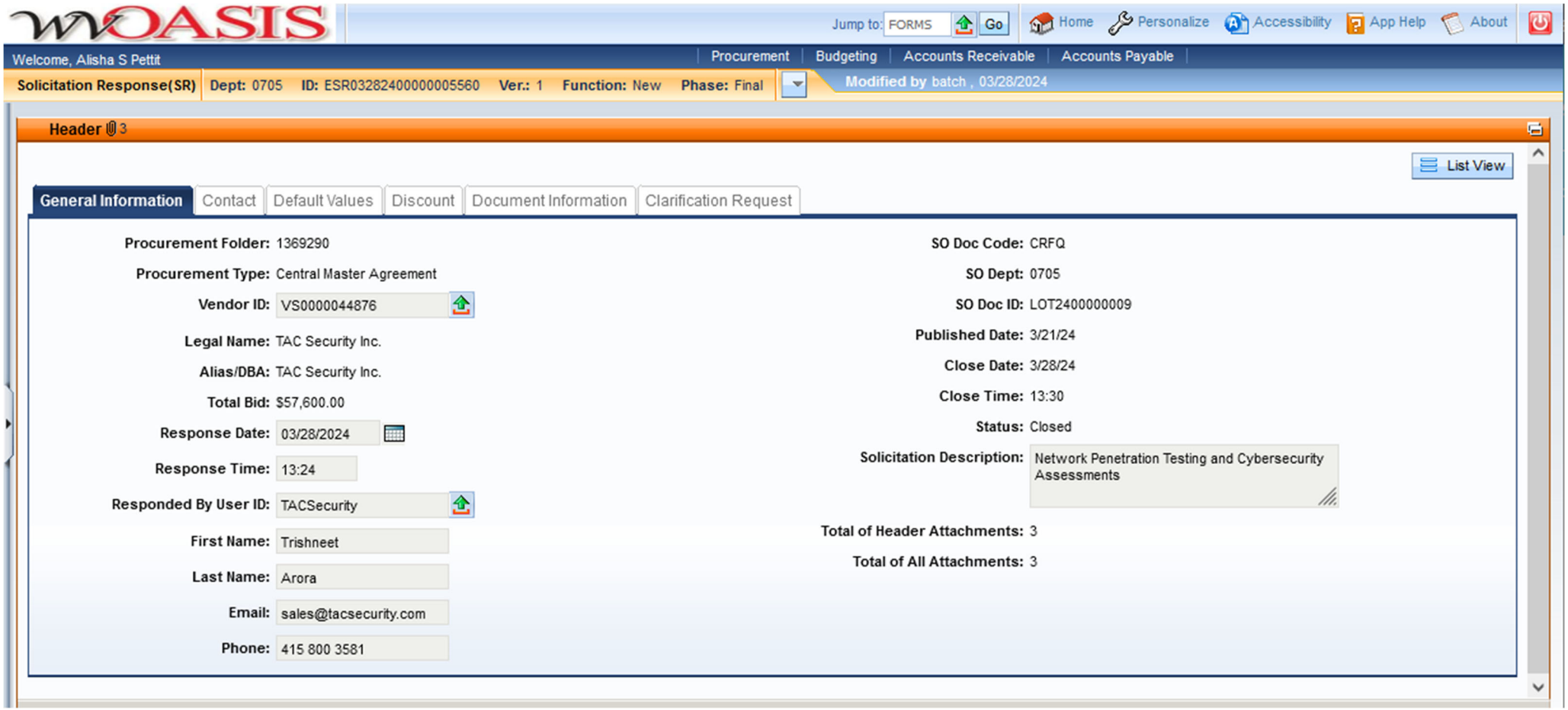
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency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


wvOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Alisha S Pettit
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR)
Dept: 0705
ID: ESR03282400000005560
Ver.: 1
Function: New
Phase: Final
Modified by batch , 03/28/2024
Header 3
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 1369290
Procurement Type: Central Master Agreement
Vendor ID: VS0000044876
Legal Name: TAC Security Inc.
Alias/DBA: TAC Security Inc.
Total Bid: $57,600.00
Response Date: 03/28/2024
Response Time: 13:24
Responded By User ID: TACSecurity
First Name: Trishneet
Last Name: Arora
Email: sales@tacsecurity.com
Phone: 415 800 3581
SO Doc Code: CRFQ
SO Dept: 0705
SO Doc ID: LOT2400000009
Published Date: 3/21/24
Close Date: 3/28/24
Close Time: 13:30
Status: Closed
Solicitation Description: Network Penetration Testing and Cybersecurity Assessments
Total of Header Attachments: 3
Total of All Attachments: 3

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 ESR03282400000005560	1

VENDOR

VS0000044876
TAC Security Inc.

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 57600 **Response Date:** 2024-03-28 **Response Time:** 13:24:56

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				14400.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				14400.00

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				14400.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				14400.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Proc Folder: 1369290
Network Penetration Testing and Cybersecurity Assessments

State of West Virginia
Centralized Request for Quote

TAC SECURITY INC.

POC: Trishneet Arora
Address: 1329, Market St #200, San Francisco, CA 94102
Contact No: 415 800 4748
Email Id: sales@tacsecurity.com
Website URL: https://tacsecurity.com/

Table of Contents

Cover Letter

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

March 26th, 2024

Dear Brandon,

I am writing on behalf of TAC Security to express our sincere gratitude for the opportunity to submit our proposal in response to the **Network Penetration Testing and Cybersecurity Assessments** issued by **State of West Virginia (hereinafter "State").** We understand the significance of this endeavour and are excited about the possibility of contributing to the Cyber Security.

TAC Security understand that the West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Lottery (Lottery) to establish a contract to perform and deliver information technology cybersecurity assessments, including external network, website, wireless, and internal/client-side penetration testing assessments.

We are thrilled to inform you that our proposal includes the completion and submission of all items required under this RFP. We have thoroughly reviewed the RFP guidelines and specifications, and our proposal complies with all the necessary requirements. Furthermore, we assure you that there are no exceptions or requested deviations from the RFP's terms and conditions in our submission.

We sincerely appreciate your consideration of our proposal. TAC Security is enthusiastic about the prospect of being your dedicated cybersecurity resource and trusted advisor. We look forward to the opportunity to collaborate with the Fund in safeguarding your critical assets and infrastructure against the ever-evolving cyber threats.

Company Information:

Company Name	**TAC Security Inc.**
Company Address	1390, Market St #200, San Francisco, CA 94102
FEIN Number	88-1247598
POC	Trishneet Arora
Title	Director
Email ID	sales@tacsecurity.com
Contact Number	415 800 3581
Website	https://tacsecurity.com/

Acceptance of the terms:

TAC Security accepts all the terms and conditions contained in the RFP & its associated document, and does not propose any exceptions or deviations.

Acceptance of the addenda:
TAC Security acknowledge the addendum no 1.

Sincerely,

Trishneet Arora
Director

Qualifications & Experience

History:

TAC Security was founded in October of 2013. TAC Security is in operation since it was founded and has seen a consistent growth in terms of Revenue, Clientele & Employees. Today we are a team of over 105 employees serving over 150+ clients in different industries and domains.

Introduction:

TAC Security Inc is a leading global provider of cutting-edge cybersecurity solutions, dedicated to safeguarding businesses and organizations from the ever-evolving threat landscape. With a relentless commitment to innovation, excellence, and client-centricity, TAC Security has emerged as a trusted partner in the fight against cyber threats.

TAC Security has seen a consistent growth, both in terms of revenue as well as employees and we have been successful in cyber security its employees as demonstrated above. TAC Security boast an excellent track record of employee retention with an average of above 50% which is higher than the industry standard.

- *Founded in 2013*
- *Gartner's Customer First Program Company*
- *Awarded by Forbes, Fortune, Entrepreneur*
- *Started in INDIA from one desk to reach Nasdaq*
- ***Google** as Strategic Partner*
- *Four(4) Product Patents Filled in the U.S.*

TAC Security has an extensive organizational experience that spans numerous successful engagements in the field of cybersecurity and Penetration Test services. Our expertise, honed through years of dedicated work, enables us to deliver exceptional solutions and meet the diverse needs of our clients. One of our key strengths lies in our deep understanding of the cybersecurity landscape. We have collaborated with Fortune 500 companies, including

industry giants like Google, to safeguard their critical digital assets and protect them from evolving threats. This experience has allowed us to develop advanced strategies and employ cutting-edge technologies to mitigate risks and ensure robust cybersecurity for our clients.

Our organizational experience extends beyond United States, as we have successfully executed projects on a national scale. Our team of highly skilled professionals, located throughout the United States, brings a wealth of knowledge and expertise to each engagement. By leveraging our diverse talent pool, we ensure that we have the right skills and capabilities to tackle any cybersecurity or IT professional services project.

In addition to our technical proficiency, we pride ourselves on our commitment to excellence and customer satisfaction. We prioritize building long-term partnerships with our clients, striving to understand their goals and deliver solutions that align with their specific objectives. This customer centric approach has earned us a reputation for reliability, quality, and innovation within the industry.

Ongoing Support:

Our knowledge and experience in government environments means we can provide the State with the expertise it requires. Our commitment goes beyond project completion; we envision a lasting partnership. We won't simply walk away after delivering results; instead, we're dedicated to providing continuous technical support and guidance, both during and after the remediation phase. We're in it for the long term.

Mission:

At TAC Security, our mission is clear and unwavering: to provide world-class cybersecurity services and technologies that empower organizations to protect their digital assets and customer data. We are driven by the belief that cybersecurity should not be a barrier to business growth but an enabler of innovation.

Global Reach:

TAC Security has a global presence, serving clients across industries and geographies. Our diverse team of cybersecurity experts is equipped to address the unique challenges faced by organizations worldwide.

Client Success Stories:

Over the years, TAC Security has helped numerous organizations bolster their cybersecurity posture and achieve peace of mind. Our client success stories serve as a testament to our dedication and expertise in the field.

Conclusion:

At TAC Security Inc, we are driven by a passion for cybersecurity excellence. We invite you to partner with us in securing your digital future. Together, we can navigate the complex cybersecurity landscape and ensure that your organization remains resilient in the face of evolving threats.

"ESOF by TAC Security was incredibly professional and efficient even when presented with logistical challenges. We now have visibility to all our servers and any cyber risks. Their work and diligence allowed us to gain visibility to any potential and actual vulnerabilities along with a user friendly cyber score. TAC Security helped us to mitigate the cyber risk and improve cyber security for our organization. Their work allowed us to have higher standards and accountability at the Office of the NM State"

Corporate Experience:

Number of Years of Corporate Experience Providing Services Described Under This Schedule, Regardless of the Specific Services Being Proposed Founded in 2016 by Trishneet Arora, TAC Security helps companies secure their cyber security footprint and increases awareness for organizations from all over the world. TAC Security specializes in assessing and securing financial transaction and helps organizations mitigate unwanted intrusions by analyzing and assessing the current state of cyber security and assigned a score depending on the results (i.e. lower scores equate to vulnerabilities). TAC Security currently manages approximately five plus million vulnerabilities for its customers with the help of the ESOF (Enterprise Security in One Framework) software suite developed by TAC Security and deployed to its customers in 2018.

Headquartered in California, TAC Security is honored to work with well-known brands and organizations from all over the world. TAC Security makes it a standard to help empower these organizations to secure their people, infrastructure, and other vulnerable surfaces. Organization's Number of Employees, Experience in the Field, and Resources Available to Enable it to Fulfill Requirements **"Vulnerability management is a relatively old idea, but innovative IT teams will continuously seek out updated solutions to stay one step ahead of bad actors, who continue to become increasingly sophisticated and resourceful in their malware development."** - Trishneet Arora, Founder/Director/CEO In response to the increasing threats of today's world, TAC Security needed to increase its own sophistication and resources to overcome the evolving challenge. Tackling the threat head on, TAC Security fulfills its requirements by delivering a product that will not only increase cyber security awareness across the organization, but will assist in managing the organization's

vulnerabilities, protecting web and app assets, and other dedicated functions with the use of the ESOF software suite. TAC Security currently has four employees in leadership positions dealing with its client's cyber security needs and has been in business for over 7 years. With the help of the ESOF software suite and current resources available, TAC Security has been able to increase its revenue by 270% year-over-year by 2019.

Brief History of the Offeror's Activities Contributing to the Development of Expertise and Capabilities Related to the Requirement

TAC Security was founded in 2016 by young entrepreneur, Trishneet Arora. Always working within the mindset of cybersecurity and with experiences of his own, Mr. Arora has been able to confidently ask, "There are two kinds of people in cyber space. One who doesn't know they are hacked, and one who knows that. Simple. So, you tell me. Which one you are?"

For Mr. Arora, finding the answer to this question was a necessity and already within his grasp at a young age. These are the driving factors behind the creation of the ESOF software suite and organizations can begin finding the answer to this question with the use of TAC Security's ESOF VACA, VMP, AppSec, and PCI ASV one framework applications.

TAC Security continues to expand its customer base by serving Fortune 500 companies, leading enterprises, and governments all over the world. TAC Security is looking forward to offering the federal government the same type of excellence provided to its existing customers, but at a competitive price on a contract that all other federal agencies can utilize.

