NCEL):*

Gus led our team in an independent security assessment and audit of North Carolina Education Lottery (NCEL) systems and gaming operations. He worked with and reported directly to the internal audit team at NCEL. The review focused on both gaming systems (i.e. RNG, ICS) as well as the supporting IT infrastructure of Federal Information Systems and Organizations revision 4 as the baseline for the audit.

In addition to performing interviews and examinations, technical vulnerability assessment scans were also conducted on the NCEL network and systems. Vulnerability scans were conducted both from external and internal perspectives. A limited web application security assessment was also conducted on mission critical applications identified by NCEL. A physical security review was performed on the headquarters in Raleigh and a field office in Greensboro.

The result of this effort was a comprehensive audit report that NCEL could use to strengthen their overall security posture.

### *Florida Lottery*

Several assessment and security reviews were performed on the Florida Lottery., Gus performed security assessments and evaluated the Lottery's security posture for compliance with NIST 800-53 and the Cybersecurity Framework. Penetration testing and web application assessments were also performed.

### **Senior Security Consultant**

**Deloitte & Touche Information Security Services | Mclean, VA | 2002 - 2003**

### **Senior Security Consultant**

**KPMG Risk and Advisory Services | Washington, DC | 2000 - 2002**

### **System Administrator**

**Rydex Mutual Funds | Rockville, MD | 1998-2000**

## Skills

- Program and Project Management
- Enterprise Security Architecture (ESA)
- **Secure Configurations:** National Institute of Standards and Technology (NIST) checklists, Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIGs), and Center for Internet Security (CIS) benchmarks for applications, networks, and database platforms
- **Networking:** Transmission Control Protocol (TCP)/Internet Protocol (IP), firewalls, Virtual Private Network (VPNs), and Cisco routers and switches
- Operating Systems: Microsoft Windows 2008/2003/2000/NT/Vista/XP, RedHat, UNIX, IBM AIX, and z/OS Mainframe
- **Security Tools:** Nessus, Nikto, Metasploit, Nmap, L0phtcrack, Burp, Wireshark, ZAP, Kismet, DISA Security Readiness Review (SRR) Scripts, WebInspect, AppScan, AppDetective, and Snort
- **Desktop Applications:** Microsoft Office Suite – Outlook, Visio, and Project
- **Certification and Accreditation:** Implementing certification and accreditation (C&A) activities of information systems, and performing security assessments and production of C&A documentation.

# Rizwan Ahmed, Security+, CISSP

Senior Security Engineer



(703) 206-9383



Rizwan.Ahmed@bulletproofsi.com



Fairfax, VA

## EDUCATION

- B.S., Network Security, Strayer University
- B.S., Commerce, Karachi University (Pakistan)

## Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Access Data Certified Examiner v6
- CEH (Certified Ethical Hacker)
- CompTIA Security +
- MCDST (Microsoft Certified Desktop Support Technician)
- MCSE 4.0, 2000, & 2003 (Microsoft Certified Systems Engineer)
- A+ Certified
- Completed Hands-on Windows XP & Vista 7, 8, 10

## PROFESSIONAL PROFILE

Rizwan is experienced in enterprise-level IT infrastructure and components as well as possesses extensive technical expertise, incident response, and desktop and call center support experience. For many of our clients, he also performs security operations and forensics. Throughout his tenure, Rizwan has also run vulnerability scans and management programs for large organizations and has developed and implemented Disaster Recovery Plans (DRPs).

## WORK EXPERIENCE

### Senior Security Engineer

**Bulletproof Solutions, Inc. | Fairfax, VA | 2014 – Present**

*For the Multi-State Lottery Association (MUSL):*

- Forensically evaluated the new lottery systems. Yearly Security Assessment and assurance program to verify the integrity of their systems.

