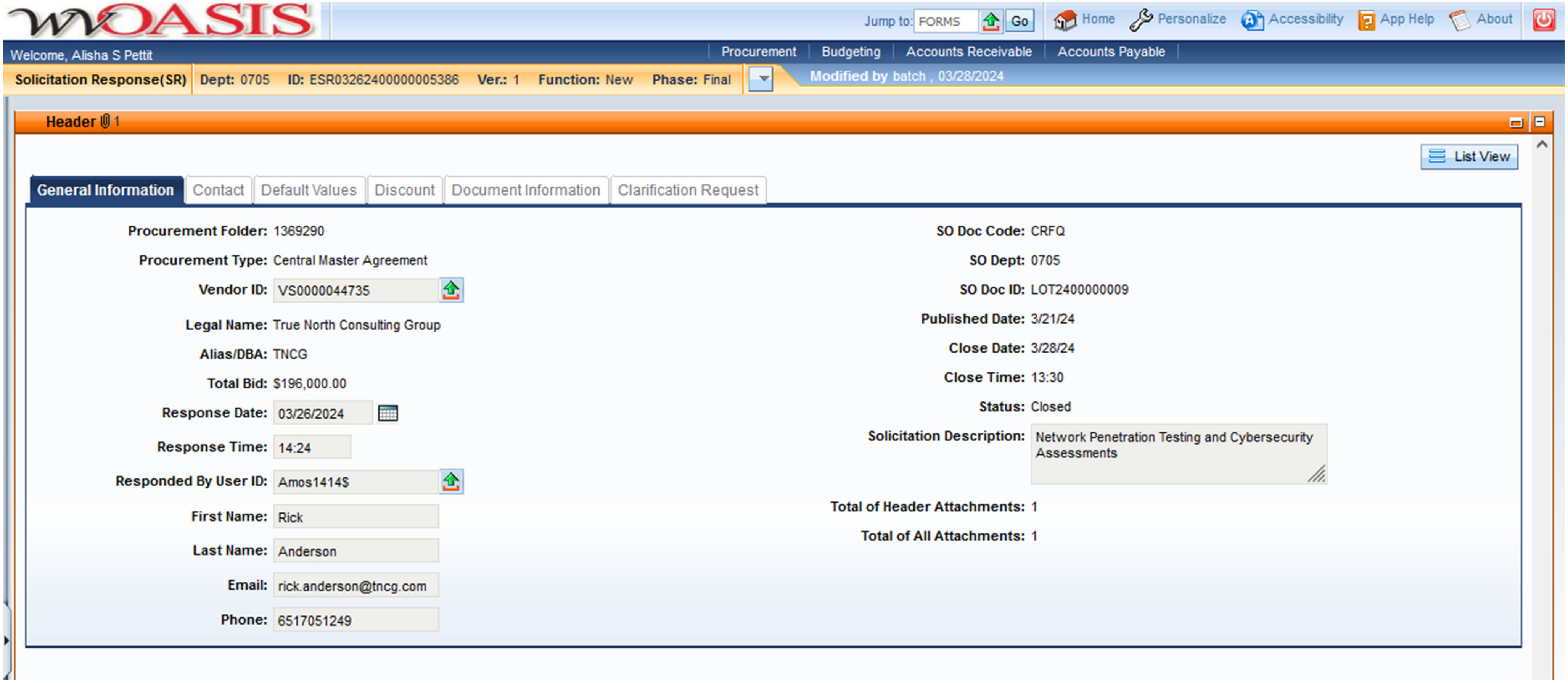
West Virginia Purchasing Division

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: ESR03262400000005386 Ver.: 1 Function: New Phase: Final

Modified by batch , 03/28/2024

Procurement Folder:	1369290	SO Doc Code:	CRFQ
Procurement Type:	Central Master Agreement	SO Dept:	0705
Vendor ID:	VS0000044735	SO Doc ID:	LOT2400000009
Legal Name:	True North Consulting Group	Published Date:	3/21/24
Alias/DBA:	TNCG	Close Date:	3/28/24
Total Bid:	$196,000.00	Close Time:	13:30
Response Date:	03/26/2024	Status:	Closed
Response Time:	14:24	Solicitation Description:	Network Penetration Testing and Cybersecurity Assessments
Responded By User ID:	Amos1414$	Total of Header Attachments:	1
First Name:	Rick	Total of All Attachments:	1
Last Name:	Anderson		
Email:	rick.anderson@tncg.com		
Phone:	6517051249		

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 ESR03262400000005386	1

VENDOR

VS0000044735
True North Consulting Group

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 196000 **Response Date:** 2024-03-26 **Response Time:** 14:24:44

Comments: 1.5% net 15 days from date of completion and sign-off of project by State of West Virginia -Lottery

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				30000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: External Network Penetration Testing as per specs and Addendum 1 based on 8 Assessments at $3,750.00 each. Please see Exhibit A -Pricing Page for NOTE just left of TOTAL BID AMOUNT

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				95000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Website Penetration Testing as per specs and addendum 1 based on 8 assessments at $11,875.00 each. Please see Exhibit A-Pricing Page for NOTE just left of TOTAL BID AMOUNT

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				50000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Internet/Client Side -Network Penetration Testing as per specs and addendum 1 based on 8 assessments at $6,250.00 each. Please see Exhibit A - Pricing Page for NOTE just left of TOTAL BID AMOUNT.

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				21000.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments: Wireless Penetration Testing as per specs and addendum based on 8 assessments at $2,625.00 each. Please see Exhibit A-Pricing Page for NOTE just left of TOTAL BID AMOUNT.

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

QUOTE FOR CONSULTING SERVICES

for

NETWORK PENETRATION TESTING AND CYBERSECURITY ASSESSMENTS

(Solicitation Number: CRFQ 0705 LOT2400000009)

March 25, 2024

PREPARED FOR:

State of West Virginia

PREPARED BY:

Rick Anderson, Senior Cybersecurity Technology Consultant
Dimitrios Hilton, Executive Security Consultant
Sandi Parr, Senior Marketing Coordinator

TRUENORTH

3408 Hillcrest Drive, Waco, TX 76708
888.650.4580 • 512.451.5445 • www.tncg.com

March 25, 2024

Mr. Brandon Barr, Buyer
West Virginia Purchasing Division
2019 Washington Street, East
Charleston, WV 25305
brandon.l.barr@wv.gov

Dear Mr. Barr:

True North Consulting Group, LLC (True North or TNCG) is pleased to have the opportunity to respond to the State of West Virginia's Centralized Request for Quote (CRFQ 0705 LOT2400000009) for Network Penetration Testing and Cybersecurity Assessments. True North understands the requirements outlined in the RFP to include no modifications to the terms and conditions. True North acknowledges Addendum No. 1 dated March 21, 2024.

True North is a security and technology consulting firm. E&A was established in March of 1984. Our firm employs over 150 staff members, operates out of multiple offices, and has served hundreds of government entities throughout the United States. In 2015, True North performed a like assessment for the State of West Virginia that met and/or exceeded expectations.

From risk, vulnerability, and threat assessments to reviewing policies, procedures, people, building modifications, and equipment to design, bid, and implementation, TNCG works with you to develop and implement a comprehensive security program and supporting systems.

True North has partnered with InfoSec Associates, LTD. (InfoSec) to ensure the assessment process's optimum success. TNCG selected InfoSec based on expertise, which aligns with overall expertise as a unified commitment to the State of West Virginia. Our corporate office in Waco, Texas, and our Stillwater, Minnesota office will be involved from a project management perspective and logistics assessment process utilizing our full-time certified security risk and IT consultants to ensure Team TNCG meets/exceeds the State's expectations.

TNCG does not sell or represent any products of any type, nor are we affiliated with any vendors or manufacturers. This neutrality allows our firm to provide an objective, unbiased assessment of your needs and recommend the best available options. **As our client, your best interest is our priority.**

We have submitted our bid electronically through *wv*OASIS. We look forward to working with you and your staff on this project and will be in contact with you soon. If we can be of any assistance in the interim, please feel free to contact Rick Anderson at (651) 705-1249 or rick.anderson@tncg.com.

Sincerely,

Mike Indergard, Director of Strategic Planning
True North Consulting Group, LLC

TABLE OF CONTENTS

Page

SECTION 1: TEAM TNCG'S TECHNICAL OVERVIEW

TEAM TNCG

True North Consulting Group, LLC

True North Consulting Group (True North/TNCG) was founded in conjunction with the Texas Division of Elert & Associates (E&A), a 40-year-old independent technology consulting firm headquartered in Stillwater, MN. In 2018, True North Consulting Group and Elert & Associates merged and became one company – True North Consulting Group. True North now includes a consulting staff of 65+ specialists. True North is based in Texas and has continued to maintain E&A client accounts and serve states nationwide.

OUR PHILOSOPHY:

- Disciplined Professional Service
- Sincere Client Interest
- Security & Technical Excellence
- Proven Concepts
- Holistic Approach to Security

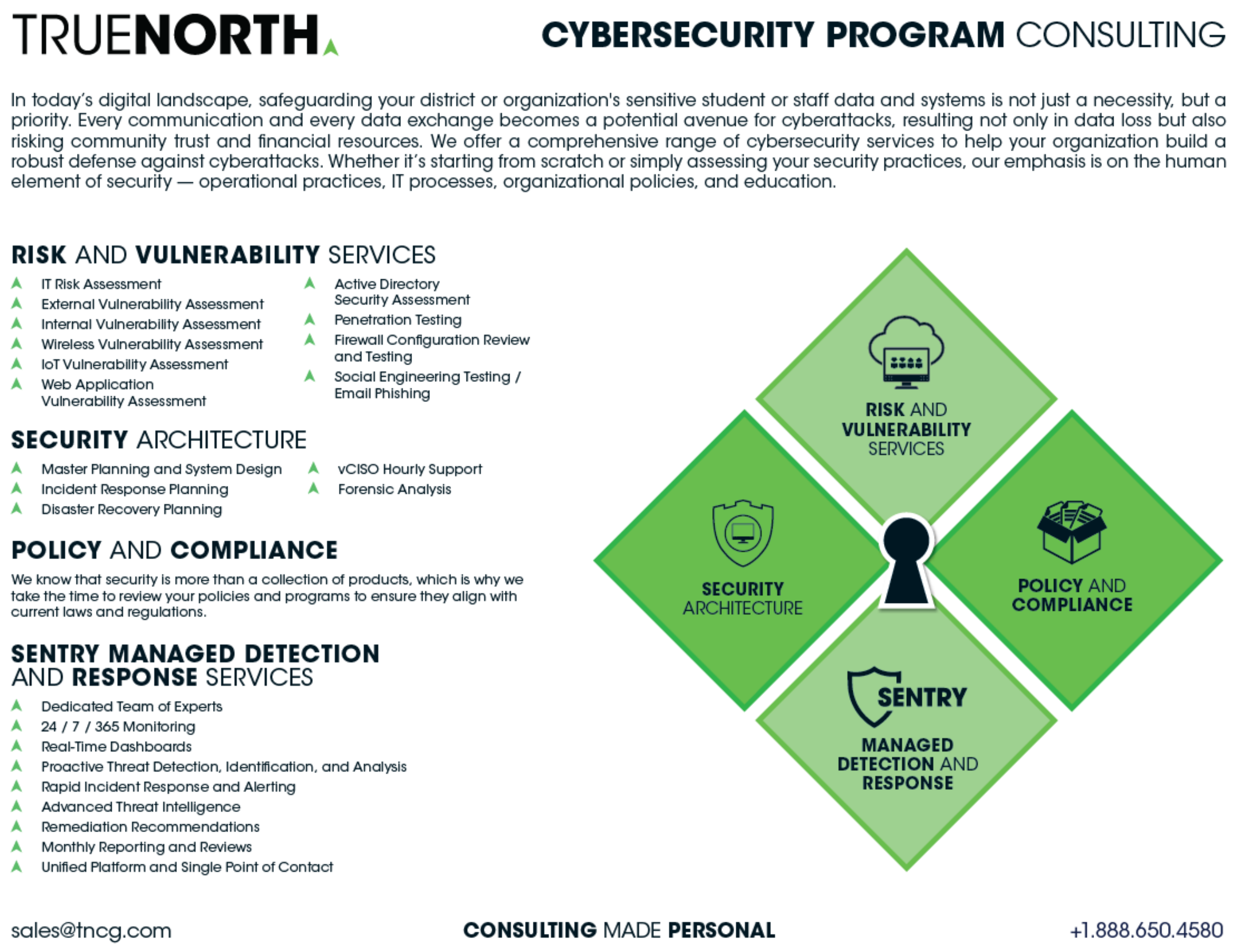
TNCG has assisted over 2,800 public- and private-sector clients by meeting their assessment needs for the past 40 years. Our services include vulnerability assessments, cybersecurity, penetration testing, IT information technology plans, PCI, SCADA compliance, and security program development and planning. Executives are IT industry veterans with technical expertise and extensive experience managing large-scale projects.

Since 1984, TNCG has provided physical security, building intrusion-managed services, assessments of security controls, cybersecurity and technical threat vulnerability assessments, and onsite consulting services. Our findings are meticulously documented in our Assessment Reports.

The primary purpose of True North Consulting Group, LLC is to provide the benefits of experienced, unbiased security and technology consulting. TNCG's philosophy starts with a disciplined professional service process and sincere client interest blended with listening to our client's needs and goals. Combining this philosophy with security and technical excellence, proven concepts, on-time delivery, budget adherence, and team communication dedication produces quality results. From security and technology assessments to design, bid, and implementation, TNCG works with you to develop and implement a comprehensive security program and supporting systems.

True North Consulting Group's authorized representative is:

Name: Mike Indergard
Title: Director of Strategic Planning
Company Name: True North Consulting Group, LLC
Company Address: 3408 Hillcrest Drive, Waco, TX 76708
Phone: (254) 266-6381
Email: mike.indergard@tncg.com



TRUENORTH

CYBERSECURITY PROGRAM CONSULTING

In today's digital landscape, safeguarding your district or organization's sensitive student or staff data and systems is not just a necessity, but a priority. Every communication and every data exchange becomes a potential avenue for cyberattacks, resulting not only in data loss but also risking community trust and financial resources. We offer a comprehensive range of cybersecurity services to help your organization build a robust defense against cyberattacks. Whether it's starting from scratch or simply assessing your security practices, our emphasis is on the human element of security — operational practices, IT processes, organizational policies, and education.

RISK AND VULNERABILITY SERVICES

- IT Risk Assessment
- External Vulnerability Assessment
- Internal Vulnerability Assessment
- Wireless Vulnerability Assessment
- IoT Vulnerability Assessment
- Web Application Vulnerability Assessment
- Active Directory Security Assessment
- Penetration Testing
- Firewall Configuration Review and Testing
- Social Engineering Testing / Email Phishing

SECURITY ARCHITECTURE

- Master Planning and System Design
- Incident Response Planning
- Disaster Recovery Planning
- vCISO Hourly Support
- Forensic Analysis

POLICY AND COMPLIANCE

We know that security is more than a collection of products, which is why we take the time to review your policies and programs to ensure they align with current laws and regulations.

SENTRY MANAGED DETECTION AND RESPONSE SERVICES

- Dedicated Team of Experts
- 24 / 7 / 365 Monitoring
- Real-Time Dashboards
- Proactive Threat Detection, Identification, and Analysis
- Rapid Incident Response and Alerting
- Advanced Threat Intelligence
- Remediation Recommendations
- Monthly Reporting and Reviews
- Unified Platform and Single Point of Contact

RISK AND VULNERABILITY SERVICES
SECURITY ARCHITECTURE
POLICY AND COMPLIANCE
SENTRY
MANAGED DETECTION AND RESPONSE

sales@tncg.com CONSULTING MADE PERSONAL +1.888.650.4580

InfoSec Associates, LTD.

InfoSec Associates is known for its experience and understanding of local government IT and the security of those systems. InfoSec is a nationally respected vCISO for many state agencies, specializing in Security Assessments, Penetration Testing and Cloud Assets, HIPAA, PCI, SCADA, and Incident Response.

InfoSec has been immersed in the Information Technology (IT) field for over 19 years, with a focus on Advanced Information Security. Over the years, InfoSec developed a strong understanding of the relationships between hardware, software, security, and common-sense business considerations, such as cost benefits.

InfoSec has extensive enterprise experience serving as CIO and CISO consultant for many organizations. Strengths include a combination of management and technical skills and an ability to explain things in an easy-to-understand manner.

CERTIFICATIONS

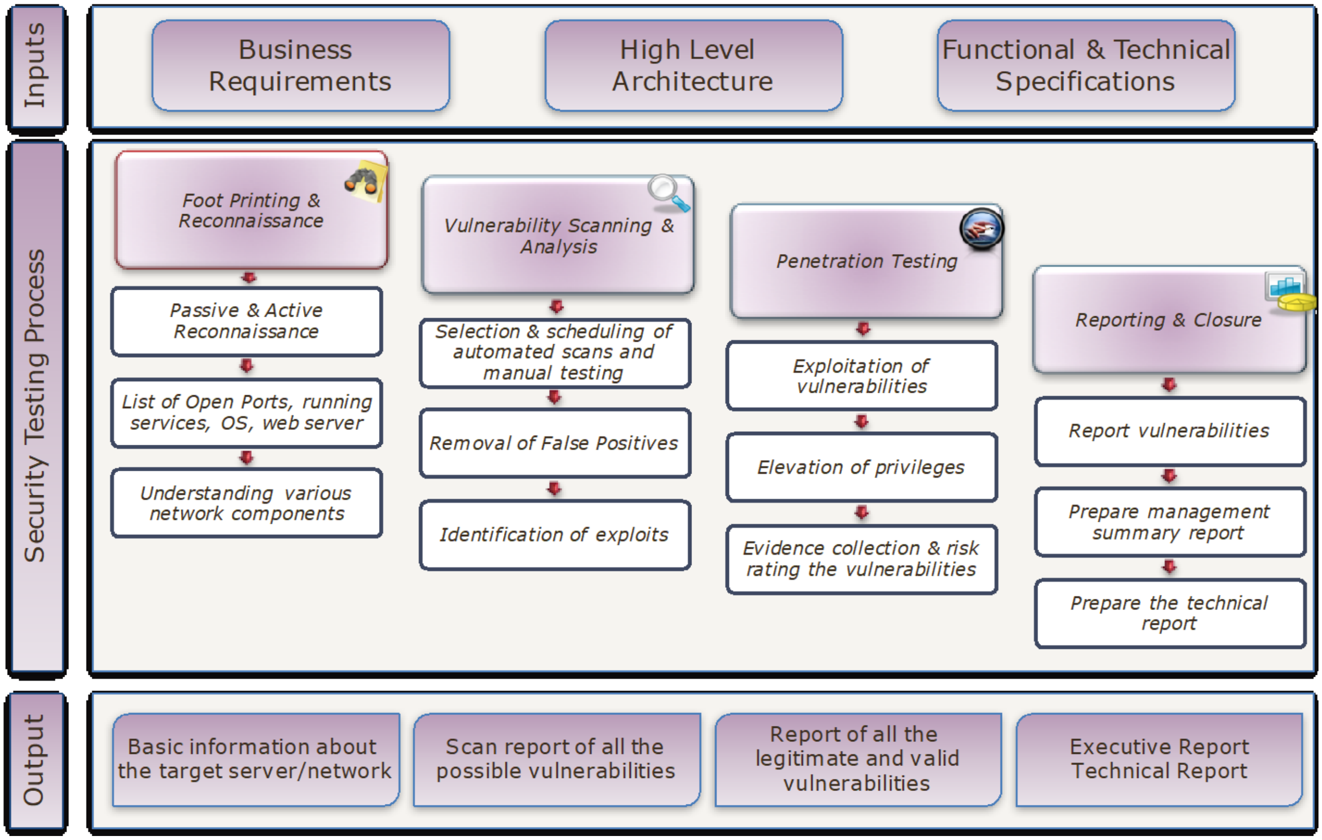
- CCDP Cisco Certified Design Professional
- CCNA Cisco Certified Network Associate, Routing and Switching
- CCNP R&S Cisco Certified Network Professional, Routing and Switching
- CCNP Security Cisco Certified Network Professional, Security
- CCNP Voice Cisco Certified Network Professional, Voice
- CEH Certified Ethical Hacker (EC-Council)
- CEPT Certified Expert Penetration Tester
- CISSP Certified Information Systems Security Professional (ISC2)
- CMWAPT Certified Mobile and Web Application Penetration Tester
- CPP Certified Protection Professional (ASIS)
- CPPT Certified Professional Penetration Tester
- CPTE Certified Penetration Testing Engineer
- CRISC Certified in Risk and Information System Controls (ISACA)
- CRTOP Certified Red Team Operations Professional
- CTS Certified Technology Specialist
- CTS-D Certified Technology Specialist - Design
- CWSP Certified Wireless Security Professional
- ECSA Certified Security Analyst
- ECSE Ekahau Certified Survey Engineer
- ENP Emergency Number Professional (NENA)
- FCC General Class Radiotelephone License
- GIAC Penetration Tester (GPEN)
- LEED AP Leadership in Energy and Environmental Design, Accredited Professional
- PCI/QSA Compliance
- PMP Project Management Professional (PMI)
- PSP Physical Security Professional (ASIS)
- RA Registered Architect (Texas)
- RCDD Registered Communications Distribution Designer (BICSI)
- RCCD/OSP Outside Plant Specialist (BICSI)
- RTPM Registered Telecommunication Project Manager (BICSI)
- SC-SDT Security Center System Design Training (IP Video and Card Access)
- Security Clearances supported by the FBI
- Texas DPS Security Consulting Company
- USGBC U.S. Green Building Council Membership

SECTION 2: APPROACH TO MANDATORY CONTRACT SERVICES REQUIREMENTS AND DELIVERABLES

NETWORK (EXTERNAL & INTERNAL) PENETRATION TESTING

Penetration testing will be performed to complement the review of security controls and ensure that the external-facing and internal-facing facets of the information system are secure. This process will provide assurance of the Customer's infrastructure's ability to withstand intentional attempts to circumvent system security. The following are the broad steps involved in the network-layer penetration testing exercise:

- Footprinting and reconnaissance
- Vulnerability scanning & analysis
- Exploitation/penetration testing
- Reporting (described in Deliverables section)


Inputs
Business Requirements
High Level Architecture
Functional & Technical Specifications
Security Testing Process
Foot Printing & Reconnaissance
Passive & Active Reconnaissance
List of Open Ports, running services, OS, web server
Understanding various network components
Vulnerability Scanning & Analysis
Selection & scheduling of automated scans and manual testing
Removal of False Positives
Identification of exploits
Penetration Testing
Exploitation of vulnerabilities
Elevation of privileges
Evidence collection & risk rating the vulnerabilities
Reporting & Closure
Report vulnerabilities
Prepare management summary report
Prepare the technical report
Output
Basic information about the target server/network
Scan report of all the possible vulnerabilities
Report of all the legitimate and valid vulnerabilities
Executive Report Technical Report

Network penetration testing stages are depicted in more detail in the below sections:

Network Penetration Testing Footprinting & Reconnaissance

- Passive reconnaissance using open-source intelligence-gathering avenues
  - Research via search engines, domain name registrars, chat groups, social networking, and other business intelligence sources: When corporations purchase domain names, they may not opt to pay for private registration for an additional fee. This may provide an attacker with an avenue to collect information about an organization, such as names, contact information, and phone numbers, which in turn can be used to launch a social engineering attack. True North will research Internet registries to check for registered domain names/IP addresses and contact information. True North will also search websites and forums to try to obtain sensitive or vulnerable information that could potentially allow an attacker to gain insight into the organization.
  - Google hacking and other automated website searches: Attackers can find information about a particular website or organization is through the use of specially crafted Google searches or web crawlers. This type of reconnaissance can help the attacker identify and unearth documents (i.e., Microsoft Word, Excel, PowerPoint, and Visio) that may be stored in search engine caches. This exercise could help discover sensitive data such as network diagrams or financial information in a directory of a publicly available site.
  - Record observations about the Customer's environment.
- Active reconnaissance – This phase can be facilitated (saving time and money) by having the customer provide information, and most of True North's penetration tests are conducted in this manner. Occasionally, the customer prefers that True North perform a 'black box' penetration test without providing any background information.
  - Gather details on target IP address ranges and verify the in-scope systems' accuracy before active testing. This step may include a review of services/technology in use as well as a security architecture review.
  - Aggregate potential target IP addresses
  - Understanding security architecture (if applicable)

Discovery (host and system services identification)

True North will use commercial, open-source, and custom tools against the targeted networks to determine the existence, location, type, and network path of network-connected devices. Port scanning allows the penetration tester to identify operating systems, services running, and, occasionally, the version of running services. Port scans are the foundation of vulnerability testing as the results provide the tester with information to select the optimal tools for subsequent testing. Tools used in this phase include Nmap, Nessus, Arpwatch, Tcpdump, and Dig.

This phase will include identifying:

- Network hosts and their operating systems
- Open ports, services, and applications
- Protocols enabled on hosts and ports
- Version and configuration of services and applications

Network Vulnerability Scanning & Analysis

True North will gauge the security posture of the targeted hosts and network segments by using a combination of vulnerability assessment tools and manual testing. This phase will help yield information pertaining to inherent weaknesses associated with patching, default settings, insecure services, poor configuration, or other attack vectors commonly used by perpetrators. This phase includes the following:

- Scheduling of systems to be scanned
- Scanning the systems in scope using automated scanners for vulnerabilities
- Selection of penetration testing tools based on vulnerabilities and ports detected by automated scanning
- Identification of exploits and scripts to be used
- Operating system testing includes checks for patches, running services, and system hardening.
- Configuration setting testing includes (to the extent they apply) checks for SSH settings, SSL settings, HTTPS settings, and insecure HTTP methods.

Tools used in this phase include Nmap, Nessus, W3af, and SSLScan.

Network-layer Penetration Testing

The exploitation phase of the vulnerability assessment is the key component that goes above and beyond 'just a vulnerability scan.' True North will manually confirm the existence of issues identified during automated scanning and then assess potential risk impact. A key part of our methodology is to address false positives by verifying and cross-referencing them against our extensive vulnerability knowledgebase as well as the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and several other knowledge bases used throughout the security community. To determine whether a vulnerability is a false positive, True North may need to attempt to exploit it. True North will work closely with the customer to coordinate all penetration efforts in these cases. This phase will include:

- Exploitation of vulnerabilities found in automated scanning
- Skill and knowledge-based exploitation of vulnerabilities using scripts developed internally, exploits, etc.
- Attack methods involve accessing and exfiltrating sensitive data, performing privilege escalation, exploiting buffer overflow attacks (if requested), executing denial of service (if requested), etc.

Tools used in this phase may include Metasploit Framework, Kali Linux, Nmap, Nessus, and customized scripts.

Web Application and API Penetration Testing

General Web Application/API Testing Approach

True North has hundreds of customers, and we utilize our methodology for customers who do not have their own requirements for executing security testing. We customize the testing program for several larger clients for whom we execute a complete test program annually to meet their objectives. This approach can mean changing our test plans to be consistent with what they use with multiple other vendors, storing and presenting results and evidence in systems our customers already utilize for testing they conduct internally, or executing the projects in a way that is standard for their organization. We are flexible and work to meet our client's requirements, and we do not require them to fit into our base project methodology.

