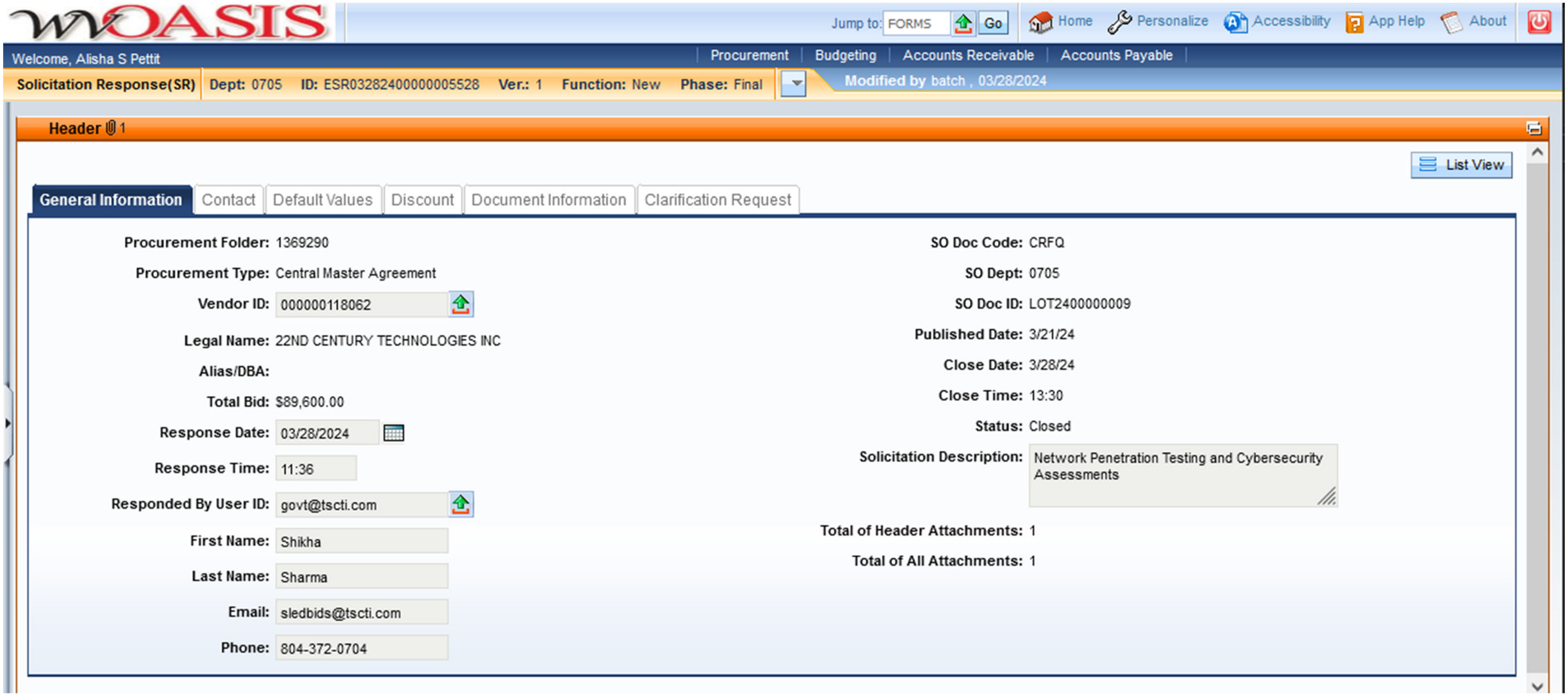
West Virginia
Purchasing Division

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

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



Welcome, Alisha S Pettit

Solicitation Response(SR) Dept: 0705 ID: ESR03282400000005528 Ver.: 1 Function: New Phase: Final

Modified by batch , 03/28/2024

Header 1

Procurement Folder:	1369290	SO Doc Code:	CRFQ
Procurement Type:	Central Master Agreement	SO Dept:	0705
Vendor ID:	000000118062	SO Doc ID:	LOT2400000009
Legal Name:	22ND CENTURY TECHNOLOGIES INC	Published Date:	3/21/24
Alias/DBA:		Close Date:	3/28/24
Total Bid:	$89,600.00	Close Time:	13:30
Response Date:	03/28/2024	Status:	Closed
Response Time:	11:36	Solicitation Description:	Network Penetration Testing and Cybersecurity Assessments
Responded By User ID:	govt@tscti.com		
First Name:	Shikha	Total of Header Attachments:	1
Last Name:	Sharma	Total of All Attachments:	1
Email:	sledbids@tscti.com		
Phone:	804-372-0704		

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 ESR03282400000005528	1

VENDOR

000000118062
22ND CENTURY TECHNOLOGIES INC

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 89600 **Response Date:** 2024-03-28 **Response Time:** 11:36:37

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				11200.00

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				6400.00

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				39200.00

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				32800.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

22nd Century Technologies, Inc.

CMMI Level 3 | ISO 27001 | ISO 20000 | ISO 9001

REQUEST FOR PROPOSALS

Network Penetration Testing and Cybersecurity Assessments

CRFQ # 0705-LOT2400000009

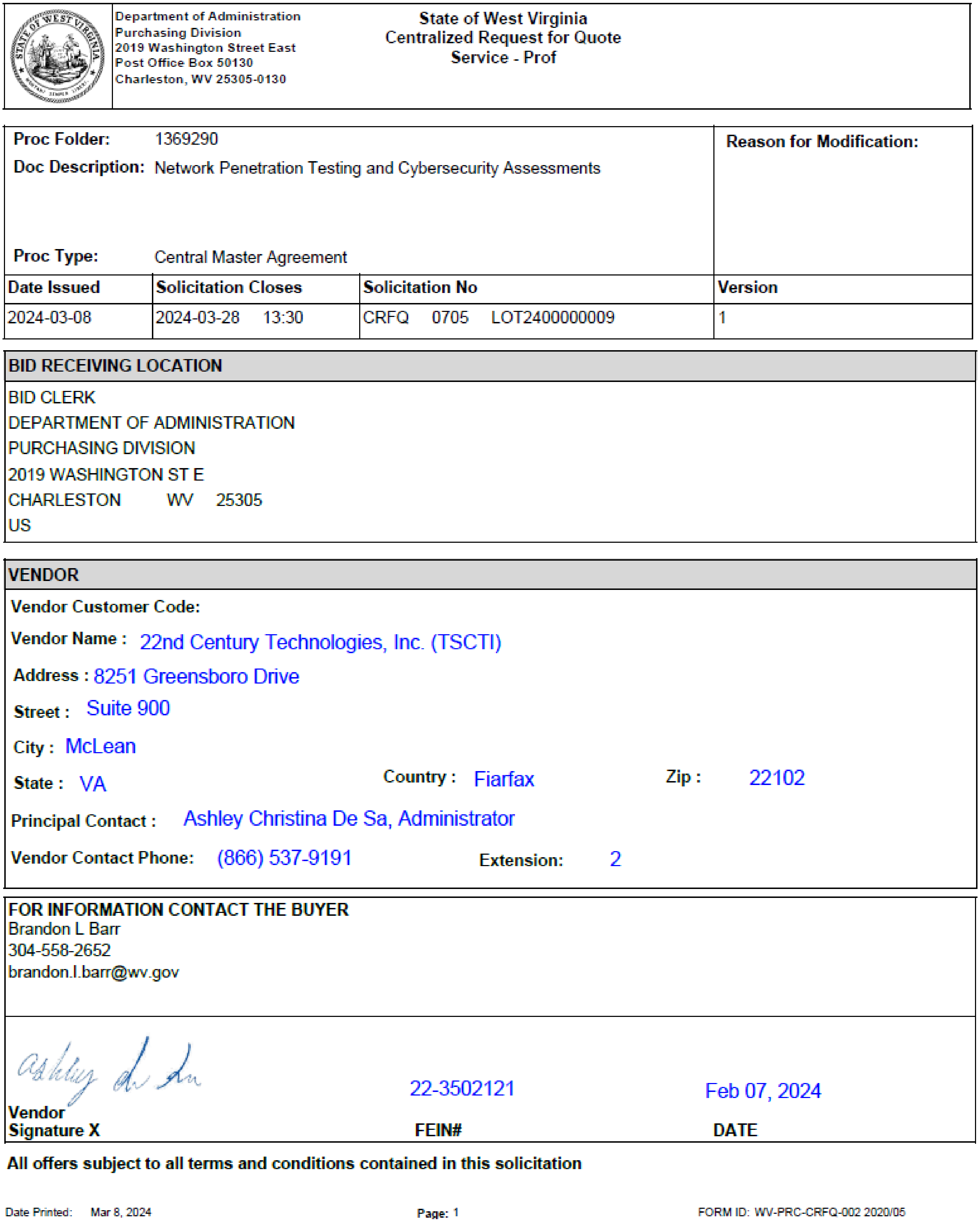
Solicitation Due Date: Mar 28, 2024 by 1:30 PM (EST)

Submitted To:
Brandon L Barr
P: 304-558-2652
Email: brandon.l.barr@wv.gov

Submitted By:
Ashley Christina De Sa, Administrator
5400 D. Big Tyler Road Charleston, WV, 25313
Phone: (866) 537-9191 Ext 2
| Fax: 732-537-0888
Email: sledproposals@tscti.com

TSCTI claims that information contained in our proposal is confidential and proprietary. We believe that the data contained in the proposal like contact information of proposed staff, technical and management approach, proposed subcontractor and price quote. Disclosure of these information can be used by our competitors to underprice us on future bids, reverse-engineer aspects of TSCTI's approach, lure away subcontractors or key employees. Thereby we request the government to provide us the opportunity to provide a redacted copy of our response for FOIA and protecting the undue advantage of FIOA disclosure.

Table of Contents



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

State of West Virginia
Centralized Request for Quote
Service - Prof

Proc Folder: 1369290

Doc Description: Network Penetration Testing and Cybersecurity Assessments

Proc Type: Central Master Agreement

Reason for Modification:

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

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name : 22nd Century Technologies, Inc. (TSCTI)

Address : 8251 Greensboro Drive

Street : Suite 900

City : McLean

State : VA **Country :** Fiarfax **Zip :** 22102

Principal Contact : Ashley Christina De Sa, Administrator

Vendor Contact Phone: (866) 537-9191 **Extension:** 2

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

ashley d Sa

Vendor Signature X 22-3502121 **FEIN#** Feb 07, 2024 **DATE**

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

Date Printed: Mar 8, 2024 Page: 1 FORM ID: WV-PRC-CRFQ-002 2020/05

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

(Printed Name and Title) Ashley Christina De Sa

(Address) 8251 Greensboro Drive, Suite 900, McLean, VA 22102

(Phone Number) / (Fax Number) 737-537-9191 Ext 2

(email address) sledproposals@tscti.com

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

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

22nd Century Technologies, Inc.
(Company)

Ashley de Sa
(Signature of Authorized Representative)

Ashley Christina De Sa, Mar 28, 2024
(Printed Name and Title of Authorized Representative) (Date)

866-537-9191 Ext 2| 732-537-0888
(Phone Number) (Fax Number)

sledproposals@tscti.com
(Email Address)

TSCTI's Qualifications

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

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

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

TSCTI was incorporated in 1997 as S-Corporation, headquartered in VA, and locally present at ***5400 D. Big Tyler Road Charleston, WV, 25313***. We have been providing a range of Information Technology (IT) Cybersecurity Services including External Network, websites, web application penetration testing, internal network vulnerability assessments, and many more like the requirements solicited by ***West Virginia Lottery (Lottery)***; in the state for ***26 years***. With more than two decades of experience, we have been a thought leader in the IT Security Testing and Assessment space, with our 800+ Security practitioners safeguarding our nation.

TSCTI is a Top-Secret cleared State and Federal Government focused company with over 300 State and local contracts and over 100 Federal contracts. The maturity of our processes is evident from our CMMI Level 3, ISO 20000, ISO 9001, and ISO 27001 certifications. Our major clients where we are providing similar IT Cybersecurity services include an active contract with the ***State of WV,*** *West Virginia University, Denver County-CO, Ohio Turnpike Lottery, Maricopa County-AZ, Cleveland Metroparks, Cleveland Airport System, Ohio Veterans Homes, Cincinnati Metropolitan Housing Authority, The Ohio Department of Developmental Disabilities, State of Ohio – Department of Administrative Services, City of Dayton, City of Piqua, Cuyahoga Metropolitan Housing Authority, Kent State University, Columbus City Schools, UN Women, Department of Corrections and Community Supervision (DOCCS), Ohio Department of Developmental Disabilities, Lucas County Corrections Center, Ohio Department of Veteran Services, the Air Force, Defense Logistics Agency, U.S. Army, U.S. Navy, Federal Bureau of Investigations, Department of Interior, USPS, Marine Corps the Department of Agriculture and many more*. TSCTI holds expertise in assisting our clients with enhanced security postures and safeguarding against potential cyber-attacks. TSCTI has supported more than 40 Federal information security programs to achieve compliance and accreditation through NIST, FISMA, RMF, FedRAMP, and DIACAP-based processes. The services we provide include ***External Network Penetration Testing***, where our three-phased methodology included enumeration, vulnerability assessment, and exploitation. We conducted social engineering exercises, gaining agency-verified email access. With client approval, we perform heavy-load attacks, ensuring transparent communication on potential disruptions. Rapid reporting of security vulnerabilities and prioritizing remediation needs are our priorities. In ***Website and Web Application Penetration Testing***, our approach covered enumeration, vulnerability assessment, and exploitation, including DOS attacks. We delivered detailed findings, risk ratings, and technical recommendations electronically. For ***Internal Network Vulnerability Assessments,*** we followed a structured methodology for all assets. We assessed security comprehensively and prioritized remediation needs. Our commitment extended to delivering Executive and Technical Reports, with a Findings Presentation to the clients.