*For the Florida Lottery:*

- Performed vulnerability assessment and penetration testing

*For the Missouri Lottery:*

- Led an external/internal security assessment of the lottery's systems and network

*For Caesars Entertainment:*

- As required by gaming regulations performed security assessments on multiple properties in various jurisdictions.
- Performed penetration testing on iGaming web applications

*Yearly forensics of RNG Machines: Hoosier, Wisconsin, Iowa, and Colorado Lotteries*

*Yearly land-based security assessment and security assessments for sports betting:*

Cesar, MGM, Tropicana, Bally's Oceans, and Borgata.

*Department of Education (Plano, TX):* Yearly security assessments of their environment

*For the City of Alexandria, Virginia:*

- Set-up and configured Nessus for Vulnerability scanning on City's network
- Enabled scanning schedule and set-up scan policies for the entire network
- Performed set-up process to patch third-party software using Scmm2012; created policy to deploy custom packages
- Installed security Onion and set-up alerts as COA didn't have any IDS in place
- Performed firewall and switch configuration security audit

*For the Department of Education (OIG):*

- Conducted internal and external vulnerability assessment of Dept. of ED's information system
- Analyzed security posture of organization's IT infrastructure by utilizing manual and automated tools
- Ran Nmap port scanner, Nessus vulnerability scanner and utilized Metasploit to verify discovered vulnerabilities
- Used Kali Linux for all automated test procedures
- Created and submitted full security assessment report to Dept. of ED OIG with all findings and remediation recommendations
- Conducted WIFI network assessment. During assessment, carried out a review of organization's wireless security policies; reviewed and analyzed current wireless infrastructure; verified wireless device configurations using automated tools and scripts; scanned ED's wireless network for rogue access points; analyzed security gaps and provided gap analysis; and submitted a detailed recommendation report.

# Rizwan Ahmed

---

---

## Clearances

---

## EXPERIENCE *CONTINUED*

---

### Network Security Analyst

SeNet International Corporation | Fairfax, VA | 2009 – 2014

*For the Health Resources and Services Administration (HRSA):*

- Management responsibility for the HRSA Incident Response function, including interaction with the Departmental counterparts
- Responsible for CSIRC Ticketing system “Riskvision” for incident reporting
- Responsible for agency Ticketing system “Service Now” for incident reporting
- Responsible for Monthly Security Dashboard for CISO & CIO
- Responsible for handling Malware detected over the network analyze them and submit report to the Brach chief for further action and remediation
- Daily Monitoring of TippingPoint IDS/IPS
- Responsible for Security Applications & Servers for any new updates and troubleshooting
- Responsible for penetration testing for networks and applications for the agency
- Responsible for Vulnerability Scans using Tenable Security Center
- Responsible for Asset Management
- Involved in Forensics Process with Encase, FTK & SIFT Workstation
- Responsible for Threat Monitoring within FireEye & TippingPoint
- Managed Tipping Point, ArcSight, Net Witness, Tenable Security Center, IBM AppScan and HRSA SOC mailbox
- Sets up the test lab environment for upcoming security scanners and applications
- Responsible for maintaining the test lab
- Helped the risk assessment team for general support system (GSS) and major application (MA) certification and credentials
- Successfully tested enterprise products like Splunk, Guardian Edge, Alien Vault, and Pointsec

