CISO GLOBAL

Statement of Work

Penetration Test Statement of Work for Moore Norman Technology Center

Prepared by True Digital Security, Inc., a CISO Global company

Presented by: Brandon Bonicard

brandon.bonicard@ciso.inc

Effective Date of Offer: 08 / 04 / 2026

Expiration Date of Offer: 10 / 09 / 2026

The following Statement of Work is considered Proprietary and Confidential Information of True Digital Security, Inc. and is not authorized for reproduction, distribution, disclosure or further dissemination without the express written consent of True Digital Security, Inc. Notwithstanding the forgoing or any other provision, the parties agree the Moore Norman Technology Center may reproduce, distribute, disclose or disseminate this Statement of Work and any other materials provided to it in order to comply with local, state, and federal laws, audits, or oversight efforts.

Statement of Work

This Statement of Work Agreement is entered in between True Digital Security, Inc. and Moore Norman Technology Center and hereby fully incorporates the Oklahoma Statewide Contract SW1042 with True Digital Security, Inc., including any addendums or amendments.

Client Contact Information

Client: Moore Norman Technology Center (“Client”)	
Client Contact	Scott Breshears
Address:	4701 12th Ave NW, Norman, Oklahoma 73069
Telephone:	(405) 801-5000
Email:	scott.breshears@mntc.edu

Delivery of invoice for processing	
Address:	4701 !2th Ave NW, Norma, Oklahoma 73069
Contact Name	Christi Duncan
Telephone:	(405) 801-5000
Email(s) to send invoices	accounts.payable@mntc.edu

TRUE/CISO Contact Information

Account Executive: Brandon Bonicard	
Address:	6900 E. Camelback Road, Ste. 900, Scottsale, AZ 85251
Telephone:	972-571-8831
Email:	brandon.bonicard@ciso.inc

Payment Remittance / Accounts Receivable: True Digital Security, Inc.	
Remit to Address:	6900 E. Camelback Road, Suite 900, Scottsdale, AZ 85251
Email:	ar@ciso.inc

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Introduction

True Digital Security Inc., a wholly owned subsidiary of CISO Global, Inc. ("CISO" or "TRUE"), is pleased to present this proposal for a Penetration Test for Moore Norman Technology Center ("Client"). This assessment focuses on both internal and external penetration testing, which will assist the client in better understanding their overall security risks. An optional re-test, performed after remediation tasks have been completed, is also included with our service to provide an opportunity to validate that any new corrective actions were successful in remediating the identified risks. Please reach out to CISO if any further information is needed to support your evaluation process, and we thank you for considering CISO for your service needs.

This SOW Agreement, deliverables, and communications concerning the provision of services and documents provided by the Client are confidential and CISO shall not disclose without prior written approval from the Client, with the following exceptions:

Moore Norman Technology Center acknowledges CISO will comply with SW1042 statewide contract usage reporting requirements and Moore Norman Technology Center project status update requests, if applicable, without prior written approval.

Project Overview & Scope

Penetration Testing Overview

CISO's Penetration Testing methodology includes extensive technical testing using the most current attack vectors and specialized analysis of findings to provide a comprehensive view of the risks associated with each vulnerability. A Penetration Test from CISO combines extensive vulnerability determination and exploitation phases.

The CISO's Penetration Test will examine the entire environment for as many vulnerabilities as possible, at all levels of the infrastructure including the network, operating systems, and common application services. Technical testing techniques include both automated scanning to find common issues, as well as full, manual exploitation attempts to simulate the same activities as hackers. Any vulnerabilities found through the automated scanning process are also manually verified to ensure the issues are truly a risk to the organization.

Upon completion of the testing, all identified vulnerabilities are documented with a detailed description of the issues, as well as recommended corrective actions to help eliminate the risks going forward. Each vulnerability's risk is evaluated from business and technical perspectives, and an overall risk rating is provided.

If any exploitation is successful, a detailed step-by-step narrative explaining how the exploits actually worked and what data could be compromised is provided. Screen captures are utilized to document and showcase the entire process so that the issues may be re-created, if necessary.