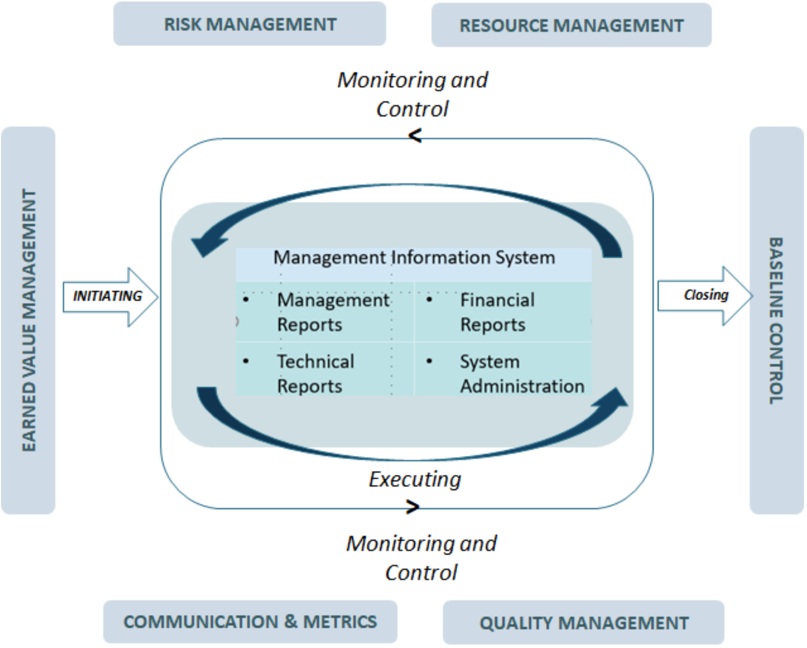
In essence, our cybersecurity proficiency, tailored methodology, and commitment to transparent communication make us a trusted partner for safeguarding the Lottery's digital infrastructure.

TSCTI offers a comprehensive range of additional services through its ***NOC, SOC, ITSM, and business operations center; a Center of Excellence and Innovation Hub located in TSCTI's WV regional office***, which can be customized based on the specific needs and preferences of the Lottery led by TSCTI's Chief Growth and Innovation Officer and Chief Technology Officer. The ***Center of Excellence (COE) and Innovation Hub is a 65000 sq office consisting of a team of more than 400 highly skilled and specialized Security Subject Matter Experts (SMEs) and Researchers including more than 100 local residents***. These experts are readily available to delve into the exploration and evaluation of emerging advancements and tools, providing valuable insights into their practical applications and potential implications within the context of the Lottery. ***Our efforts of giving jobs to local staff thereby helping them not to relocate to other big cities to find job is appreciated by Governor Jim Justice & Cabinet Secretary Mitch Carmichael - WV Department of Economic Development.*** One of the key roles of the COE and Innovation Hub is to share technological innovations that are relevant and beneficial to Lottery's requirements. By leveraging their expertise and staying at the forefront of industry trends, the COE team can identify and recommend cutting-edge technologies and solutions that can enhance the Lottery's operations and services.

They achieve this by drawing on their experience working with various customers and by leveraging the insights gained from TSCTI's own Center of Excellence Innovation Lab.

TSCTI's ability to meet Lottery's Schedule

TSCTI is committed to meeting the Lottery's schedule and ensuring timely delivery of all services. We understand the ***importance of efficient project management*** and ***have a proven track record in meeting deadlines for our clients***. Our experienced team will work closely with the Lottery to establish clear timelines and milestones for each deliverable, ensuring that all activities are completed within the agreed-upon timeframes. We ***have a streamlined and agile approach to project execution, leveraging our expertise, tools, and methodologies to maximize efficiency***. With our strong commitment to meeting deadlines and our focus on delivering high-quality results, TSCTI is well-equipped to accommodate the Lottery's schedule and deliver the required services in a timely manner. Below is a detailed overview of our robust Project Management plan, showcasing our ability to execute and meet the Lottery's schedule. Additionally, we have included testimonials from some of our major clients, highlighting their confidence in our capabilities.



TSCTI's Project Management Plan

Being ***ISO certified and accredited at CMMI level 3***, TSCTI has a well-structured ***PMBOK-compliant project management plan*** (as showcased in the figure) following which, TSCTI will provide qualified personnel with industry experience to manage this Lottery's Cyber Security Services and meet the Lottery's contract schedule. Our team's management approach focuses on being responsive and flexible to meet our client's needs, providing a stable and experienced management team that can fulfill Lottery requirements. Our project management approach utilizes industry standards, best practices, a phased approach, and techniques tailored from the ***Project Management Institute's (PMI) Body of Knowledge (PMBOK)*** process groups and knowledge areas, the Earned Value Management system, and our proven methodology to manage project activities with milestones. We will manage the overall engagement in collaboration with Lottery's PM (who will be the focal point for all communications with our team), and thus our project management approach will provide responsiveness, quality, and cost efficiencies to managing and delivering high quality, user-friendly and sustainable security assessment of systems and networks to Lottery, partners, and stakeholders.

Our rigorous management practices ensure that our project team members receive all necessary administrative, budgetary, logistical, and professional support. Our Program Management Plan (PMP) will provide several mechanisms to ensure smooth quality operations, including effective communication of project risks and task progress via formal methods. These include a simple, non-bureaucratic organizational structure and a tested corporate support system. Our corporate support system enables project staff to focus their talents on the proposed tasks and deliver superior quality service. We will ***utilize tools such as Microsoft Project and/or Microsoft Office capabilities to deliver the PIP/PMP***, including scorecard mechanisms to reflect completion (%-percentage) of the overall Task as well as individual objectives and actions.
Our management strategy is based on timely and effective client communication as well as:

- Sound project management of schedules and resources
- Responsiveness to changes
- Our Quality Control Plan (QCP).

Sound project management of schedules and resources ensures value-added benefits. Three primary documents support our management approach: ***the budget, the schedule of deliverables, and the staffing chart***. Responsiveness to change is critical to our management strategy. We have learned to anticipate the unexpected changes that too often and too easily threaten the planning and performance of less experienced teams. Our management team is prepared to respond to any changes that occur because of client modifications to a task, and we always offer alternate solutions with proposed areas of focus.

Our QCP builds quality into every activity, service, and product. Our performance measurement and quality control systems involve plans and procedures for executing, monitoring, and assessing the implementation of our management and operational activities; evaluating the resulting services and products; tracking the allocation of resources; and instituting improvements and refinements. While TSCTI PM is ultimately accountable for quality control, we emphasize the importance of quality to all staff and focus on the importance of performing any project activity right the first time.

TSCTI believes that establishing a solid ***Project Implementation Plan (PIP)/Project Management Plan (PMP)*** is a prerequisite for project success and meeting the Lottery's project schedule. Immediately after the contract award, our team will meet with the appropriate organizational, functional, facilities (physical locations and personnel logistics), IT and operational stakeholders to establish a formal approved draft PIP/PMP to guide both project execution and project control. The kickoff meeting will include discussions on scope, goals, roles, resources, objectives, communication protocols, schedule, budget, and contract requirements to further ***develop and refine the draft versions of PIP/PMP***. Team TSCTI PM will provide a draft PIP/PMP to Lottery COR/KO and will collaboratively refine and deliver the final draft of the document within 15 days of contract award. However, please note that the final draft PIP/PMP will remain a living document and will be adjusted by our team PM, on an as-needed basis. Milestones and risks will be documented and communicated with the government PM. We have experience meeting deliverable expectations through effective project management on security assessments involving infrastructure/GSS and applications (major/minor).

An example of an outline of our PIP/PMP that may include all or some of the following areas of best practice methodology:

- Project Scope
- Project Milestones
- Schedule Baseline and Work Breakdown Structure
- Change Management Plan
- Communications Management Plan
- Cost Management Plan
- Scope Management Plan
- Quality Management Plan
- Risk Management Plan
- Staffing Plan
- Resource Calendar

Following the kick-off. Team TSCTI will work diligently to manage all activities spanning over Lottery facilities (could be in parallel or serial processing depending on resource allocations and facility staff availability) and complete the task objectives relayed to Lottery via scheduled weekly meetings (in-person, telecom, or emails, as reflected in the Communications Plan). In addition, our weekly status reports will reflect details, including but not limited to, hours worked per resource (not to exceed 37.5 hours per week per resource) against assigned tasks (prior approval will be sought), accomplishments, planned activities (expected work effort) for the following week, Challenges/discussion points and risks to project (or specific objectives). We will submit a bi-weekly invoice to the government PM and/or COR.

Finally, in adherence with the tenets of the current version of the Project Management Institute's (PMI) Guide to the Project Management Body of Knowledge and the Carnegie Mellon CMMI, our PIP/PMP will include a work breakdown structure (WBS) to accurately reflect the discrete tasks and deliverables to support the overall mission as described in the solicitation. The WBS will include task and subtask levels of work generated by the identification of work packages. The final PIP/PMP will also include a staffing plan that addresses individual areas of responsibility, including the roles and responsibilities of our project team. Team TSCTI will maintain and update the document as appropriate throughout the period of performance to lead the Network Penetration Testing and Cybersecurity Assessments Program effort to success.

TESTIMONIAL #1

"We have been partnering with TSCTI for several years, and their expertise in cybersecurity has been invaluable. They conducted a thorough risk assessment of our security program, identifying vulnerabilities and providing actionable recommendations. Their annual cybersecurity consulting services, including incident response preparedness and vendor assessments, have greatly strengthened our security posture. TSCTI's professionalism, deep knowledge, and timely delivery make them an exceptional partner for our organization." - Metropolitan Transportation Authority

"TSCTI has been our trusted cybersecurity advisor for over five years. Their risk assessment services provided us with valuable insights into our security program, leading to significant improvements. Their annual consulting services, such as security awareness training and vulnerability management, have enhanced our staff's preparedness and reduced security risks. TSCTI's commitment to excellence and their ability to meet our schedule have made them an integral part of our cybersecurity strategy." - City of Phoenix Aviation Department

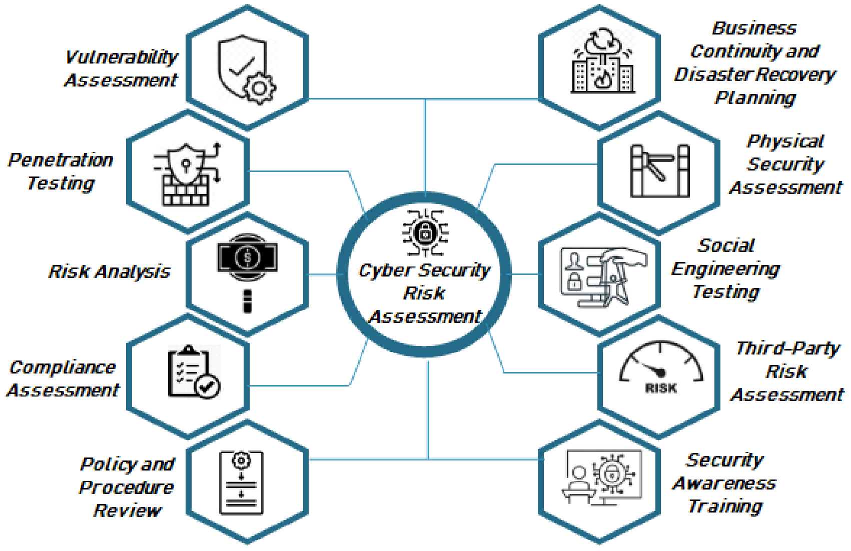
TESTIMONIAL #2

Capabilities of TSCTI to satisfy the Lottery's Requirement

We believe that TSCTI is the most qualified service provider to assist the Lottery in the cybersecurity consulting domain for several reasons enumerated below:

Our Relevant Experience: TSCTI has assisted more than 20 states with a variety of cybersecurity-related services, ranging from building information security programs to conducting vulnerability assessments and data governance program/project development. We continue to work with more than 15 states on their Centers for Cybersecurity Services security compliance activities as part of the Affordable Care Act implementations. We have also worked on multiple projects for Transportation, Aviation, and other similar industry clients, and institutions of higher education, for providing enterprise information security program development, security monitoring, risk assessments, regulatory compliance and data protection assessments, and incident response activities. Some of our major clients include but not limited to ***State of WV,*** *West Virginia University, Denver County-CO, Ohio Turnpike Lottery, Maricopa County-AZ, Cleveland Metroparks, Cleveland Airport System, Ohio Veterans Homes, Ohio Department of Veteran Services, the Air Force, Defense Logistics Agency, U.S. Army, U.S. Navy, Federal Bureau of Investigations, Department of Interior, USPS, Marine Corps the Department of Agriculture and many more***.**

Service Portfolio: TSCTI has been providing a wide range of Network Penetration and Cybersecurity Assessment and other IT Security consulting Services for 26 years, inclusive of various tasks and operations. Below are graphically (shown in **Exhibit 1**) presented the TSCT's Cybersecurity Risk Assessment Service portfolio.