Information that Demonstrates the Offeror's Organizational and Accounting Controls

TAC Security currently uses Zoho Books to accurately capture any accounting aspect found within the project cycle. TAC Security anticipates no issues when following the necessary actions and regulatory compliance actions that come with the GSA Schedule contract (Customer Assistance Visits, GSA Sales Reporting, etc.). Select organizational personnel are also being trained on the compliance actions that are required when becoming a GSA Schedule contactor and anticipates no issues and delays during contract performance, whether working with GSA with respect to the GSA Schedule contract or the agencies acquiring software from the contract.

Description of the Resources Presently In-House or the Ability to Acquire the Types and Kinds of Personnel Proposed

Current day activities require TAC Security to have the resources it needs to deliver the ESOF software suite to its expanding customer base. Product Development teams have spent numerous hours developing the ESOF suite in order to successfully bring the product to the market in 2018. Before ESOF's release to the public, TAC Security had bolstered its resources by expanding its leadership and sales teams, vastly improved its marketing efforts, updated its internal practices and policies, and established customer service channels. TAC Security's current-day success is based on these efforts and reason why TAC Security is able to handle the increased market response. Upon acquiring the GSA Schedule, TAC Security will use the same proven methodologies to engage government customers and will update as

appropriate. TAC Security is confident that is has the resources and staff currently in place to handle the government's expectations.

Description of the Marketing Strategy That Will be Used to Reach Federal Ordering Activities

Overview: As a Minority Owned, Self-Certified Small Disadvantaged, Subcontinent Asian (Asian-Indian) American Owned Small Business, TAC Security is able to offer a number of advantages to its potential federal customers by offering a threat identification total solution. TAC Security's software is able provide this solution without the need to acquire specialized labor categories found across other SINs and contracts.

Value Proposition: TAC Security can offer federal agencies peace of mind from outside cyber threats while focusing on their respective missions and build on the agency's current policy addressing cyber threat awareness and to further help mitigate unwanted intrusions.

Marketing Position: TAC Security is positioned to do well in the federal market space while offering needed services with discounted pricing.

Projected Sales: TAC Security anticipates sales of at least $400,000 for the initial 5 year period of the GSA Schedule contract. This projection was based on TAC Security's current client pool, its entrepreneurship, and the increasing need of cyber threat detection for businesses and organizations.

Marketing Strategy: TAC Security is currently engaging federal agencies and monitoring the related opportunities. While this engagement continues, the use of a GSA Schedule with discounted offerings will become a part of the marketing strategy and will advertise the contract to as many federal agencies in need. In addition to monitoring GSA eBuy for opportunities, TAC Security will actively monitor SAM.gov, attend trade shows and Industry Days, and access Federal Small Business resources.

Potential Federal Customers: TAC Security will continue to build upon its established government relationships with or without the use of the GSA Schedule contract. Once awarded, TAC Security will reengage our current relationships with the opportunity to acquire the software with the streamlined acquisition procedures that come with the GSA Schedule contract.

Why Choose TAC Security?

• **Comprehensive Solutions:** We offer a holistic range of cybersecurity services, from risk assessment to proactive defense, ensuring that every aspect of your organization's security is robustly fortified.

• **Expert Cyber Guardians:** Our team of highly skilled and certified cybersecurity professionals are your ultimate cyber guardians, tirelessly monitoring, detecting, and neutralizing threats before they even knock on your digital door.

• **Tailored to Your Needs:** We understand that every organization's cybersecurity challenges are unique. Our solutions are fully customizable, aligning perfectly with your specific requirements and risk appetite.

• **Trusted by Leading Institutions:** TAC Security is the cybersecurity partner of choice for prestigious educational and public sector entities, earning accolades for our exceptional service and unwavering commitment to excellence.

• **Proven Track Record:** With an impressive portfolio of successful projects, we have consistently demonstrated our ability to deliver exceptional results, earning the trust and loyalty of our clients.

• **Relevant Past Experience:** TAC Security takes pride in its rich experience in serving a diverse clientele, including prominent educational and public sector organizations.

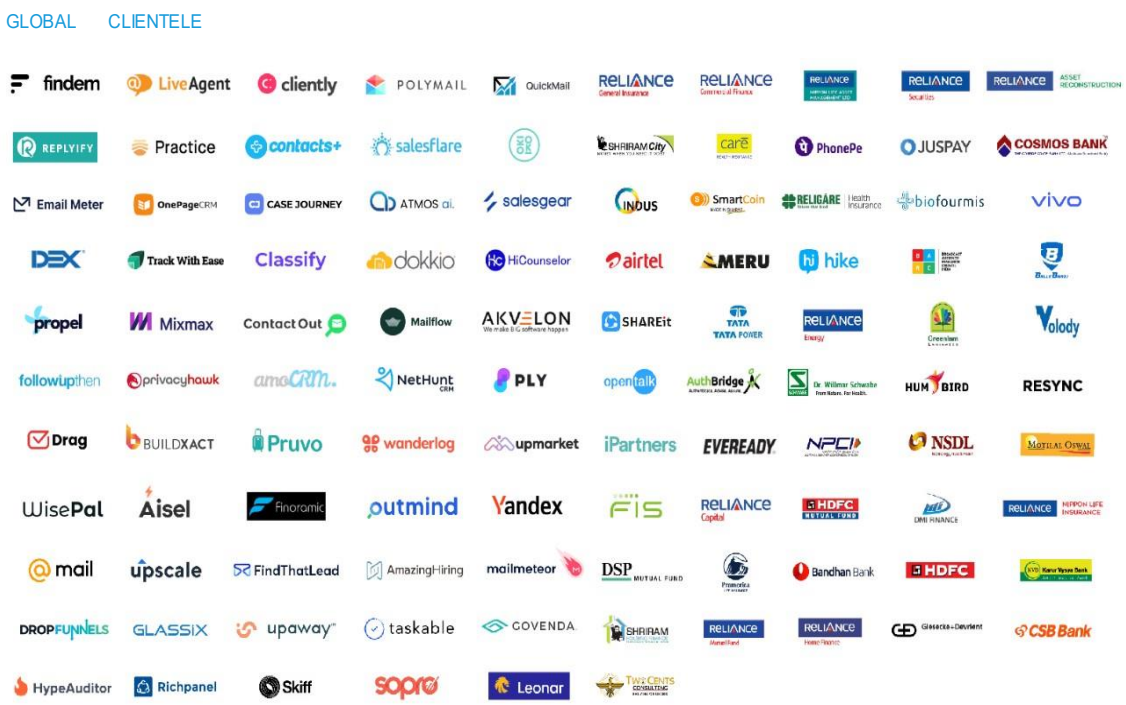
Professional Qualifications and Expertise

Our Unique Qualification:

- Gartner's Customer First program Company
- Awarded by Forbes, Fortune, Entrepreneur
- Google's Security Assessment Partner for OAuth and CASA Program
- Four (4) Product Patents Filled in the USA
- CREST Certified Penetration Testing Company
- **PCI ASV (Approved Scanning Vendor)**

Global Clients:

We take immense pride in the strong relationships we have cultivated with our global clients. Our commitment to providing world-class cybersecurity solutions has earned us the trust and loyalty of organizations across diverse industries. Here are some of our valued global clients:



TAC Security's Organizational Chart:

Role	Responsibilities
Chief Information Security Officer (CISO)	Overall cybersecurity strategy, executive leadership, compliance
Security Manager	Oversee daily security operations, team coordination, reporting
Incident Response Manager	Lead incident response planning, coordination, and execution
Security Architect	Design and implement security architecture, risk assessment
Threat Analyst	Monitor threat intelligence, analyze threats, recommend actions
Security Engineer	Implement and manage security solutions, network and system hardening
Forensic Analyst	Investigate security incidents, analyze digital evidence
Penetration Tester	Conduct security assessments, penetration testing

Role	Responsibilities
Security Operations Center (SOC) Analysts	Monitor security alerts, analyze incidents, and escalate
Compliance Officer	Ensure regulatory compliance, policy enforcement, audits
Identity and Access Management (IAM) Specialist	Manage user access, authentication, and identity systems
Network Security Specialist	Maintain and configure network security devices
Application Security Specialist	Assess and improve application security
Security Awareness Trainer	Conduct security awareness training for employees
Data Protection Officer	Manage data privacy, GDPR compliance, data handling
Legal Counsel (Cybersecurity)	Provide legal advice on cybersecurity and privacy issues
Vendor Security Manager	Evaluate and manage third-party vendor security risks
Risk Manager	Assess and manage cybersecurity risks, risk mitigation strategies
Cryptographer	Develop cryptographic solutions, secure communication
Security Operations Center (SOC) Technicians	Assist with monitoring, incident analysis, and tool management
Security Communication Specialist	Handle internal and external communication during incidents
Endpoint Security Specialist	Manage endpoint security solutions, malware analysis
Disaster Recovery Specialist	Develop and test disaster recovery plans
Security Auditor	Audit security controls, assess compliance, identify vulnerabilities

Our Leaders:

They share the unanimous goal of securing the cyberspace and that makes them unstoppable.

Trishneet Arora

Founder, Director & CEO

Trishneet Arora: Trishneet Arora is the Founder and CEO of TAC Security, a San Francisco-based Cybersecurity and Risk & Vulnerability Management Company. He is responsible for setting the overall direction and product strategy for the company and under his leadership TAC Security has expanded business globally and its product ESOF the Vulnerability Management Solution has been securing the world's top brands, Fortune 500 Companies includes US Govt. It has more than 150 clients in 15 countries, includes US, Canada, UK, Europe and India.

Trishneet was awarded "Entrepreneur of the Year" 2020 by the Entrepreneur Magazine in the Security Services Category. He is also a two-time list maker (2020 & 2021) for the "The Top 100 Great People Managers List" by Great Managers Institute in association with Forbes.

William H May

Director – North America

William H May: William has worked in the Cyber Security and Information Technology industry for over the past two decades. He is a global consulting and business transformation leader who grows, reinvents, and optimizes business-critical services and programs within and across enterprise environments.

Chris Fisher

Chief Marketing Officer

Chris Fisher: Chris Fisher brings 20 years of Marketing leadership to TAC Security, with eight years focused exclusively on enterprise security. He holds an MBA in Marketing and a BS in Computer Science from the University of Oregon.

Lt. General Iqbal Singh Singha

Director – Global & Govt. Affairs

Lt. General Iqbal Singh Singha: Lt. General Iqbal Singh Singha is the Director of Global and Government Affairs at TAC Security. With nearly four decades of experience in conflict resolution and conflict management, this highly decorated Indian Army General has attained many challenging and varied appointments in India and abroad.

Bharat Panchal: Bharat has been honoured with prestigious "Security Leader of the Year" Award in 2014 and 2017 by Data Security Council of India (DSCI) for his significant contribution in cyber security in banking sector. Computer Society of India also has awarded him "Best CRO of the year" in 2016 apart from several prestigious awards and recognitions from the industry.

Bharat Panchal

Member Board of Directors

Subinder Khurana

Member Board of Advisors

Subinder Khurana: With 30+ years of cybersecurity and entrepreneurship, Subinder Khurana brings an insight to TAC Security like never before. An entrepreneur with a successful track record. Specialize in products and platform-based solutions. Built businesses, sold and delivered products and services, both in India and globally.

Dr. Siva Subramanian: Dr. Siva is a senior Cybersecurity professional with 20 years of Cybersecurity, risk, and compliance management experience at the executive level with a solid technical background.

Dr. Siva Subramanian

Member Board of Advisors

Raphael Warren

Member Board of Advisors.

Raphael Warren: Brigadier General Raphael Warren (SDF NM) has over 25 years of US military and civilian Information technology experience and credentials. He holds the highest levels of security clearances and is nationally recognized for his expertise in Cyber Security and the development of Cyber Security teams.

TAC Security's Equal Employment Opportunity and Affirmative Action Policy:

Our policies are commonly implemented in organizations and government agencies to ensure that individuals are not discriminated against based on their race, color, religion, sex, national origin, disability, or other protected characteristics. Here's an overview of both concepts:

Equal Employment Opportunity (EEO): EEO refers to the principle that all employees and job applicants should be treated fairly and without discrimination in all aspects of employment, including recruitment, hiring, training, promotions, compensation, and more. The goal of EEO is to create a workplace environment where all individuals have an equal opportunity to succeed based on their skills, qualifications, and job performance, rather than being hindered by irrelevant factors.

Key aspects of EEO include:
Non-Discrimination: Employers are prohibited from making employment decisions based on protected characteristics. This includes not only direct discrimination but also practices that have a disparate impact on certain groups.

Reasonable Accommodation: Employers must provide reasonable accommodations to employees with disabilities to ensure they can perform essential job functions.

Harassment Prevention: Employers are required to take steps to prevent and address workplace harassment, creating a safe and inclusive environment for all employees.

EEOC: In the United States, the Equal Employment Opportunity Commission (EEOC) is the federal agency responsible for enforcing EEO laws.

Affirmative Action: Affirmative action goes beyond equal opportunity by actively seeking to address historical and systemic inequalities in employment, education, and other areas. Affirmative action policies are often implemented to increase the representation of underrepresented groups in areas where they have been traditionally marginalized. These policies aim to promote diversity and reduce disparities.

Key aspects of affirmative action include:

Goals and Targets: Employers may set specific goals and targets to increase the representation of underrepresented groups in their workforce, especially in positions where they have been historically excluded.

Outreach and Recruitment: Employers may engage in targeted outreach and recruitment efforts to attract a more diverse pool of candidates.