Our base methodology utilizes standards-based test plans such as the OWASP web application guide. We have a methodology that all our consultants follow, and the steps are recorded in a work log. Our process includes standard practices for initiating projects and recording critical information about primary contacts, scope, schedule, and any changes to this information. We have a two-phase QA process for reviewing our reports and testing work products prior to customer delivery. We have processes to store testing evidence and work products securely and will archive or wipe such information based on our customer’s preferences once an engagement is complete.

Our testing of internal environments is usually accomplished by having our clients install testing appliance virtual machines that communicate via an outbound VPN back to our test lab. However, we sometimes deliver testing via client-supplied VPNs and can go to client locations if required. We provide our clients with instructions, VPN setups, and a script to configure the testing appliance. Setting up an appliance usually takes about one hour of our client's time. For some of our customers, we have many appliances in various network locations based on their network segmentation or for performance reasons related to international geography. The testing appliance virtual machines can also be set up in cloud-based environments to enable testing of applications that are not exposed to the Internet.

We typically encourage testing in a non-production environment with the same code running in a similarly configured environment to production for web applications and APIs. Usually, that is a user acceptance testing (UAT) or similar environment. This usually limits the impact of our testing and allows us to be the most aggressive in both speed of testing and test selection. In addition, although we do not seek to create denial of service conditions, these can happen in rare circumstances through routine testing when certain conditions are encountered, and it is best to identify these in a non-production environment so that controls can then be established in production to prevent them from occurring. Many times, we test in a non-production environment and then confirm findings in a production environment if there is any doubt that differences in the environments are the cause of the issue identified.

Additional information for Cloud-based Environments

Currently, about 40-50% of our testing is in cloud-based environments, with most of the environments in AWS and Azure. However, we have also tested many others, and we see those percentages increasing as many customers take advantage of the sophisticated features offered in these cloud-based environments.

Our approach to delivering testing in cloud-based environments depends on the client architecture and environments involved. Many of our customers are using IAAS cloud-based environments and exposing web applications that are hosted on systems instances that are managed by that organization. For these, the approach is very similar to testing a typical web application hosted in a colocation facility. Reviewing the cloud provider's supporting infrastructure and pen testing policies before testing is necessary for each environment.

There are also serverless environments supported in many cloud services. The type of testing done in these environments often depends on how these environments are used in the application architecture, with many different possibilities, including using all serverless to hybrid setups. We work with customers to understand the architecture of what is being tested and then work on an agreed-upon approach to identify the risks most cost-effectively. In many of these environments, a hybrid approach of testing and configuration review is the best approach as many times a weak configuration of the service may lead to risks not easily identified with testing (for example, AWS S3 buckets that have randomized locations which are not easily discovered but if someone has the location and it has not been securely configured, can lead to data loss). In these cases, we can partner with our risk and compliance team or our customers' resources to ensure the configuration and testing provide a secure environment.

Applications, by their nature, frequently have access to sensitive, confidential data, including passwords, personally identifiable information, payment card information, and health information. Since many applications are Internet-facing, it is critical that organizations apply due diligence to implement reasonable security controls to reduce the likelihood of attack. True North's testing methodology is designed to identify security weaknesses and to present effective strategies to implement security controls to remediate or mitigate the risk.

To the extent it applies, True North recommends that the customer provide the application testing with test accounts/credentials for the various roles to be tested. True North also finds it extremely helpful to receive a demonstration of the application to understand better the business logic and data flows. When applicable, we recommend testing in a UAT, staging, or development environment (assuming it closely mirrors production).

True North will perform controlled application security assessments and exploitation attempts on Customers' applications. The primary purpose of this testing is to identify and exploit application vulnerabilities present in the in-scope applications.

The following are the broad steps involved in the application-layer penetration testing exercise.

- Information gathering
- Application security assessment
- Exploitation/penetration testing
- Reporting (described in Deliverables section)

Web Application Pen Testing Information Gathering

- Understanding application business and technical overview, including user roles (often presented in person or via web conference)
- Understanding security architecture (if applicable)
- Understanding systems functionality/component segregation
- Gathering publicly available information from various Internet sources
- Threat profiling and attempting to discover logic flaws in the surface of the application

The information gathered above will be analyzed to identify threats and associated vulnerabilities within the system's components and interfaces.

Web Application Security Assessment

The Web application review will examine the web application infrastructure for the following vulnerabilities:

- Application assessment based on OWASP, SANS, CWE, WASC standards OWASP TOP 10 2021 – Site: https://owasp.org/Top10/
  - **A1 Broken Access Control**: Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as accessing other users' accounts, viewing sensitive files, modifying other users' data, changing access rights, etc.
  - **A2 Cryptographic Failures**: Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and special precautions may be required when exchanged with the browser.
  - **A3 Injection**: Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. Cross-Site Scripting (XSS) is also an injection flaw. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

- **A4 Insecure Design**: Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.” There is a difference between insecure design and insecure implementation. Design flaws and implementation defects differ because they have different root causes and remediation. A secure design can still have implementation defects, leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as, by definition, needed security controls were never created to defend against specific attacks.
- **A5 Security Misconfiguration:** This vulnerability is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
- **A6 Vulnerable and Outdated Components:** If the software is vulnerable, unsupported, or out of date. This covers all software, including the OS, web/application server, database management system (DBMS), applications, APIs, components, runtime environments, and libraries.
- **A7 Identification and Authentication Failures:** Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens or exploit other implementation flaws to temporarily or permanently assume other users’ identities temporarily or permanently.
- **A8 Software and Data Integrity Failures:** Software and data integrity failures relate to code and infrastructure that do not protect against integrity violations. An example is when an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify, which is vulnerable to insecure deserialization.
- **A9 Security Logging and Monitoring Failure:** This category is to help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected. Insufficient logging, detection, monitoring, and active response will be tested where possible.
- **A10 Server-Side Request Forgery (SSRF):** SSRF flaws occur when a web application fetches a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

- Unvalidated Input: Information from Web requests is not validated before being used by a Web application. Attackers can use these flaws to attack back-end components through a Web application.
- Improper Error Handling: Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the Web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
- Denial of Service (DoS) – if applicable (testing limited to avoid impact): Attackers can consume Web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
- Buffer Overflows – if applicable: Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of processes. These components can include common gateway interfaces (CGIs), libraries, drivers, and web application server components.
- Controlled execution of automated tools to identify vulnerabilities that are presented to an application user in the form of an "anonymous user" and an "authorized user" (depending on the nature of the application, testing may include several authorized user roles).
- If a web application firewall or intrusion prevention system is deployed, determine if testing will include a 'shields down' phase for only the penetration tester.
- Testing will include testing for the most recent vulnerabilities and exploits (i.e., Heartbleed, Poodle, etc.).
- Use manual techniques to confirm the vulnerabilities found by automated scanning. The results of this phase are used in the later section titled "Exploitation."
- Perform testing to determine if a client session can be hijacked.

Tools used in this phase include BurpSuite and Zed Attack Proxy.

Project Management and Other Items of Interest

Project Management & Communication

TNCG regularly conducts weekly/bi-weekly/monthly project status meetings, ensuring our client-specific projects and services are delivered on time and to the level of satisfaction that the State of West Virginia Lottery staff would expect. If additional status meetings are needed at any time during the project, we quickly accommodate those requests.

Our client recommendations and testimonials prove we can deliver extremely beneficial results to local government organizations, as that is our area of expertise.

Local Government Expertise

We pride ourselves in understanding local government needs. We are active in multiple IT consortiums and will bring you the benefit of collective experiences related to emerging IT solutions and software. This approach is especially important as we continually weigh the pros and cons of cloud-based solutions.

We have additional expertise in Law Enforcement technologies and security related to the CJIS Security Policy requirements, which now heavily emphasizes cybersecurity controls. This is a perfect example of how we excel in our strategic planning approach between Administration, State IT, and Public Safety.

We are also very aware of emerging and existing technologies that help address the high mobility work environment, which now heavily emphasizes technology and security because of the COVID pandemic but has always been a part of our strategic plan for governments.

Change Controls

We use a formal Change Control process and approval method before starting the technical penetration testing. This ensures that all critical members of your team know:

- What network segments are being tested
- When (Date/Time window(s)) you approve the testing to occur
- Impact cautions to prevent service disruptions
- Emergency contacts

Our clients greatly appreciate this most professional approach and the excellent written communication and documentation it provides.

Reports

Team TNCG reports have been well-received by local government organizations in the past. Team TNCG provides a "Full Report," which includes a comprehensive outline of background, scope, methodology, detailed findings/recommendations, and additional documents that provide the greatest level of detail if anyone desires to focus on that level of detail. Team TNCG can prepare additional variations of the Full Report to meet the needs of the State of West Virginia Lottery. For example, Team TNCG can create a redacted Public Executive Summary or a slightly more unredacted Executive Summary for your Management or Board. Team TNCG can also organize the Full Report so that sections can be distributed to discrete business units, if appropriate in the State's case.

Our reports have been regarded as clear, concise, and developed in a way that meets all professional standards but delivers the content in a manner that makes life easier for top-level management. This overall process makes remediation easier and makes it possible to track those remediation efforts in other software or project management documents.

We are also very experienced in presenting findings in open and closed meetings in compliance with open meetings laws.

Security of the State's Data

As a security professional and consultant, we take the security of your data seriously. We have conducted our own NIST 800-53/CSF Risk assessment for the primary lead consultant on this project.

State of West Virginia Lottery Overall Results Example:

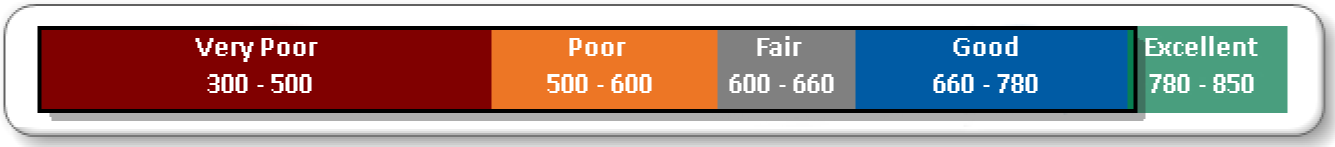
The overall S2SCORE (or risk rating) is **781.76**.

781.76 Excellent

The S2SCORE represents a comprehensive, authoritative, and objective information security risk value. The S2SCORE enables business leaders to quickly identify and relate to the amount of information security risk present in their organization, and a S2SCORE also allows the organization to communicate the level of risk to interested third parties succinctly.

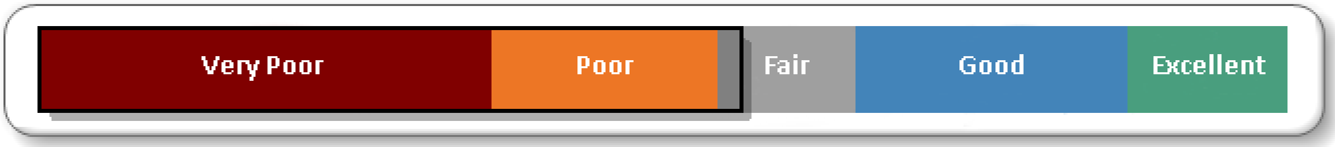
A S2SCORE of **781.76** translates to "**Excellent**." A detailed explanation of the S2SCORE and a further definition of its meaning can be found in the S2SCORE Full Report. The S2SCORE is calculated in a range from 300 to 850. The lower the score, the higher the risk, and vice versa. A S2SCORE of **660.00** or "**Good**" is acceptable to most organizations and should be the goal for the State of West Virginia Lottery.

S2SCORE Scale



S2SCORE Average Across Industries

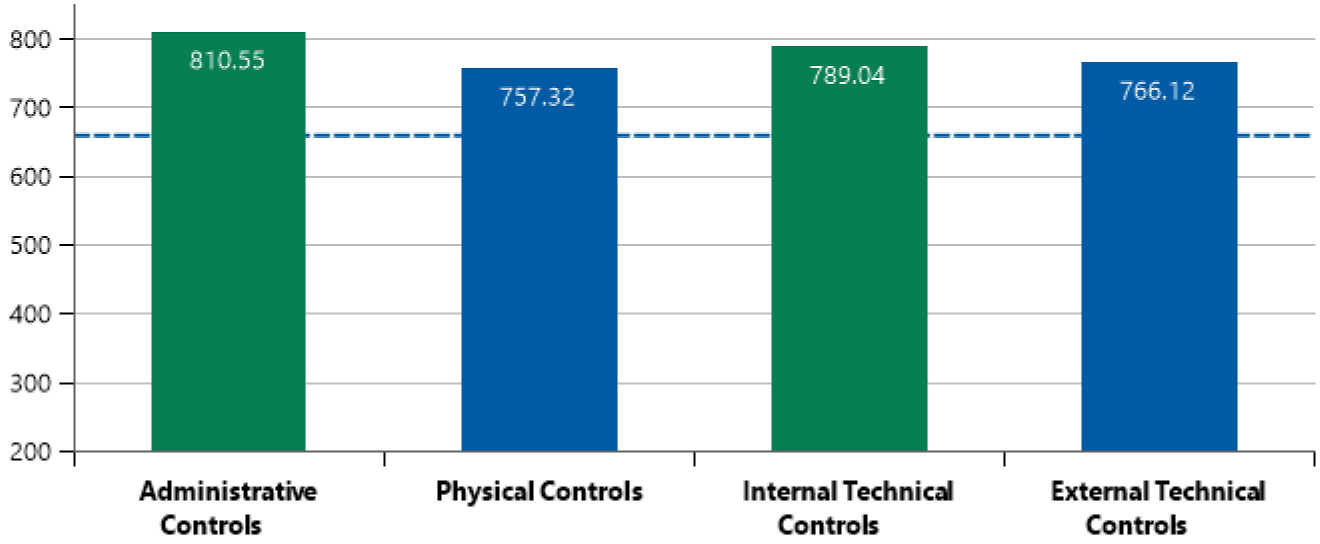
Industry: Professional, Scientific, and Technical Services (541)



The average third-party validated S2SCORE is 608.33 for Professional, Scientific, and Technical Services (541). According to our calculations, there is roughly 28.5% less risk in information security programs than in other programs in similar organizations.

S2SCORE phase-by-phase Comparison

There are four phases in a Full S2SCORE: Administrative Controls, Physical Controls, Internal Technical Controls, and External Technical Controls. An "acceptable" level of security is 660.



PROPOSED TIMELINE EXAMPLE

The timeline will be modified to meet the expectations if required.

Week #	Task
Week 1	Kick-off - Onsite Visit
Week 2	Set up Penetration Testing Equipment
Week 3	Internal Penetration Testing
Week 4	External & Application Testing
Week 5	Complete Application Testing
Week 6	Draft Full Report to Lottery Staff - Presentation
Week 7	Closing Tasks - Final Reports Issued
TBD	Formal Presentation of Project at any time after reports are complete

SECTION 3: REFERENCES

Please see Team TNCG's References below.

1. **Bi-State Development, Missouri**
Address: 1 Metropolitan Square, 211 North Broadway, Suite 700, St. Louis, MO 63102
Contact: Ms. Crystal Messner, Chief Audit Executive, (314) 982-1400 x 3001, cmmessner@bistatedev.org
Project Description: Internal/External Vulnerability and SCADA Assessments along with Summary/Executive Summary Reports and Suggested Remediation

2. **Town of Dudley, Massachusetts**
Address: 71 West Main Street, Dudley, MA 01571
Contact: Mr. Jonathan Ruda, Town Administrator, (774) 275-1923, jruda@dudleyma.gov
Project Description: Penetration Testing, Vulnerability Assessment, Policies and Procedures, Risk Assessment, Physical Security, IT Assessment, and vCISO

3. **City of New York City Finance Department**
Address: 59 Maiden Lane, 18th Floor, New York, NY 10038
Contact: Mr. Morris Cyrus, Director of Product Development and Security and Compliance, (212) 291-2954, cyrusmorris@finance.nyc.gov
Project Description: Full PCI-DSS Security Assessment for compliance including Cybersecurity Applications

4. **State of West Virginia**
Address: 2019 Washington Street East, Charleston, WV 25305
Contact: Mr. Guy Nisbet, Assistant Purchasing Director (Department of Administration, Purchasing Division), (304) 558-2596, guy.l.nisbet@wv.gov (Note: Not sure if Mr. Nisbet is still employed with the State)
Project Description: Information Security and Network Vulnerability Assessment that was conducted in 2016 and met expectations.

5. **Virginia Retirement System**
Address: 1111 East Main Street, Richmond, VA 23218
Contact: Mr. Robert Robinson, Procurement Manager, (804) 771-7355, rrobinson@varetire.org
Project Description: Penetration Testing Assessment throughout the agency as needed for a five-year contract/agreement, which was put in place on 04/2023.

6. **Missouri Housing Development Commission**
Address: 920 Main Street, Suite 1400, Kansas City, MO 64105
Contact: Mr. David Nickum, Director of Information Technology, (816) 759-6843, david.nickum@mhdc.com
Project Description: Penetration Testing and Vulnerability Assessment, including contracted vCISO

7. **Port of Long Beach, California**
   Address: 1249 Pier F Avenue, Long Beach, CA 90802
   Contact: Mr. Jeremy Vetterlein, Technical Security Consultant, (562) 283-7844, jeremy.vetterlein@polb.com
   Project Description: Penetration Testing and Vulnerability Assessment

8. **Washington Metropolitan Area Transit Authority (WMATA), DC**
   Address: 600 5th Street NW, Washington, DC 20001
   Contact: Captain Brian Heanue, Metro Transit Police, (202) 345-0809, BHeanue@wmata.com
   Project Description: Contracted to provide Threat and Vulnerability Assessments (TVA) for all Washington Metropolitan Transit Authority (WMATA) facilities and infrastructure. In Phase I of the project, verified the presence or absence of security design standards and mitigation recommendations from previous TVAs for facilities and infrastructure under construction. In Phase II of the project, conducted TVAs for all existing WMATA facilities.

GOVERNMENT CLIENT LIST EXAMPLE

The following is True North's government client list example. **Additional references are available upon request.**

AITKIN COUNTY,
Aitkin, Minnesota

ALLAMAKEE COUNTY,
Waukon, Iowa

AMTRAK,
Washington, D.C.