Vulnerability Assessment
Penetration Testing
Risk Analysis
Compliance Assessment
Policy and Procedure Review
Cyber Security Risk Assessment
Business Continuity and Disaster Recovery Planning
Physical Security Assessment
Social Engineering Testing
Third-Party Risk Assessment
RISK
Security Awareness Training

TSCTI's Cybersecurity Risk Assessment Service Portfolio

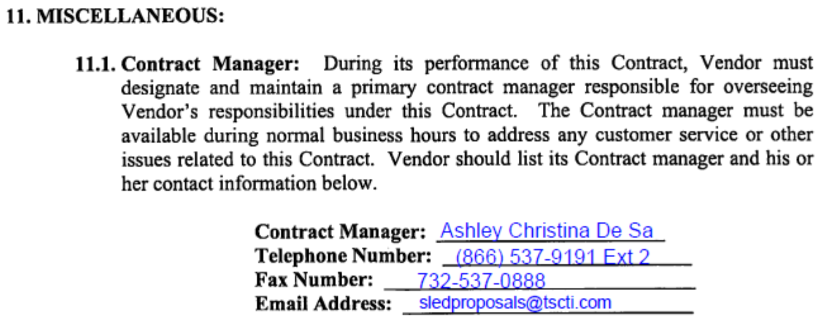
Our Team: More than 60% of our professionals possess at least one security certification; many have more than one. We have more than 2,000 CISA (Certified Information Systems Auditor), 1,100 CISSP (Certified Information Systems Security Professional), about 120 CIPP (Certified Information Privacy Professional), and 150 CISM (Certified Information Security Manager) professionals—a large pool of qualified specialists to serve you. Below we have provided TSCTI's pre-screened on-bench candidates readily available to comprehend Lottery's Security team;

Service Categories	No. of Pre-Vetted Candidates			Average Minimum Qualification
	Internal /On-Bench Candidates	In the State of WV	Across USA	

Web Application Penetration Testing	23	2200+	35000+	• OSCP: Offensive Security Certified Professional • CISSP: Certified Information Systems Security Professional • CEH: Certified Ethical Hacker • GIAC: Global Information Assurance Certification • CREST: Council for Registered Ethical Security Testers • CESG: Communication Electronic Security Group
Network Penetration Testing (External and Internal)	31	3200+	32000+	
Wireless Network Penetration Testing (physical on-site testing)	15	3100+	31000+	
Social Engineering (social media, phone, phishing, etc.)	25	3000+	30000+	
Physical Social Engineering	10	3000+	30000+	
Specialized Security Assessments; I.Firewall and Routers II.Database Architecture III.Active Directory and Azure Active Directory IV.Telecommunications V.Azure environment or other cloud environment VI.SharePoint	15	2890+	25000+	

Dedicated Account Management: TSCTI has been very careful and successful in providing our clients with un-diverted attention and services. To do so, TSCTI assigned a dedicated Account Management team who would work with the Lottery to define the requirements. Our account manager would work with the "trusted agent" to identify the Lottery's stakeholders and facilitate a meeting to document the requirements. As part of this meeting, our primary account manager would discuss and document the following security assessment requirements:

1. Scope of the security assessment, such as information assets including the data, systems, targeted IP address ranges, Web applications, databases, and IT systems selected for the Lottery Enterprise's security strategy.
2. The type of the security assessment to be performed based on the level of disclosure that would be provided (none, partial, or full).
3. Level of effort associated with testing to be performed based on the outcome of the above activity.
4. Identify Lottery's personnel to be involved in assessments.
5. Outline time frame for the security assessment, including the time range for each assessment day. To avoid interruptions, we recommend running many of the assessment tasks during non-business hours.
6. Technical prerequisites/safeguards for Lottery to establish prior to TSCTI performing the cyber security risk assessment.
7. User credentials are required to perform credential network vulnerability/penetration scanning, web application and database assessment, security code review, and configuration review.
8. Location from where the security risk assessment would be conducted.
9. Ensuring that the assessment is performed while aligning the CIS controls, security controls, NIST CSF with the Azure Revised Statues, and State's Security Policies, Standards, and Procedures.



11. MISCELLANEOUS:

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

Contract Manager: Ashley Christina De Sa
Telephone Number: (866) 537-9191 Ext 2
Fax Number: 732-537-0888
Email Address: sledproposals@tscti.com

Actionable advice: Our technical approach and advice is based on our implementation experience. While we performed more than 1000 security assessments in the past 5 years, we also assisted our clients with several implementations of security tools and processes. "Implementable advice" comes from years of hands-on experience of executing security programs that not only includes remediating vulnerabilities, but also implementing the people, process, and technology aspects of security programs.

TSCTI's Training Initiatives: At TSCTI, we prioritize the continuous development of our security professionals through a comprehensive training program designed to keep them abreast of the latest technology trends and industry best practices. Our skill enhancement opportunities align with TSCTI's commitment to fostering growth and improvement among employees. These include on-the-job training led by experienced team members, professional development programs such as workshops and seminars, cross-functional training to broaden knowledge across business areas, mentorship programs, and attendance at industry conferences and events. These initiatives ensure that our security professionals are well-equipped to excel in their roles, staying ahead in the dynamic field of cybersecurity.

TSCTI places immense value on ongoing training, recognizing its significance in maintaining a highly skilled workforce. Our Training Calendar, updated annually, ensures employees are up to date with industry advances. The Organizational Training Plan (OTP) is tailored to project, organizational, and individual needs, emphasizing quality assurance through proven methods and standards. The commitment to training is evident in our internal training budget exceeding $1 million in 2020, offering tuition and training reimbursement of up to $5,000 per employee per year, conducting three "boot camps" annually for new staff, and providing leadership development programs for high-potential individuals. TSCTI's holistic approach to employee development, including a generous compensation package, demonstrates our commitment to attracting, retaining, and motivating a dedicated team of cybersecurity professionals.

Our demonstrated approach to perform the services: TSCTI has expertly tuned its Network Penetration Testing and Cybersecurity Assessments Services Approach based on several globally recognized international standards, including ***ISO/IEC 27001:2013, NIST Cybersecurity Framework, CIS Controls, Security Controls, West Virginia Revised Statues, State's Security Policies, Standards, and Procedures, FAIR (Factor Analysis of Information Risk), COBIT (Control Objectives for Information and Related Technology) 5, and ENISA (European Union Agency for Cybersecurity) Risk Management and Assurance Framework***. With this well-structured and custom-modulated approach, TSCTI can provide clients with a comprehensive and systematic project progression that enables the identification, assessment, and management of cybersecurity risks in an efficient and effective manner. TSCTI's demonstrated risk assessment service approach typically involves the following steps:

- Understanding the client's business, objectives, and regulatory requirements
- Identifying and classifying critical assets and information
- Conducting a threat and vulnerability assessment
- Performing a gap analysis of current security controls against relevant standards and best practices
- Prioritizing risks and developing a risk treatment plan
- Implementing risk treatment strategies and controls
- Monitoring and reviewing the effectiveness of the risk management program on an ongoing basis.

TSCTI will leverage this approach to provide clients with a clear and structured roadmap that aligns with international standards and best practices, while also addressing their unique penetration testing and cybersecurity needs and concerns.

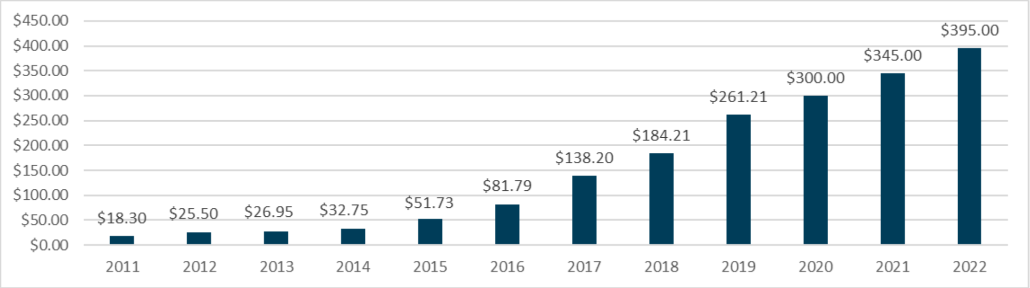
Our Tools and Frameworks: As a leading service provider in Network Penetration Testing and Cybersecurity Assessments services, TSCTI employs a range of cutting-edge tools and methods to provide clients with comprehensive assessments of their cybersecurity risks. The tools and accelerators outlined in the bullets below have been developed and customized by serving multiple state agencies or are industry standard tools that, in our experience, have found accelerated delivery and increased reliability of results. These tools may be utilized as appropriate in order to accelerate delivery and reduce the risk of gaps in each security assessment. Some of the commonly used tools and methods that TSCTI employs include:

- **Vulnerability scanning tools:** TSCTI uses state-of-the-art vulnerability scanning tools such as ***Nessus, OpenVAS, and Qualys*** to scan for vulnerabilities in the client's systems and identify potential risks.
- **Penetration testing tools:** To simulate cyber-attacks and identify vulnerabilities in the client's systems and infrastructure, TSCTI uses advanced penetration testing tools such as ***Metasploit, Nmap, and Burp Suite***.
- **Risk assessment frameworks:** Frameworks such as ***NIST Cybersecurity Framework, ISO 27001, and CIS Controls*** are used by TSCTI to provide a structured approach to cybersecurity risk assessment and help ensure that all aspects of the assessment are covered.

- **Threat modeling:** TSCTI uses the threat modeling method to identify potential threats to the client's systems and infrastructure and prioritize them based on their potential impact.
- **Security control assessments:** To evaluate the effectiveness of the client's existing security controls and identify gaps and weaknesses in the control environment, TSCTI conducts security control assessments.
- **Interviews and surveys:** TSCTI conduct interviews and surveys with key stakeholders and subject matter experts to collect information about the client's systems, infrastructure, policies, and procedures.
- **Documentation review:** To provide valuable insight into the client's security posture and help identify potential risks, TSCTI reviews the client's policies, procedures, and other relevant documentation.
- **Asset inventory and classification:** TSCTI creates an inventory of the client's assets and classifies them based on their criticality and sensitivity to help prioritize the assessment and identify potential risks.

By combining these tools and methods, TSCTI is able to provide clients with a comprehensive assessment of their cybersecurity risks, identify potential vulnerabilities and threats, and provide a roadmap to mitigate these risks. The selection of specific tools and methods is based on the client's needs, the scope of the assessment, and the expertise of TSCTI's team of cybersecurity experts.

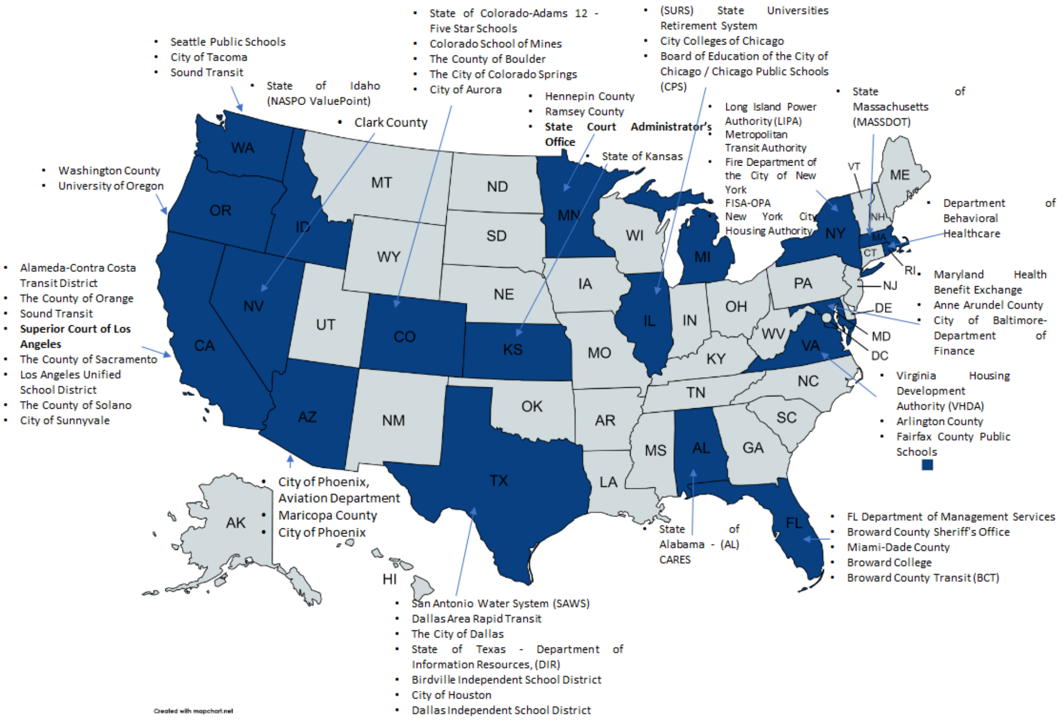
Financially Stable: TSCTI is financially stable with year 2022 net revenue of $395M+, zero debt and $2B current contract value. TSCTI possesses the necessary financial capacity, working capital, and other resources to carry out the capital, operating, planning and future maintenance activities, without assistance from any external source. TSCTI currently has a credit line of $10M and has $56M as bank deposit.



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

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

From an IT Cybersecurity Services where our major contracts services include Network Penetration and Cybersecurity services, our breadth of capabilities, knowledge, and experience in the public sector is unmatched. TSCTI has experience providing security and privacy services in the public sector for more than 26 years. The figure aside provides a snapshot of our extensive security services experience across numerous state and local agencies.