Quotas vs. Preferences: While some affirmative action policies involve setting quotas, others involve giving preferences to underrepresented groups in the hiring process. Quotas have been controversial and are subject to legal challenges.

Legality and Controversy: Affirmative action policies have sparked debates about reverse discrimination, fairness, and whether they are still necessary. Legal cases in various countries have shaped the extent to which affirmative action can be implemented.

It's important to note that the specifics of EEO and affirmative action policies can vary from country to country, and even within different jurisdictions within a country. Organizations typically develop their own policies and practices in line with the legal and regulatory framework of their region.

Bidder Information

TAC Security is pleased to present this proposal to the Authority, outlining our comprehensive cybersecurity solutions that are designed to meet the evolving security challenges of today's digital landscape. ESOF by TAC Security with, suite of products - ESOF AppSec, ESOF VMP, and ESOF VACA - represents the cutting-edge technology and expertise we bring to protect and optimize your organization's digital assets.

ESOF AppSec: ESOF AppSec is our flagship application security solution designed to shield your applications from vulnerabilities and ensure that your digital assets remain secure. Through comprehensive testing and cutting-edge methodologies, ESOF AppSec empowers organizations to identify and remediate potential security gaps before malicious actors exploit them.

ESOF VACA (Vulnerability Assessment and Configuration Assessment): ESOF VACA offers a comprehensive vulnerability assessment and configuration assessment. With meticulous scanning and assessment, this solution helps organizations meet industry standards and regulatory requirements while bolstering their overall security posture.

ESOF VMP (Vulnerability Management Program): ESOF VMP is a proactive vulnerability management platform that enables organizations to identify, prioritize, and remediate vulnerabilities across their IT landscape. This approach ensures that potential threats are addressed in a timely manner, minimizing the risk of cyber incidents.

ESOF PCI ASV (Payment Card Industry - Approved Scanning Vendor): As an Approved Scanning Vendor (ASV) by **PCI - DSS**, TAC Security specializes in conducting PCI DSS compliance scans. Our ASV services ensure that your organization meets the stringent security standards set by the Payment Card Industry, safeguarding sensitive cardholder data from breaches.

At TAC Security, we believe in delivering nothing short of excellence. With a portfolio of successful projects, a roster of satisfied clients, and a suite of robust products like ESOF AppSec, ESOF VACA, ESOF VMP, and ESOF PCI ASV, we are equipped to elevate your

Key Benefits for Authority:

- **Alignment with Authority's Needs:** Our solutions are designed to match the specific requirements of educational institutions, offering a flexible and robust defense strategy.
- **Proactive Risk Management:** Continuous monitoring and cyber risk quantification enable proactive measures to prioritize and mitigate risks.
- **Credibility and Recognition:** Our accolades and satisfied client base, including global giants, attest to the reliability and effectiveness of our solutions.

TAC Security is committed to partnering with Authority to elevate your cybersecurity to new heights. Our proposal encompasses all mandatory requirements, including insurance and

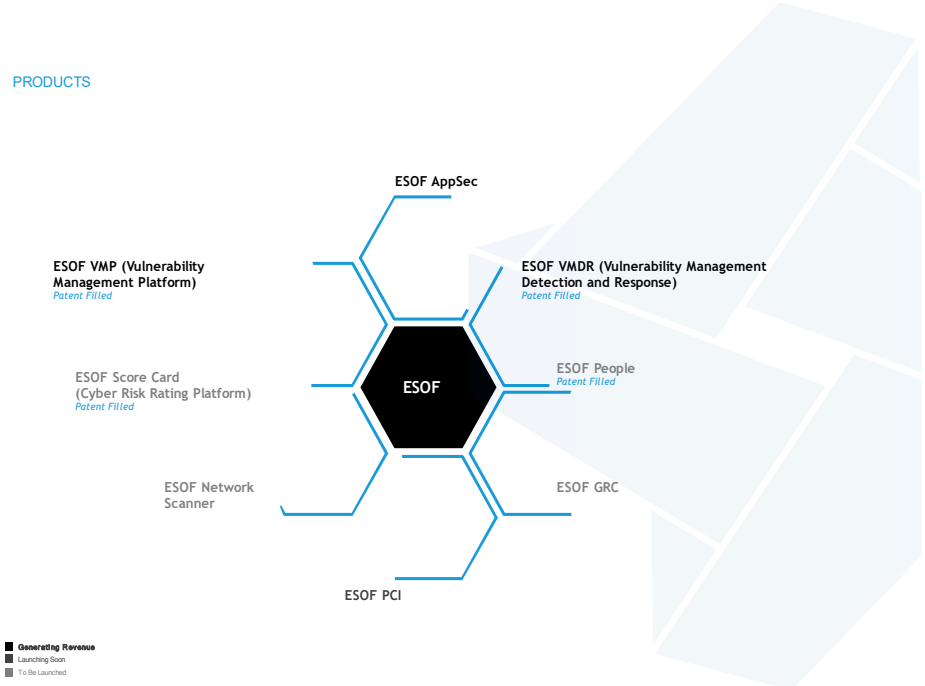
acceptance of terms. Through collaboration, we aim to protect your digital landscape, ensuring resilience, compliance, and peace of mind.

Award-Winning Recognition: ESOF VMP stands tall as the "Customer's First Choice" on Gartner Peer Insights. This prestigious honor is a testament to our dedication to customer satisfaction, innovation, and our proactive approach to tackling the most intricate cybersecurity challenges.

Trust Among the Elite: Our reputation for quality has earned the trust of industry giants such as Fortune 10 Companies, AmerisourceBergen Corporation, and Google. The partnership with these renowned organizations reflects our ability to deliver top-notch solutions and adapt to various industry needs.

Compliance Excellence: ESOF's recognition as a **PCI ASV Solution** by **PCI DSS** underscores our commitment to adhering to industry regulations and standards. This accreditation further amplifies our credibility, ensuring that clients receive services that meet and exceed regulatory requirements.

The ESOF vulnerability scanner continuously scans and detects asset threats, vulnerabilities, and risks. Also, ESOF VACA does the intel analysis to prioritize exploitable risks, catch the latest superseding patch for the vulnerable asset, and deploy remediation quickly.



ESOF® VACA allows forward-looking enterprises to do the vulnerability analysis of every asset within their IT infrastructure automatically without the need for any human intervention, which includes refractory assets, hardware/ software inventory, and so on. Once identified, these assets are tagged, and communication is done with the team for better vulnerability Assessment.

Empower your organization to proactively manage cyber risk with ESOF CRQ's precise financial risk assessment. Stay ahead of potential threats and confidently make informed decisions using diverse data sources.

Many organizations face challenges in meeting PCI DSS requirements. A lack of real-time visibility into assets and risks across global hybrid-IT landscapes, along with siloed security systems from multiple vendors, can create fragmented data and compliance gaps. Additionally, manual processes and the need for multiple tools increase operational overhead, making it difficult for security teams to keep up. TAC Security presents ESOF PCI ASV, a comprehensive and integrated solution tailored to simplify your path to PCI compliance.

At TAC Security Inc, our commitment to excellence and cybersecurity expertise have earned us the trust of a diverse range of global clients. From leading financial institutions to multinational corporations and government agencies, our solutions have consistently delivered unparalleled security.

Company Information

Company Name	**TAC Security Inc.**
Company Address	**1390, Market St #200, San Francisco, CA 94102**
FEIN Number	**88-1247598**
POC	**Trishneet Arora**
Title	**Director**
Email ID	**sales@tacsecurity.com**
Contact Number	**415 800 3581**
Website	**https://tacsecurity.com/**

Our Project Manager:

Name:	**Saransh Rawat**
Title:	Project Manager
Email ID:	sales@tacsecurity.com
Contact Number:	415 800 4748

Professional References

Reference Information	*Reference No. 1*
Company providing reference:	Office of Attorney General, New Mexico
Contact name and title/position:	Nick Eckert/Grants & Contracts Manager and Hector, Balderas, Former Attorney General
Scope of services of the engagement:	Cybersecurity Services
Engagement Budget:	$450,000
Engagement Term:	Start Date: May 2018, End Date: March 2022
Contact telephone number:	(505) 490-4831
Contact e-mail address:	neckert@nmag.gov

Reference Information	*Reference No. 2*
Company providing reference:	Office of State Auditor, New Mexico
Contact name and title/position:	Frank Valdez/Director-IT and Brian and Brian Colon, Former State Auditor
Scope of services of the engagement:	Cybersecurity Services
Engagement Budget:	$12,600
Engagement Term:	Start Date: March 2020, End Date: August 2020
Contact telephone number:	(505) 476-3800
Contact e-mail address:	frank.valdez@osa.state.nm.us

Reference Information	*Reference No. 3*
Company providing reference:	AmerisourceBergen Corporation
Contact name and title/position	Kumar C./Former Director, Vulnerability Management and Rob Taylor/CyberSecurity Threat Vulnerability Manager
Scope of services of the engagement:	Cybersecurity Services
Engagement Budget:	$2,000,000
Engagement Term:	Start Date: December 2019, End Date: December 2023
Contact telephone number:	+1 (469) 207-9529
Contact e-mail address:	taylor.robert@amerisourcebergen.com

Reference Information	*Reference No. 4*
Company providing reference:	MailoMeter
Contact name and title/position:	Corentin Brossault/CTO & Co-founder
Scope of services of the engagement:	Cybersecurity Services
Engagement Budget:	$45,000
Engagement Term:	Start Date: January 2022, End Date: December 2023
Contact telephone number:	NA
Contact e-mail address:	hello@mailmeteor.com

Project Team and Qualification

Our Staff Qualifications:

No.	Name of Employee	Qualification	Certified on Tool	Trained on Tool
1	Saransh Rawat Exp: 4 Years	Graduation (CEH)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube
2	Anuj Kulkarni Exp: 7 Years	Graduation (CEH)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube
3	Keshav Kumar Exp: 7 Years	Graduation (CISSP)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube
4	Vishal Patil Exp: 5 Years	Graduation (CEH)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube
5	Nakul Dhamale Exp: 4 Years	Graduation (CEH)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube
6	Nittin Dogra Exp: 3 Years	Graduation (CEH)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube
7	Vamshi Burugupalli Exp: 3 Years	Graduation (CEH)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube
8	Tarun Kant Exp: 4 Years	Graduation (CEH)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid

				Attacks, SonarQube
9	Rupali Sharma Exp: 2 Years	Post Graduation (CEH)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube
10	Rajeev Singh Exp: 3 Years	Graduation (CEH),	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube
11	Anusha Agarwal Exp: 3 Years	Graduation (CEH)	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube	ESOF, BurpSuite, Nessus, Nmap, Metasploit, Fluid Attacks, SonarQube

Resumes of Key Personnel

Trishneet Arora

Trishneet Arora is the Founder and CEO of TAC Security, a San Francisco-based Cybersecurity and Risk & Vulnerability Management Company.

The young tech wizard is exceptionally passionate about securing cyberspace and started his entrepreneurial journey in 2013 at 19. From there, under his leadership, TAC Security has been securing the world's top brands and Governments while disrupting cybers space.

Trishneet made it to the Top 200 **"Leaders of Tomorrow"** by **St. Gallen Symposium, Switzerland** for the second time in 2022, the first time being in 2018.

In 2021, he was listed in Fortune India's 40 Under 40 list for the second time, being the youngest on it both times.

He is a also a two-time list maker (2020 & 2021) for the "The Top 100 Great People Managers List" by Great Managers Institute in association with Forbes.

Trishneet Arora was awarded **"Entrepreneur of the Year"** 2020 by the Entrepreneur Magazine in the Security Services Category.

In the past, he was listed in the **50 Most Influential Young Indians** by **GQ Magazine** 2017.

Trishneet is also part of Entrepreneur Magazine's 35 under 35 & **Forbes 30 Under 30** Asia 2018 List.

Late Javier Gonzales, *Mayor of the City of Santa Fe, New Mexico, proclaimed 25th August as the *"Trishneet Arora Day"** in 2017.

Trishneet is responsible for setting the overall direction and product strategy for the company and under his leadership TAC Security has expanded business globally and its product ESOF the Vulnerability Management Solution has been securing the world's top brands, Fortune 500 Companies includes US Govt. It has more than 150 clients in 15 countries, includes US, Canada, UK, Europe and India.

He enjoys connecting with global leaders and divides his time amongst various by being a part at conferences as speaker.

"My vision is to help CXOs strategically assess & manage enterprise-wide risk through a single platform."

Trishneet Arora

TAC Security
CYBERSECURITY'S FUTURE

ESOF
Enterprise Security in One Framework
by TAC Security

William May

William is working as a Managing Director with TAC Security and has more than 15 years of experience in strategic planning, business development, and full lifecycle management of large business process transformation projects.

He has launched, revitalized and optimized several of IBM critical technology services and solution offerings. He is a business transformation leader who grows, reinvents and optimizes business critical services and programs within and across enterprise environments.

Global business leader who elevates the level of performance of large, internationally-dispersed teams, aligns and optimizes resources, and ultimately raises the company's competitive position in the market.