ASHLAND COUNTY,
Ashland, Wisconsin

AUDUBON COUNTY,
Audubon, Iowa

AUSTIN PUBLIC UTILITIES,
Austin, Minnesota

BARRON COUNTY,
Barron, Wisconsin

BAYFIELD COUNTY,
Washburn, Wisconsin

BEADLE COUNTY,
Huron, South Dakota

BELTRAMI COUNTY,
Bemidji, Minnesota

BENTON COUNTY,
Vinton, Iowa

BI-STATE DEVELOPMENT,
St. Louis, Missouri

BLACKHAWK COUNTY,
Waterloo, Iowa

BLUE EARTH COUNTY,
Mankato, Minnesota

BOONE COUNTY,
Belvidere, Illinois

BREMER COUNTY,
Waverly, Iowa

BREVARD COUNTY,
Viera, Florida

BROWN COUNTY,
New Ulm, Minnesota

BUFFALO COUNTY,
Alma, Wisconsin

BUREAU OF CRIMINAL
APPREHENSION,
St. Paul, Minnesota

BURNETT COUNTY,
Siren, Wisconsin

BUTLER COUNTY,
Allison, Iowa

CALHOUN COUNTY,
Marshall, Michigan

CAMPBELL COUNTY,
Rustburg, Virginia

CARROLL COUNTY,
Carroll, Iowa

CARVER COUNTY,
Chaska, Minnesota

CASS COUNTY,
Fargo, North Dakota

CASS COUNTY,
Virginia, Illinois

CEDAR COUNTY,
Tipton, Iowa

CHEROKEE COUNTY,
Cherokee, Iowa

CHIPPEWA COUNTY,
Chippewa Falls, Wisconsin

CHISAGO COUNTY,
Center City, Minnesota

CITY AND COUNTY OF
LEAVENWORTH,
Leavenworth, Kansas

CITY OF ALBERTVILLE,
Albertville, Minnesota

CITY OF ALLEN,
Allen, Texas

CITY OF ALTOONA,
Altoona, Pennsylvania

CITY OF AMES,
Ames, Iowa

CITY OF ANKENY,
Ankeny, Iowa

CITY OF ANOKA,
Anoka, Minnesota

CITY OF APPLE VALLEY,
Apple Valley, Minnesota

CITY OF ARVADA,
Arvada, Colorado

CITY OF AUSTIN,
Austin, Texas

CITY OF BATTLE CREEK,
Battle Creek, Michigan

CITY OF BELOIT,
Beloit, Wisconsin

CITY OF BISMARCK,
Bismarck, North Dakota

CITY OF BLOOMINGTON,
Bloomington, Minnesota

CITY OF BURNSVILLE,
Burnsville, Minnesota

CITY OF CASPER,
Casper, Wyoming

CITY OF CEDARBURG,
Cedarburg, Wisconsin

CITY OF CEDAR RAPIDS,
Cedar Rapids, Iowa

CITY OF CERES,
Ceres, California

CITY OF CHAMPAIGN,
Champaign, Illinois

CITY OF CHARLOTTE,
Charlotte, North Carolina

CITY OF COLLEGE STATION,
College Station, Texas

CITY OF COLUMBIA HEIGHTS,
Columbia Heights, Minnesota

CITY OF COLUMBUS,
Columbus, Wisconsin

CITY OF COTTAGE GROVE,
Cottage Grove, Minnesota

CITY OF DALLAS,
Dallas, Texas

CITY OF DAYTON,
Dayton, Ohio

CITY OF DECORAH,
Decorah, Iowa

CITY OF DES MOINES,
Des Moines, Iowa

CITY OF DUBUQUE,
Dubuque, Iowa

CITY OF DULUTH,
Duluth, Minnesota

CITY OF DURHAM,
Durham, North Carolina

CITY OF EAGAN,
Eagan, Minnesota

CITY OF EDEN PRAIRIE,
Eden Prairie, Minnesota

CITY OF EDINA,
Edina, Minnesota

CITY OF FARGO,
Fargo, North Dakota

CITY OF FARMINGTON,
Farmington, New Mexico

CITY OF FORNEY,
Forney, Texas

CITY OF FORT ATKINSON,
Fort Atkinson, Wisconsin

CITY OF FORT COLLINS,
Fort Collins, Colorado

CITY OF GAINESVILLE,
Gainesville, Georgia

CITY OF GARLAND,
Garland, Texas

CITY OF GERMANTOWN,
Germantown, Tennessee

CITY OF GOODYEAR,
Goodyear, Arizona

CITY OF GRAND FORKS,
Grand Forks, North Dakota

CITY OF GRESHAM,
Gresham, Oregon

CITY OF GROSSE POINTE FARMS,
Grosse Pointe Farms, Michigan

CITY OF HAM LAKE,
Ham Lake, Minnesota

CITY OF HASTINGS,
Hastings, Minnesota

CITY OF HERMANTOWN,
Hermantown, Minnesota

CITY OF HURST,
Hurst, Texas

CITY OF INVER GROVE HEIGHTS,
Inver Grove Heights, Minnesota

CITY OF IOWA CITY,
Iowa City, Iowa

CITY OF JANESVILLE,
Janesville, Wisconsin

CITY OF KANSAS CITY,
Kansas City, Missouri

CITY OF LINCOLN,
Lincoln, Nebraska

CITY OF MADISON,
Madison, Wisconsin

CITY OF MANKATO,
Mankato, Minnesota

CITY OF MAPLE GROVE,
Maple Grove, Minnesota

CITY OF MAPLEWOOD,
Maplewood, Minnesota

CITY OF MARSHALLTOWN,
Marshalltown, Iowa

CITY OF MCHENRY,
Mchenry, Illinois

CITY OF MINNETONKA,
Minnetonka, Minnesota

CITY OF MINOT,
Minot, North Dakota

CITY OF NEW HOPE,
New Hope, Minnesota

CITY OF NEW YORK DEPARTMENT OF FINANCE,
New York, New York

CITY OF NIXA,
Nixa, Missouri

CITY OF OAK GROVE,
Cedar, Minnesota

CITY OF OCONOMOWOC,
Oconomowoc, Wisconsin

CITY OF OLIVETTE,
Olivette, Missouri

CITY OF ORONO,
Orono, Minnesota

CITY OF OTTUMWA,
Ottumwa, Iowa

CITY OF OWATONNA,
Owatonna, Minnesota

CITY OF PINGREE GROVE,
Pingree Grove, Illinois

CITY OF PLYMOUTH,
Plymouth, Minnesota

CITY OF PORTLAND,
Portland, Oregon

CITY OF RALEIGH,
Raleigh, North Carolina

CITY OF RICHMOND HEIGHTS,
Richmond Heights, Missouri

CITY OF ROBBINSDALE,
Robbinsdale, Minnesota

CITY OF ROCKFORD,
Rockford, Illinois

CITY OF ROCKWALL,
Rockwall, Texas

CITY OF ROSEVILLE,
Roseville, Minnesota

CITY OF ROUND ROCK,
Round Rock, Texas

CITY OF ST. CLOUD,
St. Cloud, Minnesota

CITY OF ST. LOUIS PARK,
St. Louis Park, Minnesota

CITY OF ST. PAUL,
St. Paul, Minnesota

CITY OF SALEM,
Salem, Oregon

CITY OF SALINA,
Salina, Kansas

CITY OF SANTA CRUZ,
Santa Cruz, California

CITY OF SAVANNAH,
Savannah, Georgia

CITY OF SEGUIN,
Seguin, Texas

CITY OF SHOREVIEW,
Shoreview, Minnesota

CITY OF SOUTH ST. PAUL,
South St. Paul, Minnesota

CITY OF STATESBORO,
Statesboro, Georgia

CITY OF SUPERIOR,
Superior, Wisconsin

CITY OF TAMARAC,
Tamarac, Florida

CITY OF TOPEKA,
Topeka, Kansas

CITY OF VADNAIS HEIGHTS,
Vadnais Heights, Minnesota

CITY OF WAHPETON,
Wahpeton, North Dakota

CITY OF WATERTOWN,
Watertown, Wisconsin

CITY OF WAUSAU,
Wausau, Wisconsin

CITY OF WEBSTER GROVES,
Webster Groves, Missouri

CITY OF WESTLAND,
Westland, Michigan

CITY OF WILLISTON,
Williston, North Dakota

CITY OF WOODBURY,
Woodbury, Minnesota

CLARK COUNTY,
Neillsville, Wisconsin

CLAY COUNTY,
Spencer, Iowa

CLAY COUNTY,
Vermilion, South Dakota

CLAYTON COUNTY,
Elkader, Iowa

CLINTON COUNTY,
Clinton, Iowa

CODINGTON COUNTY,
Watertown, South Dakota

COLLIN COUNTY,
McKinney, Texas

COLORADO STATE PATROL,
Alamosa, Colorado

COLUMBIA COUNTY,
Portage, Wisconsin

CONVENTION AND VISITORS' BUREAU OF GREATER KANSAS CITY,
Kansas City, Missouri

COOK MEMORIAL PUBLIC LIBRARY DISTRICT,
Libertyville, Illinois

CRAWFORD COUNTY,
Prairie Du Chien, Wisconsin

CROCKETT COUNTY,
Ozona, Texas

CROW WING COUNTY,
Brainerd, Minnesota

CUMBERLAND COUNTY,
Carlisle, Pennsylvania

DAKOTA COUNTY,
Hastings, Minnesota

DAKOTA COUNTY HRA,
Rosemount, Minnesota

DALLAS AREA RAPID TRANSIT (DART),
Dallas, Texas

DANE COUNTY,
Madison, Wisconsin

DANE COUNTY REGIONAL AIRPORT,
Madison, Wisconsin

DANE COUNTY SOCIAL SERVICES,
Madison, Wisconsin

DAVIS COUNTY,
Bloomfield, Iowa

DECATUR COUNTY,
Leon, Iowa

DELAWARE COUNTY,
Manchester, Iowa

DES MOINES COUNTY,
Burlington, Iowa

DODGE COUNTY,
Juneau, Wisconsin

DODGE COUNTY,
Mantorville, Minnesota

DOOR COUNTY,
Sturgeon Bay, Minnesota

DOUGLAS COUNTY,
Alexandria, Minnesota

DOUGLAS COUNTY,
Douglasville, Georgia

DUBUQUE COUNTY,
Dubuque, Iowa

DUNKLIN COUNTY,
Kennett, Missouri

DUNN COUNTY,
Menomonie, Wisconsin

EASTSIDE SUBURBAN EMERGENCY COMMUNICATIONS CENTER,
Reynoldsburg, Ohio

EAU CLAIRE COUNTY,
Eau Claire, Wisconsin

ECTOR COUNTY,
Odessa, Texas

FAYETTE COUNTY,
West Union, Iowa

FEDERAL RESERVE BANK,
Minneapolis, Minnesota

FOND DU LAC COUNTY,
Fond Du Lac, Wisconsin

FOURTH JUDICIAL DISTRICT,
Minneapolis, Minnesota

FRANKLIN COUNTY,
Union, Missouri

FREMONT COUNTY,
Sidney, Iowa

GRAND COUNTY TELEPHONE AUTH. BOARD,
Winter Park, Colorado

GRAND RAPIDS LIBRARY,
Grand Rapids, Minnesota

GRANT COUNTY,
Lancaster, Wisconsin

GREEN LAKE COUNTY,
Green Lake, Wisconsin

GREENE COUNTY,
Springfield, Missouri

GRUNDY COUNTY,
Grundy Center, Iowa

HANCOCK COUNTY,
Carthage, Illinois

HANCOCK COUNTY,
Garner, Iowa

HARDIN COUNTY,
Eldora, Iowa

HENNEPIN COUNTY,
Minneapolis, Minnesota

HO-CHUNK NATION TRIBAL JUSTICE CENTER,
Black River Falls, Wisconsin

HOWARD COUNTY,
Cresco, Iowa

IOWA COUNTY,
Dodgeville, Wisconsin

IRON COUNTY,
Hurley, Wisconsin

JACKSON COUNTY,
Black River Falls, Wisconsin

JACKSON COUNTY,
Maquoketa, Iowa

JASPER COUNTY,
Newton, Iowa

JEFFERSON COUNTY,
Fairfield, Iowa

JEFFERSON COUNTY,
Jefferson, Wisconsin

JO DAVIESS COUNTY,
Hanover, Illinois

JOHNSON COUNTY,
Iowa City, Iowa

JONES COUNTY,
Anamosa, Iowa

JUNEAU COUNTY,
Mauston, Wisconsin

KANABEC COUNTY,
Mora, Minnesota

KANE COUNTY,
Geneva, Illinois

KANSAS CITY AREA TRANSPORTATION AUTH. (KCATA),
Kansas City, Missouri

KANSAS CITY POLICE DEPARTMENT,
Kansas City, Missouri

KENOSHA COUNTY,
Kenosha, Wisconsin

KENTON COUNTY AIRPORT BOARD,
Hebron, Kentucky

KEOKUK COUNTY,
Sigourney, Iowa

KEWAUNEE COUNTY,
Kewaunee, Wisconsin

KIT CARSON COUNTY,
Burlington, Colorado

KNOX COUNTY,
Knoxville, Tennessee

KOOTENAI COUNTY,
Coeur D' Alene, Idaho

LACROSSE COUNTY,
La Crosse, Wisconsin

LAFAYETTE COUNTY,
Darlington, Wisconsin

LAKE COUNTY,
Baldwin, Michigan

LANGLADE COUNTY,
Antigo, Wisconsin

LEE COUNTY,
Dixon, Illinois

LEE COUNTY,
Fort Madison, Iowa

LESUEUR COUNTY,
Le Center, Minnesota

LINCOLN COUNTY,
Merrill, Wisconsin

LINN COUNTY,
Cedar Rapids, Iowa

LISLE I-NET CONSORTIUM,
Lisle, Illinois

LOUISA COUNTY,
Wapello, Iowa

LOWELL HOUSING AUTHORITY,
Lowell, Massachusetts

LYON COUNTY,
Rock Rapids, Iowa

MANATEE COUNTY,
Bradenton, Florida

MANITOWOC COUNTY,
Manitowoc, Wisconsin

MARATHON COUNTY,
Wausau, Wisconsin

MARQUETTE COUNTY,
Montello, Wisconsin

MAYO CIVIC CENTER,
Rochester, Minnesota

MCDONOUGH COUNTY,
Macomb, Illinois

MCHENRY COUNTY,
Mchenry, Illinois

MCLEOD COUNTY,
Glencoe, Minnesota

METROPOLITAN AIRPORTS COMMISSION,
St. Paul, Minnesota

METROPOLITAN ATLANTA RAPID TRANSIT AUTHORITY (MARTA),
Atlanta, Georgia

METROPOLITAN COUNCIL,
St. Paul, Minnesota

METROPOLITAN TRANSIT COMMISSION,
Minneapolis, Minnesota

MILLE LACS DRIFTSKIPPERS SNOWMOBILE CLUB,
Isle, Minnesota

MILLS COUNTY,
Glenwood, Iowa

MINNEHAHA COUNTY,
Sioux Falls, South Dakota

MINNESOTA CORRECTIONAL FACILITY,
St. Cloud, Minnesota

MINNESOTA DEPARTMENT OF CORRECTIONS,
St. Paul, Minnesota

MISSOURI HOUSING DEVELOPMENT COMMISSION,
Kansas City, Missouri

MITCHELL COUNTY,
Osage, Iowa

MONONA COUNTY,
Onawa, Iowa

MONROE COUNTY,
Tomah, Wisconsin

MORRISON COUNTY,
Little Falls, Minnesota

MOWER COUNTY,
Austin, Minnesota

MUSCATINE COUNTY,
West Liberty, Iowa

NORTHWEST REGIONAL RADIO BOARD,
Bemidji, Minnesota

NUECES COUNTY,
Corpus Christi, Texas

O'BRIEN COUNTY,
Primghar, Iowa

OCEAN COUNTY,
Toms River, New Jersey

OCONTO COUNTY,
Oconto, Wisconsin

ORANGEBURG COUNTY,
Orangeburg, South Carolina

OSCEOLA COUNTY,
Sibley, Iowa

OUTAGAMIE COUNTY,
Appleton, Wisconsin

OWATONNA PUBLIC UTILITIES,
Owatonna, Minnesota

OZAUKEE COUNTY,
Port Washington, Wisconsin

PAGE COUNTY,
Clarinda, Iowa

PARK COUNTY,
Fairplay, Colorado

PIERCE COUNTY,
Ellsworth, Wisconsin

PINE COUNTY,
Pine City, Minnesota

PINELLAS SUNCOAST TRANSIT AUTHORITY (PSTA),
St. Petersburg, Florida

PLYMOUTH COUNTY,
Remsen, Iowa

POCAHONTAS COUNTY,
Pocahontas, Iowa

POLK COUNTY,
Balsam Lake, Wisconsin

POLK COUNTY,
Des Moines, Iowa

PORT OF LONG BEACH,
Long Beach, California

PORTSMOUTH METROPOLITAN HOUSING AUTHORITY,
Portsmouth, Ohio

POWESHIEK COUNTY,
Montezuma, Iowa

PRICE COUNTY,
Phillips, Wisconsin

PUBLIC BUILDING COMMISSION OF CHICAGO,
Chicago, Illinois

PUBLIC HOUSING AGENCY OF THE CITY OF SAINT PAUL,
St. Paul, Minnesota

RAMSEY COUNTY,
St. Paul, Minnesota

REDWOOD COUNTY,
Redwood Falls, Minnesota

RICE COUNTY,
Faribault, Minnesota

RICHLAND COUNTY,
Richland Center, Wisconsin

RICHLAND COUNTY,
Wahpeton, North Dakota

RICHMOND HEIGHTS,
Richmond Heights, Missouri

ROANOKE COUNTY,
Roanoke, Virginia

ROBBINSDALE POLICE DEPT.,
Robbinsdale, Minnesota

ROCK COUNTY,
Janesville, Wisconsin

ROCK COUNTY,
Luverne, Minnesota

ROCK RIVER WATER RECLAMATION DISTRICT,
Rockford, Illinois

RUSK COUNTY,
Ladysmith, Wisconsin

SAINT CROIX COUNTY,
Hudson, Wisconsin

SAINT PAUL CIVIC CENTER,
St. Paul, Minnesota

SAINT PAUL PUBLIC LIBRARY,
St. Paul, Minnesota

SAN LUIS VALLEY COUNTY,
Alamosa, Colorado

SANDOVAL COUNTY,
Bernalillo, New Mexico

SANGAMON COUNTY,
Springfield, Illinois

SARPY COUNTY,
Papillion, Nebraska

SAUK COUNTY,
Baraboo, Wisconsin

SAWYER COUNTY,
Hayward, Wisconsin

SCOTT COUNTY,
Shakopee, Minnesota

SEVEN-COUNTY METROPOLITAN PROJECT,
Minneapolis, Minnesota

SHEBOYGAN COUNTY,
Sheboygan, Wisconsin

SHERBURNE COUNTY,
Elk River, Minnesota

SIOUX COUNTY,
Orange City, Iowa

SOUTH DUNKLIN COUNTY,
Hornersville, Missouri

ST. LOUIS COUNTY,
Duluth, Minnesota

STATE OF COLORADO,
Denver, Colorado

STATE OF WISCONSIN,
Madison, Wisconsin

STEARNS COUNTY,
St. Cloud, Minnesota

STEELE COUNTY,
Owatonna, Minnesota

STEVENS COUNTY,
Morris, Minnesota

STODDARD COUNTY,
Dexter, Missouri

STORY COUNTY,
Nevada, Iowa

TAMA COUNTY,
Toledo, Iowa

TAYLOR COUNTY,
Medford, Wisconsin

TOWN OF ADDISON,
Dallas, Texas

TOWN OF DUDLEY,
Dudley, Massachusetts

TOWN OF GLASTONBURY,
Glastonbury, Connecticut

TRAVERSE COUNTY,
Wheaton, Minnesota

TREMPEALEAU COUNTY,
Whitehall, Wisconsin

VERNON COUNTY,
Viroqua, Wisconsin

VILAS COUNTY,
Eagle River, Wisconsin

VILLAGE OF DEERFIELD,
Deerfield, Illinois

VILLAGE OF GERMANTOWN,
Germantown, Wisconsin

VILLAGE OF GURNEE,
Gurnee, Illinois

VILLAGE OF WESTON,
Weston, Wisconsin

VILLAGE OF WINNETKA,
Winnetka, Illinois

WALWORTH COUNTY,
Elkhorn, Wisconsin

WAPELLO COUNTY,
Ottumwa, Iowa

WARREN COUNTY,
Warrenton, Missouri

WASHBURN COUNTY,
Shell Lake, Wisconsin

WASHINGTON COUNTY,
Blaire, Nebraska

WASHINGTON COUNTY,
Stillwater, Minnesota

WASHINGTON COUNTY,
West Bend, Wisconsin

WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY

(WMATA),
Washington, D.C.

WAUKESHA COUNTY,
Waukesha, Wisconsin

WAUSHARA COUNTY,
Wautoma, Wisconsin

WEST CENTRAL INTEROPERABILITY ALLIANCE (WCIA),
Wisconsin

WHITE COUNTY,
Carmi, Illinois

WHITESIDE COUNTY,
Morrison, Illinois

WICHITA TRANSIT,
Wichita, Kansas

WILLIAMS COUNTY,
Williston, North Dakota

WILLIAMSON COUNTY,
Georgetown, Texas

WINNEBAGO COUNTY,
Forest City, Iowa

WINNESHIEK COUNTY,
Decorah, Iowa

WINONA COUNTY,
Winona, Minnesota

WISCONSIN, STATE OF,
DEPARTMENT OF REVENUE,
Madison, Wisconsin

WOOD COUNTY,
Wisconsin Rapids, Wisconsin

WOODBURY COUNTY,
Sioux City, Iowa

SECTION 4: COMPANY AND STAFF QUALIFICATIONS (EXPERIENCE)

Please see True North’s proposed project team and resumes, which are listed below.

PROPOSED PROJECT TEAM

- Dr. Patrick Johnson
- Mike Indergard
- Dimitrios Hilton
- Tyrone E. Wilson
- Warren Campbell

DR. PATRICK JOHNSON

Patrick is the Cybersecurity Practice Manager for True North Consulting Group. Patrick has over 27 years of experience in information technology, with the last six years focused on cybersecurity. Before joining True North, Patrick was a senior manager responsible for engineering teams supporting data centers, infrastructure, and communications for a large county government. Patrick has also served K12 public schools and has been a consultant for a non-profit. At True North, common projects include applying security & risk frameworks to organizations, risk assessments, vulnerability assessments, governance planning, disaster recovery planning, and operational analysis and development.

MIKE INDERGARD

Mike is the Director of Strategic Planning for True North Consulting Group. He brings over 20 years of experience in IT administration, systems engineering, and strategic planning to every project he supports. Mike's areas of expertise include security architecture, wireless security, NGFW, VPN, security policy, and Project Management.

DIMITRIOS HILTON

Dimitrios is a Senior Cybersecurity and IT Technology Consultant. He brings over 19 years of experience and expertise to any upcoming projects. Qualifications include FBI, Homeland Security, and CJIS throughout the United States as part of overall knowledge.

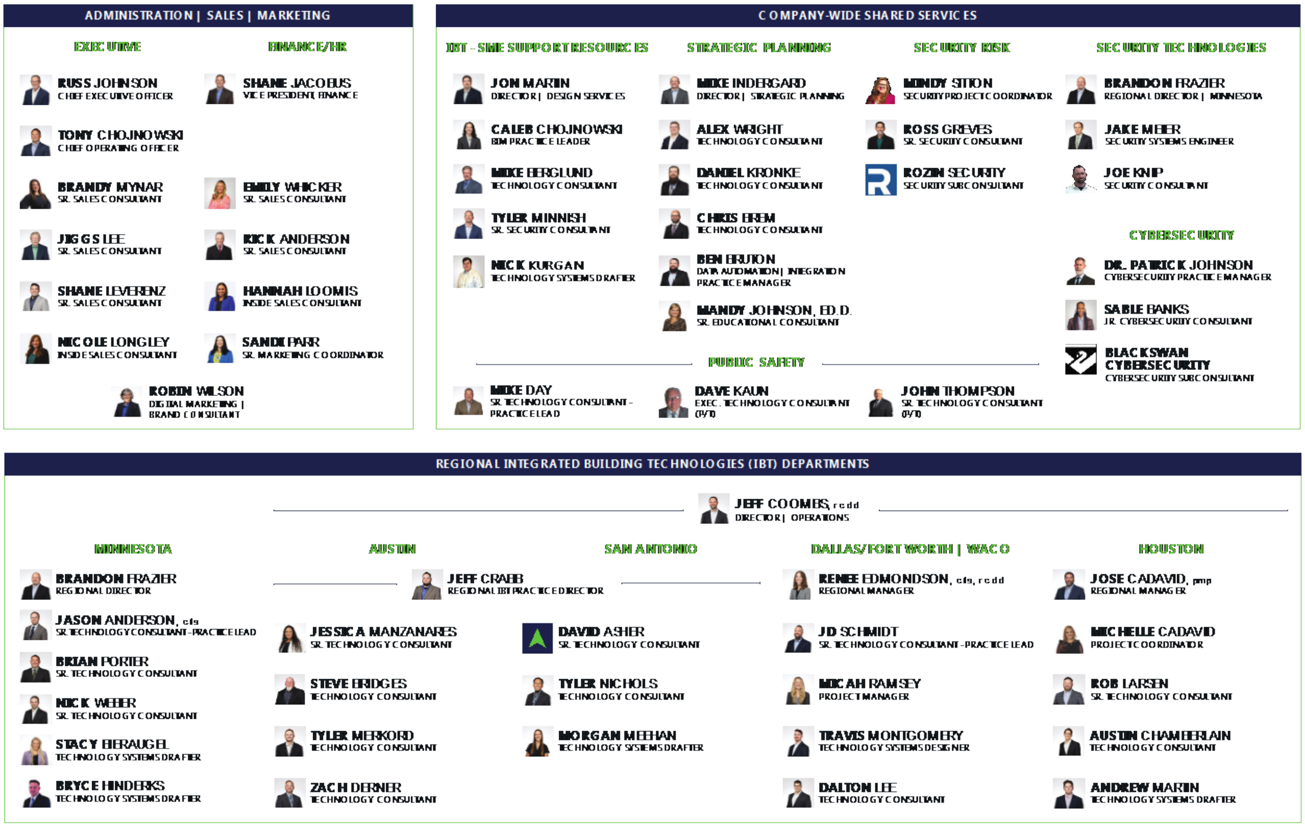
TYRONE E. WILSON

Tyrone is a Senior Cybersecurity Consultant. He brings over 20 years of expertise in IT and cybersecurity to include state and federal government agencies.

WARREN CAMPBELL

Warren is a Senior Cybersecurity Consultant. He brings over 15 years of cybersecurity expertise in penetration testing, wireless, and vulnerability assessments with a primary focus on state and federal government.

ORGANIZATION CHART



ADMINISTRATION | SALES | MARKETING

EXECUTIVE

RUSS JOHNSON
CHIEF EXECUTIVE OFFICER

TONY CHOJNOWSKI
CHIEF OPERATING OFFICER

BRANDY MYNAR
SR. SALES CONSULTANT

JIGGS LEE
SR. SALES CONSULTANT

SHANE LEVERENZ
SR. SALES CONSULTANT

NICOLE LONGLEY
INSIDE SALES CONSULTANT

FINANCE/HR

SHANE JACOBUS
VICE PRESIDENT, FINANCE

EMILY WHICKER
SR. SALES CONSULTANT

RICK ANDERSON
SR. SALES CONSULTANT

HANNAH LOOMIS
INSIDE SALES CONSULTANT

SANDI PARR
SR. MARKETING COORDINATOR

ROBIN WILSON
DIGITAL MARKETING |
BRAND CONSULTANT

COMPANY-WIDE SHARED SERVICES

IBT - SME SUPPORT RESOURCES

JON MARTIN
DIRECTOR | DESIGN SERVICES

CALEB CHOJNOWSKI
BIM PRACTICE LEADER

MIKE BERGLUND
TECHNOLOGY CONSULTANT

TYLER MINNISH
SR. SECURITY CONSULTANT

NICK KURGAN
TECHNOLOGY SYSTEMS DRAFTER

STRATEGIC PLANNING

MIKE INDERGARD
DIRECTOR | STRATEGIC PLANNING

ALEX WRIGHT
TECHNOLOGY CONSULTANT

DANIEL KRONKE
TECHNOLOGY CONSULTANT

CHRIS BREM
TECHNOLOGY CONSULTANT

BEN BRUTON
DATA AUTOMATION | INTEGRATION
PRACTICE MANAGER

MANDY JOHNSON, ED.D.
SR. EDUCATIONAL CONSULTANT

SECURITY RISK

MINDY SITTON
SECURITY PROJECT COORDINATOR

ROSS GREVES
SR. SECURITY CONSULTANT

ROZIN SECURITY
SECURITY SUBCONSULTANT

SECURITY TECHNOLOGIES

BRANDON FRAZIER
REGIONAL DIRECTOR | MINNESOTA

JAKE MEIER
SECURITY SYSTEMS ENGINEER

JOE KNIP
SECURITY CONSULTANT

CYBERSECURITY

DR. PATRICK JOHNSON
CYBERSECURITY PRACTICE MANAGER

SABLE BANKS
JR. CYBERSECURITY CONSULTANT

BLACKSWAN CYBERSECURITY
CYBERSECURITY SUBCONSULTANT

PUBLIC SAFETY

MIKE DAY
SR. TECHNOLOGY CONSULTANT -
PRACTICE LEAD

DAVE KAUN
EXEC. TECHNOLOGY CONSULTANT
(P/T)

JOHN THOMPSON
SR. TECHNOLOGY CONSULTANT
(P/T)

REGIONAL INTEGRATED BUILDING TECHNOLOGIES (IBT) DEPARTMENTS

JEFF COOMBS, rcdd
DIRECTOR | OPERATIONS

MINNESOTA

BRANDON FRAZIER
REGIONAL DIRECTOR

JASON ANDERSON, cts
SR. TECHNOLOGY CONSULTANT - PRACTICE LEAD

BRIAN PORTER
SR. TECHNOLOGY CONSULTANT

NICK WEBER
SR. TECHNOLOGY CONSULTANT

STACY BIERAUGEL
TECHNOLOGY SYSTEMS DRAFTER

BRYCE HINDERKS
TECHNOLOGY SYSTEMS DRAFTER

AUSTIN

SAN ANTONIO

JEFF CRABB
REGIONAL IBT PRACTICE DIRECTOR

JESSICA MANZANARES
SR. TECHNOLOGY CONSULTANT

STEVE BRIDGES
TECHNOLOGY CONSULTANT

TYLER MERKORD
TECHNOLOGY CONSULTANT

ZACH DERNER
TECHNOLOGY CONSULTANT

DAVID ASHER
SR. TECHNOLOGY CONSULTANT

TYLER NICHOLS
TECHNOLOGY CONSULTANT

MORGAN MEEHAN
TECHNOLOGY SYSTEMS DRAFTER

DALLAS/FORT WORTH | WACO

RENEE EDMONDSON, cts, rcdd
REGIONAL MANAGER

JD SCHMIDT
SR. TECHNOLOGY CONSULTANT - PRACTICE LEAD

MICAH RAMSEY
PROJECT MANAGER

TRAVIS MONTGOMERY
TECHNOLOGY SYSTEMS DESIGNER

DALTON LEE
TECHNOLOGY CONSULTANT

HOUSTON

JOSE CADAVID, pmp
REGIONAL MANAGER

MICHELLE CADAVID
PROJECT COORDINATOR

ROB LARSEN
SR. TECHNOLOGY CONSULTANT

AUSTIN CHAMBERLAIN
TECHNOLOGY CONSULTANT

ANDREW MARTIN
TECHNOLOGY SYSTEMS DRAFTER

- Dimitrios Hilton, Executive Security Consultant......................Reports to Mike Indergard
- Tyrone E. Wilson, Senior Cybersecurity Consultant.............Reports to Mike Indergard
- Warren Campbell, Senior Cybersecurity Consultant.........Reports to Mike Indergard

PROJECT TEAM RESUMES

Please see the project team resumes on the following pages.

PATRICK JOHNSON

CYBERSECURITY PRACTICE MANAGER

EDUCATION

CALIFORNIA INTERCONTINENTAL UNIVERSITY

- Doctor of Business Administration – Information Systems & Enterprise Resource Management

UNIVERSITY OF NORTH TEXAS

- Master of Science - Computer Education & Cognitive Systems

UNIVERSITY OF TEXAS AT ARLINGTON

- Bachelor of Science - Information Systems

AREAS OF EXPERTISE

- Cybersecurity
- Information systems development, implementations, and integration
- Networking and security infrastructure
- Project Management
- Technology Planning
- Fiscal Management
- Data Centers

TRAINING, CERTIFICATIONS, AND MEMBERSHIPS

- COBIT 5: ISACA – Control Objectives for Information and Related Technologies
- ITIL Foundations: HDI – Information Technology Infrastructure Library
- CISSP: ISC2 – Certified Information Systems Security Professional
- (ISC)2 – International Information Systems Security Certification Consortium
- LISD – Bond Oversight Committee
- LISD – Technology Advisory Committee
- COSN – Consortium of School Networks
- Phi Kappa Phi – National Honors Society - UNT Denton Chapter
- TxDLA – Texas Distance Learning Association
- TCEA – Texas Computer Education Association
- ISTE – International Society for Technology in Education
- BPA – Business Professionals of America

SIGNIFICANT PROJECTS

NETWORK SERVICES

- **INTERNET RESILIENCY ARCHITECTURE** – Architected two disparate 5Gbps links to the Internet with redundant gear for firewalls, filtering, and routing providing; intent was to provide 24/7 uninterrupted access for teaching, learning, and district operations.
- **DATA CENTER CORE RESILIENCY ARCHITECTURE** – The core access routing and switching gear was completed replaced and implemented in a tiered and redundant fashion to ensure uninterrupted access for teaching, learning, and district operations.
- **90% SERVER VIRTUALIZATION** – Using VmWare virtualization technology, 90% of physical servers were removed from the datacenter. The result was lowered costs of power, HVAC, UPS load; provided flexibility of adding removing compute resources at will, lending to extreme growth capacity.
- **STATE-OF-THE-ART WEB CONTENT FILTERING** – New content filter stack was implemented with redundancy and scale in mind; solution allows for decryption of network traffic as more and more websites begin to use HTTPS to encrypt and hide traffic content. The ability to modify Web 2.0 content is also a differentiator in services offered to students.
- **DISASTER RECOVERY (DR) PLAN IMPLEMENTED** – Architected plans for business continuity and disaster recovery which included collaboration between network, infrastructure, and data services teams. The DR site was architected with the state-of-the-art converged computing Vblock platform. EMC and VmWare tools were integral to the plan and processes.

INFRASTRUCTURE SERVICES

- **DISTRICT WIRELESS ACCESS INITIATIVE (DWAI)** – A complete overhaul of all wireless networking district-wide; included renovation of HVAC, data racks, copper cabling for 1 wireless access point for every classroom in the district at 69 campuses and 15 other facilities. Wireless access point count is 5800+. Provided 10Gbps fiber between data closets at all secondary campuses.
- **UNITE PRIVATE NETWORKS (UPN) INITIATIVE** – Provided 10Gbps fiber from each of the 69 campuses to the main LISD datacenter; partially funded through the Federal E-rate program and bond funds.

EXPERIENCE

2019 – PRESENT **TRUE NORTH CONSULTING GROUP**
CYBERSECURITY PRACTICE MANAGER

2017 – 2019 **TARRANT COUNTY**
SENIOR IT RESOURCE MANAGER

2016 – 2017 **EDUCATIONSUPERHIGHWAY**
SENIOR NETWORK CONSULTANT

2015 – 2016 **LEWISVILLE INDEPENDENT SCHOOL DISTRICT**
INTERIM DIRECTOR OF NETWORK & TECHNICAL SERVICES

MIKE INDERGARD

DIRECTOR OF STRATEGIC PLANNING

EDUCATION

BAYLOR UNIVERSITY

- Master of Information Systems

TEXAS STATE TECHNICAL COLLEGE

- Network Administration

TEXAS CHRISTIAN UNIVERSITY

- Bachelor of Arts (History)

AREAS OF EXPERTISE

- Advanced Routing and Switching
- VoIP and Video
- Enterprise Wireless
- Network Security
- Virtualization & Storage
- Strategic Planning
- Project Management
- Setting Policy
- Fostering Culture

TRAINING AND CERTIFICATIONS

- Cisco CCNA
- Cisco CCNP R/S
- Cisco CCNP Security
- Cisco CCDA
- Cisco CCDP
- Microsoft MCSE 2003
- Meraki CMNA
- Ekahau ECSE Design

SIGNIFICANT PROJECTS

KLEIN INDEPENDENT SCHOOL DISTRICT

Led a comprehensive technology assessment of all district facilities (over 60) as project manager and lead senior technology consultant, assessing the state of the LAN, WLAN, WAN and ISP services, structured cabling, compute/data storage infrastructure, data center facilities, campus security systems, telecommunications rooms, cybersecurity systems, and classroom and instructional technology, including remediation recommendations and cost estimations. Efforts also included focus groups, surveys, and interviews to assess how technology is applied to students' learning. True North is currently leveraging these findings toward technology planning for an upcoming multimillion-dollar bond.