Seattle Public Schools
City of Tacoma
Sound Transit
State of Idaho (NASPO ValuePoint)
Clark County
State of Colorado-Adams 12 - Five Star Schools
Colorado School of Mines
The County of Boulder
The City of Colorado Springs
City of Aurora
(SURS) State Universities Retirement System
City Colleges of Chicago
Board of Education of the City of Chicago / Chicago Public Schools (CPS)
Hennepin County
Ramsey County
State Court Administrator's Office
State of Kansas
Long Island Power Authority (LIPA)
Metropolitan Transit Authority
Fire Department of the City of New York
FISA-OPA
New York City Housing Authority
State of Massachusetts (MASSDOT)
Department of Behavioral Healthcare
Maryland Health Benefit Exchange
Anne Arundel County
City of Baltimore-Department of Finance
Virginia Housing Development Authority (VHDA)
Arlington County
Fairfax County Public Schools
Washington County
University of Oregon
Alameda-Contra Costa Transit District
The County of Orange
Sound Transit
Superior Court of Los Angeles
The County of Sacramento
Los Angeles Unified School District
The County of Solano
City of Sunnyvale
City of Phoenix, Aviation Department
Maricopa County
City of Phoenix
State of Alabama - (AL) CARES
FL Department of Management Services
Broward County Sheriff's Office
Miami-Dade County
Broward College
Broward County Transit (BCT)
San Antonio Water System (SAWS)
Dallas Area Rapid Transit
The City of Dallas
State of Texas - Department of Information Resources, (DIR)
Birdville Independent School District
City of Houston
Dallas Independent School District
WA
OR
ID
MT
ND
MN
WI
MI
NY
VT
ME
NH
MA
CT
RI
NJ
PA
DE
MD
DC
SD
WY
NE
IA
IL
IN
OH
WV
VA
KY
CA
NV
UT
CO
KS
MO
NC
TN
SC
AZ
NM
OK
AR
MS
AL
GA
TX
LA
FL
AK
HI
Created with mapchart.net

TSCTI takes pride in showcasing our successful track record of delivering Network Penetration Testing and Cybersecurity Assessments to organizations with similar needs and objectives as the Lottery. With a comprehensive Statement of Work (SOW) aligned with the Lottery's requirements, TSCTI has effectively operated and administered external and internal network and information security programs for numerous clients. Our dedicated team of experts has assisted these organizations in assessing compliance with information systems security controls, identifying vulnerabilities, mitigating risks, and providing recommendations to strengthen their security posture. Through collaborative efforts, we have supported the development and standardization of information technology policies and procedures, ensuring adherence to industry best practices. Our approach includes active participation in information technology security forums, fostering knowledge sharing and staying at the forefront of emerging security trends. With our proven expertise and commitment to delivering exceptional services, TSCTI is well-equipped to meet the unique challenges faced by the Lottery and contribute to the optimization of its information systems controls.

Case Study #1: State of WV

Duration: Jan 2020 – Jan 2023

Dollar Value: $1 Million

Project Overview: The State partnered with TSCTI to strengthen their network and information security infrastructure. The objective was to provide a comprehensive range of services to address vulnerabilities, enhance identity and access management, ensure regulatory compliance, optimize network architecture, implement robust monitoring systems, and establish effective incident detection and response protocols. The goal was to improve the overall security posture and safeguard against potential cyber-attacks.

Work Performed:

- Conducted a thorough vulnerability assessment to identify weaknesses and potential entry points for unauthorized access.
- Implemented robust identity and access management solutions to enhance user authentication and authorization processes.
- Conducted a comprehensive review of regulatory requirements and implemented necessary measures to achieve compliance.
- Evaluated the existing network architecture and proposed enhancements to strengthen security and resilience.
- Engineered and implemented monitoring systems to detect and respond to security incidents in real-time.
- Developed and implemented an incident response plan to ensure prompt and effective handling of security breaches.

Relevant Services:

- Network Penetration Testing
- Vulnerability assessments
- Identity and access management
- Regulatory compliance
- Network architecture enhancement
- Engineering and implementation
- Monitoring and incident detection
- Incident response planning and execution

Key Findings;

- Identified critical vulnerabilities in the network infrastructure and applications, including outdated software versions and misconfigured access controls.
- Discovered weaknesses in identity and access management processes, posing risks of unauthorized access.
- Detected non-compliance with relevant regulatory standards and provided recommendations for remediation.
- Identified potential areas of concern related to network architecture and proposed solutions for increased security

Deliverables:

- Detailed vulnerability assessment report with identified vulnerabilities and recommendations for remediation.
- Enhanced identity and access management system with improved authentication and authorization mechanisms.
- Comprehensive compliance report outlining steps taken to achieve regulatory requirements.
- Upgraded network architecture design and implementation plan for enhanced security.
- Implemented monitoring systems with real-time alerts and incident response protocols.
- Incident response plan document detailing procedures and guidelines for effective handling of security incidents.

Case Study #2: The County of Boulder, CO

Duration: Mar 2020– Mar 2021

Location: 1325 Pearl St, Boulder, Colorado, 80302

Dollar Value: $2M

Project Overview: The County of Boulder, CO engaged TSCTI to provide a comprehensive range of computer network and information security services. The objective was to assess vulnerabilities, strengthen identity and access management, ensure regulatory compliance, optimize network architecture, implement robust monitoring systems, and establish efficient incident detection and response capabilities. The County sought to enhance its security posture and protect against potential cyber threats.

Work Performed:

- Conducted a comprehensive vulnerability assessment to identify and address potential weaknesses in the County's computer network.

Relevant Services:

- Network Penetration Testing
- Vulnerability assessments
- Identity and access management

• Implemented advanced identity and access management solutions to enhance user authentication and authorization processes. • Conducted a thorough review of regulatory requirements and implemented measures to achieve and maintain compliance. • Assessed the County's network architecture and proposed improvements to enhance security and resilience. • Engineered and implemented robust monitoring systems to detect and respond to security incidents promptly. • Developed and implemented an effective incident response plan to ensure swift and efficient handling of security breaches.	• Regulatory compliance • Network architecture optimization • Engineering and implementation • Monitoring and incident detection • Incident response planning and execution
Key Findings: • Identified critical vulnerabilities in the County's computer network, including outdated software, weak access controls, and misconfigured security settings. • Discovered weaknesses in the identity and access management processes, such as inadequate password policies and unauthorized user access. • Identified areas of non-compliance with relevant regulations and provided recommendations to address the gaps. • Identified potential network architecture vulnerabilities, such as single points of failure and inadequate segmentation.	**Deliverables:** • Comprehensive vulnerability assessment report with detailed findings and recommendations for remediation. • Enhanced identity and access management system with strengthened authentication mechanisms and improved access controls. • Regulatory compliance report outlining the County's adherence to relevant regulations and suggested remediation actions. • Network architecture optimization plan with proposed improvements for increased security and resilience. • Implemented monitoring systems with real-time alerts and incident response protocols. • Incident response plan document outlining procedures and guidelines for efficient handling of security incidents.

Case Study #3: The Department of Defense Medical Examination Review Board (DoDMERB)

Duration: Oct 2021 - Present

Location:

Dollar Value: $700K

Project Overview: The Department of Defense Medical Examination Review Board (DoDMERB) enlisted the services of TSCTI to enhance their computer network and information security infrastructure. The primary objective was to conduct a comprehensive assessment of vulnerabilities, strengthen identity and access management, ensure regulatory compliance, optimize network architecture, implement robust monitoring systems, and establish effective incident detection and response capabilities. The DoDMERB aimed to fortify their security measures and safeguard sensitive medical examination data.

Similar Work Performed:	**Relevant Services:**
• Utilized industry-leading vulnerability scanning tools such as Nessus and OpenVAS to conduct a thorough assessment of the DoDMERB's computer network. • Implemented multi-factor authentication (MFA) and privileged access management (PAM) solutions to enhance identity and access management. • Conducted a detailed analysis of relevant regulations, including HIPAA and NIST guidelines, to ensure compliance throughout the organization. • Collaborated with the DoDMERB's IT team to optimize network architecture, implementing techniques such as segmentation and firewall rule tightening. • Deployed advanced security monitoring tools such as SIEM (Security Information and Event Management) systems and intrusion detection systems (IDS). • Developed and implemented an incident response plan, utilizing industry-standard frameworks such as the NIST Incident Response Lifecycle.	• Vulnerability assessments utilizing Nessus and OpenVAS • Identity and access management enhancement • Network Penetration Testing • Regulatory compliance analysis and implementation • Network architecture optimization, including segmentation and firewall rules • Deployment of SIEM and IDS for robust monitoring • Incident response planning and implementation following NIST frameworks
Key Findings; • Identified critical vulnerabilities in the DoDMERB's computer network, including unpatched systems and misconfigured security settings. • Detected gaps in identity and access management, including weak passwords and excessive user privileges. • Ensured compliance with HIPAA regulations and NIST guidelines by addressing identified gaps and implementing necessary controls.	**Deliverable:** • Comprehensive vulnerability assessment report with detailed findings and prioritized recommendations for remediation. • Enhanced identity and access management framework with MFA and PAM solutions implemented.

- Optimized network architecture for improved security, including network segmentation to isolate sensitive data and tighten firewall rules.
- Implemented advanced monitoring systems to detect and respond to security incidents in real-time.

- Compliance report outlining the DoDMERB's adherence to HIPAA and NIST guidelines, including documented controls and remediation actions.
- Network architecture optimization plan, detailing the implemented improvements for enhanced security.
- Deployed SIEM and IDS systems to monitor network activity and detect potential security incidents.
- Incident response plan document outlining procedures, roles, and responsibilities, as well as communication channels and incident handling guidelines

Case Study #4: Federal Bureau of Investigation (FBI)

Duration: Jul 2022 – Ongoing

Location: 1500 Marilla St. Dallas, TX 75201

Dollar Value: $900K

Project Overview: TSCTI is providing Information Security program development & assessment support to FBI

Work Performed

- Supports the development of security test plans, test descriptions, and test procedures and reviews result to ensure compliance with specifications.
- Provide assessments on cyber capabilities and activities of foreign intelligence, security services, and potential threats to and impact on Congressional information systems and operations. Conducted open and classified source research in support of Cyber CI initiatives. Created and updated threat profiles for congressional programs and its asset to be used for threat modeling for potential cyber-attack/spear attack.
- Assists in the development of Cloud computing and mobile devices and application security products. Development oversight of Cybersecurity processes and procedures
- Lead internal cybersecurity assessment and provide various maturity and impact analysis against established as well as emerging cybersecurity frameworks and trends.
- Evaluating the organization’s ability to identify and protect critical assets, and detect, respond, and recover from cybersecurity incidents.
- Performs system security assessments using automated tools in accordance with guidelines defined by the Department of Defense, National Security Agency and DISA (e.g. Security Technical Implementation Guides, DISA Field Security Office Gold Disk, Vulnerability Management System (VMS), eEye Retina Scanner Security Management Console appliance, etc.).
- Facilitated the implementation of both technical and

Relevant Services:

- Information Security program development and execution
- Cloud Computing
- Cybersecurity Maturity Assessment
- Risk Analysis

Key Actions; TSCTI performed the following services as a part of the security assessment:

- Forensics and Threat Hunting, detailed reporting, and data gathering/tagging
- Deploying Managed Detection Response system to ensure any future breach was discovered much sooner than this one.
- Perform vulnerability and penetration scan to identify and remove vulnerabilities.
- A complete analysis of the malicious software the threat actor left on the Client server, including insights into what would have happened if the software had been activated.
- Worked with the City’s technical team to purge the system and ensure that there were no remaining backdoors for the threat actor to sneak back in through.

Deliverables:

TSCTI completed the multi-phase security assessment within 60 continuous business days and provided the following deliverables to the FBI:

- Executive Summary Report
- Technical Report
- Findings Presentation
- Remediation Roadmap
- Ongoing support for remediation efforts.

References

Case Study #1: The Post Authority of New York & New Jersey (PANYNJ)

Duration: Apr 10 – Present

Location: 4 World Trade Centre, 150 Greenwich Street, New York, NY 10007

Dollar Value: $700K

Contact Name: Thomas K. Comerford

Contact Number: (201)595-4796

Email Address: tcomerfo@panynj.gov

Overview: PANYNJ required a comprehensive security assessment of its critical infrastructure and systems to identify potential vulnerabilities and recommend remediation strategies.

Similar Work Performed:

- TSCTI provided hands-on system accreditation, maintenance, and operation of Security Systems and cybersecurity tools.
- We ensured full compliance with NIST cybersecurity standards by updating applicable security documentation, including the system security plan.
- Our team analyzed vulnerability test reports and suggested remediation/mitigation plans with the ability to prioritize process and reporting enhancements.
- TSCTI reviewed, evaluated, and implemented all DISA Information Assurance Vulnerability Assessments and Information Assurance Vulnerability Alerts.
- We provided system accreditation for systems as per IAW Chapters 3 and 5, and AR 380-19, Information Systems Security (dated 27 February 1998), and DOD Instruction 5200.40, DOD Information Technology Security Certification and Accreditation Process (dated December 1997).
- We reviewed threats and vulnerabilities to the CTPF network and reported to the CTPF COR, CTO, and CTO DR any system anomaly that could result in an unauthorized disclosure of or access to sensitive information.
- TSCTI disseminated virus-related information and guidance in direct coordination with the CTPF.

Relevant Services:

- External network penetration testing
- Web application penetration testing
- Network Security Assessment
- Physical Security assessment
- Social Engineering

Key Findings:

TSCTI performed the following services as a part of the breach remediation:

- Forensics and Threat Hunting, detailed reporting, and data gathering/tagging.
- Deploying Managed Detection Response system to ensure any future breach was discovered much sooner than this one.
- Perform vulnerability and penetration scan to identify and remove vulnerabilities.
- A complete analysis of the malicious software the threat actor left on the Client server, including insights into what would have happened if the software had been activated.
- Worked with the client's technical team to purge the system and ensure that there were no remaining backdoors for the threat actor to sneak back in through.