Education:

- MBA, Finance, International Management from Saint Joseph's University - Erivan K. Haub School of Business logo

Qualifications, Training, and Conference participation:

- BM Global Services confirmed Partner - Issued May 2004
- IBM Global Services Certified Management Consultant- Issued Apr 2000

Professional History :

Managing Director at TAC Security

Career Work Experience:

- Providing best of class cyber-security solutions to enterprises in the USA, India and EMEA leveraging onshore and offshore capabilities. Developed first consulting sales team focused on industry verticals.
- Manage existing projects for sales and delivery excellence.
- Govt. & Regulator Compliance Management -Software Security Assessment -ISO 27001 Compliance Management -PCI DSS Compliance -Risk Advisory -SCADA Security Testing Web Application Security Assessment -Mobile Application Security Assessment -Network Security Assessment Testing -Static Code Analysis Review - Red Teaming -Secure Configuration.

– William May – Managing Director, Experience 25+years

in

TAC Security

ESOF
Enterprise Security in One Framework
by TAC Security

Chris Fisher

Chris Fisher brings 20 years of Marketing leadership to TAC Security, with 8 years focused exclusively on enterprise security. He holds an MBA in Marketing and a BS in Computer Science from the University of Oregon.

Prior to TAC Security, he has worked with Tripwire as the Vice-President and PWC to name a few.

Chris enjoys practising yoga, gardening and experimenting with gourmet cooking in his free time.

Previous Experience – Tripwire and PWC

"I'm delighted to be part of the leadership team at TAC Security, a company with an entrepreneurial spirit and innovative solutions for today's complex cyber security problems."

– Chris Fisher, Chief Marketing Officer

TAC Security
CYBERSECURITY'S FUTURE

ESOF
Enterprise Security in One Framework
by TAC Security

Saransh Rawat

Saransh is working as AppSec Manager at TAC Security with strong background in IT Infrastructure, Information Security and IT Compliance. Focused and result oriented individual who wants to continue the career as a successful cybersecurity professional in a major global organization and to work in a creative and challenging environment using cutting edge technologies, where I could learn, successfully deliver solutions to problems and establish responsibility for Information Security in the organization by safeguarding the confidentiality, integrity and availability of the information.

Education:

- Bachelor of Science - University of Delhi, India.
- Certified Information Security Consultant - Institute of Information Security.

Qualifications, Training, and Conference participation:

- Certified Ethical Hacker (CEH) - EC Council
- Certified Professional Forensic Analyst - IIS
- Certified Blockchain Expert - Blockchain Council
- ISO 27001:2013 ISMS – CERTIFIED LEAD AUDITOR
- Payment Card Industry - ASV Analyst Certified

Professional History:

- AppSec Manager with TAC Security
- Information Security Analyst at Paralok Information Security Pvt. Ltd.

CareerWork Experience:

- To Contribute skills, knowledge in security assessment of the Web Applications, Mobile Applications, Infrastructure, Source Code Review.
- Responsible for Projects Delivery to the clients & application owners.
- Responsible for consulting with application developers, systems administrators and management to demonstrate security testing results, explain the threat presented by the results, and consult on remediation. Developed and maintained security testing plans, anchoring client-side penetration tests from an insider as well as outsider threat perspective.
- Specialized in penetration testing and vulnerability assessment activities of complex applications, operating systems, wired and wireless networks, and mobile applications/devices. Performed cyber threat intelligence ops including tracking threat actors and identifying & tracking malicious infrastructure. Responsible for supporting Digital foot printing, external threat management and identifying & analyzing business violations of security policies and standards.
- Deployed at one of the biggest financial firms to assess their web applications, mobile applications, API Security, Infrastructure.
- Performed Operational technology (OT)/industrial control system (ICS) security.

– Saransh Rawat – AppSec Manager, Experience 4+years

TAC Security
CYBERSECURITY'S FUTURE

ESOF
Enterprise Security in One Framework
by TAC Security

Vishal Patil

Saransh is working as AppSec Manager at TAC Security with strong background in IT Infrastructure, Information Security and IT Compliance. Focused and result oriented individual who wants to continue the career as a successful cybersecurity professional in a major global organization and to work in a creative and challenging environment using cutting edge technologies, where I could learn, successfully deliver solutions to problems and establish responsibility for Information Security in the organization by safeguarding the confidentiality, integrity and availability of the information.

Education:

- Bachelor of Science - University of Delhi, India.
- Certified Information Security Consultant - Institute of Information Security.

Qualifications, Training, and Conference participation:

- Certified Ethical Hacker (CEH) - EC Council
- Certified Professional Forensic Analyst - IIS
- Certified Blockchain Expert - Blockchain Council
- ISO 27001:2013 ISMS – CERTIFIED LEAD AUDITOR
- Payment Card Industry - ASV Analyst Certified

Professional History:

- AppSec Manager with TAC Security
- Information Security Analyst at Paralok Information Security Pvt. Ltd.

Career Work Experience:

- Contribute skills, knowledge and ideas during security assessments and penetration testing. Responsible for testing the client asset along with reporting as well as attending walkthroughs and remediation calls addressing client's concerns by providing a practical approach with respect to the business requirement.
- Executing Red Teaming Activities, Network Security, IS Audit, ISO-27001 Audit with respect to global practice and standards.
- Responsible for consulting with application developers, systems administrators and management to demonstrate security testing results and their impact by providing detailed P.O. C's and precise steps to replicate the vulnerability.
- Demonstrating hands on experience with vast set of tools during assessments covering range of assets including Networks, Web Applications and Mobile Applications. Performing though enumeration by gauging scope of work accurately.
- Leveraging previous development experience in static testing along with well defined test cases for dynamic testing thus conducting a through testing of the asset.
- Communicate security issues to a wide variety of internal and external "customers" to include technical teams, executives, risk groups, vendors and regulators.
- Testing for clients across various verticals like Entertainment and Retail, BFSI, predominantly in India.

– Vishal Patil – Sr. SecurityEngineer, Experience 4+ years

in

TAC Security
CYBERSECURITY'S FUTURE

ESOF
Enterprise Security in One Framework
by TAC Security

Nakul Dhamale

Nakul is working as Senior Security Engineer with TAC Security with strong background in IS Audit, Red Teaming, Network Security, Web Applications, Mobile Applications and API & Thick client App Security Testing. Disciplined and result oriented individual who is willing to work in a creative environment.

Education:

- CDAC-PG-DITISS, Juhu, Mumbai.
- B.E(Bachelors in Engineering E&TC) Pune University, Pune

Qualifications, Training, and Conference participation:

- CEH V10 (Certified Ethical Hacker).
- ISO-27001 LA.

Professional History:

- Sr. Security Engineer at TAC Security
- Information Security Analyst at AQM Technologies PVT LTD

Career Work Experience:

- To Contribute skills, knowledge and ideas during security assessments and penetration testing. Responsible for testing the client asset along with reporting as well as attending walkthroughs and remediation calls addressing client's concerns by providing a practical approach with respect to the business requirement.
- Responsible for consulting with application developers, systems administrators and management to demonstrate security testing results and their impact by providing detailed P.O.C's and precise steps to replicate the vulnerability.
- Demonstrating hands on experience with vast set of tools during assessments covering range of assets including Networks, Web Applications and Mobile Applications. Performing though enumeration by gauging scope of work accurately.
- Execute firewall audit fieldwork autonomously in accordance with audit work programs. Execute IS Audit, Network Security Review, ISO-27001 Audit with respect to global practice and standards.
- Well versed with performing red teaming activities and source code review.
- Leveraging previous development experience in static testing along with well defined test cases for dynamic testing thus conducting a through testing of the asset.
- Communicate security issues to a wide variety of internal and external "customers" to include technical teams, executives, risk groups, vendors and regulators.
- Testing for clients across various verticals like Entertainment and Retail, BFSI, predominantly.

– Nakul Dhamale – Sr. SecurityEngineer, Experience 4.9 years

in

TAC Security
CYBERSECURITY'S FUTURE

ESOF
Enterprise Security In One Framework
by TAC Security

Nittin Dogra

Nittin is working as Security Engineer at TAC Security with strong background in web applications, mobile applications and API security Testing.

Education:

- Bachelor Of Engineering, Computer Science Engineering (Chitkara University, Himachal Pradesh, India)

Qualifications, Training, and Conference participation:

- Certified Information Security Consultant (CISC) (Institute Of Information Security, Chandigarh, India)
- Certified Professional Forensic Analyst (CPFA) (Institute Of Information Security, Chandigarh, India)

Professional History:

- Security Engineer at TAC Security
- Trainee at IIS (Institute of Information Security)

Career Work Experience:

- To contribute skills, knowledge and ideas in performance of security analysis and identifying possible vulnerabilities in the key derivative function. Responsible for creating vulnerability assessment reports detailing exposure that were identified, rate the severity of system & suggestions to mitigate any exposures and testing known vulnerabilities. Performing vulnerability assessment and penetration testing for clients across various vertical like Entertainment and Retail, BFSI, predominantly in India.
- Demonstrating hands on experience with vast set of tools during assessments covering range of including Networks, web applications and mobile applications. Performing through enumeration by gauging scope of work accurately.
- Responsible for consulting with application developers, systems administrators and management to demonstrate security testing results, explain the threat presented by the results, and consult on remediation. Developed and maintained security testing plans, anchoring client-side penetration tests from an insider as well as outsider threat perspective..

– Nittin Dogra – Security Engineer, Experience 2+years

in

TAC Security
CYBERSECURITY'S FUTURE

ESOF
Enterprise Security in One Framework
by TAC Security

Vamshi Burugupalli

Vamshi is working as Security Engineer with TAC Security with strong background in Web Applications, Mobile Applications API Security, Red Teaming, Infra Audit, IS Audit, ISO- 27001 Audit and firewall Audit. Disciplined and result oriented individual who is willing to work in a creative environment.

Education:

- Computer Science (CS)

Qualifications, Training, and Conference participation:

- Certified Ethical Hacker (CEH)
- Penetration Testing, Incident Response and Forensics (IBM)
- Network Defense (Cisco)
- Android Application Security (PTLA)

Professional History:

- Security Engineer at TAC Security.
- Associate Security Consultant in SecLance.

Career Work Experience:

- To Contribute skills, knowledge and ideas during security assessments and penetration testing. Responsible for testing the client asset along with reporting as well as attending walkthroughs and remediation calls addressing client's concerns by providing a practical approach with respect to the business requirement.
- Responsible for consulting with application developers, systems administrators and management to demonstrate security testing results and their impact by providing detailed P.O. C's and precise steps to replicate the vulnerability.
- Demonstrating hands on experience with vast set of tools during assessments covering range of assets including Networks, Web Applications and Mobile Applications. Performing though enumeration by gauging scope of work accurately.
- Leveraging previous development experience in static testing along with well-defined test cases for dynamic testing thus conducting a through testing of the asset.
- Well versed with Red Teaming Activities, IS and ISO-27001 Audit with respect to global practice and standards.
- Communicate security issues to a wide variety of internal and external "customers" to include technical teams, executives, risk groups, vendors and regulators.
- Testing for clients across various verticals like Banking, Healthcare, Finance, E-commerce, and Logistics in India and for foreign clients.

– Vamshi Burugupalli – Security Engineer, Experience 3.5 years

TAC Security
CYBERSECURITY'S FUTURE

ESOF
Enterprise Security in One Framework
by TAC Security

Tarun Kant Rangra

Tarun is working as Sr. Security Engineer with TAC Security with strong background in Web Applications, Mobile Applications, Red Teaming, Network Security, ISMS Audit and ISO 27001 Audit. Disciplined and result oriented individual who is willing to work in a creative environment.

Education:

- B.Tech CSE (Bachelors of Technology) SRM University.

Qualifications, Training, and Conference participation:

- Mobile Application Security.
- Wireshark.
- CNSP
- CEH
- IT Security (Google)

Professional History:

- Sr. Security Engineer at TAC Security.
- Project Engineer at CDAC-Mohali.

Career Work Experience:

- Contribute skills, knowledge and ideas during security assessments and penetration testing. Responsible for testing the client asset along with reporting as well as attending walkthroughs and remediation calls addressing client's concerns by providing a practical approach with respect to the business requirement.
- Executing Red Teaming Activities, Network Security, IS Audit, ISO-27001 Audit with respect to global practice and standards.
- Responsible for consulting with application developers, systems administrators and management to demonstrate security testing results and their impact by providing detailed P.O. C's and precise steps to replicate the vulnerability.
- Demonstrating hands on experience with vast set of tools during assessments covering range of assets including Networks, Web Applications and Mobile Applications. Performing though enumeration by gauging scope of work accurately.
- Leveraging previous development experience in static testing along with well defined test cases for dynamic testing thus conducting a through testing of the asset.
- Communicate security issues to a wide variety of internal and external "customers" to include technical teams, executives, risk groups, vendors and regulators.
- Testing for clients across various verticals like Entertainment and Retail, BFSI, predominantly in India.