HUTTO INDEPENDENT SCHOOL DISTRICT

Led a comprehensive technology assessment of all district facilities that assessed all major operational and instructional technology systems and infrastructure, major applications in use, and cybersecurity posture, including IT risk assessment and internal and external network vulnerabilities scans and remediation matrices. The assessment also included wireless LAN site surveys to illustrate coverage, interference, and throughput from the perspective of the mobile devices. Findings have led to a multiyear bond project, with TNCG chosen as HISD's technology consultant for the design, bidding, and contract administration on classroom AV, WAN, data center network, and campus renovations.

RICHARDSON INDEPENDENT SCHOOL DISTRICT

In partnership with Region 10, led a comprehensive technology assessment of all administrative, operational, instructional, and common/public areas of all district facilities (over 50) for the state of its technology and how it supports learning during and post COVID19. Also included cybersecurity assessments of the WLAN, network perimeter, and a social engineering campaign, as well as a technology department staff comparison study (to peer districts) and an applications governance review. RISD is using these findings and recommendations and the associated cost estimations to remediate them toward technology planning for the future.

ECTOR COUNTY INDEPENDENT SCHOOL DISTRICT

True North has conducted two technology assessments for ECISD: a comprehensive one in 2016 that focused and on both operational/infrastructure and instruction at all 57 district sites, and one in 2019 that focused solely on the infrastructure districtwide. Both assessments were key components toward bond planning efforts for the technology department and CTO. The 2016 assessment led to Erate projects over the next five years that increased the WLAN capacity at the campuses for digital learning and a multimillion-dollar upgrade of the wide area network to a high-speed, resilient, scalable foundation for all operational and instructional applications across ECISD.

EXPERIENCE

2017 – PRESENT **TRUE NORTH CONSULTING GROUP**
DIRECTOR OF STRATEGIC PLANNING

2011 – 2017 **TECHNOLOGY FOR EDUCATION**
DIRECTOR OF TECHNICAL SERVICES

2009 – 2011 **MCLANE INTELLIGENT SOLUTIONS**
IT CONSULTANT

2006 – 2007 **TECHNOLOGY FOR EDUCATION**
SYSTEMS ENGINEER

2001 – 2006 **COLDWELL BANKER REALTORS**
IT ADMINISTRATOR

DIMITRIOS HILTON

PROFESSIONAL SUMMARY

Accomplished Security Professional and IT Operational consultant for over 16+ years. Extensive experience and leadership in the Local Government space, as well as small and mid-sized private organizations. Uniquely combines his background in law enforcement with information security expertise to render security auditing deliverables and recommendations that are well received by management, which ultimately help organizations make immediate and long-term changes that improve their security posture.

WORK HISTORY

InfoSec Associates, LTD – Minneapolis, MN (2014 – 2021)

- Conduct Security Assessments (PCI, HIPAA, CJIS, NIST, SCADA, HITRUST)
- Conduct Security Analyst Services (SIEM, IPS/IDS, Endpoints, IR, Defense in Depth)
- Develop Security Policies & Procedures (PCI, CJIS, HIPAA, Organizational)
- Security Training (PCI, HIPAA, CJIS, custom needs)
- CIO / CISO Services (Virtual and On-Premise)
- Project Management Services

LOGIS (Local Government Information Systems) – Golden Valley, MN (2015 – 2019)

- Security Specialist for 50 local government organizations
- PCI Specialist for over ~ 100 PCI environments
- Conduct Security Assessments (PCI, HIPAA, CJIS, SCADA)
- Developed Security Budgets for numerous cities
- Internal Security Analyst duties (SIEM, IPS/IDS, Endpoints, IR)
- Developed Security Policies & Procedures (PCI, CJIS, HIPAA, Organizational)
- Security Training (Citywide, organizational, PCI, HIPAA, CJIS, SCADA, custom needs)
- Vulnerability Management Program (PCI ASV, Web Application, Network)
- Project Management (Pen Testing, Security Auditing, Payment Processing conversions)
- Law Enforcement Security (CJIS/FBI Audits, LE Technology Audits)

The IT Guy, LTD – Saint Paul, MN (2004-2014)

- Information Technology Consulting Company (President/Senior Consultant)
- Managed 1-5 Staff (Finance, IT Technicians, Developers)
- Client sizes range from 1-1000 end-users across multiple industries, including Healthcare, Retail POS/PCI, Law, SCADA/ICS, and many other business types
- Server, Storage, Workstation, Backup, Endpoint protection, and many other services

EDUCATION

- Law Enforcement Certificate Program – Hennepin Technical College (2018)
- Post Grad – University of St. Thomas (1999) Superintendent/Principal Licensure
- M.S. Ed. – University of Pennsylvania (1992) – Education
- B.S. – Rutgers College (1990) – Dual Major Chemistry/Administration of Justice

CERTIFICATIONS

- Minnesota POST Certification (March 2019)– Hennepin Tech Law Enforcement Center
- CISSP Security (Valid)
- CISA Auditor – Expected Q1 2020
- SCADA Security Certificate for Infrastructure (Valid)
- Emergency Medical Responder (Valid)
- CJIS Level 4 Training (Valid)

PROFESSIONAL ACTIVITIES & ASSOCIATIONS

- ISC2 Security Congress – PCI Workshop Presenter (2017- Present)
- ISC2 (CISSP) Twin Cities Chapter President (2019 – Present)
- MN Government Finance Officers Association – Presenter PCI Seminar (2018)
- MS-ISAC Member

TYRONE E. WILSON

PROFESSIONAL SUMMARY

- 24 years of experience in Information Technology and Systems Configuration, with 20 years focused on Information Systems & Network Security. Organizer of The D.C. Cybersecurity Professionals, a 7,800+ member meetup group. Currently holding positions of increasing responsibility while serving in the Army Reserves.
- Extensive expertise in Computer Network Defense; Project and Program Management; Vulnerability Assessments and Penetration Testing; Cyber Threat Analysis; Security Center Operations; Security System Architecture Assessments; Information Systems Engineering; Incident Response; Data Mining; Splunk; IPv6; Metasploit; Kali (Linux); Web Application Testing (Burp Suite Pro), Information Security Training (Pentester Prep, SOC Analyst Prep, Certified Ethical Hacker Practical, CISSP, CySA+, Net+, Sec+)

EXPERIENCE

ACS Cyber SEAL Program, Member **03/2017 – Present**

Agile Cyber Security Solutions, LLC (Purcellville, VA)

- Serves as a lead for various cybersecurity awareness, security assessment, and penetration testing engagements
- Developed and led multiple spear phishing engagements targeting medium to large corporations
- Assists with network security assessments and stress testing of multi-million-dollar networks varying in agency
- Assists with the development and delivery of cybersecurity awareness and penetration testing training

Founder & President **06/2013 – *Present***

Cover6 Solutions, LLC (Arlington, VA)

- Presides over day-to-day operations of a 15-person company to include decision-making on strategies and policies
- Sponsors, hosts, and presents material to a 7,800+ person Meetup group (D.C. Cyber Security Professionals) teaching various aspects of Information Security, Intro to Cyber, Penetration Testing, IPv6, and SOC Analyst Preparation
- Performs freelance penetration testing and training for various organizations and small groups

Program Manager, Penetration Testing **07/2015 – 02/2016**

Fortalice Solutions (Washington, D.C.)

- Developed and lead penetration testing team and built the underlying process framework
- Conducted penetration tests on critical infrastructure, applications, and risk management programs
- Provided technical information system security testing in support of the appropriate risk management processes
- Provided quality assurance and technical reviews of deliverables, results, and internal documentation
- Developed and lead strong working relationships with clients and client leads

Cyber Security Analyst, Subject Matter Expert (SME) **07/2014 – 08/2015**
Novetta Solutions / Department of Energy (McLean, VA / Washington, D.C.)

- Managed and coordinated services essential to protecting, defending, and sustaining the three echelons of the Department of Defense computer networks (NIPR, SIPR, and JWICS) on strategic infrastructure
- Ingested emerging threat reports to generate protection plans for the enterprise
- Coordinated the mitigation of over 20 high-threat CND events since 01 January 2015
- Presided over evaluation of endpoint applications, hardware, and network services
- Provided training on security testing tools such as (Nmap, Netcat, Metasploit, Retina, Nessus, Kali, Wireshark, etc.)

Senior Cyber Security Analyst **06/2011 – 11/2013**
Salient Federal Solutions (Fairfax, VA)

- Cyber security Subject Matter Expert (SME) responsible for the security posture of over 1000 systems at 19 locations
- Lead analyst responsible for signature management of IPv6 Intrusion Prevention & Detection System (Assure6)
- Developed and implemented incident response procedures for mitigating direct and indirect network attacks
- Coordinated the integration of the Splunk Enterprise threat management system into network structure
- Served as an Assistant Instructor for the IPv6 101 and IPv6 Security courses

Cyber Threat Analyst, Non-Commissioned Officer in Charge **06/2010 – 05/2011**
Regional Computer Emergency Response Team – Southwest Asia (RCERT-SWA) (Camp Victory, Iraq)

- Computer Network Defense (CND) SME responsible for the security posture of the DoD's Global Information Grid (GIG) in Iraq and Kuwait
- Developed the SWA Cyber Intelligence Cell SharePoint Portal; increased overall site usage by over 400%, enhancing the cyber situational awareness for SWA units
- Acted as the Sr. CND Analyst while auditing five Forward Operating Bases (FOBs) in Iraq; scanned, analyzed, and recommended upgrades to security posture for over 10,000 systems
- Trained over 50 analysts on the utilization of network defense tools such as Centaur, ArcSight, Remedy, and the Host-Based Security System (HBSS) web console

Senior Level Information Assurance Analyst/Fusion Cell Team Lead **08/2008 – 06/2010**
Joint Task Force Global Network Operations, USCYBERCOM (Ft. Meade, MD)

- Principal Engineer: Supported CND effort as a Tier 3 Information Assurance analyst and Intrusion Set SME
- Analyzed, characterized, and tracked malicious network activity within the Department of Defense (DoD)
- Performed network intrusion analysis based on logs, netflow, firewalls, and full packet capture utilizing tools unique to the intelligence community
- Collaborated with various CNDSPs, CERTs, NOCs, and Intel organizations. Analyzed origins, pathways, methodologies of cyber activities to model and predict future intrusions against the GIG

Cyber Trends Analyst, Non-Commissioned Officer in Charge **05/2005 – 05/2008**
1st Information Operations Command, Cyber Intelligence Center (Ft. Belvoir, VA)

- Produced all source intelligence fusion used for weekly Army Network Analysis Report (ANAR) intelligence assessment, which is used by the analytic community to determine possible threats to the Global Information Grid

EDUCATION

University of Phoenix
Bachelor of Science, Information Technology; Information Systems Security - 2018

CERTIFICATIONS

- EC-Council Certified Ethical Hacker (CEH) Practical (CEH Master) - 2020
- eLearn Security Junior Penetration Tester (eJPT) - 2020 CompTIA Security+ ce (Security+) - 2019
- CompTIA Network+ ce (Network+) - 2019
- Cisco Certified Network Associate (CCNA) Security – 2014
- IPv6 Forum Certified Engineer (Silver) – 2012
- EC-Council Certified Ethical Hacker (CEH) – 2007
- ArcSight Certified Advanced Security Analyst (ACASA) – 2006
- System Administrator/ Network Security Manager (SA/NSM) – 2003
- Information Assurance Security Officer (IASO) – 2003

PROFESSIONAL EDUCATION

Routing and Switching (CCNA), Secure Ninja - 2016
Advanced Leader Course – US Army - 2014 (Distinguished Honor Graduate)
IPv6 Essentials - SANS - 2012
Penetration Testing & Ethical Hacking - SANS - 2012
Basic Fiber Optics Course – US Army - 2010
Certified Ethical Hacker, Boot Camp - 2007
Securing Windows 2003 Server – US Army - 2005
Information Systems Operator/Analyst Course - 2002
Certified Information Systems Security Professional (CISSP), Intense School Boot Camp - 2007
Basic Non-Commissioned Officer Course - 2007
Computer Network Defense Course (CNDC) - 2003
Primary Leadership Development Course – US Army - 2003 (Commandants List, Appeared in Leadership Board

REVIEW BOARD POSITIONS

BSides NoVA - 2017-Present
Howard University - Cybersecurity - 2020-Present

SPEAKING ENGAGEMENTS

- SANS Webcast - 2020
- Hacker Halted - 2020, 2019 (Keynote)
- BSides NoVA - 2020, 2019, 2017
- Tactical Edge Virtual Summit -2020 BSides DC (2018, 2017)
- ISACA GWDC Cybersecurity & Risk Conference - 2018
- HashtagVOA: #OPMHack - 2015

WARREN CAMPBELL

PROFESSIONAL SUMMARY

Warren is a Senior Security Consultant who specializes in Penetration Testing. He has worked with customers throughout the US to help secure their systems from malicious intruders. Warren's passion for technology and learning has led him to always discover new ways to help customers implement proactive methods for hardening their networks.

SKILL SUMMARY

Wireless Penetration Testing
Warren has worked with securing wireless networks using offensive security tactics to test the encryption methods and authentication of access points.

Infrastructure Penetration Testing
Warren has an extensive history of penetration testing for external and internal networks. He utilizes a wide variety of tools to infiltrate systems, following industry best practices and giving extensive recommendations on how companies can stop attackers in their tracks.

Web Application Penetration Testing
Warren has worked to identify vulnerabilities within web applications utilizing industry-recognized methodologies such as the OWASP Top 10. He identifies potential exploitable security gaps within applications and delivers recommendations to the company on how to best secure the system.

TECHNICAL EXPERTISE

- Penetration Testing
- Wireless Penetration Testing
- Open Source Intelligence Gathering
- Network Architecture
- Nessus
- Metasploit
- Burp Suite Pro
- NMap
- Docker
- VMware
- Linux
- Windows
- Vulnerability Scanning
- Password Cracking
- Segmentation Scanning

WORK HISTORY

Infrastructure Penetration Tester
Large Telecommunications Company
Large-scale PCI infrastructure penetration testing effort to assess the hardening status and exploitability of over a thousand hosts within the internal network. Machines included end-user workstations, Windows and Linux Server, Firewalls, Load Balancers, and Credit Card processors.

Warren's responsibilities included:

- Leading a small team of five penetration testers on the engagement.
  - Organizing the team and assigning individual roles.
  - Interfacing with the client to outline schedule and scope.
  - Regular check-ins with the client on status and findings.
- Testing of the environment, including segmentation scanning and penetration testing of the cardholder data environment perimeter.
- Reporting on findings, including rapid high-priority vulnerabilities.

Web Application Penetration Tester
Medium Sized Real Estate Company
Penetration Testing engagement of ten web applications to identify vulnerabilities that would allow attackers a method to compromise the company or its customers.

Warren's responsibilities included:

- Leading a team of three penetration testers on the engagement.
  - Organizing the team and assigning individual roles.
  - Interfacing with the client to outline testing windows and scope.
  - Checking in with the client regularly to report on status and findings.
- Testing of the environment using penetration testing industry best practices for web applications such as the OWASP Top 10.
- Reporting on findings, including rapid high-priority vulnerabilities.

Security Consultant
Large HVAC Company
Multi-year contract with a nationwide HVAC company to assess the general security status of more than one hundred locations across the United States. The assessment included an evaluation of security practices on-site as well as within the internal network.

Warren's responsibilities included:

- Performing security assessments on-site at over a dozen locations.
  - Analyzing the security status of the wireless network, including methods of encryption and authentication.
  - Scanning the internal network to identify high-risk vulnerabilities that may put the location at risk.
  - Reviewing the status of hardening within Windows and Linux machines, including servers and workstations.
  - Developing a detailed series of recommendations to help remediate identified vulnerabilities.
- Reporting on findings, including rapid high-priority vulnerabilities.

EDUCATION

- Bachelors in Anthropology, University of Central Florida, Orlando, FL

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Offensive Security Certified Professional (OSCP)

RELEVANT COURSES

- Penetration Testing with Kali Linux
- Offensive Security Wireless Attacks

INDUSTRY EXPERIENCE

- Healthcare
- Payment Card Industry
- Energy
- Small Government
- Retail

SECTION 5: EXHIBIT A – PRICING PAGE

Please see Team TNCG's completed Exhibit A – Pricing Page below.

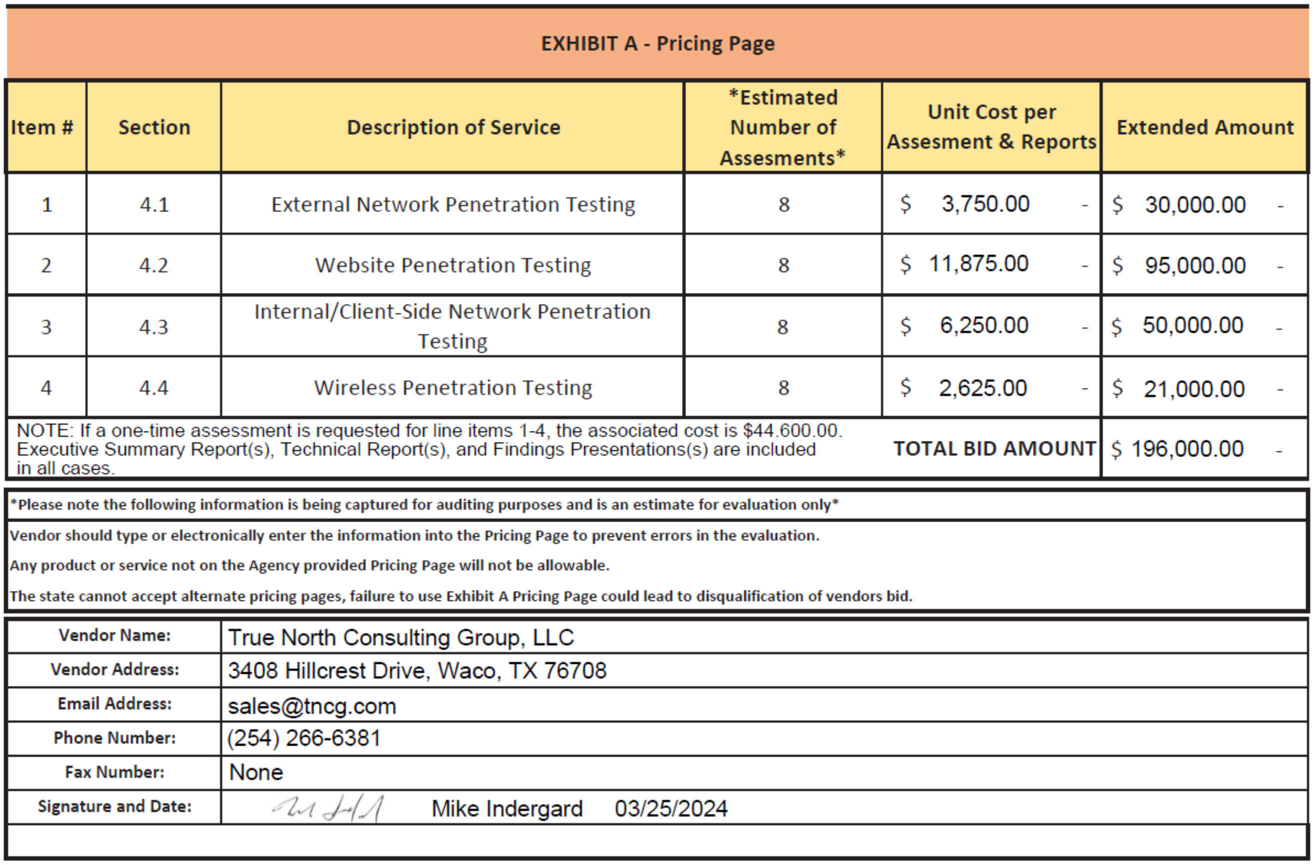


EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	$ 3,750.00 -	$ 30,000.00 -
2	4.2	Website Penetration Testing	8	$ 11,875.00 -	$ 95,000.00 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 6,250.00 -	$ 50,000.00 -
4	4.4	Wireless Penetration Testing	8	$ 2,625.00 -	$ 21,000.00 -
NOTE: If a one-time assessment is requested for line items 1-4, the associated cost is $44.600.00. Executive Summary Report(s), Technical Report(s), and Findings Presentations(s) are included in all cases.				TOTAL BID AMOUNT	$ 196,000.00 -

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

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

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

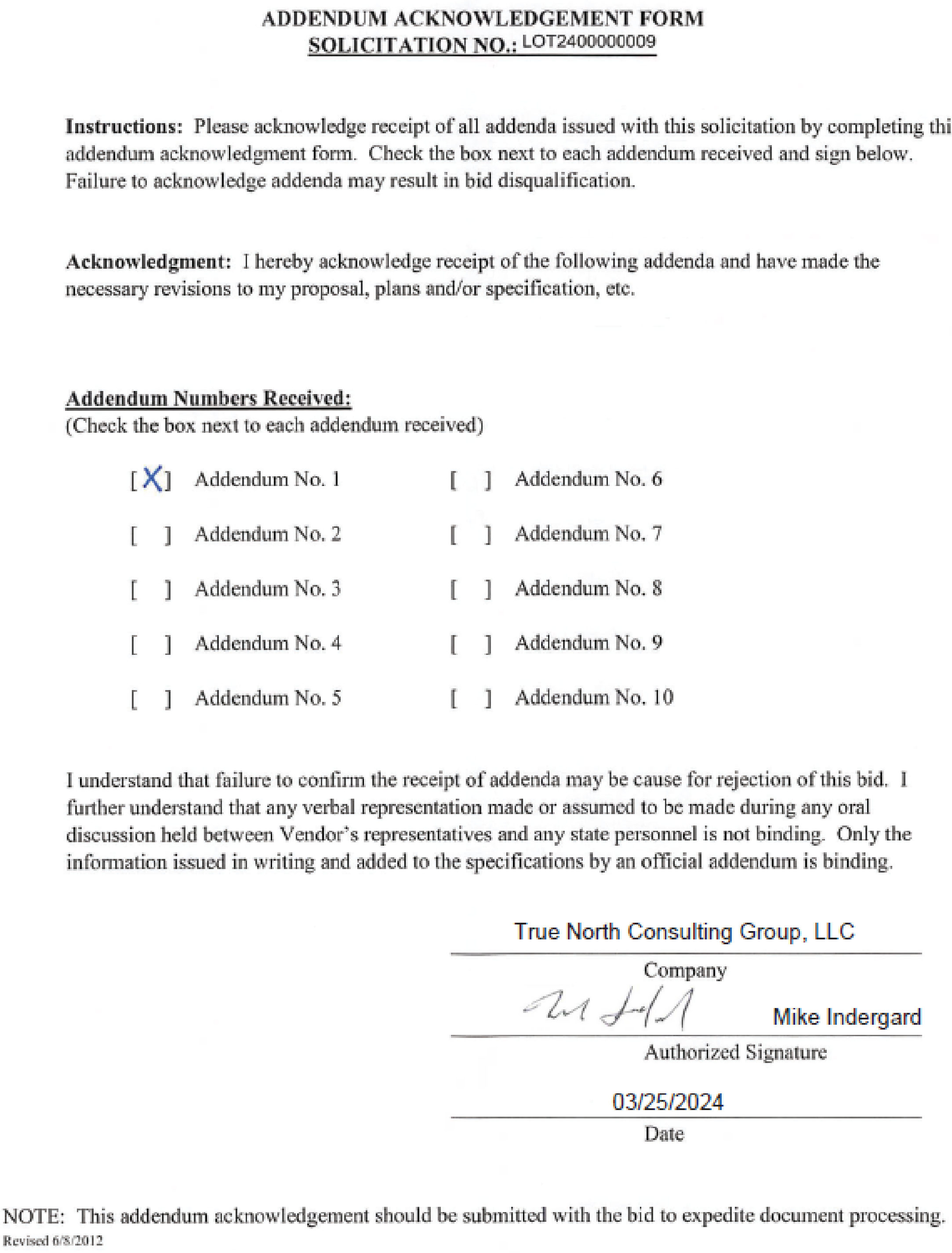
The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	True North Consulting Group, LLC
Vendor Address:	3408 Hillcrest Drive, Waco, TX 76708
Email Address:	sales@tncg.com
Phone Number:	(254) 266-6381
Fax Number:	None
Signature and Date:	Mike Indergard 03/25/2024

SECTION 6: ADDENDUM ACKNOWLEDGEMENT FORM & SIGNATURE PAGES

Please see Team TNCG's completed Addendum Acknowledgement Form and signature pages for the CRFQ and Addendum No. 1 on the following pages.

Addendum Acknowledgement Form



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.