Deliverable:

TSCTI completed the multi-phase security assessment within 45 continuous business days and provided the following deliverables to PANYNJ:

- Executive Summary Report
- Technical Report
- Findings Presentation
- Remediation Roadmap
- Ongoing support for remediation efforts

Case Study #2: Ohio Turnpike Commission, OH

Duration: Jul 2023 – Present

Location: 682 Prospect Rd, Berea, OH 44017

Dollar Value: $270K

Contact Name: Ryan Schreiber, CAPM

Contact Number: 440-971-2068

Email Address: ryan.schreiber@ohioturnpike.org

Project Overview: The City of Dallas hired TSCTI to conduct a comprehensive security assessment of its critical infrastructure and systems to identify potential vulnerabilities and recommend remediation strategies.

Work Performed

- Project Management, Compliance advisory projects, Data Security & Privacy, SOX, IT Audits, FISMA, C&A, enhancement of IT processes & security controls, vulnerability assessments, penetration testing and SAS70 projects.
- Security and risk Assessments. Develop policies and procedures.
- Design, implementation, and support of security solutions to protect networks from both external and internal threats.

Relevant Services:

- External network penetration testing
- Web application penetration testing
- Network Security Assessment
- Physical Security assessment
- Social Engineering

- Provide network/application vulnerability assessment and penetration testing services through a comprehensive testing process, as well as identifying weaknesses and vulnerabilities within the system and proposing counter measures.
- Network security, access control, security architecture, and security operations
- Design and deploy an operational network infrastructure for the silver line IT and train operations vital side network, and integration into City's existing MPLS infrastructure.
- Perform vulnerability assessments and penetration testing.
- Firewalls, VPNs (IPSec & SSL), Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), access control and authentication schemes (two-factor, single sign-on, etc.), wireless protocols (802.11a/b/g/n), internetworking elements (routers, switches, load balancers, etc.), end-point security (anti-virus, anti-Spyware, etc.), network admission control (NAC), vulnerability scanning, and data leakage prevention.
- Support all IT security projects as required by City.
- Analyze results and provided source code security and reliability solution for app developers.

Key Actions; TSCTI performed the following services as a part of the security assessment:

- Forensics and Threat Hunting, detailed reporting, and data gathering/tagging.
- Deploying Managed Detection Response system to ensure any future breach was discovered much sooner than this one.
- Perform vulnerability and penetration scan to identify and remove vulnerabilities.
- A complete analysis of the malicious software the threat actor left on the Client server, including insights into what would have happened if the software had been activated.
- Worked with the City's technical team to purge the system and ensure that there were no remaining backdoors for the threat actor to sneak back in through.

Deliverables:

TSCTI completed the multi-phase security assessment within 60 continuous business days and provided the following deliverables to the city:

- Executive Summary Report
- Technical Report
- Findings Presentation
- Remediation Roadmap
- Ongoing support for remediation efforts.

Case Study #3: Cochise County, AZ

Duration: Jun 2022 - Present

Location: 1415 Melody Lane, Building G Bisbee, AZ 85603

Dollar Value: $1M+

Contact Name: Joe E. Casey

Contact Number: 520-234-7038

Email Address: jcasey@cochise.az.gov

Project Overview: The County wanted contractor support for Penetration Testing and Specialized Security support. TSCTI was one of the awarded vendors providing complete Security Penetration Testing Services

Work Performed

- Performed system process capability and maturity assessments against controls (CISCO) framework.
- Conducted risk assessments and regulatory self-assessments.
- Assisted and performed a comprehensive threat intelligence assessment.
- Provided reporting on assessment results as well as risk mitigation and remediation recommendations and plans.
- Lead campaigns for Data Loss Prevention, Identity and Access Management, and Compliance Risk Assessments.
- Developed and aligned security improvement initiatives to be consistent with the business objectives.
- Lead the Info Security Risk Management team in the resolution of complex, mission-critical cybersecurity incidents.
- Ensured that all unauthorized vulnerabilities found during the risk assessments were properly removed or mitigated to an acceptable level.

Relevant Services:

- External network penetration testing
- Web application penetration testing
- Network Security Assessment
- Physical Security assessment
- Social Engineering

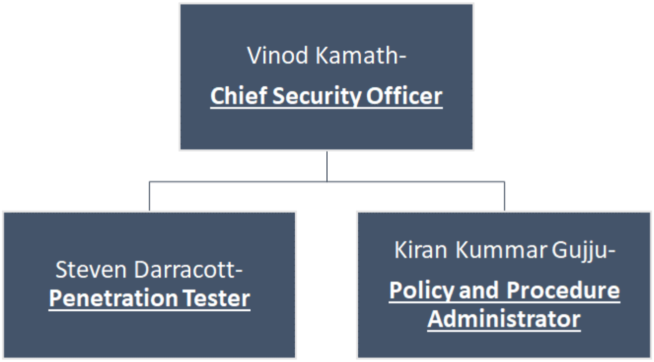
• Participated in investigations for problematic activity, designed and executed vulnerability assessments, penetration tests, and security audits.	
Key Actions and outcome: Separation of Development, Testing & Operational Environments, Secure Coding Requirements, Configuration of Endpoints, Encryption of Endpoints, Protection Against Malware, Controls Against Malware, Cryptography Procedures, IT Asset Inventory Management, Backup Procedure Requirements, Network Segregation Procedures	**Deliverables:** TSCTI completed the multi-phase security assessment within 50 continuous business days and provided the following deliverables to the City of Dallas: • Executive Summary Report • Technical Report • Findings Presentation • Remediation Roadmap • Ongoing support for remediation efforts.

Key Personnel

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

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

We have a well-documented team management methodology to structure the engagement and meet the Lottery's requirements. To support the Lottery's requirement for Network Penetration Testing and Cybersecurity Assessment services, the following highly qualified and excellent experienced team members will be available immediately after the award of the contract and perform the Task stated in this Section 4- Mandatory Requirements. All are highly experienced (min 10+ experience) and have extensive experience to execute these types of similar services. The ***following fig (Shown above)*** lists the name, title, and experience of the Project Team who will be assigned (upon receiving approval from Lottery) to the Lottery's contract;



Vinod Kamath-
Chief Security Officer

Steven Darracott-
Penetration Tester

Kiran Kummar Gujju-
Policy and Procedure Administrator

The majority of tasks will be assigned to TSCTI's proposed team under the leadership of ***CSO- Vinod Kamath (PMP, CISSP Certified)***. By delegating these responsibilities, each team member can contribute their expertise and ensure a comprehensive approach to information security and compliance within the project. This division of responsibilities allows for efficient collaboration and effective execution of tasks, ultimately leading to the successful achievement of project objectives. The team is given an authority to speak for the company on policy and contractual matters and been working on the similar contracts for 10+ years, are familiar with the services required by Lottery. We would conduct formal checkpoint meetings with a larger group of project sponsors and stakeholders, as required for External Network Penetration Testing, Website and Web Application Penetration Testing, and Internal Network Vulnerability Assessment. Additionally, as changes to project scope or deliverables (Executive Summary Report, Technical Report, and Findings Presentation) are required, change control processes would be used to record and monitor the impact to the work plan and/or budget. The foundation for strong project management would be a clearly defined communication channel, which would enable stakeholders to have both the required input as well as visibility into the progress of the project.

Name/Position	Years of Experience and Certifications	Professional Background		
		Client	**Position**	**Duration**
Vinod Kamath- CSO	15+ Years • PMP Certified • ***Certified Information Systems Security Professional (CISSP)*** • Member: International IS Systems Security Certification Consortium (ISC)2	22nd Century Technologies, Inc.	Chief Security Officer (CSO)	Feb 2014 – Present
		InCadence Strategic Solutions	Administrative Program Manager	Oct 2012 – Jun 2014
		Telefocus Communications	Lynchval Systems Worldwide, Inc.	Mar 2011- Oct 2012
		Systems Planning and Analysis, Inc.,	Technical Lead	Sep 2001 – Mar 2011
		Lucent Technologies	Lucent Technologies	Mar 2000 – Mar 2001

	Top Secret Security Clearance			
Steven Darracott-Penetration Tester	12+ years • GIAC GYPC • Offensive Security OSCE • GIAC GAWN • Offensive Security OSCP • Offensive Security OSWP	**Client**	**Position**	**Duration**
		22nd Century Technologies, Inc. (Amazon Web Services)	Information Security Consultant	April 2020 – Present
		Optiv Security	Senior Information Security Officer	Jan 2015 – April 2020
		TrustWave	SOC Firewall Security Analyst	Oct 2014 – Jan 2015
		US Air Force	Staff Sergeant	Dec 2007 – Sep 2014
Kiran Kummar Gujju-Policy and Procedure Administrator	15+ years • ISO 27001:2005 • CEH v6 • ITIL • CCNA • CISSP • MCSE • MCDBA • Prince 2 Foundation and Practitioner • MCP	**Client**	**Position**	**Duration**
		22nd Century Technologies, Inc. (Delviom LLC)	Policy and Procedure Administrator	Oct 2019 – Present
		USDA (United State Department of Agriculture)	Security Engineering and Architect	Nov 2017– Sep 2019
		T-Mobile	Senior Cyber Security Architect	2017 - 2017
		Unisys	Cyber-security Program: EPS, Data Security, Network Security, Mobility	2014–2017
		Mphasis	Senior Project Management Lead	2008–2014
		Symantec	IT Analyst	2006-2008
		VCustomer (Linksys a Cisco Proprietary)	Team Lead	2004-2006

Description of the experience and professional background of corporate officers

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

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

We appreciate the comprehensive guidelines outlined in section 3.4, emphasizing the importance of certifications for vendor staff performing information technology cybersecurity assessments. In alignment with these requirements, we are pleased to introduce our proposed team for the engagement.

VINOD M. KAMATH/ CHIEF SECURITY OFFICER

Summary

Accomplished, resourceful and result-oriented professional with extensive experience of 18 years in **IT Security for Network Penetration Testing and Cybersecurity Assessment projects**, Program Management and contract administration. Proficient with Software and Systems Engineering for large, complex business and government/military projects. Proficient in CMMI level 3 practices, PMP certified and Certified Information Systems Security Professional. He has expertise with modeling processes, preparing data for analysis, clarifying business requirements and human resource planning related to project staff. Experienced in managing and the administrative and daily operations and ensuring projects are delivered on-time, within scope and within budget. Skilled in handling related to invoices and contract administration. Expert and has solid experience with providing technical and coordination and leadership in the execution of day-to-day program/project activities and objectives. Skilled in developing, reviewing, and improving administrative systems, policies, and procedures. Solid experienced with government contracts while ensuring contract work is performed efficiently, accurately, on time, and in compliance with the contract requirements.

Education & Certification

- Master of Science, Computer Science, University of Baltimore, MD
- Bachelor of Engineering, Chemical Engineering, Mysore University
- Information Systems Security Professional (CISSP)
- Project Management Professional, since 2017 ID: [redacted]
- Member: International IS Systems Security Certification Consortium (ISC)2
- Top Secret Security Clearance

Relevant Experience

Client Name	USDA/ DISA/FBI
Position	Administrative Program Manager
Duration	Jun 2014 – Present

Responsibilities:

- Management of various security focused projects across a large complex organization, including facilitating the planning and the prioritization of complex IT Security CRA services.
- Work directly with partners, staff, and stakeholders to ensure project success.
- Responsible for managing and planning staff for the project and reporting staff performance.
- Coordinate with stakeholders and departments to ensure successful project rollout, communications and adoption.
- Complete on-site security risk assessments in multiple office locations throughout the United States as part of a comprehensive project to ensure optimal preparedness for cyber-attacks.
- Planning and managing the delivery of InfoSec roadmap projects and initiatives
- Proactively identify risks and issues on projects - leading team to develop risk management and issues management plans
- Managing high-profile, fast-paced IT Security programs and supporting establishing (Cyber) Identity Programme for Group
- Manages and oversees the administrative and daily operations and ensures all projects are delivered on-time, within scope and within budget.
- Responsible for all issues pertaining to contract administration for the subject contract and for the submission of all work function task orders and invoices.
- Provide remote troubleshoot as necessary when suspected cyber-attacks occurred to ensure that all essential data was secure
- Oversee the supervision of personnel, including work allocation, training, enforcement of internal procedures and controls, and problem resolution; evaluates performance and recommendations for personnel actions and performance.
- Technical lead for obtaining Authority to Operate (ATO), using Risk Vision for FBI Infragard portal hosted on Amazon Web Services (AWS). Responsible for app/system security. Continually performed reviews to ensure compliance with InfoSec directives. Stayed up-to-date with latest vulnerabilities to proactively mitigate new threats. Worked with IA team for POA&Ms.
- TSCTI lead for Department of Defense (Pentagon)'s system for Headquarters Air Force (HAF)/Air Force Information Management and Publishing Tool (AFIMPT), Back office (BO) portal and Warehouse Management System (WMS), including 508 Compliance.
- Responsible for ensuring contract work is performed efficiently, accurately, on time, and in compliance with the contract requirements.
- Providing technical and/or professional coordination and leadership in the execution of day-to-day program/project activities, as appropriate to program objectives and area of expertise.
- Participates in the development of annual operating budgets and provides fiscal direction to the unit.
- Responsible for working on 2 projects of migrating the user permissions from 15,000 sites in SharePoint 2003, 2010 portal servers to SharePoint 2013 farms, using CSOM web services and designing the data model for SQL server 2012 for the project with both SSIS and SSRS. This achievement saved client from slow and complex error prone manual operations and finished the migration job 3 month earlier.