– Tarun Kant Rangra – Sr. Security Engineer, Experience 4+ years

in

Similar Projects:

Project Experience No. (1, 2, 3, etc.):	SIN(s) to which this project applies:	Specific services being proposed under the SIN(s):
3	54151HACS	IT Cybersecurity Services, Application Security Testing, Penetration Testing, Risk/Vulnerability Assessment, High Value Asset Assessment, Cyber Hunt

This project was completed within the last two years OR ☒ **Note: Projects that were completed more than two years prior to the date of the offer submission will not be accepted by the Government.**	**This project is an ongoing contract with a base year and option years, or is a multi-year task order. At a minimum, the base year or first year has been completed.** ☐ **Note: Projects that are in their base or first year and that year is incomplete as of the date of the offer submission will not be accepted by the Government.**
Customer/Client Name:	HiCounselor
Project Name/Contract Number:	ESOF-AppSec Premium
Customer Point of Contact (POC) for Project:	Ashish Mishara
POC's Current Phone Number and Email:	P. +91-9930441902 E. ashish@hicounselor.com
Project Performance Period (include months/years):	START DATE: 1/25/2022 END DATE: 5/20/2022
Dollar Value of the Entire Project:	$12,600
Dollar Value Received for the Work Performance Relevant to the SIN(s) Offered:	$12,600
Brief Summary of Project:	Offered a comprehensive suite of cybersecurity services to HiCounselor ensuring their digital assets remained secure.

Detailed Description of SIN Relevant Work performed and results

HiCounselor, a leading career accelerator, seamlessly combines technology with professional mentorship to empower job seekers in landing tech roles swiftly. As an organization heavily reliant on its web platforms to deliver services, they needed a robust tool to safeguard their digital assets. TAC Security was enlisted by HiCounselor and provided the customer with its ESOF AppSec to satisfy the request.

Methodology, tools, and/or processes utilized in performing the work

HiCounselor chose TAC Security's ESOF AppSec, which provided:

- Continuous web application scanning to detect vulnerabilities in real-time.
- Comprehensive reporting that allows the technical team to prioritize and remediate issues effectively.
- Integration capabilities, ensuring the solution dovetailed with existing security infrastructure.

Project Experience No. (1, 2, 3, etc.):	SIN(s) to which this project applies:	Specific services being proposed under the SIN(s):
2	54151HACS	IT Cybersecurity Services, Application Security Testing, Penetration Testing, Risk/Vulnerability Assessment, High Value Asset Assessment, Cyber Hunt

This project was completed within the last two years OR ☒ Note: Projects that were completed more than two years prior to the date of the offer submission will not be accepted by the Government.	This project is an ongoing contract with a base year and option years, or is a multi-year task order. At a minimum, the base year or first year has been completed. ☐ Note: Projects that are in their base or first year and that year is incomplete as of the date of the offer submission will not be accepted by the Government.
Customer/Client Name:	AmeriSourceBergen Corporation
Project Name/Contract Number:	Web, Mobile and Network Security Assessment with ESOF AppSec/VMP
Customer Point of Contact (POC) for Project:	Robert Taylor
POC's Current Phone Number and Email:	robert.taylor@amerisourcebergen.com +1 (803) 415-2679
Project Performance Period (include months/years):	STATE DATE: March 2020 END DATE: March 2022
Dollar Value of the Entire Project:	$216,000
Dollar Value Received for the Work Performance Relevant to the SIN(s) Offered:	$216,000
Brief Summary of Project:	Offered a comprehensive suite of cybersecurity services to AmeriSourceBergen ensuring their digital assets remained secure.

Detailed Description of SIN Relevant Work performed and results

AmeriSourceBergen Corporation, a Fortune 10 Company, is globally renowned for its pharmaceutical sourcing and distribution services. As a pivotal player in the healthcare supply chain, the security and seamless integration of its tech infrastructure were paramount. TAC Security was enlisted by AmeriSourceBergen to find a vulnerability management platform capable of integrating effortlessly with existing tools and real-time insights and responses to potential threats. TAC Security deployed its ESOF AppSec and VMP service and software suites and was able to secure and enhance AmeriSourceBergen's cybersecurity footprint.

Methodology, tools, and/or processes utilized in performing the work

AmeriSourceBergen turned to TAC Security's ESOF VMP. ESOF VMP offered:

- An API-driven framework, ensuring smooth integration with AmeriSourceBergen's existing security tools.
- Real-time vulnerability detection and reporting, allowing for immediate action on potential threats.

TAC Security

Project Experience No. (1, 2, 3, etc.):	SIN(s) to which this project applies:	Specific services being proposed under the SIN(s):
1	54151HACS	IT Cybersecurity Services, Penetration Testing, Risk/Vulnerability Assessment, High Value Asset Assessment, and Cyber Hunt

This project was completed within the last two years OR ☒ **Note: Projects that were completed more than two years prior to the date of the offer submission will not be accepted by the Government.**	**This project is an ongoing contract with a base year and option years, or is a multi-year task order. At a minimum, the base year or first year has been completed.** ☐ **Note: Projects that are in their base or first year and that year is incomplete as of the date of the offer submission will not be accepted by the Government.**
Customer/Client Name:	Quality Unit, LLC.
Project Name/Contract Number:	IT Cybersecurity Services
Customer Point of Contact (POC) for Project:	Jan Perdoch
POC's Current Phone Number and Email:	P. 1-888-257-8754 E. support@liveagent.com
Project Performance Period (include months/years):	STATE DATE: 10/8/2021 END DATE: 3/4/2022
Dollar Value of the Entire Project:	$22,500
Dollar Value Received for the Work Performance Relevant to the SIN(s) Offered:	$22,500
Brief Summary of Project:	Offered a comprehensive suite of cybersecurity services to Quality Unit, LLC (Live Agent) ensuring their digital assets remained secure.

Detailed Description of SIN Relevant Work performed and results

TAC Security provided critical IT Cybersecurity Services to Quality Unit, LLC (Live Agent) with cybersecurity services falling under SIN 54151S and all GSA identified subcategories of this SIN. The scope of services encompassed security automation, compliance, threat detection, vulnerability management, and Information security reports management.

Methodology, tools, and/or processes utilized in performing the work

TAC Security employed several tools and methodologies tailored to meet Quality Unit's cybersecurity needs. Key software from the TAC Software security suite was implemented to detect and address potential threats, and to furnish Quality Unit, LLC (Live Agent) with thorough security reports. Quality Unit was provided with Tac Security's AppSec and VMP software and service suites.

Case Studies of Top Clients

Case Study 1: Google

Challenge: With a vast array of web applications of the Partners and Developers, Google required a solution that would ensure all its Developers and Partners' platforms were free from vulnerabilities that could be exploited.

Solution: ESOF AppSec was chosen for its comprehensive web application scanning capabilities for Google 0Auth and Google CASA (Cloud Application Security Assessment) Program

Outcome: Google saw a 30% improvement in the early detection of potential vulnerabilities in the development phase, leading to cost savings for their partners and developers and more secure applications at launch for more than 100+ Partners Globally.

Case Study 2: AmerisourceBergen Corporation's Security Assessment & Penetration

Background: AmerisourceBergen Corporation, a global powerhouse in the pharmaceutical sourcing and distribution services field, consistently ranks among Fortune 10 Companies. Integral to the healthcare supply chain, AmerisourceBergen ensures timely and accurate medicine distribution. As digital operations expanded, the protection and security of web platforms became paramount.

Objective: The primary goal was to integrate a robust web scanning solution, guaranteeing the security of AmerisourceBergen's web platforms. This solution needed to ensure user data protection and strict adherence to pharmaceutical regulations worldwide.

Solution: After careful consideration, AmerisourceBergen chose TAC Security's ESOF AppSec due to its innovative features:

Continuous Web Application Scanning: Using ESOF AppSec, automated scanners consistently monitored AmerisourceBergen's platforms, recognizing vulnerabilities in real-time.

Detailed Analysis: Once a vulnerability was identified, the platform provided an in-depth breakdown, assisting the IT team in setting remediation priorities.

User-Friendly Dashboards: AmerisourceBergen teams accessed and managed security data through customizable dashboards tailored to their needs.

Outcome:
Following the integration of ESOF AppSec, AmerisourceBergen noted a substantial decrease in potential security threats on its web platforms. This rigorous approach to security bolstered AmerisourceBergen's esteemed reputation for data integrity, assuring users that their personal and medicinal data remained in safe hands.

Case Study 3: Office of Attorney General of New Mexico's Implementation of ESOF VACA (formerly ESOF VMDR)

Background: The Office of the Attorney General of New Mexico plays a pivotal role in upholding the rule of law, representing the state in legal proceedings, and ensuring the rights of its residents. As the digital landscape expanded, so did the need for robust cybersecurity measures to safeguard sensitive information and digital assets.

Objective: To deploy a comprehensive vulnerability assessment and infrastructure scanning solution that would ensure data integrity, confidentiality, and availability for the state's highest legal office.

Solution: After a thorough evaluation of available solutions, the Office of the Attorney General decided to onboard TAC Security's ESOF VACA, and here's why:

Infrastructure Scanning: ESOF VACA's capabilities offer an in-depth examination of the entire digital infrastructure, identifying potential vulnerabilities and weak points.

Real-time Detection: With ESOF VACA, vulnerabilities are identified in real-time, giving the IT team an edge in ensuring swift countermeasures.

Risk Prioritization: Detected vulnerabilities are categorized based on their severity, allowing for a structured and efficient response mechanism.

Comprehensive Reporting: Detailed reports are generated, shedding light on identified vulnerabilities, their potential impact, and strategies for remediation.

Outcome:
With the deployment of ESOF VACA, the Office of the Attorney General of New Mexico fortified its digital defenses. The platform's proactive measures allowed for immediate

detection and rectification of vulnerabilities, strengthening public trust and ensuring uninterrupted service to the state's residents.

Case Study 4 : HiCounselor and ESOF AppSec Integration (Penetration Testing)

Background: HiCounselor, a leading career accelerator, seamlessly combines technology with professional mentorship to empower job seekers in landing tech roles swiftly. As an organization heavily reliant on its web platforms to deliver services, they needed a robust tool to safeguard their digital assets.

Objective: Implement a continuous web scanning solution that ensures the integrity and security of HiCounselor's web platforms, keeping both mentor and mentee data safe.

Solution: HiCounselor chose TAC Security's ESOF AppSec, which provided:

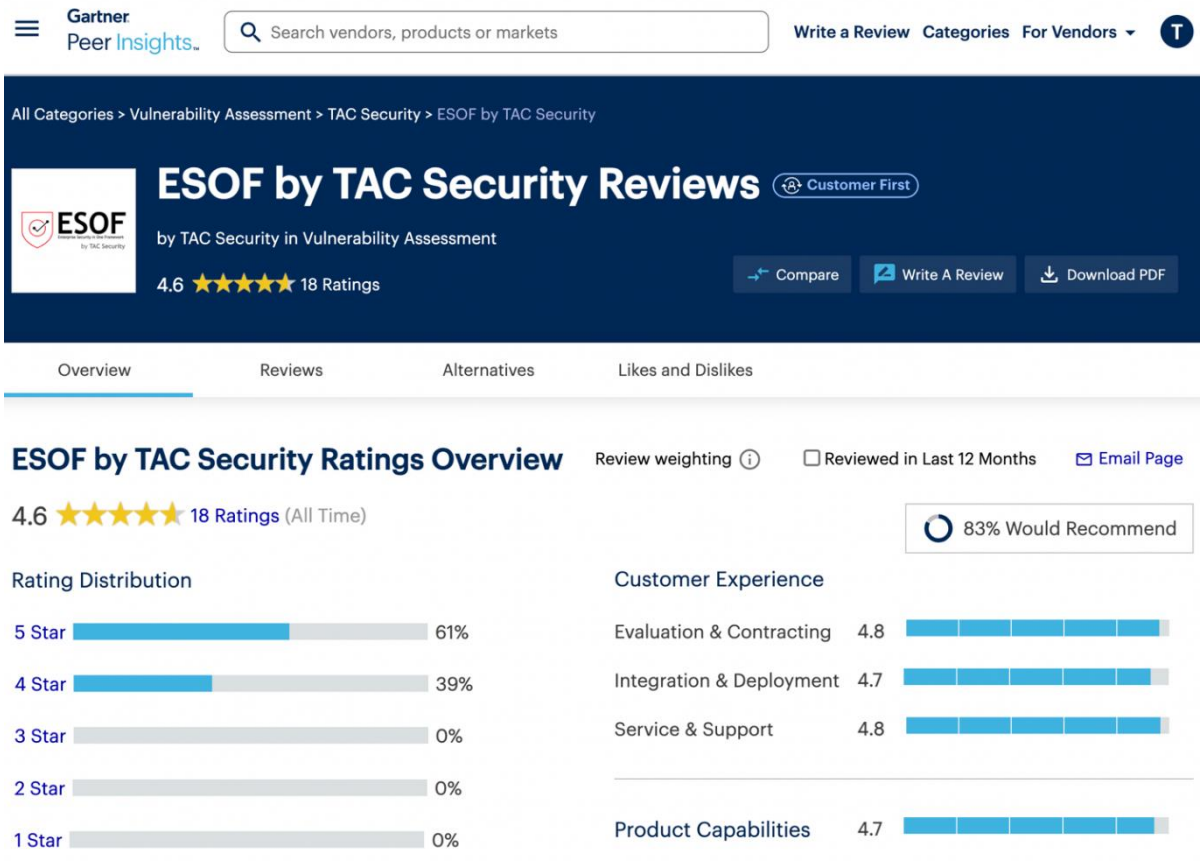
Continuous web application scanning to detect vulnerabilities in real-time.
Comprehensive reporting that allows the technical team to prioritize and remediate issues effectively.
Integration capabilities, ensuring the solution dovetailed with existing security infrastructure.

Outcome: With ESOF AppSec, HiCounselor bolstered its web platform's security, enhancing trust among its user base and fortifying its reputation as a secure career accelerator in the tech industry.