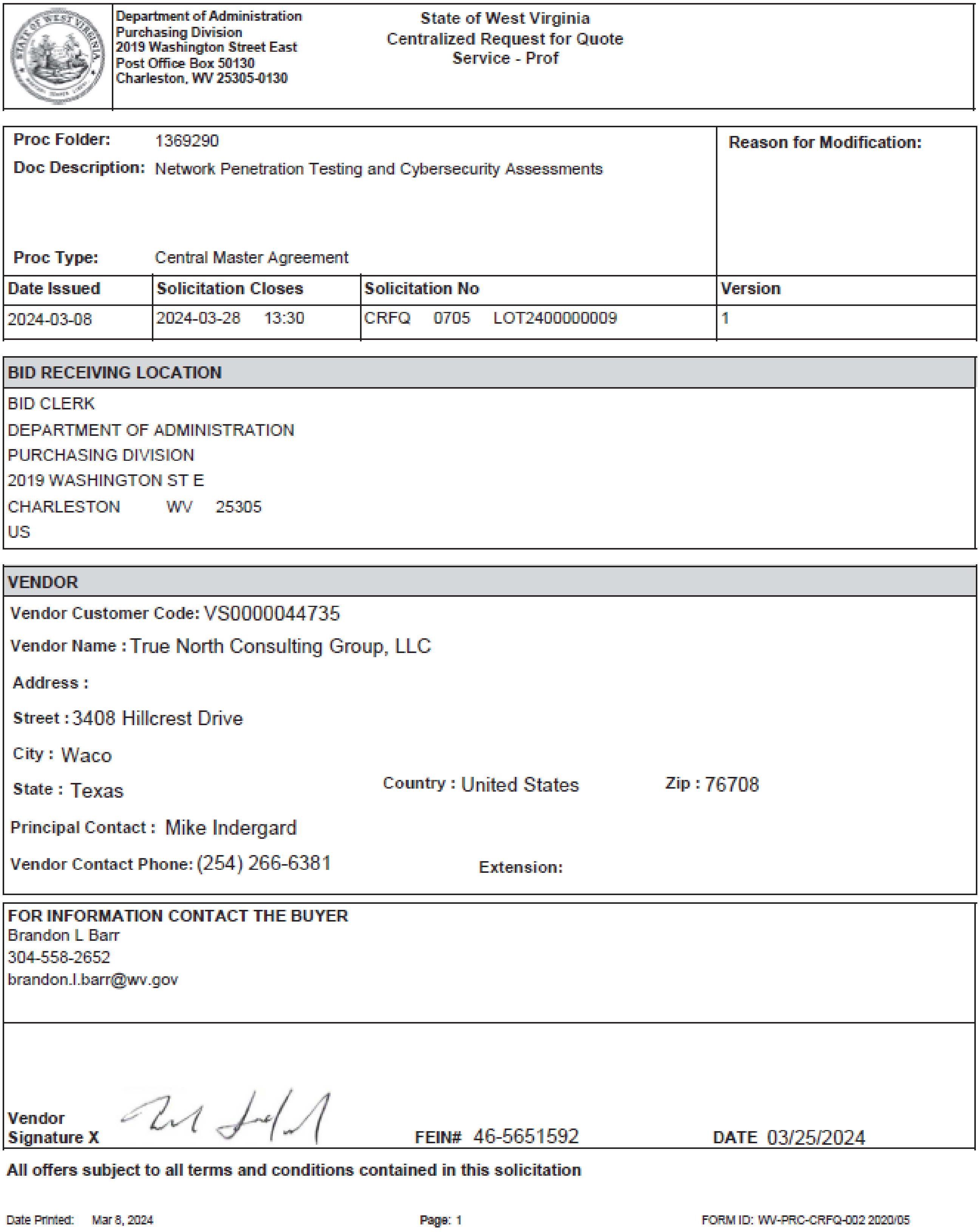
True North Consulting Group, LLC
Company

Mike Indergard
Authorized Signature

03/25/2024
Date

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

CRFQ Form Signature Page



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

State of West Virginia
Centralized Request for Quote
Service - Prof

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: VS0000044735

Vendor Name : True North Consulting Group, LLC

Address :

Street : 3408 Hillcrest Drive

City : Waco

State : Texas **Country :** United States **Zip :** 76708

Principal Contact : Mike Indergard

Vendor Contact Phone: (254) 266-6381 **Extension:**

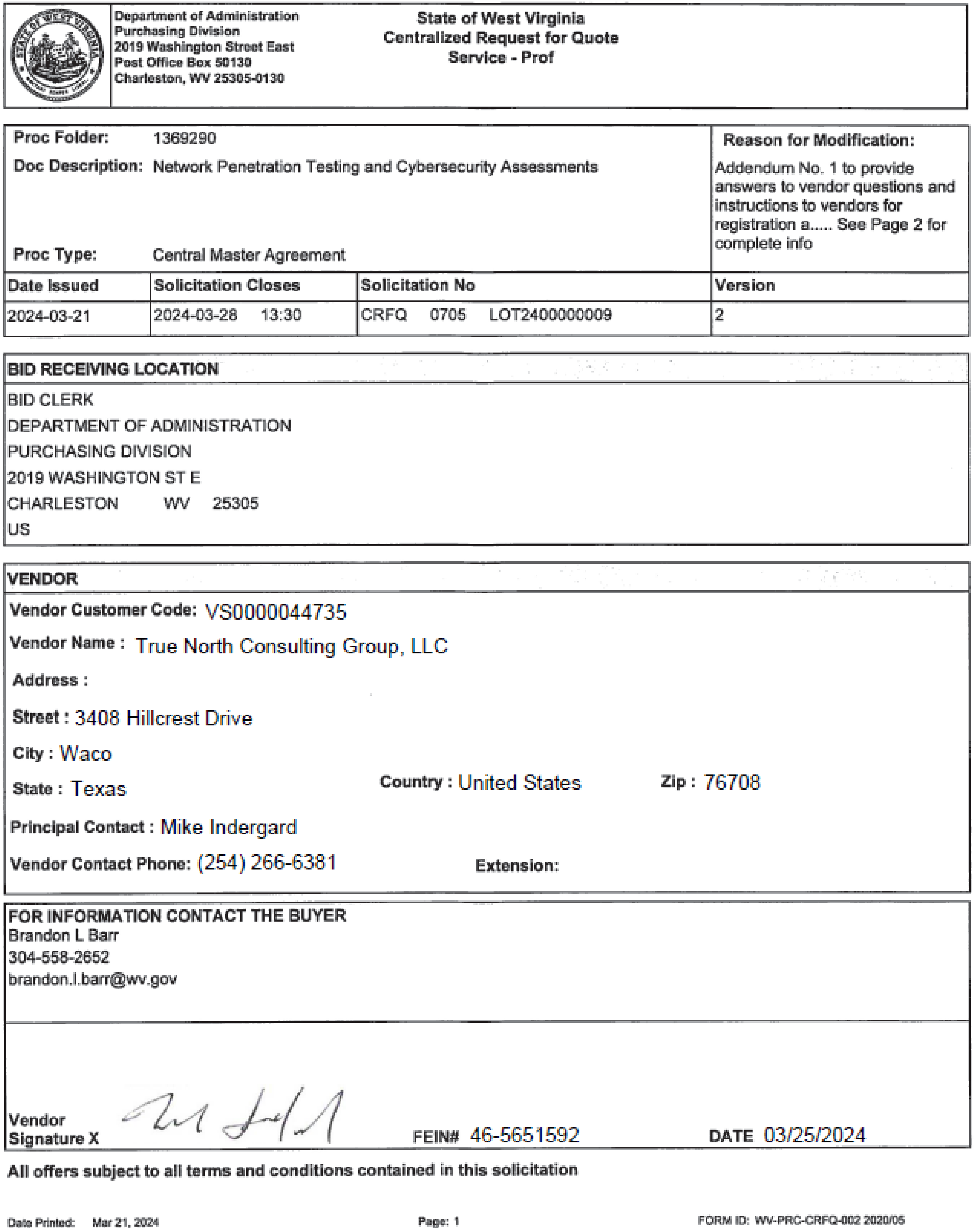
FOR INFORMATION CONTACT THE BUYER
Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

Vendor Signature X **FEIN#** 46-5651592 **DATE** 03/25/2024

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

Addendum No. 1 Signature Page



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

State of West Virginia
Centralized Request for Quote
Service - Prof

Proc Folder: 1369290

Doc Description: Network Penetration Testing and Cybersecurity Assessments

Proc Type: Central Master Agreement

Reason for Modification:
Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration a..... See Page 2 for complete info

Date Issued	Solicitation Closes	Solicitation No	Version
2024-03-21	2024-03-28 13:30	CRFQ 0705 LOT2400000009	2

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: VS0000044735

Vendor Name : True North Consulting Group, LLC

Address :

Street : 3408 Hillcrest Drive

City : Waco

State : Texas **Country :** United States **Zip :** 76708

Principal Contact : Mike Indergard

Vendor Contact Phone: (254) 266-6381 **Extension:**

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

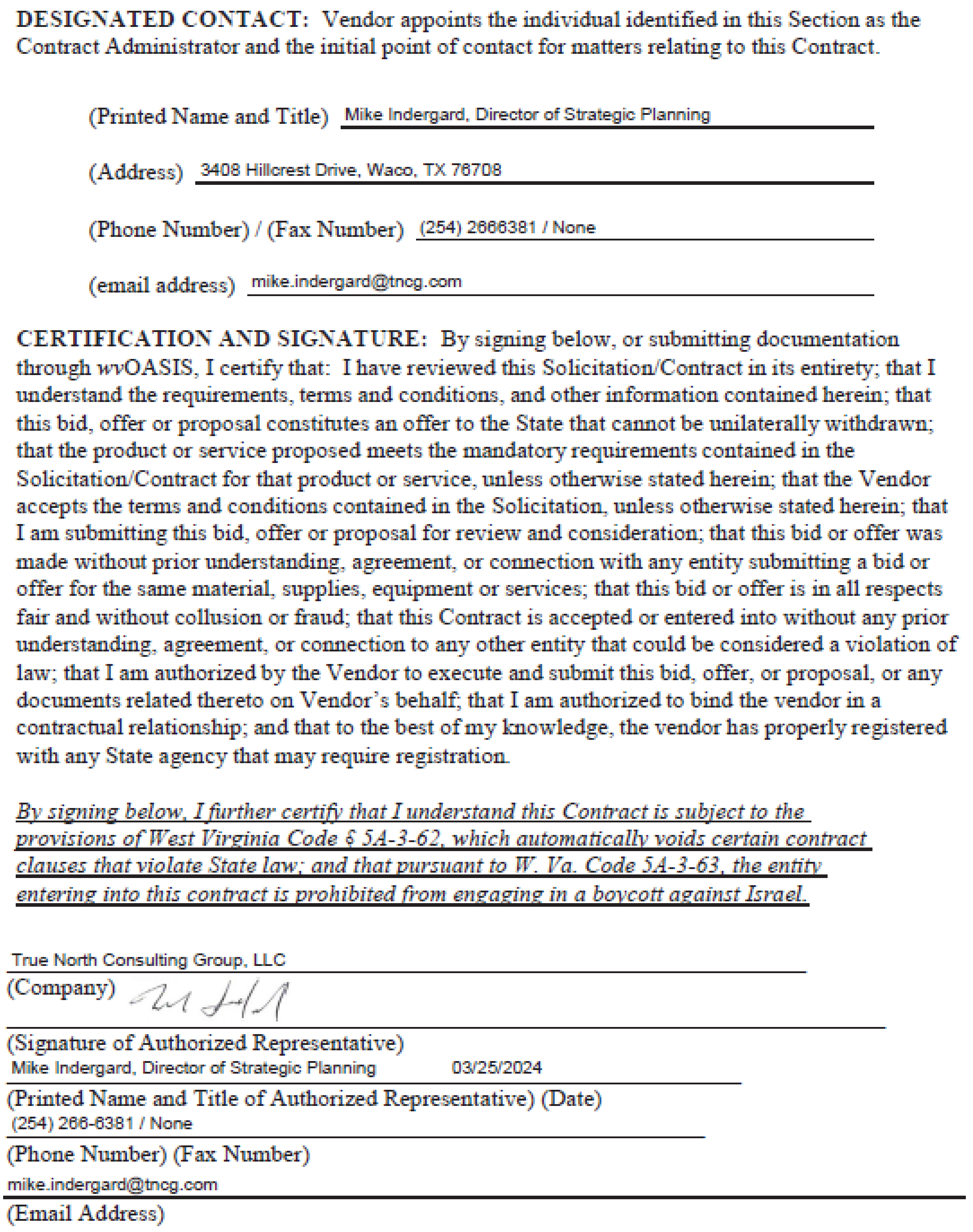
Vendor Signature X **FEIN#** 46-5651592 **DATE** 03/25/2024

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

SECTION 7: DESIGNATED CONTACT / CERTIFICATION AND SIGNATURE PAGE

Please see Team TNCG's Designated Contact / Certification and Signature Page below.



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) Mike Indergard, Director of Strategic Planning

(Address) 3408 Hillcrest Drive, Waco, TX 76708

(Phone Number) / (Fax Number) (254) 2666381 / None

(email address) mike.indergard@tncg.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.

True North Consulting Group, LLC
(Company)

(Signature of Authorized Representative)

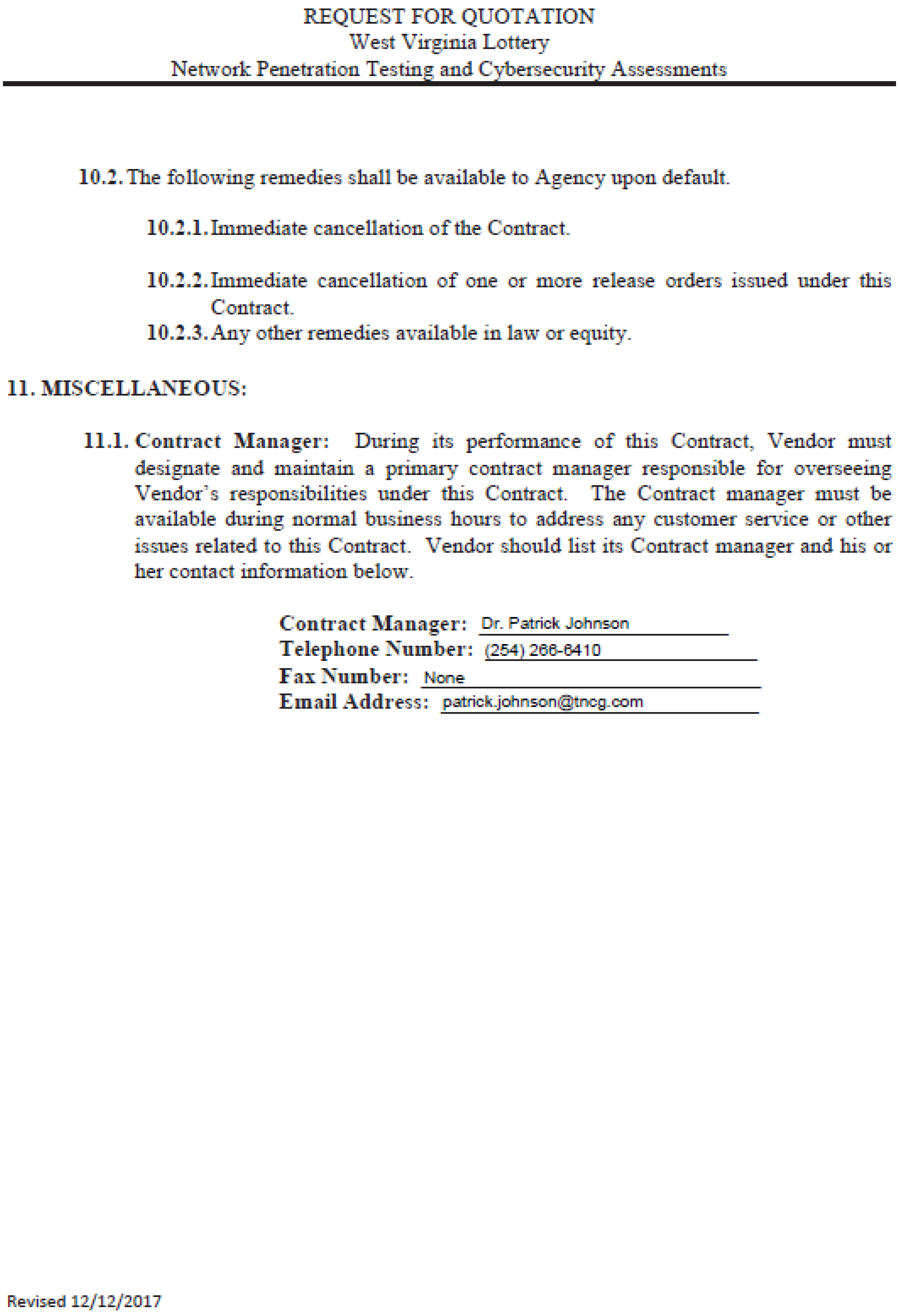
Mike Indergard, Director of Strategic Planning 03/25/2024
(Printed Name and Title of Authorized Representative) (Date)

(254) 266-6381 / None
(Phone Number) (Fax Number)

mike.indergard@tncg.com
(Email Address)

Revised 8/24/2023

SECTION 8: CONTRACT MANAGER



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

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

10.2.1. Immediate cancellation of the Contract.

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

10.2.3. Any other remedies available in law or equity.

11. MISCELLANEOUS:

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

Contract Manager: Dr. Patrick Johnson
Telephone Number: (254) 266-6410
Fax Number: None
Email Address: patrick.johnson@tncg.com

Revised 12/12/2017

SECTION 9: NON-DISCLOSURE AGREEMENT (NDA)

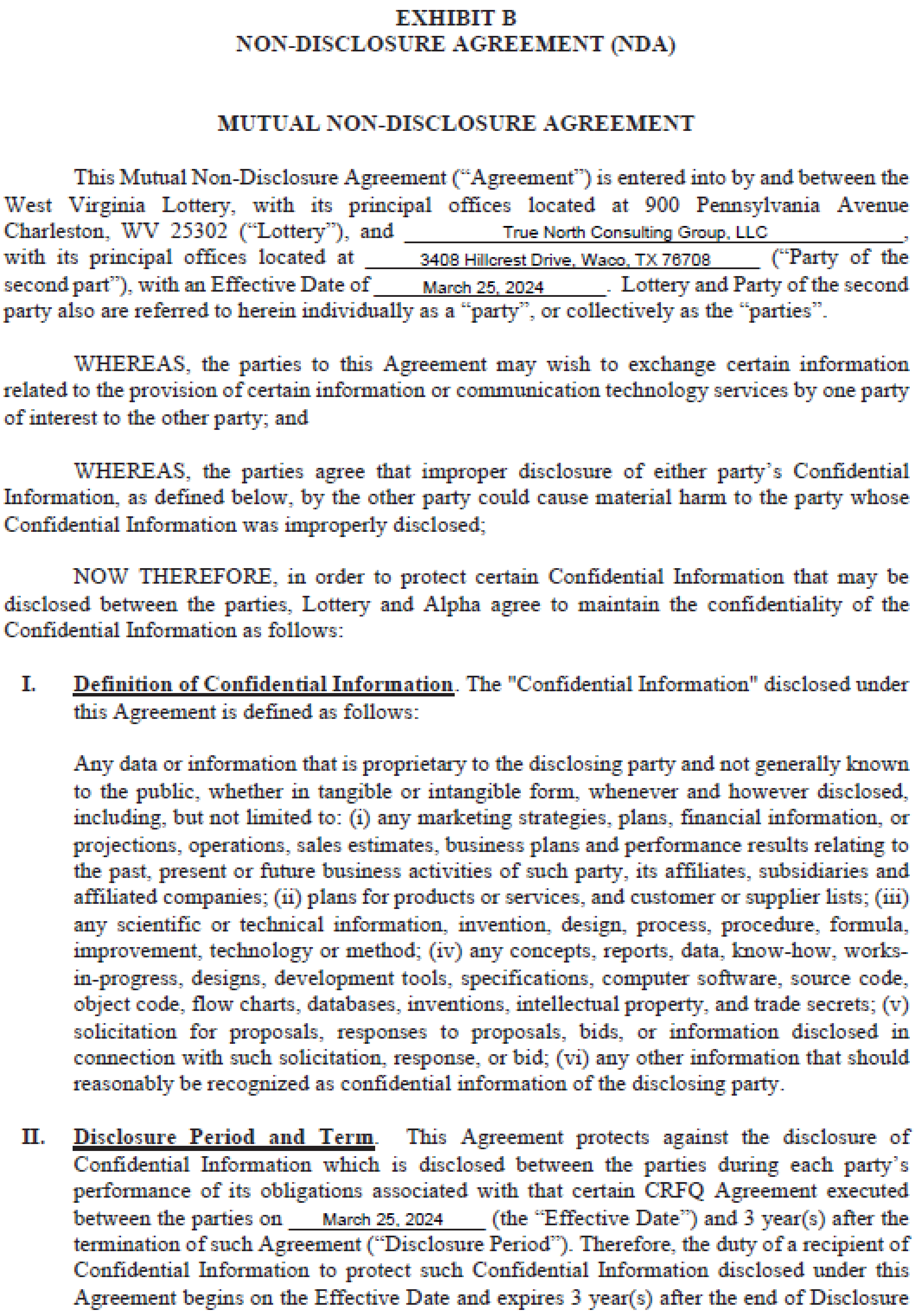


EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

MUTUAL NON-DISCLOSURE AGREEMENT

This Mutual Non-Disclosure Agreement ("Agreement") is entered into by and between the West Virginia Lottery, with its principal offices located at 900 Pennsylvania Avenue Charleston, WV 25302 ("Lottery"), and True North Consulting Group, LLC, with its principal offices located at 3408 Hillcrest Drive, Waco, TX 76708 ("Party of the second part"), with an Effective Date of March 25, 2024. Lottery and Party of the second party also are referred to herein individually as a "party", or collectively as the "parties".

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

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

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

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

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

II. **Disclosure Period and Term**. This Agreement protects against the disclosure of Confidential Information which is disclosed between the parties during each party's performance of its obligations associated with that certain CRFQ Agreement executed between the parties on March 25, 2024 (the "Effective Date") and 3 year(s) after the termination of such Agreement ("Disclosure Period"). Therefore, the duty of a recipient of Confidential Information to protect such Confidential Information disclosed under this Agreement begins on the Effective Date and expires 3 year(s) after the end of Disclosure

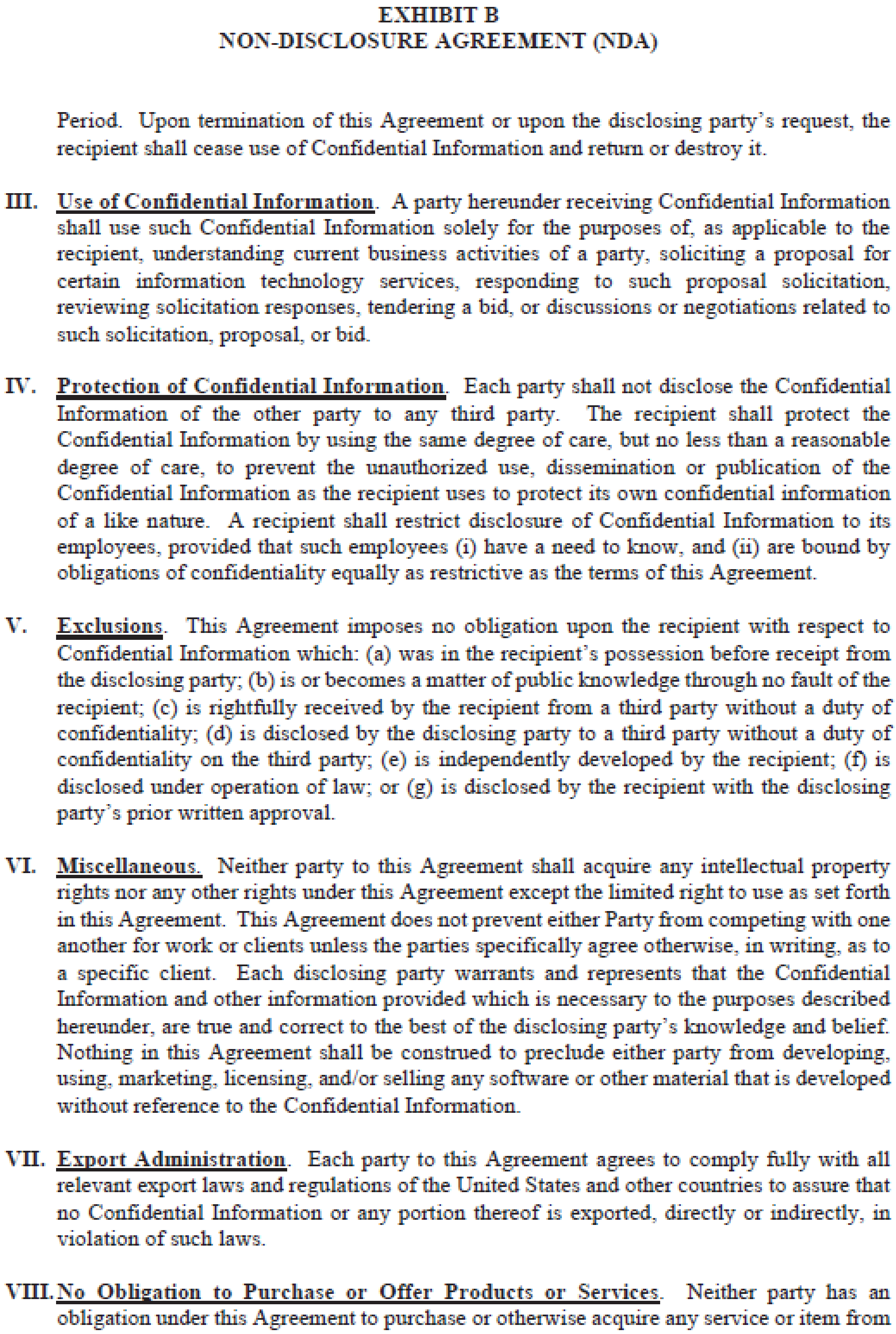


EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

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

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

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

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

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

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

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

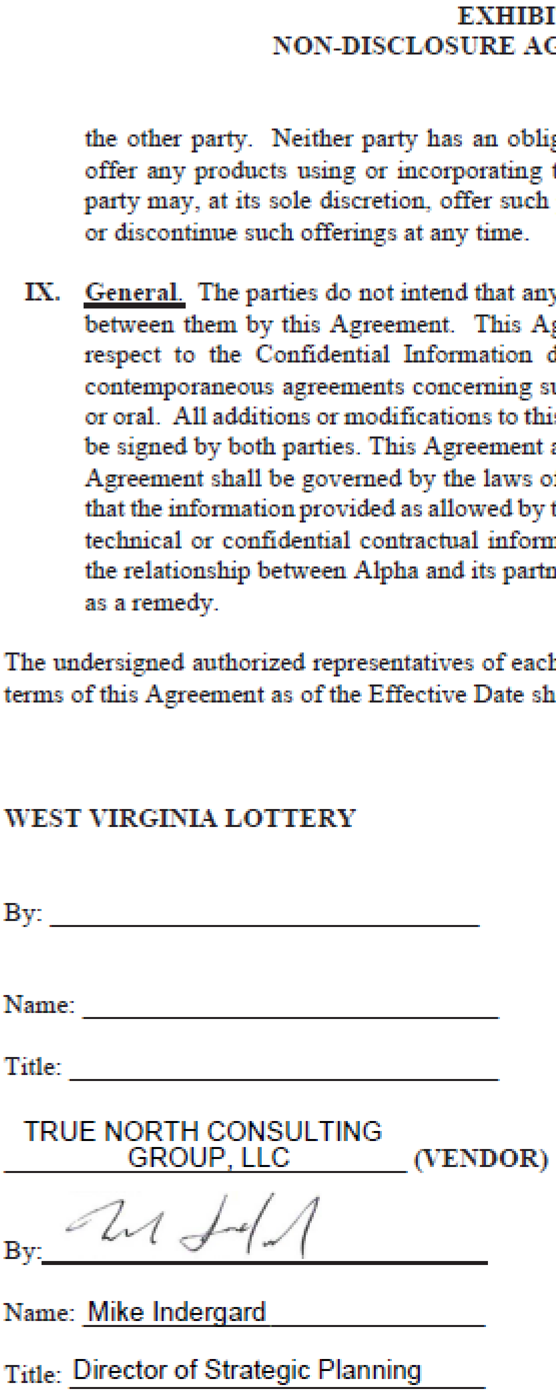


EXHIBIT B
NON-DISCLOSURE AGREEMENT (NDA)

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

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

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

WEST VIRGINIA LOTTERY

By: ______________________________

Name: ______________________________

Title: ______________________________

TRUE NORTH CONSULTING GROUP, LLC (VENDOR)