Client	**InCadence Strategic Solutions, Manassas, VA**
Position	**Administrative Program Manager**
Duration	**Oct 2012 – Jun 2014**

Responsibilities

- Developing, reviewing, and improving administrative systems, policies, and procedures.

- Oversaw and/or coordinated the collection, compilation, and analysis of CRA activity data; develops, writes, and presents comprehensive statistical and narrative Assessment reports.
- Developed and responsible for implementation of policies and procedures consistent with those of the organization to ensure efficient operation of the program/project.
- Delivered complete analysis of software components in .NET platform –WCF, AngularJS scripts, as related to deployment of MARS and BAT, including third party software, plug-ins, etc. The source control was using Team Foundation Server (TFS) 11.0
- Supervising day-to-day operations of the administrative department and staff members.
- In charge of Application security and development STIG by scanning software using HP FORTIFY. Developed custom reports and templates.
- Facilitated with accreditation of system image by ensuring the software running on accredited federal network meets STIG requirements.
- Ensured all projects are delivered on-time, within scope and within budget and as per compliance set.
- Assisted with weekly vulnerability scans to assess the security posture of computer systems.
- Developed components using Visual Studio 2012 and .NET frame work 4.0 and 4.5
- Worked with InstallShield for development of installation of modules.
- Reviewed, evaluated the design and operational effectiveness of security controls and countermeasures used to protect organizational applications, services and solutions.
- Ensured the development of security architecture artifacts and deliverables (models, templates, standards and procedures) that can leverage by other organizational project & operations teams.

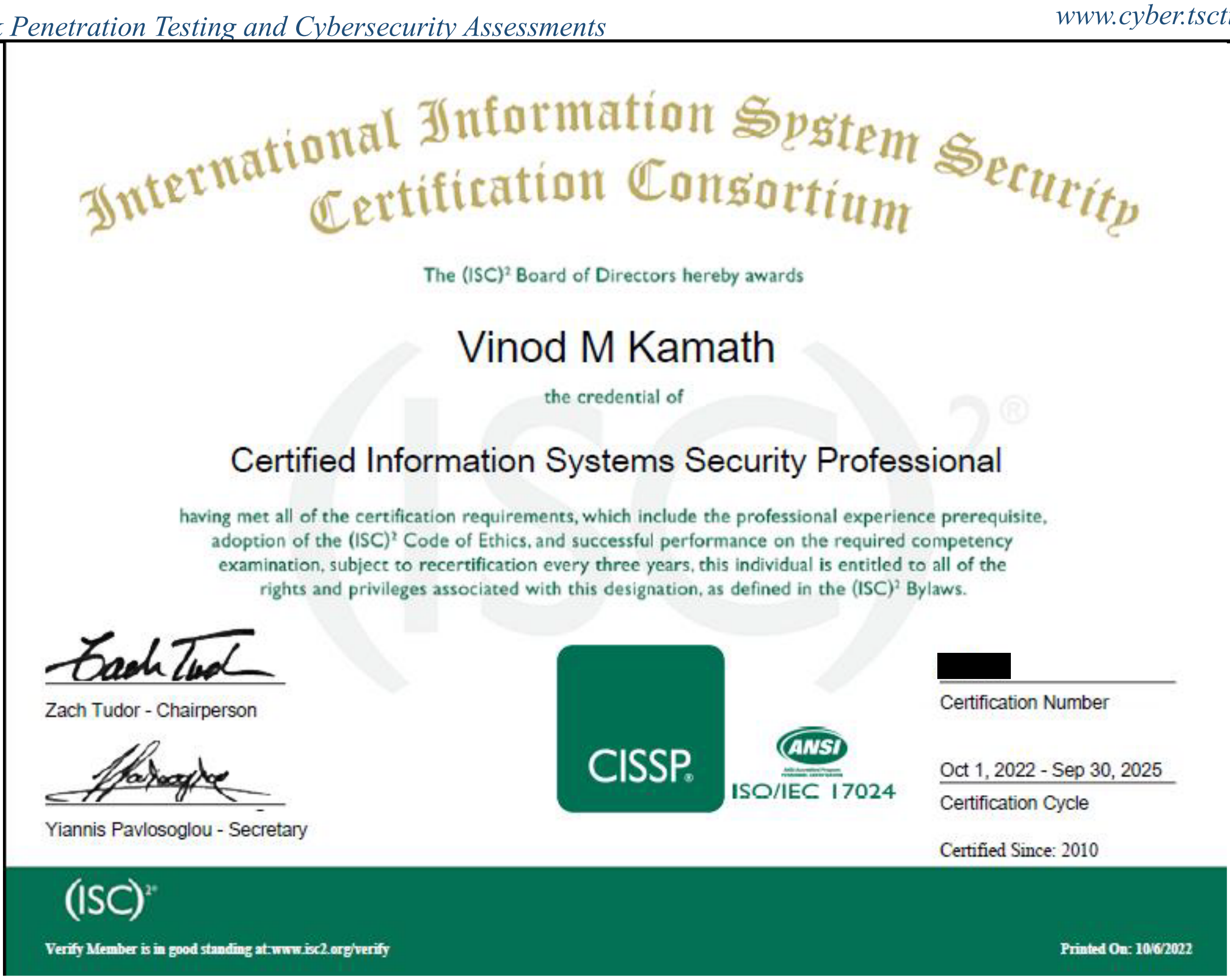
Client	**Lynchval Systems Worldwide, Inc. in Chantilly, VA**
Position	**Program Manager/ Technical Lead**
Duration	**Mar 2011 – Oct 2012**

Responsibilities

- Developed and maintained a project delivery schedule/Gantt chart and projected project activations.
- Ensured all projects are delivered on-time, within scope and within budget.
- Single point of contact for communication between all project stakeholders, including internal teams and clients.
- Delivered multiple releases of the software (developed on .NET platform), on time and within budget requiring implementation of new functionality, improving efficiency and code review, interacting with actuaries.
- Worked with IA in terms of creating POAM, analyzing logs from Intrusion Prevention System (similar to Security Information and Even Event Management SIEM tools using HP ArcSight)
- Experienced in Information Technology Life Cycle Methodology (ITSLCM), including development of technical specifications, plans, procedures and security in accordance with NIST 800-53.
- Implemented methodology for testing of IPVFB in Continuity of Operations (COOP) plan.
- Worked with IA staff to update System Security Plan (SSP).
- In charge of Operation and Maintenance of the software including: Development, Quality Assurance, Integrated Technical Control and Production environments. All the software was developed in Visual Studio .NET environment.

Other Professional Experience

Client Name	Position	Duration
Systems Planning and Analysis, Inc., VA	Technical Lead	Sep 2001 – Mar 2011
Lucent Technologies, NJ	Software Engineer	Mar 2000 – Mar 2001



International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Vinod M Kamath

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.

Zach Tudor - Chairperson

Yiannis Pavlosoglou - Secretary

CISSP.

ANSI ISO/IEC 17024

[redacted]
Certification Number

Oct 1, 2022 - Sep 30, 2025
Certification Cycle

Certified Since: 2010

(ISC)²

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

Printed On: 10/6/2022

Steven Darracott – Penetration Tester

Brief Profile

Possess over **12 years of expertise** as Senior Penetration Tester. Responsible for creating wireless testing strategy and methodology for wireless assessments of products, facilities, and events. Experience in identifying security vulnerabilities and reverse engineering IoT and embedded devices. Immense expertise in conducting Red Team and Adversary Simulations, conducting Penetration Tests and Vulnerability Assessments against Perimeter/Internal networks, Web Applications, and Firewalls. Hands-on experience in conducting Wireless Security Assessments, developing and performing on-site and remote Social Engineering scenarios. Additionally, under general supervision, assists in analyzing, planning, implementing, maintaining, troubleshooting and enhancing large complex systems or networks consisting of a combination that may include mainframes, mini-computers, personal computers, mobile devices, LANS, WANs, servers, data storage and the physical and logical components that integrate these systems together as an enterprise networking backbone. An excellent understanding of technology infrastructures using Firewalls, VPN, Data Loss Prevention, IDS/IPS, Web-Proxy, and Security Audits. Comfortable working with a variety of technologies, security problems, and troubleshooting of the network, data centers, cyber cells, etc.

Education & Certifications

- GIAC GYPC
- Offensive Security OSCE
- GIAC GAWN
- Offensive Security OSCP
- Offensive Security OSWP

Relevant Professional Experience

22nd Century Technologies, Inc./ West Virginia, April 2020 – Present
Penetration Tester
Responsibilities:

- Senior Security Engineer on Wireless Security Evaluations team. Created wireless testing strategy and methodology for wireless assessments of products, facilities, and events.
- Engineered remote wireless testing platform to perform evaluations worldwide during global pandemic.
- Experience identifying security vulnerabilities and reverse engineering IoT and embedded devices.

- Engineering experience solving problems with C/C++, C#, Python, and BASH.

Optiv Security, Jan 2015 – April 2020
Senior Security Consultant
Responsibilities:

- Senior Security Consultant on the Attack & Penetration Team.
- Experience conducting Red Team and Adversary Simulations.
- Experience conducting Penetration Tests and Vulnerability Assessments against Perimeter/Internal networks, Web Applications, and Firewalls.
- Experience conducting Wireless Security Assessments.
- Experience Developing and Performing on-site and remote Social Engineering scenarios.
- Experienced with Burp Suite Pro, Nessus, NMAP, Metasploit, Cobalt Strike, and Kali Linux.
- Programming experience with C/C++, C#, Python, and BASH.
- Strong communication skills and ability to work with customers directly.

TrustWave, Oct 2014 – Jan 2015
SOC Firewall Security Analyst
Responsibilities:

- Remotely managed and monitored firewalls, web proxies, VPNs, and spam filters
- Developed understanding of several command-line tools including tcpdump, vi, curl, wget, and tail on multiple operating systems
- Became proficient with several different firewalls including Juniper, ASA, Proventia, and Palo Alto.

Military Experience, Dec 2007 – Sep 2014
Staff Sergeant – US Air Force
Responsibilities:

- Troubleshot desktop & local area network issues
- Administered hardware, software & network diagnostic repairs
- Installed & configured applications system upgrades
- Organized, created, maintained & validated user & organizational accounts
- Implemented and enforced information protection standards
- Coordinated local IT service requests
- Provided technical solutions & schedule voice equipment installations
- Oversaw system diagnostics and computer system repairs
- Performed initial disk drive formatting & partitioning

Kiran K. Gujju- Infrastructure Information Security Specialist

Brief Profile

Senior Cybersecurity focused resource, possessing **15 years' experience** in the space of Cyber Application Security, Data Security, Threat Detection, SIEM, Compromise Assessment, Risk Assessment and Management, Enterprise IT Strategy and Design, Vendor Management coupled with Endpoint Security solutions program implementation, Penetration Testing, Network Vulnerability Assessments, Data Backup Review, Internal and External Control Reviews, Documentation of the readings and findings, Preparing recommendations for IT security based on the analysis made out of the tests and assessments conducted. Focused on building security and compliance programs by developing and delivering strategic, risk-based security and technology strategy implementation initiatives, to protect corporate assets. Ability to step into an uncontrolled space and bring security structure. Ability to consult internally with Sr. Engineers to apply security principles and best practices that meet business objectives. Excellent leadership and presentation capabilities.

Education & Certifications

- MBA, Certification in Business Basics
- BCA, Roland Institute of Technology
- ISO 27001:2005
- CISSP
- CEH v6
- ITIL
- SOX Training
- CCNA
- MCSE
- MCDBA
- Prince 2 Foundation and Practitioner

- MCP

Relevant Professional Experience

22nd Century Technologies, Inc./ West Virginia, April 2017 – Present
Cyber Security Architect
Roles and Responsibilities:

- Maintaining Palo Alto firewall rule sets, responding to firewall tickets, Creating the appropriate NAT rules to permit routing, inventorying all layer3/4 devices and making sure management information is captured to be used in the firewall orchestration tool (Tufin), WAF rules front-end several critical applications.
- The primary solution is Imperva SecureSphere, adjusting the learning profiles and responding to alerts within that system will be a regular responsibility, F5's ASM is a lesser used WAF but the same responsibilities will be required on that platform, and other duties as assigned by manager.
- Provide expert guidance to developers on the appropriate selection and implementation of relevant security controls
- Design, develop and deliver presentations focused on raising awareness for crucial security relevant considerations and defensive programming techniques.
- Support the planning and execution of the application security testing and evaluation program with possibility to mentor junior team members.
- Advise and consult internal clients on appropriate application of security practices and existing security services to solve problems or enable new business opportunities. Research and implement new security technologies to be used as point solutions for IT initiatives unable to take advantage of or needing greater functionality than reusable enterprise security services.
- Review, triage, and prioritize control output. Recommend actions to resolve identified security discrepancies.
- Recommend new security service development ideas based on accumulated knowledge of project-specific security requirements. Identify and implement improvements to application security team processes and supporting software tools to continually improve the team's effectiveness and efficiency.
- Assist with adherence to technology policies and comply with all security controls. Ensure all work products meets /exceeds Worldpay standards.