Gartner Reviews

ESOF by TAC Security is Customer First Choice Product in VM/VA Category on Gartner Peer Insights

Source Gartner Peer Insights: https://www.gartner.com/reviews/market/vulnerability-assessment/vendor/tac-security/product/esof-by-tac-security/reviews?marketSeoName=vulnerability-assessment&vendorSeoName=tac-security&productSeoName=esof-by-tac-security&sort=-helpfulness&pageNum=2


Gartner Peer Insights
Search vendors, products or markets
Write a Review
Categories
For Vendors
All Categories > Vulnerability Assessment > TAC Security > ESOF by TAC Security
ESOF by TAC Security Reviews
Customer First
by TAC Security in Vulnerability Assessment
4.6 18 Ratings
Compare
Write A Review
Download PDF
Overview
Reviews
Alternatives
Likes and Dislikes
ESOF by TAC Security Ratings Overview
Review weighting
Reviewed in Last 12 Months
Email Page
4.6 18 Ratings (All Time)
83% Would Recommend
Rating Distribution
5 Star 61%
4 Star 39%
3 Star 0%
2 Star 0%
1 Star 0%
Customer Experience
Evaluation & Contracting 4.8
Integration & Deployment 4.7
Service & Support 4.8
Product Capabilities 4.7

5.0 ★★★★★ Mar 16, 2023

Review Source: ⓘ

Opportunity to use this tool has been a game-changer for the task we need to accomplish

Reviewer Function: IT Security and Risk Management

Company Size: 250M - 500M USD

Industry: Finance (non-banking) Industry

Overall experience with this tool has been excellent

4.0 ★★★★☆ May 10, 2021

Review Source: ⓘ

Best solution for Automated Security Vulnerability Reporting and Management

Reviewer Function: IT Security and Risk Management

Company Size: 500M - 1B USD

Industry: Finance (non-banking) Industry

The ESOF platform made our job so easy to manage entire Vulnerability Management process with so much of ease and automation. The remarkable thing is there is very less human intervention of Information Security personel to manage the entire process.

Read Full Review

5.0 ★★★★★ Mar 27, 2021

Review Source: ⓘ

The best quantitative analytic tool for cyber security maturity

Reviewer Function: General Management

Company Size: 10B - 30B USD

Industry: Banking Industry

Quantifying the state of cybersecurity is the biggest challenge irrespective of state-of-the-art tools, technology, and people. ESOF designed by TAC has given incredible visibility about cybersecurity maturity level in their respective environment to the cybersecurity professionals. ...

Read Full Review

4.0 ★★★★☆ Mar 21, 2023

Review Source: ⓘ

A great company for your security reviews.

Reviewer Function: Engineering - Other

Company Size: <50M USD

Industry: Software Industry

Overall it has been a positive experience. They have shown us how to improve the application, with detailed reports. Also, the communication has been good in both directions, with quick answers and meetings.

Read Full Review

5.0 ★★★★★ Apr 25, 2023

Review Source: ⓘ

Tac security and their ESOF solution is a great choice, and they got superb support.

Reviewer Function: Engineering - Other

Company Size: <50M USD

Industry: Software Industry

The communication with Tac security was very easy, being able to move fast was very important to us, pricing is fair, and the overall experience and communication was very good.

Read Full Review

5.0 ★★★★★ Mar 30, 2023

Review Source: ⓘ

Great penetration testing capabilities and outstanding service support.

Reviewer Function: IT Security and Risk Management

Company Size: 50M - 250M USD

Industry: Healthcare and Biotech Industry

We use the service for vulnerability assessment and penetration testing, the in-depth analysis of vulnerabilities along with screenshots is really helpful. The dashboard is insightful with just the required amount of visualizations.

Read Full Review

5.0 ★★★★★ May 9, 2023

Review Source: ⓘ

Excellent security firm

Reviewer Function: IT

Company Size: <50M USD

Industry: IT Services Industry

From the very beginning of our security audit to the final results, TAC Security team has been very proactive. They provided guidances and made sure we were able to get our security certification in time.

Read Full Review

Certifications

Staff Qualifications certifications:

SR. NO.	NAME OF EMPLOYEE	QUALIFICATION
1	Vishal	Graduation (CEH)
2	Nakul	Graduation (CEH), (ISO 27001)
3	Nittin	Graduation (CEH)
4	Vamshi	Graduation (CEH)
5	Tarun	Graduation (CEH)
6	Rupali	Post Graduation (CEH)
7	Rajeev	Graduation (PCI ASV), (CEH)
8	Saransh	Lead, AppSec at TAC Security (CEH) and PCI ASV
9	Keshav	Graduation (CISSP)
10	Anuj	Graduation (CEH)
11	Anusha	Graduation (CEH)
12	Rahul	AWS Certified (CEH)
13	Syed	CREST Certified (CEH)
14	Akash	ISO 27001 LA
15	Ayush	Graduation (CEH) (CAP) (LPT)
16	Rakesh	Graduation (CEH)(ECSA)(MCP)
17	Jeetendra	Graduation (CEH) (OSCP)
18	Akanksha	Graduation (CEH)
19	Ankit	OSCP
20	Uttam	ISO 27001 LA
21	Yogita	CNSP
22	Sheel Bhatt	CEH
23	Piyush Patil	CEH
24	Chetan Bharambe	CEH

Certificates:

Certificate of Qualification

This is to certify that

Syed Sheeraz Ali

CREST ID

[redacted]

Was awarded the qualification of

CREST Registered Penetration Tester

On

19 September 2022

Rowland Johnson, CREST President

Certificate is valid for three years from the examination date
Authenticate this Certificate at: www.crest-approved.org/verify-a-certificate

This Certificate remains the property of CREST (International) Ltd
Registered Office: CREST (International) Ltd, Seven Stars House, 1 Wheler Road, Coventry, West Midlands, CV3 4LB, United Kingdom.
Company number: 09805375

Certificate of Qualification

This is to certify that

Syed Sheeraz Ali

CREST ID

[redacted]

Was awarded the qualification of

CREST Practitioner Security Analyst

On

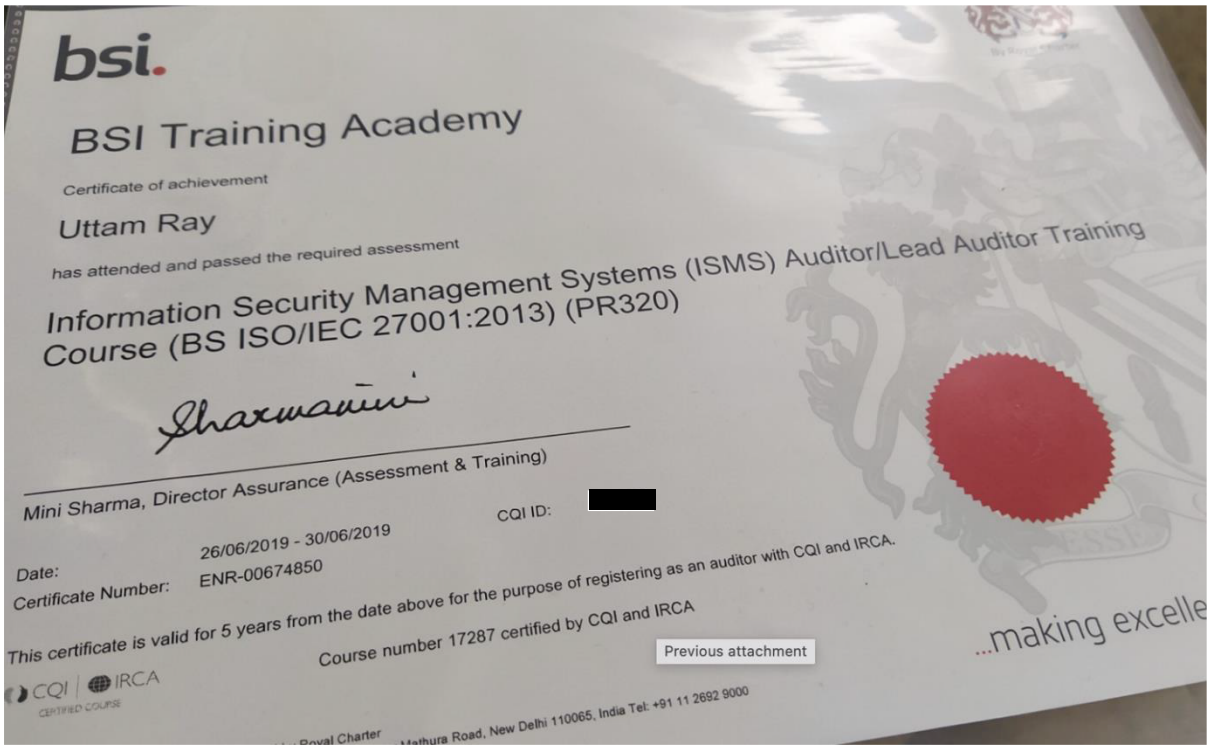
19 September 2022

Rowland Johnson, CREST President

Certificate is valid for three years from the examination date

Authenticate this Certificate at: www.crest-approved.org/verify-a-certificate


Next attachment
C|EH
Certified Ethical Hacker
ETHICAL HACKER
PRACTICAL
THIS IS TO ACKNOWLEDGE THAT
RUPALI SHARMA
IS AWARDED THE "CERTIFIED ETHICAL HACKER (PRACTICAL)" CERTIFICATION
FOR COMPLETING THE RIGOROUS CHALLENGES GIVEN IN THE STIPULATED TIME.
ISSUE DATE: 07 August, 2023
EXPIRY DATE: 06 August, 2026
CERTIFICATION NUMBER
[redacted]
EC-Council
Sanjay Bavisi, President



bsi.

BSI Training Academy

Certificate of achievement

Uttam Ray

has attended and passed the required assessment

Information Security Management Systems (ISMS) Auditor/Lead Auditor Training Course (BS ISO/IEC 27001:2013) (PR320)

Mini Sharma, Director Assurance (Assessment & Training)

CQI ID: [redacted]

Date: 26/06/2019 - 30/06/2019

Certificate Number: ENR-00674850

This certificate is valid for 5 years from the date above for the purpose of registering as an auditor with CQI and IRCA.

Course number 17287 certified by CQI and IRCA

Previous attachment

...making excelle

CQI | IRCA CERTIFIED COURSE

Royal Charter

Mathura Road, New Delhi 110065, India Tel: +91 11 2692 9000

OffSec

This is to acknowledge that

Ankit Sisodiya

is certified as an

OSCP

(OffSec Certified Professional)

and successfully completed all requirements and criteria for said certification through examination administered by OffSec.

This certification was earned on

August 6, 2023

[redacted]

OffSec OSCP

1/1


EC-Council
Certification Number
C|EH
Certified Ethical Hacker
Certified Ethical Hacker
This is to acknowledge that
Rajeev Singh
has successfully completed all requirements and criteria for
Certified Ethical Hacker
certification through examination administered by EC-Council
Issue Date: 28 September, 2021
Expiry Date: 27 September, 2024
ANSI ACCREDITED
#0732
ISO/IEC 17024
Personnel Certification Program
Sanjay Bavisi, President


EC-Council
Certification Number
C|EH
Certified Ethical Hacker
Certified Ethical Hacker
This is to acknowledge that
Akanksha Dogra
has successfully completed all requirements and criteria for
Certified Ethical Hacker
certification through examination administered by EC-Council
Issue Date: 18 July, 2023
Expiry Date: 17 July, 2026
ANSI ACCREDITED
#0732
ISO/IEC 17024
Personnel Certification Program
Sanjay Bavisi, President

International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Keshav Kumar

the credential of

Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Jill Slay - Chairperson

Laurie-Anne Bourdain - Secretary

CISSP

ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 17024 PERSONNEL CERTIFICATION BODY

[redacted]
Certification Number

Apr 1, 2022 - Mar 31, 2025
Certification Cycle

Certified Since: 2022

(ISC)²

Verify Member is in good standing at:www.isc2.org/verify

Printed On: 6/22/2023

EC-Council

Certification Number

C|EH Certified Ethical Hacker

Certified Ethical Hacker

This is to acknowledge that

Vishal Patil

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: 18 December, 2021

Expiry Date: 17 December, 2024

ANSI ACCREDITED #0732 ISO/IEC 17024 Personnel Certification Program

Sanjay Bavisi, President


EC-Council
Certification Number
[redacted]
C|EH Certified Ethical Hacker
Certified Ethical Hacker
This is to acknowledge that
Rajeev Singh
has successfully completed all requirements and criteria for
Certified Ethical Hacker
certification through examination administered by EC-Council
Issue Date: 28 September, 2021
Expiry Date: 27 September, 2024
ANSI ACCREDITED
#0732
ISO/IEC 17024
Personnel Certification Program
Sanjay Bavisi, President


PCI Security Standards Council, LLC
acknowledges that
Rajeev Singh
TAC Security Inc.
has successfully fulfilled the requirements for
Approved Scanning Vendor (ASV) Employee
as defined in the Payment Card Industry (PCI) Data Security Standard Qualification Requirements for Approved Scanning Vendors (ASV).
Certificate Number: [redacted]
Expiration Date: 28 June 2024
PCI Security Standards Council
Lance J. Johnson,
Executive Director, PCI SSC

GAQM
Global Association for Quality Management

Certificate Of Excellence

This is to Certify that

Akash

Has passed the exam successfully as per the requirements prescribed by the GAQM for the Title of **ISO 27001:2013 ISMS - Certified Lead Auditor**
The exam was delivered via ProctorU

Mark Shultz
CEO

Certificate Number: [redacted]
Certification Date: 18 September 2020

Global Association for Quality Management (GAQM)®

The Title mentioned is a trademark of GAQM

PCI Security Standards Council, LLC

acknowledges that

Saransh Rawat

TAC Security Inc.

has successfully fulfilled the requirements for

Approved Scanning Vendor (ASV) Employee

as defined in the Payment Card Industry (PCI) Data Security Standard Qualification Requirements for Approved Scanning Vendors (ASV).