Benefits

- Rapid identification of issues
- Comprehensive security posture evaluated
- Extensive risk analysis for all findings
- Clear, concise prioritized results

Methodology

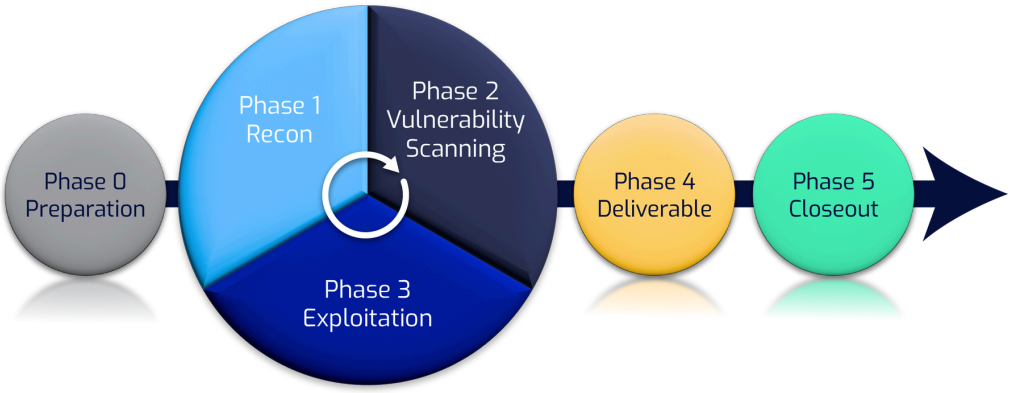
Overview

The CISO methodology for conducting Penetration Testing engagements is based on a proven track record of providing high quality results and detailed corrective actions, which can help lower the overall risk of the tested environment. Each engagement, however, is a specialized event unique to each client. The following steps provide a high-level outline of the overall process that can be customized specifically to each client's unique business needs.

Assessment Phases

CISO has developed a robust assessment methodology that maximizes technical results, while minimizing the impact to the testing environment. Although this methodology has been customized, it is based on proven industry best practices from NIST SP800-115, the Open-Source Security Testing Methodology (OSSTM), and the Open Web Application Security Project (OWASP).

The CISO methodology can be summarized in the following phases:



Project Details

Preparation

Before testing begins, CISO works with our clients to fully define the rules of engagement for each penetration test. This information is documented in a brief questionnaire that will help identify all the testing criteria that CISO will need to properly define the exact scope of the assessment. Only the systems identified in the questionnaire will be considered in-scope, effectively creating a virtual "sand-box" for the testers.

In this important step, clients can provide details on specific goals of the penetration test, such as obtaining maximum control over company systems, or targeting specific types of systems or important organization data. The customer can also identify specific time windows for testing or hosts that should be subject to higher scrutiny or more care.

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Phase 1 – Passive And Active Reconnaissance

During this phase, all networks and systems identified in the questionnaire will be analyzed to determine how many and what types of systems, services, applications, and information are present in the target environment. This analysis serves to validate the scope provided by the client and provides the foundation for formulating a plan to effectively test the environment.

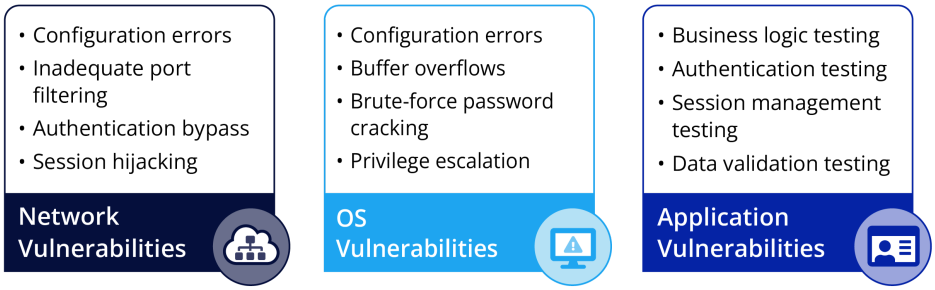
The testing activities included in the Passive and Active Reconnaissance Phase can be summarized with the following tasks and associated methods and tools:

Tasks	Methods	Tools
Review available information on the company, systems, configurations, or other data	• Query search engines • Examine network, DNS, and Mail relay registration information • Collect company and personnel data for use in subsequent phases	• Search engines • Whois/Dig • Social Media • Company publications • Manual testing
Probe system and services	• Network scans • Ping sweeps • TCP/UDP port scans • SNMP sweeps • VPN detection • System enumeration • Port scans • Banner grabs • OS Fingerprinting • SSL cipher strength analysis • Examine web sites, applications, and file services	• Nmap/MassScan • SSL Cert Query • Custom tools

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Phase 2 – Vulnerability Determination And Analysis

Utilizing results from Phase 1, work begins identifying potential vulnerabilities in the accessible systems and services. Using best-of-breed automated scanning tools provides an initial vulnerability inventory of the environment as quickly and efficiently as possible. Testing will encompass all layers of the environment to include network, OS, and application vulnerabilities:



Because automated scanning can only provide a limited view of any environment, a significant portion of the work performed by CISO involves the use of manual review and a customized toolset that can be employed based on the unique environments encountered. Most of the testing in this phase consists of manual validation and exploitation testing. The activities included in the Vulnerability Determination and Analysis Phase can be summarized with the following tasks and associated methods and tools:

Tasks	Methods	Tools
Scan for potential vulnerabilities	• Automated vulnerability scanning against active IPs	• Nessus • Burp Suite • Custom tools
Analyze services for configuration and implementation flaws	• Intelligent and brute force password testing • Review file system and application service access controls • Analyze network traffic	• Hydra, Medusa • Metasploit • Wireshark, Impacket, Responder • Burp Suite • Custom tools • Manual testing

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Phase 3 -Validation And Exploitation

Once potential vulnerabilities are identified, they are analyzed to determine both if they are valid issues and the extent to which they can impact the affected system and the overall environment.

Any identified vulnerabilities are manually exploited in an effort to gain access to the systems and the data they contain. These vulnerabilities are then used either on their own or in combination to further the goals of the test. In cases without explicitly stated goals, the general process followed by CISO is to identify and access important systems or data:

- To gain elevated privileges, especially administrator access, by exploiting system level vulnerabilities or misconfigurations. Once full system access is gained, the tester will then try to continue to further expand their access throughout the internal network leveraging any existing “trust relationships” this system may have on the network (i.e., local user to local admin to domain admin/LDAP user).
- To gain access to business data and critical information (PII, financials, source code, credentials). Typically, backend systems like databases contain critical business data that is often easily accessed without requiring any escalated network privileges. CISO will attempt to search for and gain access to these types of data.

This process is iterative, with the expanded view provided by exploiting vulnerabilities being used to perform additional reconnaissance, vulnerability testing, and further penetration into the environment in order to reach the project goals.

The activities included in the Validation and Exploitation Phase can be summarized with the following tasks and associated methods and tools:

Tasks	Methods	Tools
Elevate privileges	• Identify higher privileged systems & users • Capture credentials or trust relationships	• Mimkatz • John, Ophcrack, rainbow tables • Metasploit • Custom tools • Manual testing
Pivot systems / lateral movement	• Evaluate vulnerabilities in systems made accessible through other flaws • Use access gained to move to systems closer to target or in protected zones	• Metasploit • Custom tools • Manual testing

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Deliverable

All identified and validated vulnerabilities are analyzed from an overall risk perspective. The risk rating is first evaluated from a technical risk perspective, and the vulnerability's Common Vulnerability Scoring System (CVSS) rating is documented. Then any additional information regarding other compensating controls or likelihood of occurrence is factored into an overall "ease of exploitation" risk rating. These two risk factors are then combined into an overall risk perspective that is specific to the client environment. This unique approach provides a more detailed analysis that can then be easily utilized to help prioritize the client's remediation efforts.

Once active testing is completed, the final report deliverable is prepared to document all findings from the assessment and provide detailed recommendations to help prioritize remediation efforts.