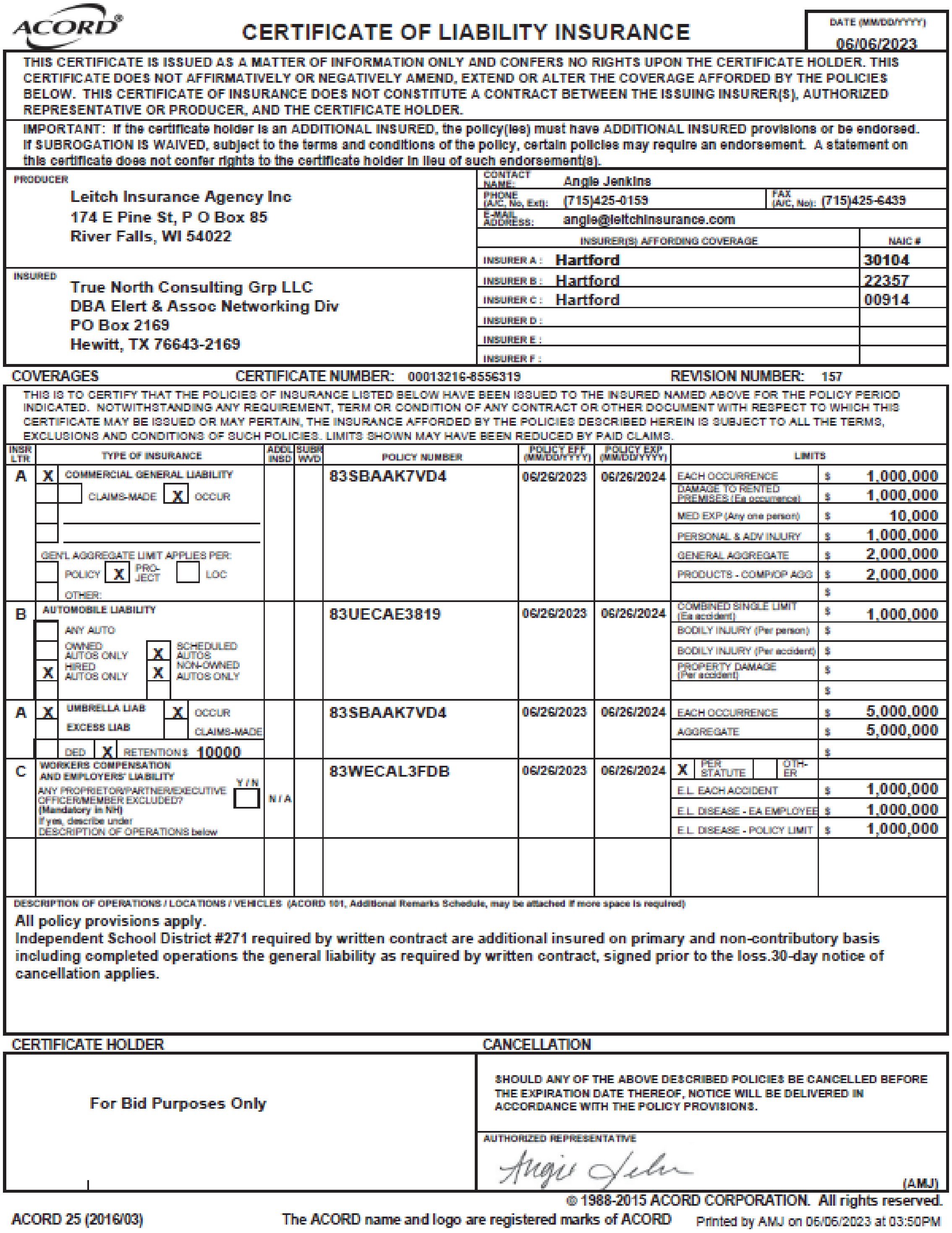
By: ______________________________

Name: Mike Indergard

Title: Director of Strategic Planning

SECTION 10: OTHER INFORMATION

GENERAL LIABILITY INSURANCE CERTIFICATE EXAMPLE



ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 06/06/2023

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

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

PRODUCER
Leitch Insurance Agency Inc
174 E Pine St, P O Box 85
River Falls, WI 54022

CONTACT NAME: Angie Jenkins
PHONE (A/C, No, Ext): (715)425-0159 FAX (A/C, No): (715)425-6439
E-MAIL ADDRESS: angie@leitchinsurance.com

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A :	Hartford	30104
INSURER B :	Hartford	22357
INSURER C :	Hartford	00914
INSURER D :		
INSURER E :		
INSURER F :		

INSURED
True North Consulting Grp LLC
DBA Elert & Assoc Networking Div
PO Box 2169
Hewitt, TX 76643-2169

COVERAGES CERTIFICATE NUMBER: 00013216-8556319 REVISION NUMBER: 157

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

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	☒ COMMERCIAL GENERAL LIABILITY □ CLAIMS-MADE ☒ OCCUR			83SBAAK7VD4	06/26/2023	06/26/2024	EACH OCCURRENCE	$ 1,000,000
							DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
							MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$ 2,000,000
	□ POLICY ☒ PRO-JECT □ LOC						PRODUCTS - COMP/OP AGG	$ 2,000,000
	OTHER:							$
B	AUTOMOBILE LIABILITY			83UECAE3819	06/26/2023	06/26/2024	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
	□ ANY AUTO						BODILY INJURY (Per person)	$
	□ OWNED AUTOS ONLY ☒ SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	☒ HIRED AUTOS ONLY ☒ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
								$
A	☒ UMBRELLA LIAB ☒ OCCUR			83SBAAK7VD4	06/26/2023	06/26/2024	EACH OCCURRENCE	$ 5,000,000
	□ EXCESS LIAB □ CLAIMS-MADE						AGGREGATE	$ 5,000,000
	□ DED ☒ RETENTION $ 10000							$
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY	Y / N		83WECAL3FDB	06/26/2023	06/26/2024	☒ PER STATUTE □ OTH-ER	
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? □ (Mandatory in NH)	N / A					E.L. EACH ACCIDENT	$ 1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	$ 1,000,000

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

All policy provisions apply.
Independent School District #271 required by written contract are additional insured on primary and non-contributory basis including completed operations the general liability as required by written contract, signed prior to the loss.30-day notice of cancellation applies.

CERTIFICATE HOLDER

For Bid Purposes Only

CANCELLATION

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

AUTHORIZED REPRESENTATIVE

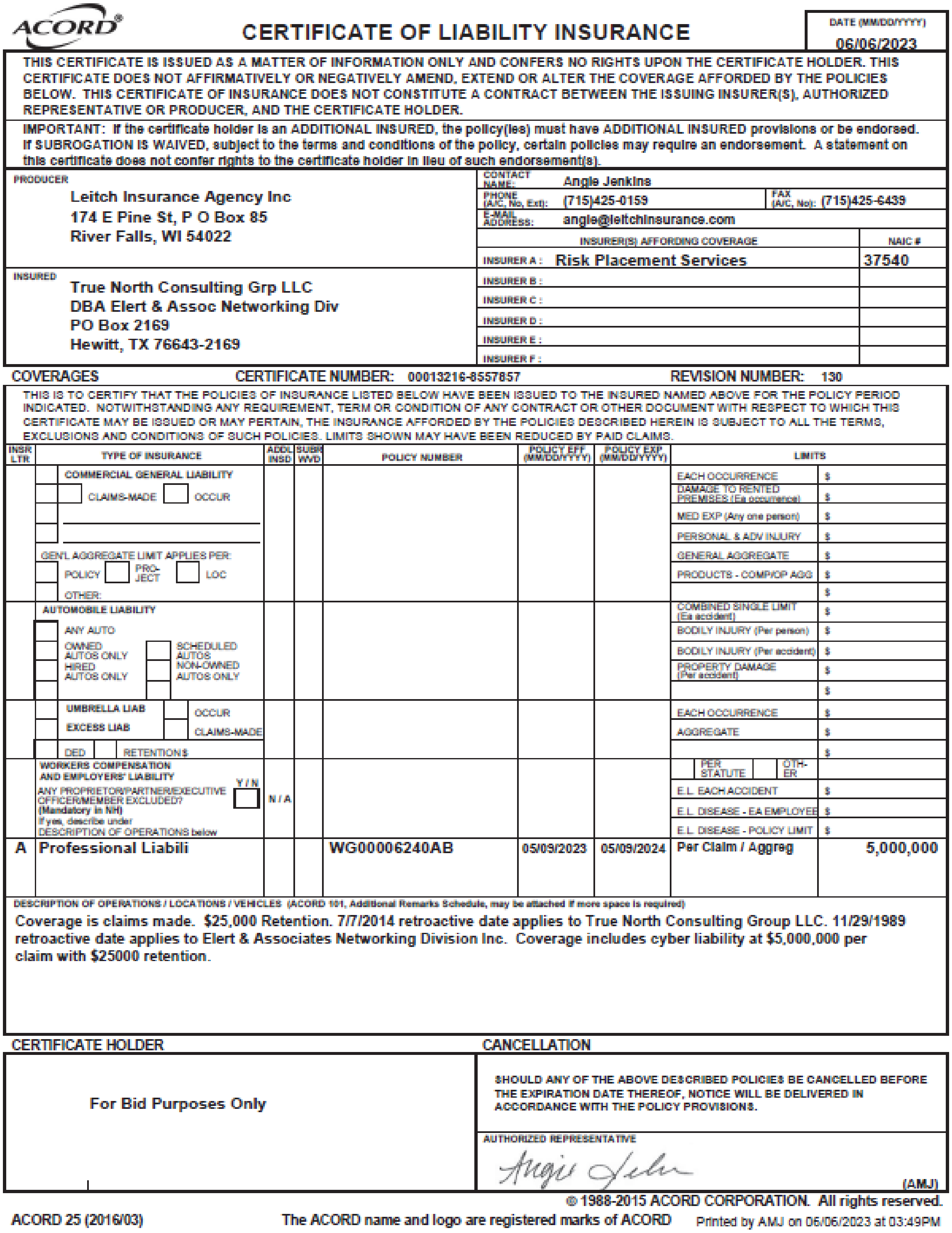
Angie Jenkins

(AMJ)

ACORD 25 (2016/03)

Printed by AMJ on 06/06/2023 at 03:50PM

PROFESSIONAL LIABILITY INSURANCE CERTIFICATE EXAMPLE



ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 06/06/2023

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

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

PRODUCER
Leitch Insurance Agency Inc
174 E Pine St, P O Box 85
River Falls, WI 54022

CONTACT NAME: Angie Jenkins
PHONE (A/C, No, Ext): (715)425-0159
FAX (A/C, No): (715)425-6439
E-MAIL ADDRESS: angie@leitchinsurance.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : Risk Placement Services	37540
INSURER B :	
INSURER C :	
INSURER D :	
INSURER E :	
INSURER F :	

INSURED
True North Consulting Grp LLC
DBA Elert & Assoc Networking Div
PO Box 2169
Hewitt, TX 76643-2169

COVERAGES CERTIFICATE NUMBER: 00013216-8557857 REVISION NUMBER: 130

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

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	□ COMMERCIAL GENERAL LIABILITY □ CLAIMS-MADE □ OCCUR □ □ GEN'L AGGREGATE LIMIT APPLIES PER: □ POLICY □ PRO-JECT □ LOC OTHER:						EACH OCCURRENCE	$
							DAMAGE TO RENTED PREMISES (Ea occurrence)	$
							MED EXP (Any one person)	$
							PERSONAL & ADV INJURY	$
							GENERAL AGGREGATE	$
							PRODUCTS - COMP/OP AGG	$
								$
	AUTOMOBILE LIABILITY □ ANY AUTO □ OWNED AUTOS ONLY □ SCHEDULED AUTOS □ HIRED AUTOS ONLY □ NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident)	$
							BODILY INJURY (Per person)	$
							BODILY INJURY (Per accident)	$
							PROPERTY DAMAGE (Per accident)	$
								$
	□ UMBRELLA LIAB □ OCCUR □ EXCESS LIAB □ CLAIMS-MADE □ DED □ RETENTION $						EACH OCCURRENCE	$
							AGGREGATE	$
								$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? □ (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N / A					□ PER STATUTE □ OTH-ER	
							E.L. EACH ACCIDENT	$
							E.L. DISEASE - EA EMPLOYEE	$
							E.L. DISEASE - POLICY LIMIT	$
A	Professional Liabili			WG00006240AB	05/09/2023	05/09/2024	Per Claim / Aggreg	5,000,000

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

Coverage is claims made. $25,000 Retention. 7/7/2014 retroactive date applies to True North Consulting Group LLC. 11/29/1989 retroactive date applies to Elert & Associates Networking Division Inc. Coverage includes cyber liability at $5,000,000 per claim with $25000 retention.

CERTIFICATE HOLDER

For Bid Purposes Only

CANCELLATION

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

AUTHORIZED REPRESENTATIVE

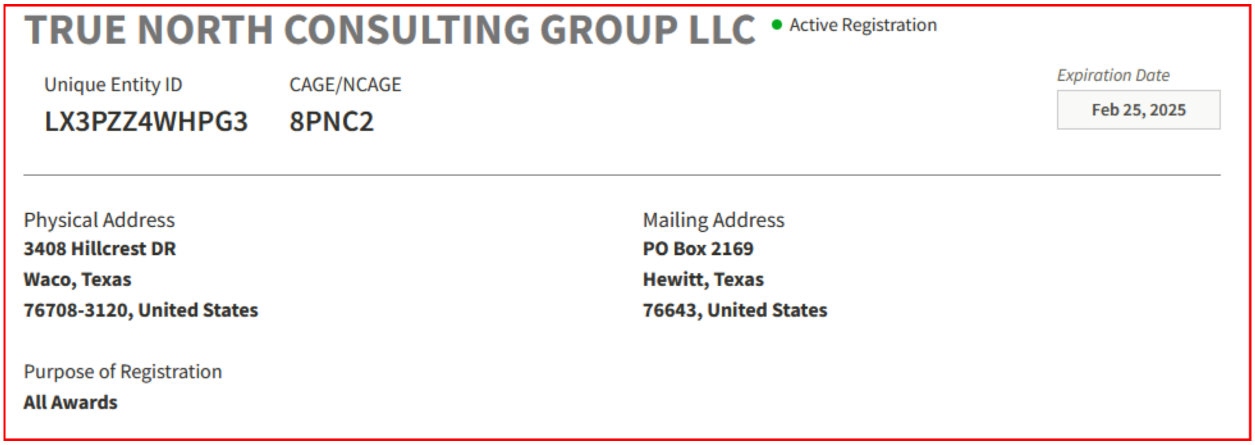
Angie Jenkins (AMJ)

© 1988-2015 ACORD CORPORATION. All rights reserved.

ACORD 25 (2016/03) The ACORD name and logo are registered marks of ACORD Printed by AMJ on 06/06/2023 at 03:49PM

SYSTEM FOR AWARD MANAGEMENT (SAM) REGISTRATION

- **Company Name:** True North Consulting Group, LLC
- **Company Principal:** Russ Johnson
- **SAM Unique Entity ID:** LX3PZZ4WHPG3



TRUE NORTH CONSULTING GROUP LLC ● Active Registration

Unique Entity ID
LX3PZZ4WHPG3

CAGE/NCAGE
8PNC2

Expiration Date
Feb 25, 2025

Physical Address
3408 Hillcrest DR
Waco, Texas
76708-3120, United States

Mailing Address
PO Box 2169
Hewitt, Texas
76643, United States

Purpose of Registration
All Awards

SAMPLE REPORTS

Please see Team TNCG's sample reports on the following pages:

- Sample 1: Internal Network Penetration Test Report
- Sample 2: External Network Penetration Test Report
- Sample 3: Web Application Penetration Test Report
- Sample 4: Application Security Test Report
- Sample 5: Executive Memo – IT Risk Assessment

The five sample reports included are a part of many examples available. Upon request, additional examples will be provided.

trueNORTH
consulting group

Client Name

Internal Network Penetration Test Report

Version 1.0

February 20, 2022

Statement of Confidentiality

This Confidential Information is being provided to **Client Name** as a deliverable of this consulting engagement. The sole purpose of this document is to provide you with the results of, and recommendations derived from this consulting engagement. Each recipient agrees that, prior to reading this document, it shall not distribute or use the information contained herein and any other information regarding **TNCG** for any purpose other than those stated.

Table of Contents

1 Results

1.1 Introduction

Team TNCG was engaged by **Client Name** to perform an Internal Network Penetration Testing of their internal network segments. Throughout all testing, **Team TNCG** did not perform any tests that would deliberately lead to system outages or affect application availability, such as denial-of-service tests.

Team TNCG remotely accessed the **Client Name** internal segments in order to replicate the scenario where attacker is sitting in the internal network. The testing had been conducted from **January 10, 2022** to **February 20, 2022.** All testing was performed using a variety of industry leading security scanning tools and applications.

The internal network scope included **ten (10) subnets** provided to **Team TNCG** by **Client Name.** A firewall or other network traffic-filtering device restricted access to these host.

1.2 Conclusion

Team TNCG was not able to penetrate into the **Client Name's** internal network under scope using the identified vulnerabilities. **Team TNCG** concludes that **Client Name** has **PASSED** the Internal Network Penetration Test.

1.3 Goals & Objectives

The objective of this assessment on **Client Name's** internal network was to detect any vulnerability in the organization's IT System & Network to exploit and for checking how effective the controls are in preventing any potential unauthorized information access.

Other Considerations:

As both the vulnerability assessment and the penetration test provide only a snapshot of the security posture, and with security exposure never a constant, information security management needs to be regularly monitored, reviewed and audited, and an ongoing process be implemented for making improvements and taking corrective actions.

We are of the opinion that even when all the below mentioned vulnerability have eventually been addressed – in order to maintain on-going security posture of the network infrastructure, **Client Name** should consider the following:

To conduct periodic External and Internal Vulnerability Assessment and Penetration Testing as well as Security Audit Reviews especially after major changes in the systems and infrastructure.

2 Methodology

2.1 Methodology Description

Team TNCG assessor follow the methodology below when performing Internal Network Penetration Testing. This methodology was created to promote a more consistent and thorough approach to vulnerability assessment and penetration testing. The methodology is broken down into these five components:

- **D**iscovery - aims at identifying all potential assets for investigation. The information gained through the discovery process creates a road map for the investigation module.
- **A**nalysis - utilizes the list of assets from the discovery process and thoroughly examines them for potential vulnerabilities. The raw data resulting from the investigation must be analyzed and verified.
- **V**alidation - tests vulnerabilities to ensure that all false positives and inaccuracies are removed from the raw investigation data. This often-neglected step ensures accuracy, painting a nearly complete picture of the security posture.
- **E**xploitation - involves the in-depth analysis and execution of advanced testing techniques against all verified vulnerabilities. This effort completes the security picture and provides the information necessary to fully mitigate the findings.
- **R**eporting - provides an overview of the assessment methodology, vulnerability and threat assessment observations, recommendations and corrective actions and a copy of all data collected.

Team TNCG assessor used this methodology to perform penetration testing and to assess the security of the **Client Name's** internal network. Specifically, the following sections highlight the various tests that were used to complete each step of the methodology.

Discovery

Client Name provided **ten (10) subnets** for the internal network to be reviewed by **Team TNCG** which are shown below:

Internal IP Addresses:

- xx.xx.xx.xx/24
- xx.xx.xx.xx/24
- xx.xx.xx.xx/24
- xx.xx.xx.xx/24
- xx.xx.xx.xx/24
- xx.xx.xx.xx/24
- xx.xx.xx.xx/24
- xx.xx.xx.xx/24
- xx.xx.xx.xx/24
- xx.xx.xx.xx/24

Team TNCG used the security tool NMAP to identify live services on the tested IP addresses. NMAP is designed to identify live systems, as well as services being offered by those systems.

Investigation

As a follow-up to the information gathered, Team TNCG used the security tool Nessus v8.15.2 to perform checks for known vulnerabilities on the **Client Name's** internal network. Nessus is a security-scanning tool that checks for over 1,53,418 different known vulnerabilities on networked systems. The Nessus tool performs extensive checks for vulnerabilities based upon predefined attack signature criteria. All tests were complemented with additional manual checks performed by Team TNCG engineers to ensure accuracy of the results.

Verification

Team TNCG assessor manually verified the outputs of all security tools to determine if any results were inconsistent and warranted additional examination and review. Outputs from the various tools used were compared and crosschecked for accuracy. False positives and duplicate entries were removed from the Investigation results. Vulnerabilities that could be neither confirmed nor disputed were categorized separately for follow-up checks and review. Those vulnerabilities that could not be tested and confirmed without endangering the systems on which they exist are noted as well.

Exploitation

Team TNCG performed exploitation attempts against any internal network host exhibiting vulnerability symptoms. These attempts included numerous manual exploitation attempts, information gathering and password guessing for well-known accounts using techniques developed and tested in our lab environment. All attacks were designed to limit the danger to services on the systems in order to prevent disruption of service during the testing.

Reporting

The culmination of all observation is reported in this document using the **Team TNCG** standard reporting template.

2.2 Project Team

The engagement involved contributions from the following team members:

Team TNCG Team	Client Name Team
Team TNCG Assessor	John Doe

2.3 Penetration Timeline

The following table outlines key milestones during the penetration test:

Penetration Timeline

Date	Milestone
January 10, 2022	Start of Project
February 20, 2022	Final Deliverable

3 Details of Work Performed

3.1 Phase 1 – Port Scanning

Port Scans are attempts to connect to ports corresponding to services on the assessed hosts. By scanning ports which are available on the hosts, potential weaknesses on them can be further exploited.

Any ports that are found visible on the hosts should be verified if they are supposed to be opened there. Unexpected open ports should be closed. The firewall should also be checked if the listening ports on the hosts should expose to the internet or to the internal networks. It is recommended to remove any unnecessary services and implement firewall rules to prevent exposure of any legitimate services that are not meant for the internet.

Ports on which the connection attempts were made are shown below. The table consists of host IP addresses, protocol types, port numbers and the probable services. It is recommended to remove any unnecessary ports/services as identified below.

Following table shows the Port Scan Results:

Address of Host (Hostname)	Protocol/Port/Service/Status	Comments
xx.xx.xx.xx	TCP / 443 / HTTPS / CLOSED TCP / 587 / SUBMISSION / CLOSED	All ports on the target host which are not listed here were observed to be in state as FILTERED.
xx.xx.xx.xx	NO OPEN PORTS OBSERVED	All ports on the target host were observed to be in state as FILTERED.
xx.xx.xx.xx	TCP / 443 / HTTPS / OPEN	All ports on the target host which are not listed here were observed to be in state as FILTERED.
xx.xx.xx.xx	TCP / 443 / HTTPS / OPEN	All ports on the target host which are not listed here were observed to be in state as FILTERED.
xx.xx.xx.xx	NO OPEN PORTS OBSERVED	All ports on the target host which are not listed here were observed to be in state as FILTERED.
xx.xx.xx.xx	TCP / 443 / HTTPS / OPEN	All ports on the target host which are not listed here were observed to be in state as FILTERED.

3.2 Phase 2 – Observations

This phase has been completed successfully. The vulnerabilities that were observed during the internal network penetration testing are listed below:

3.2.1 Apache Server and Apache Tomcat Multiple Vulnerabilities

Port	TCP 80, 8080, 8443, 443
Observation	Assessor observed that the version of Apache Server and Apache Tomcat running on the identified hosts is affected with multiple vulnerabilities.
Affected Resource	xx.xx.xx.xx
POC	Vulnerability Screenshots
Results	It was observed that the version of Apache Server and Apache Tomcat running on the identified hosts is affected with multiple vulnerabilities which can cause remote code execution, information disclosure, unauthenticated access, privilege escalation and denial of service.
Risk Mitigation	It is recommended to upgrade to the latest version of Apache and Tomcat
CVE	CVE-2021-40438, CVE-2021-34798, CVE-2021-39275, CVE-2017-3167
CVSS Base Score	10

3.2.2 DNS Server Cache Snooping Remote Information Disclosure

Port	TCP 53
Observation	Assessor observed that the remote DNS server is vulnerable to cache snooping attacks.
Affected Resource	xx.xx.xx.xx
POC	Vulnerability Screenshots
Results	The remote DNS server responds to queries for third-party domains that do not have the recursion bit set. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited. For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more. Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.
Risk Mitigation	It is recommended to contact the vendor of the DNS software for a fix.
CVE	NA
CVSS Base Score	5

3.2.3 TLS/SSL Server Multiple Vulnerabilities

Port	TCP 443
Observation	Assessor observed that the remote services are vulnerable to below given multiple vulnerabilities: 1. SSL Certificate Cannot Be Trusted 2. SSL Certificate Chain Contains RSA Keys Less Than 2048 bits 3. SSL Certificate Chain Contains Weak RSA Keys 4. SSL Certificate Signed Using Weak Hashing Algorithm 5. SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened encryption) 6. SSL Medium Strength Cipher Suites Supported (SWEET32) 7. SSL RC4 Cipher Suites Supported (Bar Mitzvah) 8. SSL Self-Signed Certificate 9. SSL Version 2 and 3 Protocol Detection 10. SSL Weak Cipher Suites Supported 11. SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) 12. SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam) 13. SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) 14. SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) 15. TLS Version 1.0 Protocol Detection
Affected Resource	xx.xx.xx.xx
POC	Vulnerability Screenshots
Results	The SSL certificate for this service cannot be trusted. The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits. The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 1024 bits. An SSL certificate in the certificate chain has been signed using a weak hash algorithm. The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic. The remote service supports the use of medium strength SSL ciphers. The remote service supports the use of the RC4 cipher. The SSL certificate chain for this service ends in an unrecognized self-signed certificate. The remote service encrypts traffic using a protocol with known weaknesses. The remote service supports the use of weak SSL ciphers. The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. The remote host supports a set of weak ciphers.

	It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services. The remote service encrypts traffic using an older version of TLS.
Risk Mitigation	Following are the recommendations for each vulnerability: 1. Purchase or generate a proper SSL certificate for this service. 2. Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate. 3. Replace the certificate in the chain with the weak RSA key with a stronger key, and reissue any certificates it signed. 4. Contact the Certificate Authority to have the SSL certificate reissued. 5. Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections. 6. Reconfigure the affected application if possible, to avoid use of medium strength ciphers. 7. Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. 8. Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead. 9. Reconfigure the affected application, if possible, to avoid the use of weak ciphers. 10. Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. 11. Reconfigure the service to remove support for EXPORT_DHE cipher suites. 12. Reconfigure the service to remove support for EXPORT_RSA cipher suites. 13. Disable SSLv3. 14. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. 15. Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
CVE	CVE-2004-2761, CVE-2016-0800, CVE-2016-2183, CVE-2013-2566, CVE-2015-2808, CVE-2015-4000, CVE-2015-0204, CVE-2014-3566
CVSS Base Score	5.0

3.3 Phase 3 – Exploitation

Team TNCG assessor observed vulnerabilities which may allow an attacker to compromise the target systems however were not able to find public exploits or exploit any of the reported vulnerabilities with found exploits.

3.4 Assessor's Note

Assessor attempted to discover vulnerabilities at network layer using automated as well as manual techniques. The vulnerability scanning and penetration testing of the target systems included, but was not limited to, following attack vectors:

Sr. No.	Attack Vectors	No. of Observations
1.	Operating System Vulnerabilities	No Vulnerabilities Observed
2.	Service Mis-configuration	Three Vulnerabilities Observed
3.	Network Mis-configuration	No Vulnerabilities Observed
4.	Web Interfaces Discovery	No Vulnerabilities Observed
5.	Common ports used by backdoors / Viruses / Worms	No Vulnerabilities Observed
6.	DNS Recursion / Zone Transfer / Poisoning	No Vulnerabilities Observed

trueNORTH
consulting group

Client Name

External Network Penetration Test Report

Version 1.0

February 20, 2022

Statement of Confidentiality

This Confidential Information is being provided to **Client Name** as a deliverable of this consulting engagement. The sole purpose of this document is to provide you with the results of, and recommendations derived from this consulting engagement. Each recipient agrees that, prior to reading this document, it shall not distribute or use the information contained herein and any other information regarding **TNCG** for any purpose other than those stated.