Certificate Number: [redacted]

Expiration Date: 27 April 2023

PCI Security Standards Council®

Lance J. Johnson,
Executive Director, PCI SSC

Certification Number [redacted]

C|EH Certified Ethical Hacker

This is to acknowledge that

Saransh Rawat

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: 28 January, 2020

Expiry Date: 27 January, 2023

ANSI

EC-Council

Sanjay Bavisi, President

EC-Council

Certification Number [redacted]

C|EH Certified Ethical Hacker

This is to acknowledge that

Sheel Bhatt

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: 14 September, 2020

Expiry Date: 13 September, 2023

ANSI

Sanjay Bavisi, President


CERTIFICATE
OF ACHIEVEMENT
The SecOps Group
CONGRATULATIONS
Yogita P
FOR SUCESSFULLY PASSING THE EXAM
CERTIFIED NETWORK SECURITY PRACTITIONER (CNSP)
DATE: 23-MAR-2023
CERTIFICATE ID: [redacted]
EXAM VERSION: 1.01
EXAMINER
S. Siddharth
CERTIFIED NETWORK SECURITY PRACTITIONER
THE SECOPS GROUP


EC-Council
Certification Number
[redacted]
C|EH
Certified Ethical Hacker
Certified Ethical Hacker
This is to acknowledge that
piyush patil
has successfully completed all requirements and criteria for
Certified Ethical Hacker
certification through examination administered by EC-Council
Issue Date: 16 July, 2022
Expiry Date: 15 July, 2025
ANSI ACCREDITED
#0732
ISO/IEC 17024
Personnel Certification Program
Sanjay Bavisi, President

Compliance

TAC Security agree 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.

Background Checks

TAC Security will provide the upon request names, addresses, and fingerprint information for a law enforcement background check for any Vendor staff working on the Lottery project team.

Certificate of Insurance

Here, we attached sample Insurance copy.

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
05/0/2023

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. Renewal

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
INSURED TAC Security Inc TAC Security 1390 Market Street 200 San Francisco, CA 94102	INSURER(S) AFFORDING COVERAGE / NAIC # INSURER A : Berkshire Hathaway Direct Insurance Company 10391 INSURER B : INSURER C : INSURER D : INSURER E : INSURER F :

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

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

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY CLAIMS-MADE X OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: POLICY PRO-JECT LOC X OTHER:	X		N9BP466512	02/17/2023	02/17/2024	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$ 2,000,000 $ 50,000 $ 5,000 $ Included $ 4,000,000 $ 4,000,000
	AUTOMOBILE LIABILITY Renewal ANY AUTO OWNED AUTOS ONLY HIRED AUTOS ONLY SCHEDULED AUTOS 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 ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N 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)
PCI Security Standards Council, LLC are listed as additional insured as it pertains to general liability (see endorsement attached)

CERTIFICATE HOLDER	CANCELLATION
PCI Security Standards Council, LLC 401 Edgewater Place Suite 600 Wakefield, MA USA 01880	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

ACORD 25 (2016/03) The ACORD name and logo are registered marks of ACORD

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	$ 1800.00 -	$ 14,400.00 -
2	4.2	Website Penetration Testing	8	$ 1800.00 -	$ 14,400.00 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 1800.00 -	$ 14,400.00 -
4	4.4	Wireless Penetration Testing	8	$ 1800.00 -	$ 14,400.00 -
				TOTAL BID AMOUNT	$ 57,600.00 -

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:	TAC Security Inc.
Vendor Address:	1390, Market St #200, San Francisco, CA 94102
Email Address:	sales@tacsecurity.com
Phone Number:	415 800 3581
Fax Number:	NA
Signature and Date:	3/28/2024

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

State of West Virginia
Centralized Request for Quote
Service - Prof

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

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name :

Address :

Street :

City :

State : **Country :** **Zip :**

Principal Contact :

Vendor Contact Phone: **Extension:**

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

Reason for Modification:
Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration and bid submittal compliance

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 PO BOX 2067 CHARLESTON US	WV	LOTTERY 900 PENNSYLVANIA AVE CHARLESTON US	WV

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

Comm Code	Manufacturer	Specification	Model #
81111801			

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

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

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

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

SOLICITATION NUMBER: CRFQ LOT2400000009
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[✓] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[✓] Other

Description of Modification to Solicitation:

Addendum No. 1 is issued for the following:

1) To attach vendor questions and Agency responses.

2) To attach "Doing Business - Vendor Registration and Bid-Submittal Compliance" instruction sheet.

--No Other Changes--

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

CRFQ LOT2400000009

Addendum No. – 1

Vendor Questions & Agency Response

1. We have a question in regard to Section 3 Qualifications; 3.1 that requires vendors to have been in business for at least fifteen (15) years. Just to be sure, is this a requirement for the vendor (i.e., business), or for the vendor staff?

   A1) No, this only applies to the organization. See section 3.3 and 3.4 for vendor staff requriements.

2. Would the West Virginia Lottery consider accepting vendor submissions (or allow a waiver) who may fall short of the 15-year requirement, but can show evidence of their organization's Network Penetration Testing and Cybersecurity Assessments competence through other means rather than tenured years of service, such as accreditation through organizations such as ISO/IEC?

   A2) No, the 15 year requirement is mandatory.

3. **Opinion:** The competitive nature of this RFQ, requirement 4.3.1., inadvertently places highly qualified remote teams at a disadvantage. **Question:** Would the Lottery consider waiving this requirement to level the playing field for all qualified bidders?

   A3) Clarification: 4.3.1 of the specifications states "Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. Assessing locations remotely or from one central location is prohibited"; **Answer: No, Vendor qualifications for this solicitation are defined in section 3. QUALIFICATIONS, specifically section 3.1.**

4. Could the Lottery agree to exclude the costs associated with visas, travel, and lodging in the eight WV locations from the financial evaluation process?

   A4) No, vendors must submit a fixed price cost for each service on the pricing page. Separate fees are prohibited.

5. Understanding this will help us tailor the proposals to better meet the needs, do you have preferences or restrictions on the geographical location of the consultants?

   A5) External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.

6. Is Data Residency in Canada acceptable?

   A6) No, all information obtained during assessments must be stored in the continental United States. E.g. IP addresses, usernames, passwords, vulnerabilities, proof of exploitability, etc. Please note, assessments are prohibited from performing data exfiltration.

CRFQ LOT2400000009
Addendum No. – 1
Vendor Questions & Agency Response

7. Does the lottery want separate (4) Executive Summary Reports, (4) Technical Reports delivered and findings presentations after each test (External, Internal, Wi-Fi, and Website and Web Applications)?

   A7) Correct, each type of report and findings presentation is required and separate for each type and instance of an assessment. Reports and presentations cannot be combined across assessments.

8. Is it acceptable to provide (1) Executive and (1) Technical Report and (1) findings presentation upon conclusion of the testing?

   A8) No, each type of report and findings presentation is required and separate for each type and instance of an assessment. Reports and presentations cannot be combined across assessments.

9. For the Website: how many static and dynamic pages are hosted on it? And how many user roles?

   A9) Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, and discovery phases of the service. See section 4.2.3. No roles or authenticated testing will be performed. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.

10. For the Cisco network devices & other servers in scope: Are they wanting any build reviews, or configuration reviews performed against these?

    A10) Yes, configuration reviews.

11. For the Active Directory Domain: Is this part of one of the internal IP address blocks, or is it a separate network? If it is a separate network, roughly how many IPs are in this, or how many active directory users are there?

    A11) Additional information on the AD server will be provided to the successful vendor. There are approximately 200 active directory users.

12. Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?

    A12) No incumbent vendor, no past contract for Lottery; Yes, if there were an incumbent vendor they would be eligible to bid unless otherwise debarred.

CRFQ LOT2400000009
Addendum No. – 1
Vendor Questions & Agency Response

13. Specify the VLAN details how many are included in the Scope?

A13) 62 total VLANS across all Lottery sites.

14. How much (%) of the infrastructure is in the cloud?

A14) 0%

15. In the IT department/environment, how many employees work?

A15) This information is not for bidding purposes, neither the Purchasing Division nor the Lottery can disclose this information to the bidders at any time prior to the conclusion of the procurement process.

16. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

A16) All data centers are owned and operate by the WV Lottery.

17. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?

A17) This information is not for bidding purposes, neither the Purchasing Division nor the Lottery can disclose this information to the bidders at any time prior to the conclusion of the procurement process.

18. External: Estimated number of IPs/Services per assessment?

A18) 15 external IP addresses (approximate) please see the Existing Technology Environment section.

19. Internal: Estimated number of IPs/Services per assessment?

A19) 500 internal IP addresses (approximate) please see the Existing Technology Environment section.

20. Website: Estimated number of websites per assessment?

A20) One (1), Please see the Existing Technology Environment section.

21. Wireless: Estimated number of access points and IPs per assessment?

A21) Currently 11, with a future total estimate 32 in the next 12 months. IP addresses served on the wireless access points must be authoritatively determined in the reconnaissance, mapping, and discovery phases of the service.

CRFQ LOT2400000009
Addendum No. – 1
Vendor Questions & Agency Response

22. Which Contract Vehicle, if any, would this be procured through?

A22) Open-End Centralized Master-Agreement (CMA) with delivery orders (release orders) against the master agreement authorizing services to be delivered, and will be processed as an Agency Delivery Order (ADO).

23. Would there be any requirements at all for having a resource on-site through any of the Pen Testing?

A23) Yes, External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.

24. How many dynamic pages are hosted on your website?

A24) Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, discovery phases of the service. See section 4.2.3.

25. Would you like authenticated testing against your website? If so, how many unique user roles are to be tested?

A25) Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, discovery phases of the service. See section 4.2.3. No roles or authenticated testing will be performed. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.

26. Will you require after-hours testing?

A26) See sections 4.1.2, 4.2.2, 4.3.2, and 4.2.2 which state: Hours of operations, testing schedule, and exclusions will be determined in conjunction with the successful vendor.

27. For the web application assessment, would you provide URL or login credentials if behind login portal to understand scope?

A27) www.wvlottery.com Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, discovery phases of the service. See section 4.2.3. No roles or authenticated testing will be performed. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.

CRFQ LOT2400000009
Addendum No. – 1
Vendor Questions & Agency Response

28. How in-depth would you like the web application testing (i.e., basic or in-depth)?

A28) In depth.

29. Would the work be conducted remotely or on site?

A29) External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.

30. On page 40 of "CRFQ LOT24-09 Solicitation Documents.pdf", it lists 8 separate external pen-tests, internal pen-tests, website penetration tests, and wireless penetration tests. Are these per location or can some tests be shared across locations?

A30) Clarification: The Background Information section states the Lottery expects to consume at least one of each service annually. The pricing page lists two (2) of each type of four (4) assessments to allow the vendor to identify the fixed price cost per assessment based on potential total consumption. This number is separate and independent from the number of locations to be tested. **Answer:** Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations and are considered one assessment per consumption. **i.e.** One Wireless penetration assessment will test the wireless infrastructure at all eight (8) Lottery locations.

31. If we must test on-site from each Lottery location, are there 8 locations that must be visited?

A31) Yes, see the Existing Technology Environment section for locations and addresses.

32. How far apart are the 8 locations from which testing must be conducted?

A32) Travel time can be calculated from Lottery Main Office see addresses in Existing Technology Environment.

Approximate times from Lottery Main Office: Mardi-Gras – 15 minutes; Bridgeport – 2 hours; Weirton – 4 hours; Greenbrier – 2 hours; Hollywood – 6 hours; Mountaineer 4 hours; Wheeling – 4 hours.

33. If you select one internal network penetration test annually, will it include one site or all 8?

A33) All eight (8) for each Internal/Client Side Network Penetration assessment.

CRFQ LOT2400000009
Addendum No. – 1
Vendor Questions & Agency Response

34. Are wireless tests to be conducted for all 8 locations each year? If not, for how many annually?

A34) Yes, all eight locations must be tested for each Wireless Penetration assessment.

35. Are we to include the CRFQ form (pages 1-3) in our proposal?

A35) Yes, if not submitting electronically through wvOASIS fill out pages 1-3 accordingly.

36. Are we to include the entire CRFQ in our response?

A36) All qualified vendors SHOULD provide all requested information stated in section 3. QUALIFICATIONS with their bid, and MUST provide all information requested in section 4. MANDATORY REQUIREMENTS.

37. Are we to submit a signed NDA (Exhibit B) with our response or is it to be submitted post-award?

A37) You may submit with bid, however section 3.7 states "Prior to Award both parties, the Vendor and Lottery must sign".