Where applicable, the report will contain the following major details:

- **Executive Summary** – Includes a high level overview of the risks as it pertains to the business, remediation priorities, gap analysis, and timelines
- **Passive and Active Reconnaissance** – Includes summary of identified systems, ports, software versions, and SSL encryption configurations
- **Vulnerability Determination** – Includes a detailed list of each specific vulnerability identified, prioritized by risk level with specific recommendations for remediation
- **Adversary's Perspective** – Includes a detailed description of how the information and vulnerabilities can be used to obtain elevated privileges or access to system data
- **Conclusions** – Includes summary of the overall findings from the assessment and provides overall risk comparisons to other like organizations. Additional strategic recommendations will also be made that might help address the root cause of the technical issues identified in the findings.

Closeout

CISO does not stop with documenting the findings in a deliverable but will work with the client to ensure the findings are understood, and that there is a clear path to implementing the recommendations. If the client has particular questions surrounding any of the findings, CISO will gladly review the risk analysis process in depth with the client, and will incorporate any required changes in the deliverable. The ultimate goal of the Closeout Phase is to ensure the highest level of client satisfaction.

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Scope And Logistics

In Scope Activities

- Unless otherwise specified, penetration testing will be performed remotely
- When performing internal testing, it may be necessary for to test from an internal system, VM, or server appliance provided by CISO
- If any web applications are included within the IPs to be tested, CISO will perform baseline unauthenticated application testing as part of this engagement unless otherwise indicated

Out Of Scope Activities

- Denial of Service (DoS) attacks are never intentionally carried out as part of the testing
- If systems are owned by a third party (e.g., a hosting company) then the third party must authorize this testing in writing prior to the start of the engagement
- Although the testing team will make every effort to identify as many vulnerabilities as possible within the allotted testing windows, the consultants will only target those systems with the highest value of success for full exploitation.
- Remediation of any issues, deficiencies, errors, or problems discovered during the penetration testing process is out of scope. If Client desires to receive remediation-related services, then those services must be agreed upon in a separate SOW or, alternatively, in a written amendment to the current SOW.

Testing Risks

Client is responsible for reviewing “Appendix: Security Testing Risk Disclosure Statement,” incorporated into this Statement of Work Agreement.

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Client Responsibilities

- Designate a point of contact for project activities, access, logistics, budget, communications, and all other items related to supporting this engagement
- Assist with secure connectivity to Client's network (if needed)
- Provide internal coordination to assist CISO as needed
- Provide access to documentation needed to support service activities
- Communicate CISO's security testing activities to all responsible parties, including all hosting services, device and data owners and administrators
- Within ten (10) days after being directed to do so, Client will remove, package and ship, at Client's expense and in a commercially reasonable manner, all hardware, equipment, and accessories provided to Client that were used in the provision of the Services. If Client fails to timely return all equipment, or if the equipment is returned to us damaged (normal wear and tear excepted), then Client will be charged, and Client hereby agrees to pay, the replacement value of all such unreturned or damaged equipment.
- Unless otherwise expressly stated in writing Client agrees to use and CISO agrees to deliver all services under this Statement of Work during the period ending one (1) year following execution of this Statement of Work.
- Any changes to this Statement of Work must be made in writing utilizing an approved Change Order Form referencing this Statement of Work and agreed to and signed by both parties.
- Client is responsible for reviewing "Appendix: Security Testing Risk Disclosure Statement" within this document that includes client responsibilities to reduce the risks associated with security testing.

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Engagement Scope

Services to be Performed
Penetration Testing CISO will perform a Penetration Test tailored specifically for client's business environment as detailed in the client questionnaire. Testers will use multiple tools and techniques to simulate an attack on systems without causing a destructive or denial of service (DoS) condition. Penetration testing goals are to identify, and then verify application or operating system vulnerabilities, as well as security configuration weaknesses that can give an attacker a foothold in the environment. All testing will be conducted remotely so no other expenses are anticipated during this phase. ***Scope*** • External Network Penetration Test (with Exploitation): Includes up to 23 IPs • Internal Network Vulnerability Assessment (No Exploitation): Includes authenticated testing of up to 100 IPs that include 62 servers and a sampling of other devices • 3 Hyper-V servers ***Activities*** • Reconnaissance and device discovery • Automated network and application vulnerability scanning • Manual verification of findings to reduce false positives • Manual exploitation techniques to simulate realistic hacker activity and identify systems or data that are at risk of compromise ***Requirements*** • Testing windows will be set by the end client • Any required internal testing will be conducted through an approved VPN connection • Prior approval for any hosted systems is required before the start of testing ***Deliverables*** • Single point of contact (Project Manager) for all tasks and deliverables • Final Assessment Report describing identified vulnerabilities, and recommendations for remediation • Letter of Attestation (upon request) **Remediation Validation Test: Included upon Request** • Remediation testing is available upon request. Client is responsible for requesting scheduling of the remediation testing. Scope includes a re-test of all high and medium level vulnerabilities that were identified in the initial assessment. • Deliverable for this phase is a revised Final Assessment Report showing remediated items. • Re-testing can only be scheduled once all remediation items are completed, and the request must be received no later than 90 days from the services described in this SOW.