Table of Contents

1 Results

1.1 Introduction

Team TNCG was engaged by **Client Name** to perform an external network penetration testing of their internet facing network segments. Throughout all testing, **Team TNCG** did not perform any tests that would deliberately lead to system outages or affect application availability, such as denial-of-service tests.

All network vulnerability testing was conducted from **Team TNCG** testing networks from **January 10, 2022** to **February 20, 2022.** All testing was performed using a variety of industry leading security scanning tools and applications.

The external network included six (06) IP addresses provided to **Team TNCG** by **Client Name.** A firewall or other network traffic-filtering device restricted access to these hosts.

1.2 Conclusion

Team TNCG was not able to penetrate into the **Client Name's** external network under scope using the identified vulnerabilities. **Team TNCG** concludes that **Client Name** has **PASSED** the External Network Penetration Test.

1.3 Goals & Objectives

The objective of this assessment on **Client Name's** external network was to detect any vulnerability in the organization's IT System & Network to exploit and for checking how effective the controls are in preventing any potential unauthorized information access.

Other Considerations:

As both the vulnerability assessment and the penetration test provide only a snapshot of the security posture, and with security exposure never a constant, information security management needs to be regularly monitored, reviewed and audited, and an ongoing process be implemented for making improvements and taking corrective actions.

We are of the opinion that even when all the identified vulnerabilities have eventually been addressed – in order to maintain on-going security posture of the network infrastructure, **Client Name** should consider the following:

To conduct periodic External and Internal Vulnerability Assessment and Penetration Testing as well as Security Audit Reviews especially after major changes in the systems and infrastructure.

2 Methodology

2.1 Methodology Description

Team TNCG engineers follow the methodology below when performing External Network Penetration Testing. This methodology was created to promote a more consistent and thorough approach to vulnerability assessment and penetration testing. The methodology is broken down into these five components:

- **D**iscovery - aims at identifying all potential assets for investigation. The information gained through the discovery process creates a road map for the investigation module.
- **A**nalysis - utilizes the list of assets from the discovery process and thoroughly examines them for potential vulnerabilities. The raw data resulting from the investigation must be analyzed and verified.
- **V**alidation - tests vulnerabilities to ensure that all false positives and inaccuracies are removed from the raw investigation data. This often-neglected step ensures accuracy, painting a nearly complete picture of the security posture.
- **E**xploitation - involves the in-depth analysis and execution of advanced testing techniques against all verified vulnerabilities. This effort completes the security picture and provides the information necessary to fully mitigate the observations.
- **R**eporting - provides an overview of the assessment methodology, vulnerability and threat assessment observations, recommendations and corrective actions and a copy of all data collected.

Team TNCG engineers used this methodology to perform the vulnerability assessment and penetration testing and to assess the security of the **Client Name's** external network. Specifically, the following sections highlight the various tests that were used to complete each step of the methodology.

Discovery

Client Name provided six (06) IP addresses for the external network to be reviewed by **Team TNCG.** The IP addresses which were provided for the assessment are shown below:

External IP Addresses:

- xx.xx.xx.xx
- xx.xx.xx.xx
- xx.xx.xx.xx
- xx.xx.xx.xx
- xx.xx.xx.xx
- xx.xx.xx.xx

Team TNCG used the security tool NMAP to identify live services on the tested IP addresses and domains. NMAP is designed to identify live systems, as well as services being offered by these systems.

Investigation

As a follow-up to the information gathered, Team TNCG used the security tool Nexpose v6.6.98 to perform checks for known vulnerabilities on the **Client Name's** external network. Nexpose is a security-scanning tool that checks for over 210,000 different known vulnerabilities on networked systems. The Nexpose tool performs extensive checks for vulnerabilities based upon predefined attack signature criteria. All tests were complemented with additional manual checks performed by Team TNCG engineers to ensure accuracy of the results.

Verification

Team TNCG manually verified the outputs of all security tools to determine if any results were inconsistent and warranted additional examination and review. Outputs from the various tools used were compared and crosschecked for accuracy. False positives and duplicate entries were removed from the Investigation results. Vulnerabilities that could be neither confirmed nor disputed were categorized separately for follow-up checks and review. Those vulnerabilities that could not be tested and confirmed without endangering the systems on which they exist are noted as well.

Exploitation

Team TNCG performed exploitation attempts against any external network host exhibiting vulnerability symptoms. These attempts included numerous manual exploitation attempts, information gathering and password guessing for well-known accounts using techniques developed and tested in our lab environment. All attacks were designed to limit the danger to services on the systems in order to prevent disruption of service during the testing.

Reporting

The culmination of all observations is reported in this document using the **Team TNCG** standard reporting template.

2.2 Project Team

The engagement involved contributions from the following team members:

Team TNCG	Client Name Team
Team TNCG Assessor	John Doe

2.3 Penetration Timeline

The following table outlines key milestones during the penetration test:

Penetration Timeline

Date	Milestone
January 10, 2022	Start of Project
February 20, 2022	Final Deliverable

3 Details of Work Performed

3.1 Phase 1– Reconnaissance

Reconnaissance is an information gathering phase for the target IP address or IP addresses range in the scope of penetration test.

Team TNCG team examined the target by passive techniques such as

- **Internet Service Registration** – The global registration and maintenance of IP address information;
- **Domain Name System** – Local and global registration and maintenance of host naming;
- **Search Engines** – Specialist retrieval of distributed material relating to an organization or their employees;
- **Email Systems** – Information contained within and related to emails and email deliver processes. Mainly information disclosed via "Contact Us" features;
- **Website Analysis** – The information intentionally made public, that may pose a risk to security;

Observations of reconnaissance whether technical or non-technical in nature, can be used against target IP address to plan further attack scenarios. This phase uses various search engines, mailing groups, online forums, collaboration sites etc. for collecting information. A subset of the same is –

1. Search engines such as Google, Yahoo, Bing etc.
2. GHDB (Google Hacking Database leverage to an external attacker)

Team TNCG assessors observed that no CRITICAL information about the given IP addresses/domains of **Client Name's** is available over internet which can be of any leverage to an external attacker. Furthermore, Team TNCG assessor observed that target IP addresses/domains are not listed in well-known public databases as spamming hosts and are not blacklisted as known malicious IP addresses/domains either.

3.2 Phase 2 – Port Scanning

Port Scans are attempts to connect to ports corresponding to services on the assessed hosts. By scanning ports which are available on the hosts, potential weaknesses on them can be further exploited.

Any ports that are found visible on the hosts should be verified if they are supposed to be opened there. Unexpected open ports should be closed. The firewall should also be checked if the listening ports on the hosts should expose to the internet or to the internal networks. It is recommended to remove any unnecessary services and implement firewall rules to prevent exposure of any legitimate services that are not meant for the internet.

Ports on which the connection attempts were made are shown below. The table consists of host IP address, protocol types, port numbers and the probable services. It is recommended to remove any unnecessary ports/services as identified below.

Following table shows the Port Scan Results:

Address of Host (Hostname)	Protocol/Port/Service/Status	Comments
xx.xx.xx.xx	TCP / 443 / HTTPS / CLOSED TCP / 587 / SUBMISSION / CLOSED	All ports on the target host which are not listed here were observed to be in state as FILTERED.
xx.xx.xx.xx	NO OPEN PORTS OBSERVED	All ports on the target host were observed to be in state as FILTERED.
xx.xx.xx.xx	TCP / 443 / HTTPS / OPEN	All ports on the target host which are not listed here were observed to be in state as FILTERED.
xx.xx.xx.xx	TCP / 443 / HTTPS / OPEN	All ports on the target host which are not listed here were observed to be in state as FILTERED.
xx.xx.xx.xx	NO OPEN PORTS OBSERVED	All ports on the target host which are not listed here were observed to be in state as FILTERED.
xx.xx.xx.xx	TCP / 443 / HTTPS / OPEN	All ports on the target host which are not listed here were observed to be in state as FILTERED.

3.3 Phase 3 – Observations

This phase has been completed successfully and following are the observations which were noted during the External Network Penetration Test:

3.3.1 SSL/TLS Server Multiple Vulnerabilities

Port	TCP 443
Observation	Assessor observed that, the remote service is vulnerable to below given multiple vulnerabilities: • Diffie-Hellman group smaller than 2048 bits • TLS Server Supports TLS version 1.1 • TLS/SSL Server Supports the Use of Static Key Ciphers • Untrusted TLS/SSL server X.509 certificate • X.509 Certificate Subject CN Does Not Match the Entity Name
Affected Resource	xx.xx.xx.xx
POC	Vulnerability Screenshots
Results	The TLS server uses a Diffie-Hellman group with a prime modulus of less than 2048 bits in length. Current estimates are that that an academic team can break a 768-bit prime and that a state-level actor can break a 1024-bit prime. The PCI (Payment Card Industry) Data Security Standard requires a minimum of TLS v1.1 and recommends TLS v1.2. In addition, FIPS 140-2 standard requires a minimum of TLS v1.1 and recommends TLS v1.2. The server is configured to support ciphers known as static key ciphers. These ciphers don't support "Forward Secrecy". In the new specification for HTTP/2, these ciphers have been blacklisted. The server's TLS/SSL certificate is signed by a Certification Authority (CA) that is not well-known or trusted. This could happen if: the chain/intermediate certificate is missing, expired or has been revoked; the server hostname does not match that configured in the certificate; the time/date is incorrect; or a self-signed certificate is being used. The use of a self-signed certificate is not recommended since it could indicate that a TLS/SSL man-in-the-middle attack is taking place The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate. Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Thus, standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. For example, in a certificate presented by ""https://www.example.com/"", the CN should be ""www.example.com"". In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, or else an attacker could then launch a man-in-the-middle attack and gain full control of the data stream. Of particular importance is the validity of the subject's CN, that should match the name of the entity (hostname).

	A CN mismatch most often occurs due to a configuration error, though it can also indicate that a man-in-the-middle attack is being conducted.
Risk Mitigation	It is recommended to follow below security measures: • Use a Stronger Diffie-Hellman Group • Disable insecure TLS/SSL protocol support • Disable TLS/SSL support for static key cipher suites • Obtain a new certificate from your CA and ensure the server configuration is correct • Fix the subject's Common Name (CN) field in the certificate
Reference	https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509 https://support.mozilla.org/en-US/kb/connection-untrusted-error-message https://www.thesslstore.com/blog/cipher-suites-algorithms-security-settings/
CVE ID	NA
CVSS Base Score	6.0

3.3.2 Closed Port Detection

Ports	For detailed Port Scanning results please refer to section 3.2 Phase 1 – Port Scanning
Observation	Assessor observed that few TCP ports on the affected resources are not being filtered by any filtering device like firewall, Router, IPS or IDS. Thus, the port scanning attempts successfully discovered the exact state of ports as being closed. It seems that the firewall/filtering device allows traffic to pass affected resources which send RESET packet as a response to SYN request. Another possibility is that the firewall / filtering device itself sends the RESET response for such requests.
Affected Resources	Refer to section 3.2 Phase 1 – Port Scanning
POC	Vulnerability Screenshots
Results	Port scanning attempts on affected resources are showing few TCP ports as closed. Revealing the correct states of the port to any user results into information discloser. An attacker can leverage the information about closed ports to deduce what other ports may be open / filtered. This also shows that the ports are not being filtered by firewall and thus an attacker can use those for installing backdoors as part of post-exploitation.
Risk Mitigation	Network and security devices shall be configured in a way that they won't reveal the status of closed ports to port scan attempts. Also, mentioned affected devices shall follow the configuration which detects and filters port scanning attempts. This kind of attack can be prevented on router by using TCP Intercept which can be configured to intercept all incoming SYN packets, or an ACL can be written to identify the source and destination for packets that should be intercepted. It can also be run in watch mode, a more passive mode than intercept mode. In watch mode, the router does not intercept the SYN packets, but passes them through to the TCP server.
CVSS Base Score	2.2

3.4 Phase 4 – Exploitation

Team TNCG assessor did not observe any vulnerability which can be exploited within a given period and based on that determined that the identified vulnerabilities cannot affect confidentiality or integrity of critical information. The necessary information was gathered for the identified observations and provided in the "POC" section of each vulnerability table.

3.5 Assessor's Note

Assessor attempted to discover vulnerabilities at network layer using automated as well as manual techniques. The vulnerability scanning and penetration testing of the target systems included, but was not limited to, following attack vectors:

Sr. No.	Attack Vector	No. of Observations
1.	Operating System Vulnerabilities	No Vulnerabilities Observed
2.	Service Misconfiguration	One Vulnerability Observed
3.	Network Misconfiguration	One Vulnerability Observed
4.	Web Interfaces Discovery	No Vulnerabilities Observed
5.	Common Ports used by Backdoors/Viruses/Worms	No Vulnerabilities Observed
6.	DNS Recursion/Zone Transfer/Poisoning	No Vulnerabilities Observed

Client Name

Web Application Penetration Test Report

Version 1.0

January 18, 2022

Statement of Confidentiality

This Confidential Information is being provided to **Client Name** as a deliverable of this consulting engagement. The sole purpose of this document is to provide you with the results of, and recommendations derived from this consulting engagement. Each recipient agrees that, prior to reading this document, it shall not distribute or use the information contained herein and any other information regarding **TNCG** for any purpose other than those stated.

Table of Contents

1 Executive Summary

1.1 Introduction

Client Name engaged **Team TNCG** to conduct a Web Application Penetration Test of their **Sample** web application. The purpose of the engagement was to identify and prioritize the potential areas of security vulnerability.

The engagement began on **January 01, 2022** and included multiple phases of testing, analysis and documentation. All testing was performed from **Team TNCG Testing Labs**.

This document summarizes the analysis, Observations and recommendations for the assessment carried out by **Team TNCG**.

1.2 Goals & Objectives

The purpose of this assessment was to identify technical as well as logical vulnerabilities in the application and provide recommendations for risk mitigation that may arise on exploiting these vulnerabilities. The idea behind this testing was to discover whether an attacker can leverage flaws in the application to compromise the confidentiality, integrity and availability of the information. **Team TNCG** worked with **Client Name** to achieve the following key objectives:

To determine whether adequate information security controls have been built into the application.

Perform supplemental research and development activities to support analysis.

Prioritize vulnerabilities based upon the ease of exploit, level of effort to remedy, and severity of impact if exploited.

Assess current practice against industry best practices.

Deliver report which includes **Team TNCG's** Observations, analysis and recommendations.

Transfer knowledge.

1.3 Approach & Methodology

Team TNCG Application Security consultants follow the **OWASP** (**O**pen **W**eb **A**pplication **S**ecurity **P**roject) an established guideline in application security methodology. In the course of the assessment, Team TNCG consultants use a variety of commercial, open-source tools as well as homegrown scripts & tools.

Team TNCG has defined following approaches while doing application security assessment.

Black box testing – This is a technique to attempt to penetrate application where the source code of the application is not available to the tester. Team TNCG team will attempt to elicit exception conditions and anomalous behavior from the Web Application by manipulating the identified inputs - using special characters, SQL keywords, maliciously crafted requests, and so forth. Any unexpected reaction from the Web Application is noted and investigated. This may take the form of scripting error messages, server errors or half-loaded pages. The goal of this method is to simulate an attack by an external hacker.

Grey box testing – This approach is similar to black box testing; however, the attack team is given the same privileges as an 'admin/normal' user of the application and the goal is to simulate an attack by a malicious insider. The attack team tries to escalate the privileges of a normal user to administrator user.

Types of tests performed	**Checked**
1. Application Security Assessment Test	
• Automated scanning of possible web application vulnerability	✓
• Manual exploit on discovered vulnerability	✓
• Compliance Specific checks (e.g. PCI DSS)	✓
2. OWASP Top 10 2021	
• A01:2021-Broken Access Control	✓
• A02:2021-Cryptographic Failures	✓
• A03:2021-Injection	✓
• A04:2021-Insecure Design	✓
• A05:2021-Security Misconfiguration	✓
• A06:2021-Vulnerable and Outdated Components	✓
• A07:2021-Identification and Authentication Failures	✓
• A08:2021-Software and Data Integrity Failures	✓
• A09:2021-Security Logging and Monitoring Failures	✓
• A10:2021-Server-Side Request Forgery (SSRF)	✓

1.4 Project Team – Contact Information

The engagement involved contributions from the following team members:

Team TNCG Team	Client Name Team
Team TNCG Assessor	John Doe

1.5 Penetration Timeline

The following table outlines key milestones during the penetration test:

Penetration Timeline

Date	Milestone
January 01, 2022	Start of Project
January 10, 2022	Submission of first round of report
January 18, 2022	Final Deliverable

1.6 Target Description

The penetration testing for **Client Name's Sample** web application was carried out on one (01) application URL. The approach conducted was a black box testing followed by grey box testing.

Technical Details of the Target:

Total one (01) application was subjected to assessment. The target application's URL is given below:

Sr. No.	Application Name	Application URL(s)	Production/UAT
1.	Sample Application	https://sample-app.com/	Production

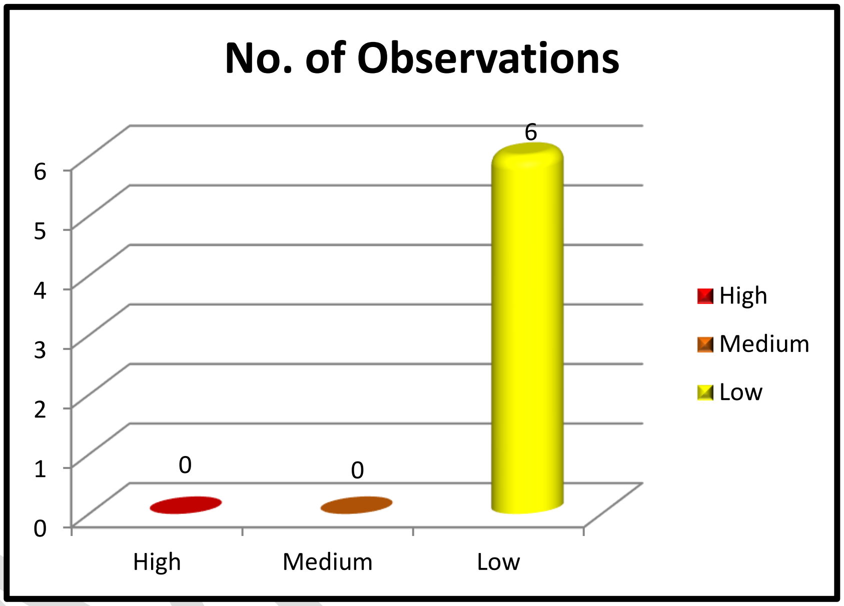
1.7 Summary of Observations

It was observed that the tested web application was affected with one (01) high and (05) low-risk vulnerabilities that an attacker can target. **Client Name** has provided business justification for one (01) high risk vulnerability based on which it has been reclassified as Low. Based on this, there are total six (06) low risk vulnerabilities affecting the target application.

It is important to periodically check, review and modify the application logic if any kind of change is being applied to the application.

The graph below gives the status of severity of the vulnerabilities found during the Application Security Assessment.

Risk Severity Level	No. of Observations
High	00
Medium	00
Low	06
Total	06



Given below is the summary of the Observations:

Sr. No.	Observations	Risk Level	Mitigation Status
1.	Source Code Disclosure	High → Low	Not Mitigated – Business Justification
2.	Header Information Disclosure	Low	Not Mitigated
3.	Missing Security Headers	Low	Not Mitigated
4.	Out-of-date Version (jQuery)	Low	Not Mitigated
5.	Missing Cookie Attributes	Low	Not Mitigated
6.	Autocomplete Attribute not set to Off	Low	Not Mitigated

1.8 Statement on Compliance

Team TNCG has determined that **Client Name's Sample** web application is **Compliant** with **Team TNCG** validation requirement as mentioned in section 1.3.

2 Detailed Observations

2.1 Overview

The following format shows a typical vulnerability representation and provides in detail information of vulnerabilities discovered during Application Vulnerability Test.

2.2 Vulnerability Table

1. Vulnerability Title	
Risk Level	🟥
OWASP Category	
Abstract	
Ease of Exploitation	
Impact	
Recommendations	
Substantiated Assessment	
Affected URL	
Note	
Reference	
CWE	

- **Vulnerability Title – A short title that describes the vulnerability.**

  The title bar for each vulnerability table is color coded for a quick identification of the risk level. Title bar color codes are as follows:

Risk Level	**Description**
🟥	**High risk** vulnerability can be exploited by an attacker to gain full administrative access to the application or its underlying operating system.
🟧	**Medium risk** vulnerability reveals information about the application and its underlying infrastructure that can be used by an attacker in conjunction with another vulnerability to gain administrative control of the application or its underlying operating system.
🟨	**Low risk** vulnerability can result in enumeration of vital information held by or about the Application or its underlying operating system.

- **OWASP Category –** Refers to OWASP top 10-2017 vulnerability category.
- **Abstract –** Describes the flaw or bugs that cause the vulnerability.

- **Ease of Exploitation –** Provides a metric for the skill level required to exploit the vulnerability. The categories are:

Metric	Skill-level
Easy	Casual user
Medium	Computer-savvy individual
Hard	Determined hacker

- **Impact –** Describes the possible business impact if this vulnerability is successfully exploited.
- **Recommendation –** Provides solutions or workarounds to mitigate the risk arising from this vulnerability.
- **Substantiated Assessment –** The evidence of the vulnerability being present, wherever possible, is provided in the form of screenshots.
- **Affected URL –** Provides URLs and respective parameters which are affected with that specific vulnerability
- **Note –** A brief description of how the vulnerability can be exploited by internal/external attacker or limitations for exploitation which may result in minimizing the risk of the reported vulnerability.
- **Reference –** It provides reference to outside resource such as OWASP, SANS etc.
- **CWE –** Provides Common Weakness Enumeration ID

2.3 Vulnerability Discovery Phase

This phase has been completed successfully. Assessor observed six (06) low-risk vulnerabilities during the application penetration test.

2.3.1 Source Code Disclosure

Risk Level	**Low**
OWASP Category	A04:2021-Insecure Design A05:2021-Security Misconfiguration
Abstract	Assessor observed that the application's source code is being disclosed within JavaScript files.
Ease of Exploitation	Easy
Impact	An application's source code contains the core logic of the application and if an attacker can access the source code, they can manipulate the application in malicious ways as well as steal the intellectual property of the organization. Source Code disclosure can lead to complete compromise of the application. In this case, JavaScript files containing the source code are loaded along with the application and it is trivial to access these files and access the source code.
Recommendations	It is recommended to have all application source code on the server side and not on the client side so that it is not trivial for an attacker to access the source code such as in this case which is in JavaScript
Substantiated Assessment	Screenshot
Affected URLs	URLs
References	https://portswigger.net/kb/issues/006000b0_source-code-disclosure
CWE	200
Note	This vulnerability was reported as High risk but was reclassified as Low based on following business justifications provided by Client Name: • Client Name have provided proper documented business justification • Provided contact details in case of any impact on the application • This system is only accessible via network VPN connectivity to these systems

2.3.2 Missing Cookie Attributes

Risk Level	**Low**
OWASP Category	A05:2021-Security Misconfiguration
Abstract	Assessor observed that session attributes like as "Secure", "Domain" and “HTTPOnly” attributes are not set with Session IDs.
Ease of Exploitation	Hard
Impact	Without “Secure” attribute the application can transfer the session cookie over unencrypted channel. Without “Domain” attribute the cookie can be used by other domains and facilitate cross-site request forgery. Without ""HTTPOnly"" attribute, the cookie is accessible by client-side scripts and can be combined with a cross site scripting attack which can disclose session IDs. Also, by combining this vulnerability with others an attacker can perform attacks on session ID such as session hijacking.
Recommendations	It is recommended that application should be configured to set the session attributes HTTPOnly, Domain and Secure with session ID. This can be achieved by changing cookie element values as below in the Web.config file – <httpCookies domain=""String"" httpOnlyCookies=""true "" requireSSL=""true "" />
Substantiated Assessment	Screenshot
Affected URLs	URLs
References	https://www.owasp.org/index.php/SecureFlag https://www.owasp.org/index.php/HttpOnly
CWE	614, 1004

2.3.3 Missing HTTP Security Headers

Risk Level	**Low**
OWASP Category	A05:2021-Security Misconfiguration
Abstract	Assessor observed that the following HTTP Headers which improve the security of the application have not been enabled: • Content Security Policy • X-XSS-Protection • HTTP Strict Transport Security (HSTS) • X-Frame-Options • Expect-CT • X-Content-Type-Options • Feature-Policy
Ease of Exploitation	Hard
Impact	Lack of HTTP Security Headers may reduce the complexity faced by an attacker while exploiting certain vulnerabilities as these headers are implemented in order to protect from a number of vulnerabilities such as Cross Site Scripting, Cache Attacks, SSL Downgrade etc.
Recommendations	It is recommended to implement all the security headers mentioned in the Abstract. Refer the following URL for complete details about these headers and how to implement them: https://www.keycdn.com/blog/http-security-headers
Substantiated Assessment	Screenshot
Affected URLs	URLs
References	https://www.keycdn.com/blog/http-security-headers
CWE	1032

2.3.4 Out-of-date Version (jQuery)

Risk Level	**Low**
OWASP Category	A06:2021-Vulnerable and Outdated Components
Abstract	Assessor observed that target web site is using jQuery and detected that it is out of date.
Ease of Exploitation	Hard
Impact	Since this is an old version of the software, it may be vulnerable to attacks.
Recommendations	It's recommended to upgrade installation of jQuery to the latest stable version.
Substantiated Assessment	Screenshot
Affected URL	URLs
References	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE	1104

2.3.5 Header Information Disclosure

Risk Level	**Low**
OWASP Category	A05:2021-Security Misconfiguration
Abstract	Assessor observed that the application headers disclose the running version of Web Server.
Ease of Exploitation	Hard
Impact	Attackers can exploit known high risk vulnerabilities to gain complete access of the target web server using remote code execution apart from sensitive information disclosure, bypass of security controls and also cause denial of service. Information Disclosure such as this allows attackers to easily know the exact version of software running on the target system
Recommendations	It is recommended to disable headers which disclose the version of software running on the target system. Check references for further details.
Substantiated Assessment	Screenshot
Affected URLs	URLs
References	https://doc.sitecore.com/developers/90/platform-administration-and-architecture/en/remove-header-information-from-responses-sent-by-your-website.html
CWE	200

2.3.6 Autocomplete Attribute not set to Off

Risk Level	**Low**
OWASP Category	A05:2021-Security Misconfiguration
Abstract	Assessor observed that auto-complete attribute is not disabled for password fields on the affected resource. The affected resource contains at least one HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
Ease of Exploitation	Hard
Impact	While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.
Recommendations	It is recommended that: • The attribute "autocomplete" should be added to the source code for all the input fields accepting sensitive information; • And the value of this attribute should be set to ""off"" Note that autocomplete=""false"" doesn't work in all browsers.
Substantiated Assessment	Screenshot
Affected URLs	URLs
References	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
CWE	200

Assessment Report for:

Sample XYZ Company

Application Security Test

December 20xx

Prepared by: Team TNCG

Table of Contents

Limitations on Disclosure and Use of This Report

This report contains information concerning potential vulnerabilities of XYZ Client system and methods for exploiting them. Team TNCG recommends taking special precautions to protect the confidentiality of both this document and the information contained herein. Team TNCG has retained and secured a copy of the report for customer reference. Team TNCG delivered all other copies of the report to XYZ Client.