USDA (United State Department of Agriculture), Nov 2017– Sep 2019
Cyber Security SEA (Security Engineering and Architect)
Roles and Responsibilities:

- Support the delivery and maintenance of agency Enterprise Security Services (such as but not limited to) Web Application Firewall (WAF), Enterprise Data Masking and Scrubbing, Application Audit Logging, Service Oriented Architecture (SOA) Security, Cyber Analytics, Role-Based Access Control (RBAC)
- Vulnerability scanning following the SDLC guidelines and process.
- Provide support and document artifacts during: Solution Pre-Select support, Security Requirements Analysis, and Integrated Security Architecture and Design.
- Configure networks hosts, cloud environments, and software to operate securely
- Evaluate current system security measures and recommend enhancements that serve to strengthen and ensure compliance with all federal security requirements
- Conduct analysis of alternatives (AoA) for technology acquisitions that support new requirements
- Support the creation of new (or edit existing) documentation required for the Authority to Operate (ATO) packages to include the system security plans (SSP) and IS contingency plans
- Use tools and techniques to collaborate with software development teams to ensure that federal security standards, NIST and other security frameworks are being implemented and used when developing and testing the software
- Attend meetings concerning security architecture, security review, stage gates and others as required
- Document and track risks, issues, and action items as identified in meetings.
- Support other team members with their duties to include app and network vulnerability scanning
- Project – Enterprise Vulnerability Management:
    - Implementation and use of Sonar Cube for initial debugging in CI in integration environment
    - Implementation of Fortify (SAST and DAST solution) and use it in cert, scan and deployment environment.
    - Follow the VA process of providing feedback to developer and PM and getting memo from leadership prior to deployment.
- Project – Data Masking
    - Work closely with privacy office in defining data classification, policies and process.
    - Policies to be complaint to GDPR, PCIDSS and federal privacy requirements.
    - Incorporate the privacy policies in data discovery and masking tool.
    - Incorporate the privacy policies in the DLP tool.
    - Conduct data discovery on databases and file systems
        - Perform masking of PII and sensitive data prior the data is accessible in lower environments.
- Project – Web Application Firewall

  - Implement and maintain the firewall
  - Inspect the traffic to the web applications
  - Tuning and maintaining the firewall rules and policies
  - Capture, document and report identified or suspected security, privacy and confidentially incidents
  - Tune the traffic on F5 and cisco L2 switch to limit to http and https traffic.
- Project – Cyber Analytics
  - Implementation of Qradar on prem
  - Install and integrate the sensors, Watson.
  - Collect event logs and perform tune Qradar to generate reports and sensible analysis report
  - Perform analysis and threat hunting

Operational Roles Include:

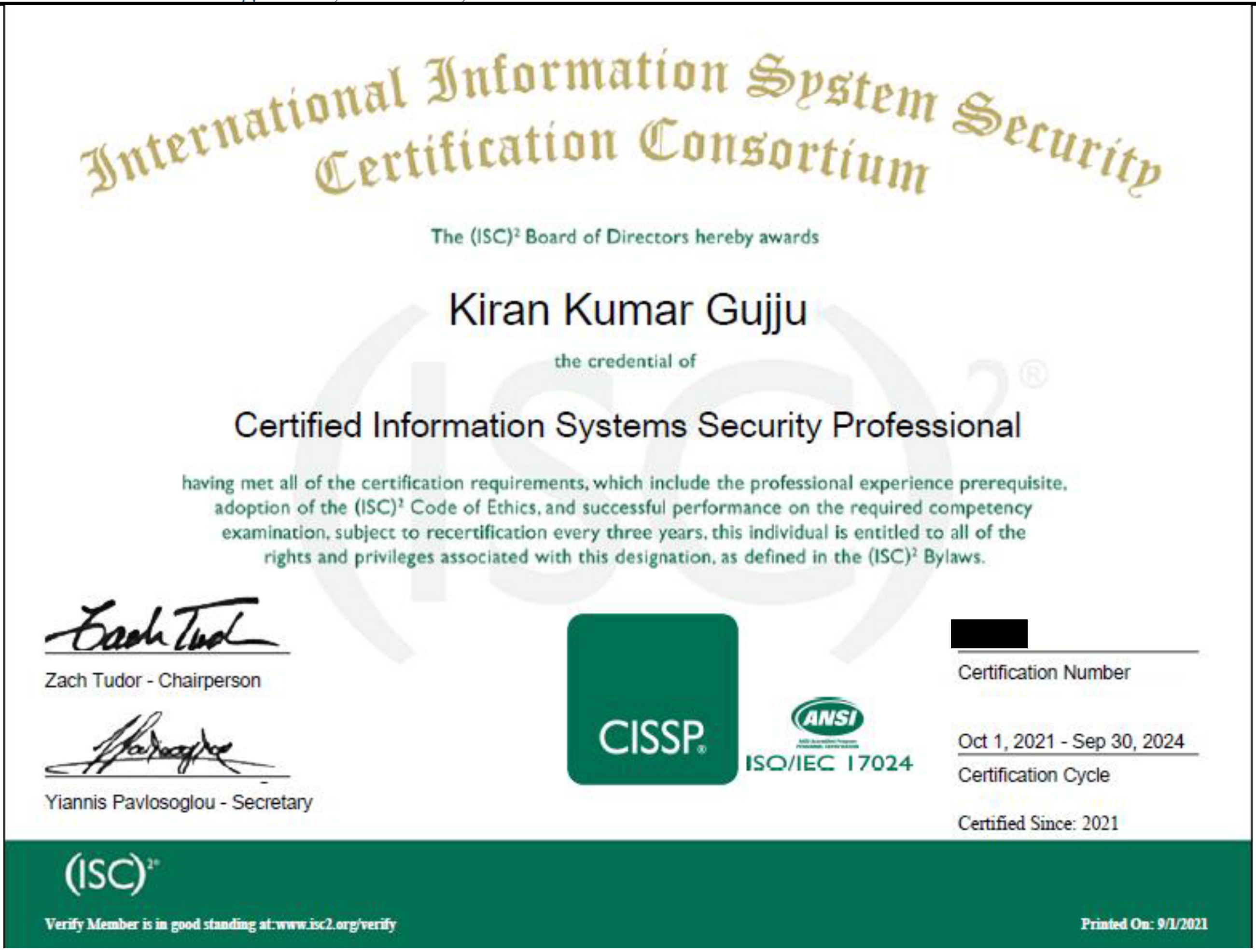
- PII and Sensitive data discovery and masking/scrubbing
- Vulnerability Management
  - SAST based VA analysis
  - DAST based VA analysis
  - Source Code Analysis
- Web Application Firewall monitoring and analysis
  - Network packet Analysis
- Threat Modeling
- Incident Response
- Change and Problem Management

Projects Implemented:

- Enterprise Vulnerability Assessment (DAST): Successfully designed and built a new EVA Architecture in USDA private cloud infrastructure. The infrastructure is very efficient in performing multiple DAST scans.
- Automation of Enterprise Vulnerability Assessment (SAST): Implementation of Appscan Automation with Jenkins is in progress.
- Data Masking: Design and implementation of Data Guise infrastructure. Phase 1 is complete.
  - Phase 1: Scanning of databases. Identification and reporting of sensitive data.
  - Phase 2: Scanning of file systems
  - Phase 3: Data Masking
- SIEM: Implementation of Qradar and integration with network entities.
  - Analyzing the reports and co-relating them to identify threats.
- WAF: Successfully completed the following activities.
  - Planning, Designing and Procurement
  - Implement the appliance in NRCS private cloud
  - Configure SecureSphere policies
  - Adding web services and profiling
  - Configure x-forwarded-for in F5 LB
  - Fixing F5 issues with SecureSphere like OneConnect and sticky sessions
- Designed WAF for applications on AWS and Azure
- WAF integration with Qradar and WAF Phase 2 implementation in progress

Prior Experience

Client	Position	Duration
T-Mobile	Senior Cyber Security Architect	2017 - 2017
Unisys	Tower Lead (Cyber-security Program: EPS, Data Security, Network Security, Mobility)	2014–2017
Mphasis	Senior Project Management Lead	2008–2014
Symantec	IT Analyst	2006-2008
VCustomer (Linksys a Cisco Proprietary)	Team Lead	2004-2006



International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Kiran Kumar Gujju

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.

Zach Tudor - Chairperson

Yiannis Pavlosoglou - Secretary

CISSP®

ANSI

ISO/IEC 17024

[redacted]

Certification Number

Oct 1, 2021 - Sep 30, 2024

Certification Cycle

Certified Since: 2021

(ISC)²®

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

Printed On: 9/1/2021

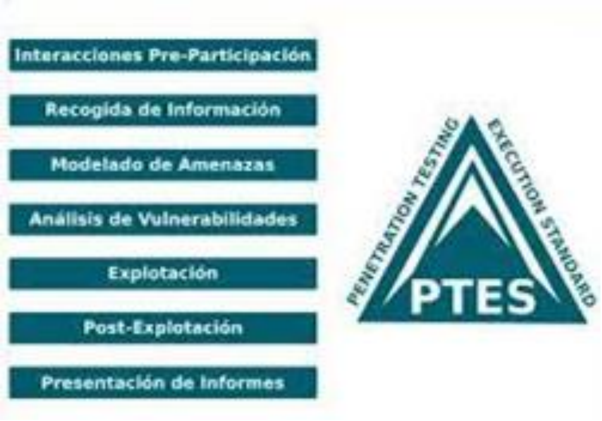
Technical Approach

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

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

TSCTI's proposed solution ensures strict adherence to industry standards and compliance, specifically the Penetration Testing Execution Standard (PTES). We will adopt a well-documented methodology that aligns with the three-phased structure outlined in the Mandatory Contract Services Requirements. This methodology covers enumeration, vulnerability assessment, and exploitation in the External Network Penetration Testing, Website and Web Application Penetration Testing, and Internal Network Vulnerability Assessments.

To demonstrate compliance, below TSCTI provides comprehensive documentation with a case study with various clients- of the industry standard, PTES, and the testing methodology leveraged.



Client	Services Required	Solution Provided	Results
State of West Virginia	The State of West Virginia sought a robust cybersecurity assessment to fortify its digital infrastructure. Key objectives included identifying vulnerabilities, prioritizing remediation needs, and ensuring compliance with industry standards, particularly the Penetration Testing Execution Standard (PTES).	TSCTI proposed a meticulous three-phased structure methodology aligned with PTES guidelines. The External Network Penetration Testing focused on enumeration, vulnerability assessment, and exploitation, incorporating social engineering exercises and explicit approval for heavy load attacks. The Website and Web Application Penetration Testing adopted PTES principles, covering enumeration, vulnerability assessment, exploitation, and including Denial of Service (DOS) attacks. For Internal Network Vulnerability Assessments, a comprehensive three-phased structure methodology per PTES was employed, assessing all networked assets across government offices.	Comprehensive documentation demonstrating PTES compliance was provided to the State of West Virginia. The detailed breakdown of the three-phased structure methodology for each assessment type showcased adherence to industry standards. The State's cybersecurity posture was significantly strengthened, with identified vulnerabilities addressed promptly. TSCTI's commitment to PTES principles ensured consistency, thoroughness, and effective risk mitigation.
West Virginia University	West Virginia University faced evolving cybersecurity threats and gotten a proactive approach to assess and fortify its information systems. Compliance with industry standards, particularly PTES, was a priority.	TSCTI implemented a tailored methodology based on PTES guidelines for each assessment. External Network Penetration Testing included enumeration, vulnerability assessment, and exploitation, with social engineering exercises. Website and Web Application Penetration Testing adhered to PTES, covering all specified phases and incorporating DOS attacks. Internal Network Vulnerability Assessments, aligned with PTES, ensured a comprehensive evaluation of networked assets across campuses.	Documentation showcasing PTES compliance and a detailed breakdown of the methodology were provided to West Virginia University. The university's information systems were fortified against potential threats, and vulnerabilities identified through PTES-aligned assessments were promptly addressed. TSCTI's approach not only met industry standards but also exceeded the university's expectations for a robust cybersecurity posture.
Denver County, Colorado	Denver County faced the imperative to enhance its cybersecurity resilience amid growing cyber threats. Compliance with PTES and a thorough understanding of its methodology were paramount.	TSCTI employed a PTES-aligned methodology for External Network Penetration Testing, Website and Web Application Penetration Testing, and Internal Network Vulnerability	Denver County received comprehensive documentation demonstrating PTES compliance and a detailed methodology breakdown. The assessments

		Assessments. The documentation provided showcased a meticulous breakdown of each assessment type, emphasizing PTES principles. Denver County's assessments included social engineering exercises, DOS attacks, and comprehensive internal network evaluations.	identified vulnerabilities and provided prioritized remediation needs. TSCTI's commitment to industry standards, specifically PTES, empowered Denver County with a resilient cybersecurity framework.
Ohio Turnpike and Infrastructure Commission	The Commission faced increasing cyber threats and sought a partner to conduct comprehensive cybersecurity assessments. Compliance with industry standards, specifically PTES, was crucial.	TSCTI implemented a PTES-focused methodology for External Network Penetration Testing, Website and Web Application Penetration Testing, and Internal Network Vulnerability Assessments. The assessments adhered to PTES guidelines, ensuring a consistent and thorough evaluation. Special attention was given to social engineering exercises, DOS attacks, and a detailed internal network vulnerability assessment.	Comprehensive documentation showcasing PTES compliance and the methodology breakdown was submitted to the Commission. Identified vulnerabilities were addressed, and TSCTI's approach contributed to enhancing the Commission's cybersecurity resilience, aligning with PTES principles.
Maricopa County, Arizona	Maricopa County faced the challenge of fortifying its cybersecurity defenses and sought a partner with expertise in adhering to industry standards, particularly PTES.	TSCTI implemented a PTES-centric methodology for External Network Penetration Testing, Website and Web Application Penetration Testing, and Internal Network Vulnerability Assessments. The assessments adhered to PTES guidelines, encompassing enumeration, vulnerability assessment, exploitation, and social engineering exercises. Special emphasis was placed on DOS attacks and a detailed internal network evaluation.	Comprehensive documentation showcasing PTES compliance and a detailed methodology breakdown were provided to Maricopa County. The assessments identified vulnerabilities, enabling the County to strengthen its cybersecurity posture. TSCTI's commitment to PTES principles contributed to a robust and resilient cybersecurity framework for Maricopa County.