38. The pricing form requests pricing for 8 instances of each assessment. Is that for each of the 8 locations, or is it because Lottery intends to repeat each assessment, say, up to two times a year, over the course of a multi-year contract?

A38) Correct, the pricing page uses an estimated consumption of two (2) assessments of each of the four (4) types per year.

39. Is Lottery looking for detailed configuration reviews of any of the following: Firewalls, Routers/switches, VPN appliances, Windows workstations, and Windows servers?

A39) Yes

40. Is this a portal or hard copy submission? RFP section 6 states both. If this is a hard copy submission, should vendors submit 1 technical proposal and 1 cost proposal?

A40) Yes, you may submit through wvOASIS VSS Portal at https://prd311.wvoasis.gov/PRDVSS1X1ERP/Advantage4 sign-in or sign-up and create an account; or hand delivery, as well as USPS, UPS or FEDX; you may also FAX your bid. Vendors should submit technical and cost proposals as one bid submission. Please read the RFQ thoroughly.

CRFQ LOT2400000009
Addendum No. – 1
Vendor Questions & Agency Response

41. Please specify the process for ensuring confidentiality of certain information within the proposal. Sections that contain methodologies and/or reporting pages could harm our business if they were to be disclosed to the public. Similarly, client names that are disclosed to the public could violate privacy agreements with said clients.

A41) Please see specification section 3.7 Non-Disclosure (NDA) and Exhibit – B; also see Section 21 YOUR SUBMISSION IS A PUBLIC DOCUMENT in the INSTRUCTIONS TO VENDORS SUBMITTING BIDS (page-9).

(A41-continued) ***Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.***

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

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

42. Will authenticated testing be required? Will credentials be required or is the app self-register?

A42) No, roles and authenticated testing will not be tested. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.

43. What is the app?

A43) There is no app, only a website.

44. What does the app do?

A44) There is no app, only a website.

45. What type of data does the app handle?

A45) There is no app, only a website.

46. Page 31, section 4.2.4 -- RFP says any environment can be tested. Will there be a client preference?

A46) The Lottery will designate which environment will be tested for each assessment.

CRFQ LOT2400000009

Addendum No. – 1

Vendor Questions & Agency Response

47. Page 31, section 4.2.4 -- RFP says each environment will be assessed separately. Will all need to be tested?

A47) This will be determined at the discretion of the Lottery.

48. Page 33, section 4.2.8 -- RFP says DoS attacks will be required as a part of testing. SCA wants to confirm they WANT an actual DoS attack to test their defenses?

A48) Correct. Per section 4.2.8 Denial of Service Attacks are required to be included in the pricing for Website Penetration testing. The use of DoS attacks is at the discretion of the Lottery, and requires Lottery approval.

49. Does the State Lottery anticipate that key infrastructure components will be both similar and accessible at each site? For example, each site connects to the same Domain Controller, uses primary similar file shares, etc.

A49) For security purposes, this information will be provided to the successful vendor.

50. The RFP explicitly forbids "Assessing locations remotely or from one central location". Can onsite personnel be augmented by a remote workforce to lower travel costs? For example, the onsite tester will facilitate a connection for a remote employee to conduct scans, thereby freeing the onsite tester to begin wireless assessments.

A50) No

51. Would the State Lottery accept all work to be done remotely?

A51) No, External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.

52. The RFP states, "The Lottery expects to consume at least one of each service annually." Clarification on this phase would be appreciated. Is it fair to assume that all onsite testing will be executed in a logistically feasible consecutively schedule (e.g. back-to-back test events)? This question is intended to predict travel costs to/from onsite testing locations.

A52) No, different assessments are not required to be scheduled concurrently or adjacently. Pricing should reflect independent assessments.

53. Per the Exhibit-A Pricing Page, could you please describe or expand upon the need for 8 individual assessments?

A53) The Background Information section states the Lottery expects to consume at least one of each service annually. The pricing page lists two (2) of each type of four (4) assessments to allow the vendor to identify the fixed price cost per assessment based on potential total consumption.

CRFQ LOT2400000009
Addendum No. – 1
Vendor Questions & Agency Response

54. "The vendor must have been in business for at least fifteen (15) years, performing and delivering information technology cybersecurity assessments." Does this requirement apply to individuals performing the work, or to the corporate entity? Will the purchaser revise this qualification to require the corporate entity to have been in business for at least six (6) years, performing and delivering information technology cybersecurity assessments?

A54) Applies to the corporate entity; No, the 15 year requirement is mandatory.

55. Is it sufficient to include only one example executive summary report and one example technical report, or is the bid response required to include one example executive summary report and one example technical report for each service (External Network Penetration Testing, Website Penetration Testing, Internal/Client-Side Network Penetration Testing, and Wireless Penetration Testing) to be provided?

A55) One example per report.

56. Is it true that a single Assessment & Report for Internal/Client-Side Network Penetration Testing or Wireless Penetration Testing services requires onsite visits to all eight (8) Lottery locations, therefore the "Extended Amount" for each of these services should represent bidders' costs for 64 total onsite visits to Lottery locations?

A56) No, the pricing page identifies the consumption of two (2) of each type of assessment. In this scenario that would results in two (2) each of two (2) assessments involving eight (8) sites each for a total of 32 onsite visits. (2*2*8=32)

57. How many hosts would you like to have included for the External Penetration Test?

A57) 15 external IP addresses (approximate) please see the Existing Technology Environment section.

58. How many web applications are to be included in testing?

A58) There is no app, only a website.

59. What is the name of the web application(s)?

A59) There is no app, only a website.

60. How many user roles will be tested per application?

A60) No roles or authenticated testing will be performed. See section 2.11 which states: Testing during this type of assessment represents an uninformed, anonymous threat targeting the Lottery's external infrastructure.

CRFQ LOT2400000009
Addendum No. – 1
Vendor Questions & Agency Response

61. How many dynamic pages are there per application?

A61) Currently known estimates are 25 static and 25 dynamic pages, a total of 50 pages. This information must be authoritatively determined in the reconnaissance, mapping, discovery phases of the service. See section 4.2.3.

62. As an estimate, how many hosts are there on the internal network?

A62) 500 internal IP addresses (approximate) please see the Existing Technology Environment section.

63. How many subnets exist that need to be tested?

A63) 27 (approximate) please see the Existing Technology Environment section.

64. For the internal test, will you be able to provision a non-administrator account to test assumed breach scenario?

A64) Yes, see section 2.12 which states, Part one simulates an attack by an untrusted outsider or an unauthenticated user without working knowledge of the Lottery's network. Part two will be performed with the low-level credentials of an authenticated user.

65. How many wireless access points exist?

A65) Currently 11, with a future total estimate 32 in the next 12 months. IP addresses served on the wireless access points must be authoritatively determined in the reconnaissance, mapping, and discovery phases of the service.

66. Is there a guest network in addition to a corporate network?

A66) Yes

67. Are there multiple locations / buildings that have access points?

A67) Yes, see the Existing Technology Environment section for locations and addresses.

68. Are there any unique nuances to any of these assessments that you feel is important for the testers to know before hand?

A68) No

69. What are the expectations for the report?

A69) See sections 4.1.10 – 4.1.13; 4.2.10 – 4.2.13; 4.3.6 – 4.3.9, and 4.4.6 – 4.4.9. Please read the RFQ thoroughly.

CRFQ LOT2400000009
Addendum No. – 1
Vendor Questions & Agency Response

70. When are each of the assessments expected to be performed by and delivered?

A70) See sections 4.1.2, 4.2.2, 4.3.2, and 4.2.2 which state: Hours of operations, testing schedule, and exclusions will be determined in conjunction with the successful vendor.

71. Is there an expectation of these assessments to be conducted on-site? Or can they be conducted remotely?

A71) External network and Website penetration tests may be performed remotely. Wireless Penetration Testing and Internal/Client Side Network Penetration Testing must be performed onsite at all Lottery locations. See sections 4.1.1, 4.2.1, 4.3.1 and 4.4.1.

72. Is "off hours" testing acceptable?

A72) See sections 4.1.2, 4.2.2, 4.3.2, and 4.2.2 which state: Hours of operations, testing schedule, and exclusions will be determined in conjunction with the successful vendor.

73. How many total locations will be in scope for wireless testing?

A73) All eight (8) locations must be tested for each Wireless Penetration assessment.

74. Is the external website in scope for the overall external penetration test or to be considered as part of a separate Web Application Security Assessment?

A74) No, the external website is only in scope for the Website Penetration Testing assessment.

75. Please confirm that this bid response can be submitted via *wv*OASIS.

A75) Yes, you may submit through wvOASIS VSS Portal at https://prd311.wvoasis.gov/PRDVSS1X1ERP/Advantage4 sign-in or sign-up and create an account; or hand delivery, as well as USPS, UPS or FEDX; you may also FAX your bid. Vendors should submit technical and cost proposals as one bid submission. Please read the RFQ thoroughly.

76. Do we need to include the following filled out and/or signed pages with our bid response, or are these not needed at this time?

a. CRFQ Page 1 – Yes
b. CRFQ Page 23 – Yes
c. CRFQ Page 39 – Yes
d. CRFQ Exhibit B – **You may submit with bid, however section 3.7 states "Prior to Award both parties, the Vendor and Lottery must sign".**

CRFQ LOT2400000009

Addendum No. – 1

Vendor Questions & Agency Response

77. Is it acceptable to the Lottery to submit one sample executive summary report to represent all four categories (External Network Penetration Testing, Website Penetration Testing, Internal/Client-Side Network Penetration Testing, and Wireless Penetration Testing)?

A77) Yes, one example per report.

78. Is the Lottery seeking an overview of our methodology and approach to each of the four categories of penetration testing in our bid response?

A78) No, per section 3.5 which states 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. Vendors must provide information and evidence how they comply with the CIS methodology, OWASP Top 10 and NIST SP 800-115.

79. Will this be a single or multivendor award?

A79) Single award to one vendor.

80. If at time of execution of the contract our shared staff in the proposal response aren't available, can we replace them?

A80) Yes, must still follow the requirements in section 3. QUALIFICATIONS for vendor staff to be assigned to the project.

Doing Business - Vendor Registration and Bid-Submittal Compliance:

Solicitations out for bid can be viewed by going to www.wvoasis.gov, click on Vendor Self Service, If you are using Vendor Self Service for the first time, please click on the 'SIGN UP' button to create your user account. Once account is created and the site has loaded SEARCH providing the solicitation number (*Example:* CRFQ: LOT2200000001). To the right are the closing date and time, and the time remaining to submit a bid.

Find the solicitation and click on Details, there you will need to click on attachments to find the specifications, terms and conditions, etc.

In order to submit an electronic bid, Vendors must create your user account, when prompted to pay Vendor Registration Fee, you may select "pay later" to allow the submission of electronic bids.

However, the vendor of the winning bid must pay a $125 vendor registration fee either by completing the application in VSS user account and paying via credit card, or by calling 304-558-2311 with credit card information, or mailing a check to:

Vendor Registration Section
WV Purchasing Division
2019 Washington Street East, Charleston, WV 25305.

VENDOR REGISTRATION:
The following is optional, not required, when submitting bids. However, Vendors who have received Notice of Apparent Bid Award are required to meet the following:
To conduct business in this state, according to West Virginia Legislative Rule 148 CSR1.6.1.7 agencies must verify Vendor registration status with the West Virginia Purchasing Division, West Virginia Secretary of State's Office (WVSOS) and West Virginia Tax Department (WVTD).

All West Virginia Agencies are prohibited from issuing a purchase order to any vendor until Vendor compliance can be verified that it has been properly registered with:

1. The Purchasing Division.
As stated above, the fee is $125 annually and can be paid with a credit card when registering in VSS. Otherwise, you may complete a WV-1 form and submit with a check to: WV Purchasing Division. www.state.wv.us/admin/purchase/forms.html

2. The Secretary of State's Office.
Registration with the WV Secretary of State's Office is required for all Vendors doing business with the State of West Virginia and may incur a fee of $100.00 depending on the business registration category.
Business registration with the Secretary of State falls into one of Two (2) categories:

a. Domestic (formed in West Virginia), or
b. Foreign (formed out-of- state)

Vendors may complete an Application for Exemption from Certificate of Authority with the WVSOS if you feel your company qualifies. Please mail the completed form and include a check for $25.00, made payable to WVSOS, along with a copy of the company's home state issued Certificate of Good Standing / Certificate of Corporation.

NOTE: You may also contact the WV Secretary of State's Office with your questions @ 304-558-8000

3. The WV Tax Department.
All entities doing business in the State of West Virginia must be registered with WVTAX and pay a one-time fee of $30.00.
An exemption with WV Secretary of State does not mean you are exempt from registering with the WV Tax Department.
If you need to speak to someone at the West Virginia Tax Department, please call 304-558-8693. NOTE: If you are using the Business4WV website to register with the WV Secretary of State and the WV Tax Department, you may do it on-line at www.business4wv.com. Please note there is a one-time fee of $130.00.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: LOT2400000009

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)

[X] Addendum No. 1	[ ] Addendum No. 6
[ ] Addendum No. 2	[ ] Addendum No. 7
[ ] Addendum No. 3	[ ] Addendum No. 8
[ ] Addendum No. 4	[ ] Addendum No. 9
[ ] Addendum No. 5	[ ] 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.

TAC Security Inc.
Company

Authorized Signature

3/28/2024
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012