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

One-Time Pricing

Name	Price	Payment Terms	Billing Frequency
Penetration Testing	$15,000.00	Net 45	**Milestone 1 (Project Kickoff)** 33% Invoiced Net 45 at completion of Milestone 1 **Milestone 2 (Deliverable Acceptance)** 67% Invoiced Net 45 upon client acceptance of final deliverable *Client acceptance of final deliverable or five (5) days after CISO's delivery of final deliverable, whichever is earlier* Contractor shall be paid upon submission of proper invoice(s) to the agency at the prices stipulated. Invoices shall contain the purchase order number. Failure to provide proper invoices may result in delay of processing invoices for payment. Pursuant to 74 O.S. §85.44(B), invoices will be paid in arrears after products have been delivered or services provided. Interest on late payments made by the State of Oklahoma is governed by 62 O.S. §34.71 and 62 O.S. §34.72.

Subtotal **$15,000.00**

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Note: While CISO will attempt to uncover as many threats as possible, it is impossible to guarantee the disclosure of all threats.

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

Acceptance And Authorization

The parties hereby agree to the terms of this Statement of Work, including all terms outlined in the Oklahoma Statewide Contract No. 1042 with CISO, including any addendums or amendments. The effective date of this SOW is the last signature date shown below.

Acknowledged and agreed by:

Moore Norman Technology Center	**True Digital Security, Inc., a CISO Global company**
	Deb Smith
(Signature)	(Signature)
	CFO
Title	Title
	Deb Smith
Printed Name	Printed Name
	08 / 10 / 2026
Date	Date

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.

APPENDIX:
SECURITY TESTING RISK DISCLOSURE STATEMENT

CISO has created this disclosure statement to inform its clients of the risks involved in conducting security testing procedures and ensure all parties understand and acknowledge their roles in reducing this risk.

Representation And Warranties

CISO's staff works diligently to avoid the risks of security testing; however, this risk can never be fully eliminated. The purpose of this Appendix is to inform all resources and parties associated with this engagement within Moore Norman Technology Center that these risks exist in the performance of the testing associated with this engagement. Such risks may include data destruction/modification, system crashes, or network interruptions, among other issues. Moore Norman Technology Center acknowledges these risks and agrees that they are responsible for mitigating any risks they deem necessary prior to approving CISO's testing windows.

Steps CISO Takes To Minimize Risk

CISO takes the following steps to minimize risk:

- CISO does not use brute forcing or explicit denial of service testing.
- CISO employs prompt communication strategies. Planning and coordination between Moore Norman Technology Center and CISO will play a significant role in reducing the risk of impact to Moore Norman Technology Center information systems.
- Per client requirements, CISO is available to perform testing during non-business hours.
- “Dangerous” tests (e.g., penetration testing) are to be performed only with client approval.

Steps Client Should Take To Minimize Risk

CISO recommends Moore Norman Technology Center take the following steps to minimize the risk associated with security testing:

- Moore Norman Technology Centershould communicate testing procedures to all impacted internal and third parties, subject to the guidelines of the engagement.
- Moore Norman Technology Centershould maintain current backups of all data and systems.
- Moore Norman Technology Centershould closely monitor availability and performance during testing.
- Moore Norman Technology Centershould have an incident response plan in place and be immediately accessible by a phone that does not rely on Moore Norman Technology Center's network infrastructure.

CISO Global, Inc. | © 2026 CISO Global. All rights reserved.