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

At TSCTI, each candidate is required to provide at least three professional references which are cross-checked by the TSCTI screening team. This verifies the candidates' performance, strengths & weaknesses, and the general attitude toward complying with rules & regulations. Also, TSCTI gathers information concerning the candidate's sincerity, integrity, and general reputation about the candidate. TSCTI touches base with the referee telephonically and administers a questionnaire in the specified format. TSCTI will conduct reference checks to:

- Confirm any details on the BGV form (through relationship-neighbor/friend)
- Check for any prior discipline problems;
- Learn new information about a candidate; and
- Ask questions that may predict a candidate's performance, integrity

By conducting all these activities, TSCTI will prepare a pool of qualified consultants for the Lottery. The finest available candidates undergo a rigorous vetting process designed to assess each candidate's work history and performance on the job. We target two to three former employers to investigate start and end dates, past job titles and job descriptions, punctuality/reliability, team relationships, highlights, and concerns. Once a candidate will be interviewed or selected by Lottery, TSCTI will execute the rest of the recruiting phases, which will include Background and Drug Screening, Onboarding and Training, etc.

Drug Screening: An independent third-party certified agency will perform background checks on the selected candidates. The candidate is notified and is required to sign a consent and authorization form as to the procedures outlined in our Background Check Policy. We notify the Client in writing regarding the result of the background checking conducted for a candidate. The candidates successfully cleared the background check to proceed to join Lottery's project. TSCTI's partnered agency has the resources to perform a variety of background checks at a local, Lottery, and state level, including:

- Academic Record Check
- Civil Litigation Check
- Credentials Check
- Criminal Record Check
- Database Check
- Emerging Background Checks
- Employment Eligibility Check
- Identity Check
- Reference Check
- Residence Check
- Social Security verification
- Social Media Check

TSCTI will perform competent background checks (i.e., criminal, employment, education, fingerprint information, driver's license, drug and alcohol, and medical) of all their contracted workers offered for assignment with Lottery. If needed, TSCTI can conduct electronic drug test screening and a 5-panel drug test which will include: Phencyclidine, THC, Opiate, Amphetamine/Methamphetamine, Cocaine, and more. Please note that TSCTI is capable to conduct the 7-panel, 10-panel, or 12-panel drug tests if required by Lottery. TSCTI conducts such drug tests through third-party vendors like Sterling Information Systems, Quest Diagnostics for Drug Test, etc. **Following are the important steps followed in this regard:**

- The candidate is notified and is required to sign a consent and authorization form as to the procedures outlined in the Drug Policy.
- Drug testing consists of the collection of a urine sample from the candidate under the supervision of a clinical laboratory technician.
- Each urine sample is analyzed for the presence of banned drugs by an independent laboratory contracted by TSCTI to provide such services.
- An independent laboratory meeting Lottery requirement for collection, security, screening and transportation, storage, and analysis and certified by the College of American Pathologists, Athletic Drug Testing (CAP-ADT) will test the samples.
- The laboratory reports all test results to TSCTI.
- TSCTI reviews the results to determine which, if any, of the testing, are considered positive as reported by the independent laboratory.
- A positive result is defined as a urine sample revealing the presence of one or more of the banned drugs or metabolites.
- TSCTI notifies Lottery in writing regarding the result of the drug screening conducted for a candidate.

The candidates with negative drug test results proceed to join Lottery.

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

TSCTI has carefully understood the requirements and adhere to comply. TSCTI will sign and provide the signed NDA (Exhibit B) upon receiving the contract award notification. We accept to provide it upon clarification (if applicable).

Cost Proposal

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	$ 1,400.00 -	$ 11,200.00
2	4.2	Website Penetration Testing	8	$ 800.00 -	$ 6,400.00
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 4,900.00 -	$ 39,200.00
4	4.4	Wireless Penetration Testing	8	$ 4,100.00 -	$ 32,800.00
				TOTAL BID AMOUNT	$ 89,600.00

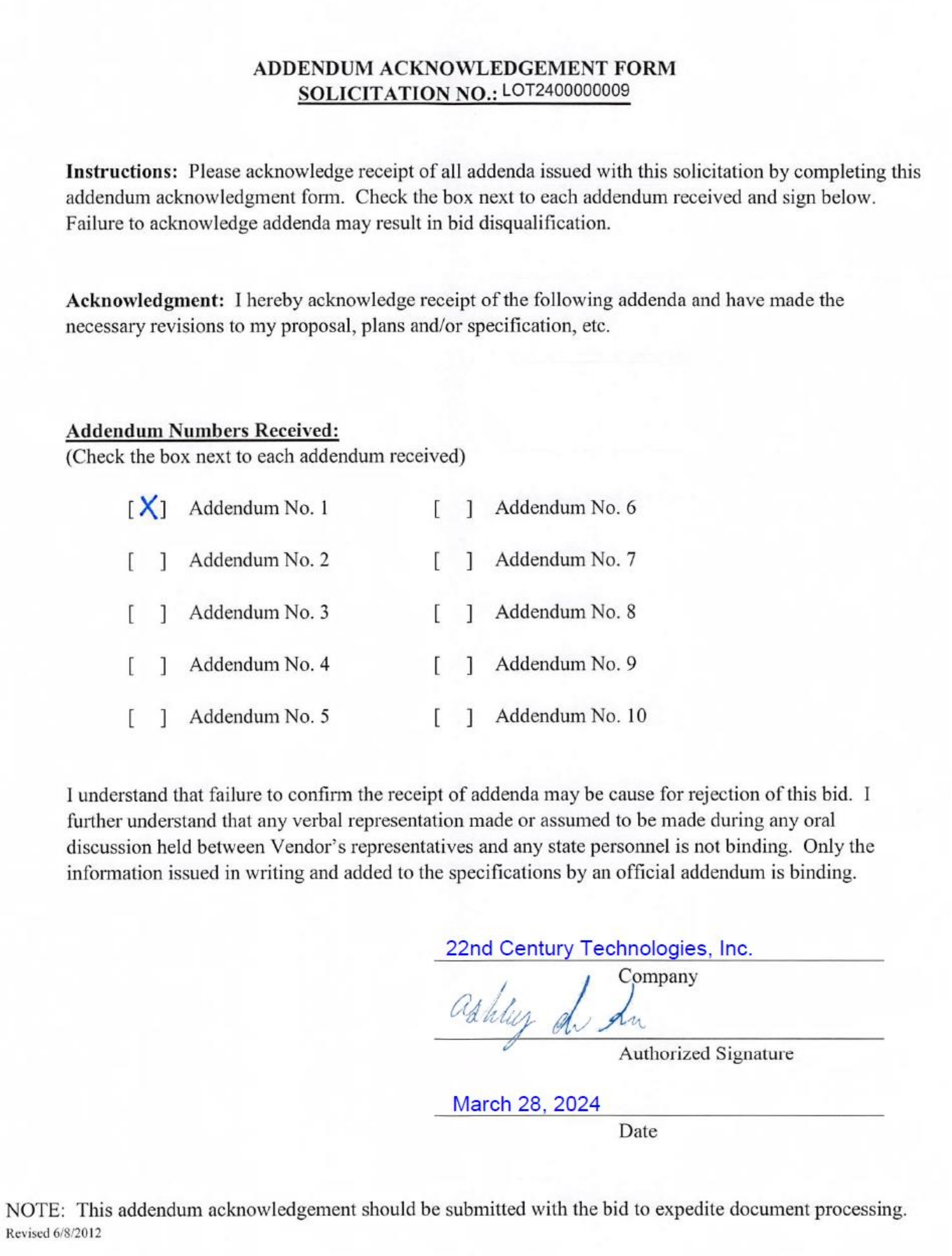
Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

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:	22nd Century Technologies, Inc.
Vendor Address:	8251 Greensboro Drive, Suite 900, McLean, VA 22102
Email Address:	sledproposals@tscti.com
Phone Number:	(866) 537-9191 Ext 2
Fax Number:	732-537-0888
Signature and Date:	March 28, 2024 Ashley



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. 2
[ ] Addendum No. 3
[ ] Addendum No. 4
[ ] Addendum No. 5
[ ] Addendum No. 6
[ ] Addendum No. 7
[ ] Addendum No. 8
[ ] Addendum No. 9
[ ] Addendum No. 10

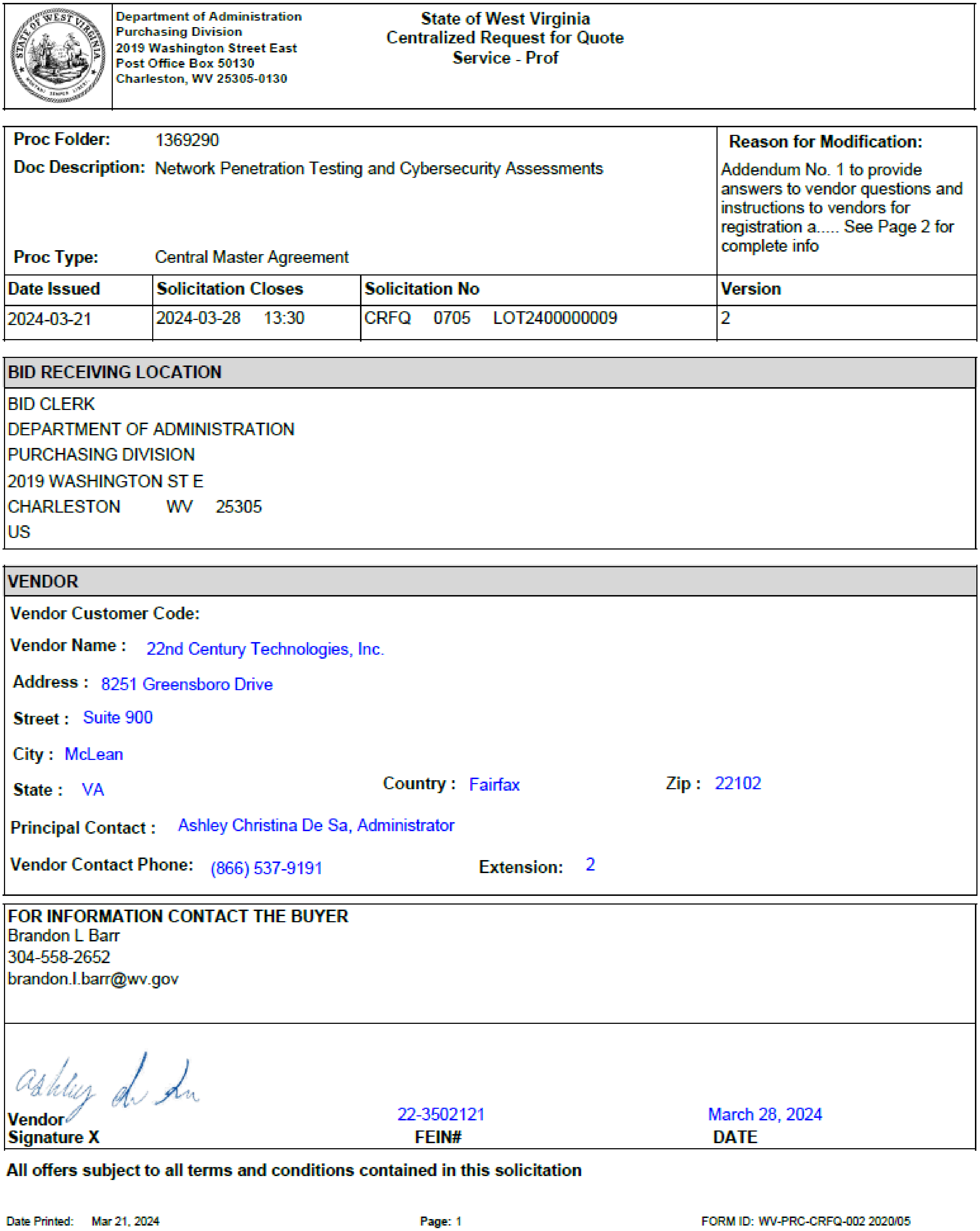
I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information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

22nd Century Technologies, Inc.
Company

Authorized Signature

March 28, 2024
Date

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



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

State of West Virginia
Centralized Request for Quote
Service - Prof

Proc Folder:	1369290		**Reason for Modification:** Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration a..... See Page 2 for complete info
Doc Description:	Network Penetration Testing and Cybersecurity Assessments		
Proc Type:	Central Master Agreement		
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 : 22nd Century Technologies, Inc.

Address : 8251 Greensboro Drive

Street : Suite 900

City : McLean

State : VA **Country :** Fairfax **Zip :** 22102

Principal Contact : Ashley Christina De Sa, Administrator

Vendor Contact Phone: (866) 537-9191 **Extension:** 2

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

ashley de sa

Vendor Signature X 22-3502121 **FEIN#** March 28, 2024 **DATE**

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

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