### Senior Desktop Support

HRSA | Rockville, MD | December 2007 – September 2009

## Skills

- **Security Tools:** FireEye, RedSeal, Netwitness, ArcSight, TippingPoint SMS, Tenable Security Center, Symantec Risk Automation Suite, IBM Security AppScan Standard & Enterprise, Wireshark, Alien Vault, and SecureFusion
- **Forensics Tools:** Guidance Encase Enterprises, AccessData FTK (Forensics Toolkit), Kali Linux, and SANs SIFT Workstation
- **Encryption Tools:** Pointsec, Bitlocker, PGP, Guardian Edge, and Safend & Dell Credant Encryption
- **Operating Systems:** Windows 8/7/Vista/XP/2000 Professional & Enterprise, Microsoft Windows NT/2000/2003/2008 Server, Macintosh OS9 and OSX, Linux, and Ubuntu (all distributions)
- **Enterprise Tools:** Lumension Patch Management, MacAfee ePolicy Orchestrator, Symantec Endpoint Protection Manager, BellArc, and LANDesk
- **Network Hardware:** Cisco switches 1900/2900, Cisco routers 800/1600/2500, hubs, switches 10/100/1000BaseT interface cards
- **Networking:** LAN/WAN, Ethernet, Fast Ethernet, Gigabit, Frame Relay, ATM, and ISDN
- **Protocols:** TCP/IP, NetBEUI, DHCP, DNS, PPP, SMTP, POP3, SNMP, and AppleTalk



# Nicholas Rosasco

C y b e r s e c u r i t y   C o n s u l t a n t  
| |



(703) 206-9383



Nicholas.Rosasco@bulletproofsi.com



Colorado

## EDUCATION

Cybersecurity Bachelor's Degree – Stevens  
Institute of Technology

## Certifications

Certified Ethical Hacker (CEH)  
Offensive Security Certified  
Professional (OSCP)  
Offensive Security Web Expert  
(OSWE)

## PROFESSIONAL PROFILE

Nicholas Rosasco is a consultant in Bulletproof's Cybersecurity Services Practice within the Governance Risk and Compliance Division. He has experience with network troubleshooting, web application penetration testing, and internal penetration testing. Nicholas has also created and managed a cybersecurity training program while at an MSP, as well as provided security vulnerability management services to customers as part of the Bulletproof team.

## WORK EXPERIENCE

### Senior Security Engineer

#### Bulletproof Solutions | October 2017-Present

- Responsible for participating in audits on the Information Systems of clients to evaluate whether they comply with the requirements as set by regulators and/or to ISO, PCI or other relevant standards.
- Takes part in audit planning, field work documentation and audit reporting.
- Helps maintain/update engagement and reporting tools.
- Helps train and mentor new recruits.
- Performs variety of security consulting services including internal and external penetration testing and vulnerability assessments, red team penetration testing, and more.

Clients include:

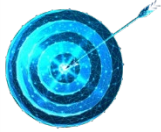
- South Carolina Department of Motor Vehicles (June 2022): Cybersecurity Assessment (adversarial engagement using Cobalt Strike)
- Colorado Lottery (June 2020): SmartPlay ADM Assessment
- Churchill Downs (April 2020): Cybersecurity Assessment

### Managed Solutions Engineer

#### Network Doctor | December 2014-September 2017

- Lead cybersecurity trainings for clients. Responsible for proposing the idea and creating training presentation.
- Wrote up executive summaries for Penetration Tests performed for clients.
- Involved in Incident Response when a client gets hit by malware or a breach.
- In charge of performing daily audits on clients' backups, OpenDNS traffic, and IDS alerts as well as various other monthly audits ranging from server utilization to AV protection by using knowledge in PowerShell scripting to speed up process.
- Directly involved in setting up new backup solutions for clients as well as troubleshooting current solutions.
- Involved in researching and testing new managed service tools.
- Heavily involved in backend operations for CRM (Connectwise), Client Experience Platform (DeskDirector), as well as reporting tool (Brightgauge) which used SQL queries to pull data for reports.

## *Bulletproof's Why, Vision, & Values*



### OUR **WHY**

We believe everyone has the right to feel safe and secure. Our mission is to serve and protect organizations to ensure their success.



### OUR **VISION**

To serve, secure, and empower the world through people and technology; one customer at a time.

### OUR **VALUES**



**People First:** We take care of our people, so they can take care of our customers.

**Customer Obsessed:** We have a "first responder" mentality and a serving spirit.

**Respect Always:** We value and respect everyone equally.

**Trustworthy:** We seek what's right, not who's right. Do the right thing.

**Authentic Communication:** We are committed to responsive and thoughtful communication.



**BULLETPROOF**

a GLI company