Vulnerability assessments are an uncertain process, based upon experience, currently available information, and known threats. All information security system, which by their nature are dependent upon human beings, are vulnerable to some degree. Therefore, while Team TNCG considers the major security vulnerabilities of the analyzed system identified, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures.

In addition, the basis of the analysis set forth herein is the technologies and known threats as of the date of this report. As technologies and risks change over time, the vulnerabilities associated with the operation of XYZ Client system described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities will change. Team TNCG makes no undertaking to supplement or update this report based on changed circumstances or facts of which Team TNCG becomes aware of after the date hereof, absent a specific written agreement to perform supplemental or updated analysis.

This report may recommend that XYZ Client use certain software or hardware products manufactured or maintained by other vendors. Team TNCG bases these recommendations upon its prior experience with the capabilities of those products. Nonetheless, Team TNCG does not and cannot warrant that a particular product will work as advertised by the vendor, nor that it will operate in the manner intended.

Team TNCG prepared this report for the exclusive benefit of XYZ Client. Team TNCG considers it proprietary information. The Permission to Perform Testing Agreement and Non-Disclosure Agreement (NDA) in effect between Team TNCG and XYZ Client govern the disclosure of this report to all other parties, including product vendors or suppliers.

Executive Summary

Team TNCG was engaged by to perform third party independent security testing for XYZ Client. The security testing included Vulnerability tests against the defined client applications to proactively discover flaws, weaknesses and vulnerabilities. Testing for this project was done in accordance with Information Security Best Practices. The objective of this service was to identify and safely exploit vulnerabilities which could lead to critical infrastructure service interruption, destruction of facilities or compromise of sensitive system and data. By providing details on successful attack scenarios and specific remediation guidance, Team TNCG's intent is to help XYZ Client protect its business-critical system, networks, and data.

ABC Application Vulnerability Test

The risk of compromise based on the web application ABC attack scenario was **HIGH.** Upon the web application, multiple instances of JavaScript code injection were discovered, which can allow for an attacker to hijack valid sessions and potentially exploit a valid users web browser. As well, insecure configurations surrounding cookie configurations, cryptography and disclosures of sensitive information were found to be in place.

ABC APPLICATION VULNERABILITY TEST – SUMMARY OF FINDINGS		
ID	**Vulnerability**	**Severity**
1	**Stored Cross-Site Scripting**	**HIGH**
2	**Reflected Cross-Site Scripting**	**MEDIUM**
3	**Session Token in URL**	**MEDIUM**
4	**Insecure Cookie Configuration**	**LOW**
5	**Weak SSL Ciphers in Use**	**LOW**
6	**Private IP Address Disclosure**	**LOW**

Recommendations

Based upon the findings summarized above, Team TNCG has the following remediation guidance:

ABC Application Vulnerability Test

- Sanitize all user-input to prevent injecting and processing JavaScript payloads
- Remove all instances of session tokens being transmitted via the URL
- Implement the Secure and HTTPOnly security flags on all cookies in use that deal with authentication
- Upgrade the TLSv1 cipher suites in use to TLSv1.2, and upgrade all cipher suites to utilize a bit-length of 128 or greater
- Prevent the disclosure of the internal IP address within the ‘remoteAddress’ field during requests

Objectives, Scope, and Approach

Scope

The following table provides a synopsis of target system which were within scope of this engagement.

APPLICATION URL
ABC: https://ABC.gold.ec2.qa.messageone.com/

Vulnerability Testing Process

Approach

In addition to the process described below, every Vulnerability test is approached with varying amounts of prior knowledge about the environment. These approaches can be black-box, white-box or grey-box (defined in the Glossary of Terms). The following approach was used:

- Application Vulnerability Test
    - Grey-box. Team TNCG was provided URLs and multiple user test credentials which were used for testing purposes.

ABC Application Vulnerability Test Details

ABC Application Attack Narrative

This section provides a detailed attack narrative and description of the vulnerabilities which were exploited to gain unauthorized access to protected system or sensitive data in the client environment via application Vulnerability testing. The objective of this section is to provide sufficient detail for XYZ Client to reproduce the "kill chain" and create a remediation plan to correct the discovered vulnerabilities.

Testing began by mapping out the application in its entirety within Burp Suite Pro, as well as running various automated vulnerability scanning tools against the service. As shown below, the Horde RPC interface was discovered to be externally accessible:

Figure 3.2.1: The tool Nikto exposing the presence of RPC.php

After navigating to this resource, the assessor was greeted with a login page. Horde RPC does not use default credentials upon initial setup, so instead a small wordlist was generated along with keywords found upon the site in order to perform a very minimally invasive brute-force style attempt to login:

Figure 3.2.2: The login prompt returned once the RPC.php was requested

After all attempts failed, testing focus shifted elsewhere in order to prevent potential account lockouts. Multiple attempts to seek out privilege escalation vulnerabilities outside of those seen in Findings 1.1 and 1.2 were performed. These included various tests upon the cookies in use as well as attempts to access resources that were restricted to the user-level accounts. As shown below, several attempts to fuzz various cookie values were utilized. After requests were made with the modified values, the responses were observed for anomalies:

Figure 3.2.3: Selecting a parameter to use for fuzz testing

Figure 3.2.4: A sample of the various payloads used for fuzz testing

As well, a potential LDAP injection was discovered by an automated scanning tool within the 'searchPersonalMail.do' resource of the application. In order to test the validity, several different LDAP queries were generated, sent to the server and the responses observed:

Figure 3.2.5: Injecting an LDAP payload

Figure 3.2.6: The response returned. The LDAP queries appear to return results synonymous with auto-population generated by entered keywords

This potential LDAP injection was deemed to be a false-positive, generated by the mechanism utilized server-side in order to search through matches to related queries. While this appears to be a false positive, it is not possible to know with 100% certainty due to the logic embedded within the feature, and it is **highly** recommended to confirm this internally due to the potential severity of this vulnerability if it is indeed present.

ABC Application Detailed Findings

This section of the report provides details regarding vulnerabilities that represent significant threats to the environment. Each vulnerability is described in detail along with screenshots or other evidence to support the findings.

FINDING 1	
Title	Stored Cross-Site Scripting
Resources Affected	
Severity	**HIGH**
Impact	Stored cross-site scripting (XSS) vulnerabilities allow for an attacker to inject HTML code or execute JavaScript code in a victim's browser each time they visit the affected resource. Stored XSS vulnerabilities allow for an attacker to perform actions such as cookie retrieval and session hijacking. They also contain the potential to redirect the end user to a malicious resource, install Trojans or exploit the user's browser directly.
Recommendations	Sanitize all forms of user input server-side to strip or alter dangerous characters into safe ones.
Testing Process and Evidence	

During testing, multiple instances of code-injection related vulnerabilities were manually tested for. A JavaScript payload was injected into the 'email' parameter with the intent to reflect the cookies in use back to the attacker. As shown below, the JavaScript was processed and the cookies in use were displayed:

Figure 1.1.1: Injecting the JavaScript payload within a POST request

Figure 1.1.2: The JavaScript stored and processed, reflecting the cookies back to the attacker

The JavaScript payload that was injected into the 'email' parameter was then saved to the web page, and the values were reflected back to the attacker upon each visit made to the page. As shown below, due to the payload being interpreted as application logic, it's location on the page was very hard to notice, with its presence only being indicated by a vague "Remove" label.

Figure 1.1.3: The discrete location of the email address containing the payload

The potential for privilege escalation is present due to this vulnerability. If an administrator accessed this webpage, the JavaScript can be configured to send the cookies used for authentication back to the attacker, which can be used to authenticate as the administrator.

FINDING 2	
Title	Reflected Cross-Site Scripting
Resources Affected	
Severity	**MEDIUM**
Impact	Reflected cross-site scripting (XSS) vulnerabilities allow for an attacker to inject HTML code or execute JavaScript code in a victim's browser by provoking a user to click a link under control of the attacker. Successful exploitation can allow an attacker to perform malicious activities such as stealing session cookies, overwriting page content, and possibly gaining access to sensitive data in HTTP responses. Theft of session tokens allow attackers to hijack user sessions and interact with the application in the context of the authenticated victim.
Recommendations	Sanitize all forms of user input server-side to strip or alter dangerous characters into safe ones.
Testing Process and Evidence	

Further testing for potential code-injection related vulnerabilities, an instance of a reflected XSS was discovered. As shown below, after injecting a similar JavaScript payload as the one shown in Finding 1.1 within the 'reason=' parameter, the cookies in use were reflected back to the assessor:

Figure 1.2.1: Injecting the JavaScript payload within a GET request

Figure 1.2.2: The cookies in use reflected back to the assessor

FINDING 3	
Title	Session Token in URL
Resources Affected	
Severity	**MEDIUM**
Impact	The session token used to authenticate with the Mailbox feature may be logged in various locations both client-side and server-side and retrieved by an attacker, which can be used to authenticate as the valid user and perform actions on their behalf.
Recommendations	Utilize an alternative means of transmitting the session token, such as via cookies with proper security flags set, or in hidden fields in forms submitted via POST request.
Testing Process and Evidence	

While testing the mailbox feature of the application, it was discovered that the session token utilized to access the mailbox was transmitted in cleartext within the URL:

Figure 1.3.1: The session token transmitted within the URL

As the URL itself is not obfuscated within logs are traffic analyzers, the token in use can be recovered in multiple ways and utilized to authenticate as the legitimate user to perform arbitrary actions on their behalf.

FINDING 4	
Title	Insecure Cookie Configuration
Resources Affected	
Severity	**LOW**
Impact	JavaScript code can access cookies not set using the HttpOnly flag. Tokens used to identify users or are used for authentication should always be set using this flag to prevent access or manipulation stemming from exploitation of distinct vulnerabilities, such as cross-site scripting. As well, the Secure flag was found to be missing. The Secure flag is utilized to prevent the cookie being transmitted in clear text over an HTTP connection.
Recommendations	Implement the HTTPOnly and Secure flags on each cookie in use dealing with authentication.

FINDING 4	
Title	Insecure Cookie Configuration
Testing Process and Evidence	

After discovering Finding 1 and 2, it was noticed that the Secure and HTTPOnly security flags were not in place on cookies potentially utilized within the authentication process. If these flags were in place, specifically the HTTPOnly flag, the cookie would not have been reflected back to the assessor after exploiting the XSS vulnerability.

Figure 1.4.1: Sending a GET request to authenticate with the webmail feature

Figure 1.4.2: The response from the application, setting the cookies without the Secure or HTTPOnly security flags

FINDING 5	
Title	Weak Cipher Suites in Use
Resources Affected	
Severity	**LOW**
Impact	The application supports ciphers using bit-lengths less than 128 as well as TLSv1. This configuration has potential to allow cleartext data to be recovered from ciphertext. Greater bit-lengths require a greater level of effort on part of the attacker to recover the cleartext data.
Recommendations	Upgrade all cipher suites in use to utilize a bit length of at least 128 bits. As well, discontinue the use of TLSv1 in favor of TLSv1.2.
Testing Process and Evidence	

Multiple tests regarding the security posture of the cryptography in use were performed. As shown below, the tool SSLScan was utilized to display the cipher suites in use upon the application. Cipher suites utilizing a bit length of less than 128 bits were discovered, TLSv1 was discovered, which reached its end-of-life in June of 2018.

Figure 1.5.1: Using SSLScan to expose the weak cipher suites utilized by the application

FINDING 6	
Title	Private IP Address in Disclosure
Resources Affected	
Severity	**LOW**
Impact	Unveiling the internal IP address of the application's host can aid in an attacker carrying out network-layer attacks upon the organization.
Recommendations	Prevent disclosure of the application host's internal address. This can be done by utilizing an innocuous identifier for the host, or if possible, removing it from the response altogether.
Testing Process and Evidence	

Within requests made to the resources listed above, the internal IP address of the host operating system was unveiled. This can aid an attacker in multiple ways with crafting an exploitation methodology designed to exploit host operating system itself. As this is not a vulnerability in itself and instead a case of sensitive information disclosure, it is only listed as low severity.

Figure 1.6.1: The GET request performed to the /wfe/ directory

Figure 1.6.2: The internal IP address revealed in the response

Appendix A – The DREAD Threat Matrix Model

To determine the risk level of a particular vulnerability, Team TNCG has employed the DREAD Threat Matrix to objectively classify operational vulnerabilities. Results from our assessment activities are then filtered through the below threat matrix to indicate vulnerability severity.

Rating	High (3)	Medium (2)	Low (1)
Damage potential	The attacker can subvert the security system and get full trust authorization.	Leaking sensitive information	Leaking trivial information
Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
Exploitability	A novice programmer can perform the attack in a short period of time.	A skilled programmer can perform the attack, and then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. Successful exploitation would take some effort.	The issue is obscure, and it is unlikely that users will work out damage potential.

Risk Levels

A number of factors are taken into account to determine the level of risk, including the frequency of a given vulnerability, the ease with which vulnerabilities might be exploited, or the level of data compromise that might occur in the event vulnerabilities are exploited. Additionally, vulnerabilities are evaluated for domino effect in the rating of its risk level. Thus, the analysts to a High may escalate a risk that is considered Low by an automated tool if it is felt that an exploitation of this vulnerability could lead to considerably greater damage or data compromise for our client.

Level	Vulnerability/Possible Vulnerability	Informational Finding
High	Intruders can possibly gain control of the host, which can lead to the compromise of areas within the network system. Vulnerabilities at this level include authentication, encryption, and code issues leading to data manipulation.	Possible findings include unencrypted customer information, data manipulation, and authentication bypass.
Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of installed software. With this information, intruders can easily exploit known vulnerabilities specific to software versions.	Intruders may be able to determine the configuration settings on the host or other system within the environment.
Low	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.	Intruders may be able to retrieve sensitive information related to the host.

Executive Memo

IT Risk Assessment – 20xx
Date: November 30, 20xx

Table of Contents

EXECUTIVE SUMMARY REPORT

November 30, 20xx

John Smith

Chief Operating Officer
Texas Bank
Houston, Texas 78041

Dear John:

Team TNCG recently performed an Information Technology ("IT") Risk Assessment of the Texas Bank's ("TB") IT environment. The review was performed at the TB Corporate facility in Houston, Texas between October 5, 20xx and October 16, 20xx.

This letter summarizes the scope and objectives of the engagement and also provides a summary of Team TNCG's Risk Assessment methodology.

Team TNCG appreciates the cooperation of TB personnel in completing this engagement.

SCOPE AND OBJECTIVE

The scope of this engagement was to perform the 20xx TB IT Risk Assessment. As part of the IT Risk Assessment, Team TNCG performed interviews with key IT personnel, and reviewed the technology environment, including vendors, significant projects, personnel turnover, and IT related controls. Team TNCG's Accounting Standard 5 (AS5) risk-based approach focuses on the IT controls that support the security, confidentiality, availability, and reliability of information and data processing activities.

ASSESSMENT METHODOLOGY AND APPROACH

Team TNCG utilized a risk-based methodology tailored to the TB IT environment and included the identification of key IT personnel, processes, controls, and third-party support functions relative to the TB IT environment. The Team TNCG IT Risk Assessment tool can be readily maintained and updated by TB personnel as the organization, and/or IT environment changes. During the review, Team TNCG utilized best efforts and practices to identify possible business and technical risks, and vulnerabilities that may exist within the IT organization. However, Team TNCG's approach did not necessarily identify all risks, threats, and vulnerabilities in the IT environment, as periodic IT assessments are only one part of a comprehensive risk and control program which should include audits and detailed testing of controls within the IT environment. The IT Risk Assessment process did not include actual testing of identified controls but relied on input obtained during interviews and review of provided IT documentation.

The risk assessment approach used to complete this review is based on the Information Systems and Control Association (ISACA) methodology and guidelines for assessing risk and included developing a risk model for TB.

The risk model was assembled through the definition of seven identified IT risk factors, conducting interviews with IT Management and support personnel, and risk ranking the identified IT processes utilizing factors for risk, probability, and impact. The results of this effort include 1) a Risk Appraisal Profile; and 2) an Audit Plan for detailing the residual risks for IT risk factors and sub-processes, facilitating the prioritization and scheduling of IT Audits.

RISK MODEL

An essential step in developing the risk assessment model is determining applicable elements / indicators of risk.

The TB IT risk assessment model included seven pre-determined risk factors or risk families to evaluate risk within IT. Using these risk families, IT was subjectively measured on (1) the likelihood of a control breakdown occurring, (2) the potential impact such a breakdown would have on achieving business objectives, (3) Team TNCG's Industry Knowledge, and (4) IT interview comments.

As part of the IT Risk Assessment process, interviews were held with key TB personnel to:

- **Gain an understanding** of current IT practices and defined processes.
- **Develop an understanding of the IT environment, organizational structure**s, and technologies and systems currently in use.
- **Discuss short-term changes** to the IT environment, such as new system implementations and/or significant projects.
- **Identify any current areas of concern**.

RISK FAMILIES

The following seven risk families were reviewed for Client's IT environment:

IT Risk Families
1. IT Operations
2. Information Security
3. Systems Development
4. System Software and Database Support
5. Network and Telecommunications Support
6. IT Strategy / Organization
7. IT Applications

SUMMARY OF RESULTS

The results of Team TNCG's IT Risk Assessment disclosed that TB IT management and personnel were control conscious and receptive to improving and maintaining the overall IT control environment. Many of the observations did not change since the last assessment. TB as an organization works well to insure the bank functions as an efficient entity. Overall, the IT controls environment was assessed at a **Medium Low Risk** composite risk score.

TB has determined that it will:

- Move hosting of all Jack Henry Associates (JHA) in-house devices to JHA to reduce the bank's maintenance requirements and improve its Disaster Recovery capability.
- Host its IT services with JHA Gladiator Network Hosting. This will move all servers and appliances to a JHA COLO for management and maintenance.
- Rely on JHA for backup and recovery of all bank data hosted at JHA's COLO.

Observations and Recommendations

Based on the information provided by TB management and IT personnel and the understanding of the IT environment gained throughout this assessment, the following were identified as areas where there were risk observations and should be reviewed by IT management: (Additional details are included in Attachment A – 20xx Risk Workbook)

1. Update, Develop, and / or Formalize the internal TB IT policy and procedures to reflect the current technology environment, including:

   a. Change management – although **no formal Change Management process exists**, the bank follows the JHA process and schedule for updating JHA applications. Since the last IT Risk Assessment, the Bank has begun implementation a change request process. Due to the Bank's decision to host all JHA devices (services, etc.) and IT services with JHA, the Bank will follow the JHA process and schedule for updating JHA application. **Recommend that TB formalize the JHA procedures into an IT policy and standardized procedures.**

   b. Project management – **TB does not have a formal Project Management process**, however, for the current JHA migration project, project management is being run by JHA and is executed by TB personnel as required per JHA's schedule. **Recommend that if further projects are to be executed within the Bank's purview, contract with JHA to manage the projects**.

2. Changes noted since the last assessment include:

   a. Decision has been made to move from Broadleaf Remote Network Management to having all servers, appliances and applications hosted by JHA Gladiator Network Hosting Solutions.

   b. The IT Vendor Management Program has become a mature example of vendor management. Hosted on ERM365, the vendor review process for new vendors and annual reviews for existing vendors is in place and operating efficiently. John Smith has taken the lead for this program and has done an outstanding job.

Risk Scores

The following table presents the resulting risk scores for each IT sub-process reviewed as part of the IT Risk Assessment.

A high-risk score does not indicate that significant problems exist in a process. "High Risk," as used throughout this report, is defined as a high likelihood of unfavorable events occurring in the process combined with a potentially high negative impact on the related process objectives should an unfavorable event occur.

IT Risk Family	IT Sub-Process	20xx Risk Score
IT Operations		
	Problem Management and Event Monitoring	**Medium Low**
	Segregation of Production and Development Environments	**Medium Low**
	Backup and Restore Operations	**Medium Low**
	Disaster Recovery and Business Continuity	**Medium Low**
	Vendor Management	**Medium Low**
	Data Center Environment	**Medium Low**
Information Security		
	Physical Security of Hardware	**Medium Low**
	Security Administration	**Medium Low**
	Authentication Controls	**Medium Low**
	Restrictions on Storage of Sensitive Data	**Medium Low**
	Anti-Virus Administration	**Medium Low**
	Intrusion Detection and Prevention	**Medium Low**
Systems Development		
	Developers Restricted from Production Environment	**Medium Low**
	Change Management (Methodology and Tools)	**Medium Low**
	Project Management	**Medium Low**
Systems and Database Support		
	Patch Management Methodology	**Medium Low**
	Configuration Standards	**Medium Low**
	Systems and Database Administration	**Medium Low**
Network / Infrastructure Support		
	Network Architecture and Design	**Medium Low**
	Network Management and Monitoring	**Medium Low**
IT Strategy / Organization		
	Business Alignment / IT Strategy	**Medium Low**
	Organization and Personnel	**Medium Low**
	Compliance / Oversight	**Medium Low**
IT Applications		
	Segregation of Duties	**Medium Low**
	Reporting and Confidentiality	**Medium Low**

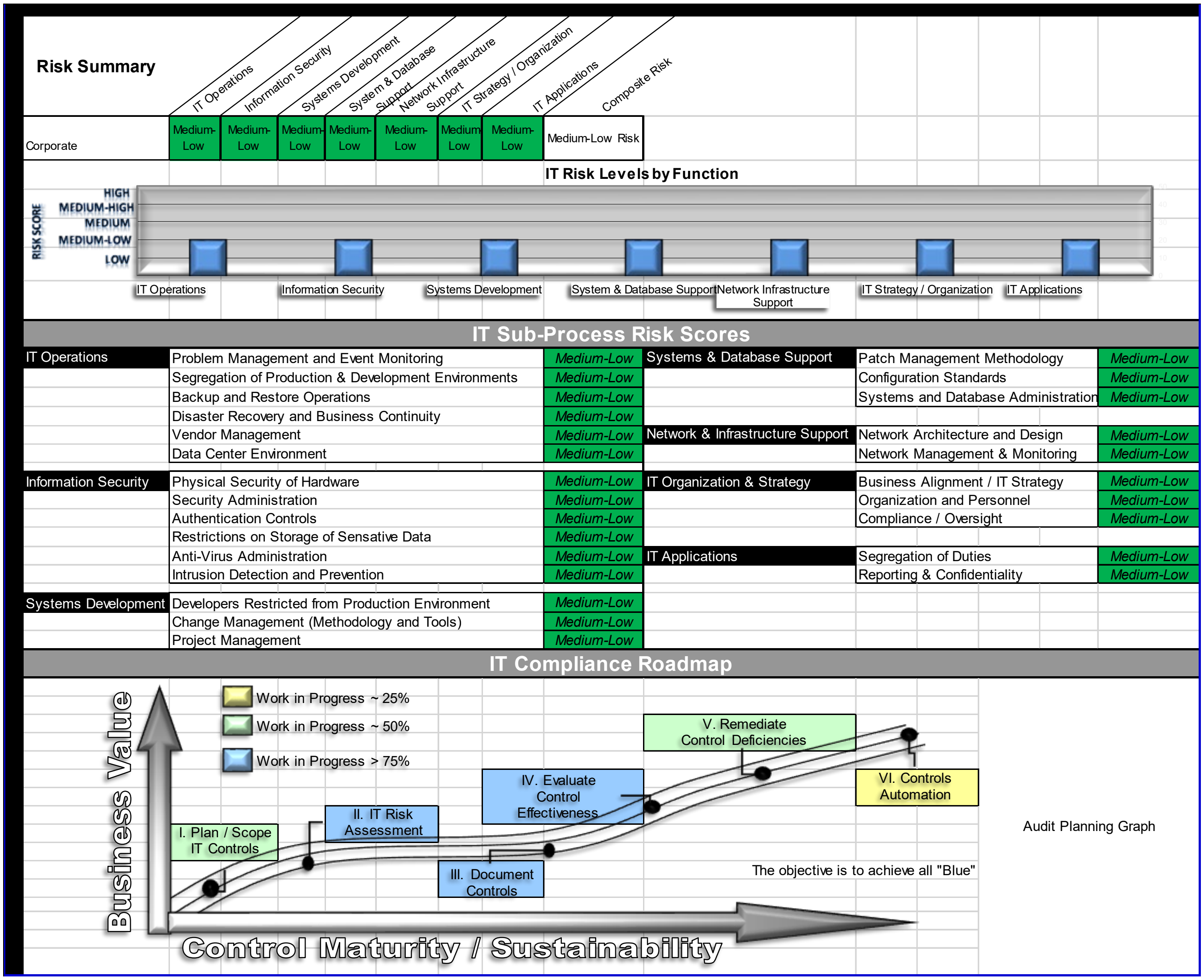
* * *

This report is intended solely for the use of TB internal management, external auditors, and/or regulatory agencies and is not intended to be and should not be used by any other parties without the prior written consent of Team TNCG.

Team TNCG enjoyed the opportunity to assist you in the completion of this assignment. If you have any questions or comments, please do not hesitate to contact me at (555) 555-5555.

Sincerely,

RISK DASHBOARD OCTOBER 20XX



Risk Summary

	IT Operations	Information Security	Systems Development	System & Database Support	Network Infrastructure Support	IT Strategy / Organization	IT Applications	Composite Risk
Corporate	Medium-Low	Medium-Low	Medium-Low	Medium-Low	Medium-Low	Medium-Low	Medium-Low	Medium-Low Risk

IT Risk Levels by Function

IT Sub-Process Risk Scores

IT Operations	Problem Management and Event Monitoring	Medium-Low
	Segregation of Production & Development Environments	Medium-Low
	Backup and Restore Operations	Medium-Low
	Disaster Recovery and Business Continuity	Medium-Low
	Vendor Management	Medium-Low
	Data Center Environment	Medium-Low
Information Security	Physical Security of Hardware	Medium-Low
	Security Administration	Medium-Low
	Authentication Controls	Medium-Low
	Restrictions on Storage of Sensative Data	Medium-Low
	Anti-Virus Administration	Medium-Low
	Intrusion Detection and Prevention	Medium-Low
Systems Development	Developers Restricted from Production Environment	Medium-Low
	Change Management (Methodology and Tools)	Medium-Low
	Project Management	Medium-Low

Systems & Database Support	Patch Management Methodology	Medium-Low
	Configuration Standards	Medium-Low
	Systems and Database Administration	Medium-Low
Network & Infrastructure Support	Network Architecture and Design	Medium-Low
	Network Management & Monitoring	Medium-Low
IT Organization & Strategy	Business Alignment / IT Strategy	Medium-Low
	Organization and Personnel	Medium-Low
	Compliance / Oversight	Medium-Low
IT Applications	Segregation of Duties	Medium-Low
	Reporting & Confidentiality	Medium-Low

IT Compliance Roadmap

The objective is to achieve all "Blue"

Audit Planning Graph

IT Risk Workbook - (Risk Workbook – TB Oct 20xx Final)

Risk Dashboard

Risk Appraisal Profile

Business Monitoring Plan

Audit Planning

Roadmap Worksheet

Methodology

Risk Workbook -
Sample.xlsx