STATEMENT OF WORK

Project Name:	External Network Penetration Test	**Seller Representative:** Liam McNamara +1 (703) 2628156 liammcn@cdw.com
Customer Name:	WILLIAMSON COUNTY, TX	
CDW Affiliate:	CDW Government LLC	
Subcontractor:	Liquid PC Inc	**Solution Architect:**
Date:	March 04, 2025	
Drafted By	Sasha Beard	

This statement of work ("**Statement of Work**" or "**SOW**") is made and entered into on the last date that this SOW is fully executed as set forth below ("**SOW Effective Date**") by and between the undersigned, CDW Government LLC ("**Provider**," and "**Seller**,") and WILLIAMSON COUNTY, TX ("**Customer**," and "**Client**,").

This SOW is subject to the terms and conditions of the OMNIA Partners Region 4 Education Services Center "ESC" Contract #R210401 held by CDW Government LLC with an effective date of June 1, 2021 (the "**Agreement**"). If there is a conflict between this SOW and the Agreement, then the Agreement will control, except as expressly amended in this SOW by specific reference to the Agreement.

PROJECT DESCRIPTION

PROJECT SCOPE

- External Network Penetration Test

DESCRIPTION

1. When performing scanning activities over the past years, we have noticed that automated tools are often finding fewer and fewer critical vulnerabilities. While this trend is a good thing, we are also discovering many organizations are vulnerable due to Low or even Informational findings. This is one of the major differentiators for Black Hills Information Security (BHIS). We look at scanning and exploitation as more of an endeavor of learning about your environment, the same way a targeted attacker would. We do not simply run a scanner, look for critical, and then search tools like Metasploit for an exploit. We use our scanning information to try to understand your network and the individual roles of the computers that comprise it. We want to understand how these points of technology support the overall organizational objectives. With this approach, we find far more vulnerabilities than what is reported by a simple scan.
2. During the assessment and penetration testing phases, we will perform reconnaissance, vulnerability scans, and testing for an organization's assets, cloud configurations, exposed services, and login portals. We will validate the scans to weed out false positives by manually verifying a subset of results within particular vulnerability classes. However, the true value of a penetration tester over a scanner is going the extra mile of looking at vulnerabilities (including the Low and Informational findings) and then manually probing the in-scope networks, looking for additional methods of entry or compromise not flagged by a scanner.

3. Black Hills Information Security will use specialized techniques (if applicable) such as document metadata analysis, custom password dictionaries, and other proprietary methods. Remediation guidance will be provided for each vulnerability documented in the report, as well as strategic recommendations for improving the security of the organization as a whole.

TARGETS

1. Up to
   a. External (Public) Live Systems:
      i. < 40 Live Ips
         1) This scope item will be completed remotely.

OBJECTIVES

1) Perform reconnaissance through numerous OSINT tools
2) Investigate breach data and associated organizational leaks
3) Provide a profile of the organization and threat modeling available to potential attackers
4) Identify systems and key assets exposed to attackers
5) Enumerate vulnerabilities present on systems
6) Review corporate web application exposures for unpatched framework components and missing multi-factor authentication enforcement Provide recommendations for protecting key company assets
7) Identify areas where sensitive information is exposed
8) Provide evidence of the effectiveness of current defensive mechanisms and attack detection methodologies
9) Provide an in-depth understanding of discovered vulnerabilities and repercussions via exploit attempts, where applicable
10) Provide recommendations for remediation of the identified practices and/or exposures based on the above testing

WEB APPLICATION SECURITY ASSESSMENT: NETWORK-LEVEL OVERVIEW

For web applications, please note that in-depth testing is best serviced by a dedicated BHIS Web Application Penetration Test that follows an industry-standard methodology, such as the one compiled by the Open Worldwide Application Security Project (OWASP). However, as part of a network level assessment, a limited scan with the following high-level goals may be performed from a network perspective:

1) Identify publicly accessible web sites and/or portals associated with the organization
2) Determine whether identified endpoints may pose a risk or create a potential vulnerability
3) Provide recommendations for mitigating select exposures in web applications
4) Provide a limited inventory of select vulnerabilities in the organization's web applications that may expose users to malicious exploits
5) Provide high-level understanding and verification, via exploit attempts, of select vulnerabilities in the organization's web applications

a. METHODOLOGY

i. Assessment and testing focus on identifying key assets and targeting them to harvest information, just as an attacker would on the inside of the network. These tests will include:
   1) **In-Depth Company Profiling and Threat Modeling** – One of the values provided by testing is an understanding of what information can be gathered about your organization from open sources and, more importantly, what attackers can do with it. We will use various tools and resources to collect public information about your organization and couple it with custom threat modeling to perform targeted attacks and report on them.

2) **Host Discovery and Service Identification** – BHIS identifies hosts using several network scanning techniques. By employing different techniques, we can quickly obtain a list of assets and enumerate the services on them.

3) **Vulnerability Discovery** – To further identify risk, a vulnerability scan is specifically tuned for the environment and then executed. This scan can be run across the network and is used as a baseline for exploitation.

4) **Web Services Enumeration** – BHIS will investigate the web applications discovered during vulnerability scanning. This investigation is intended to provide a high-level overview of the individual application configurations at a high level. BHIS will look for application framework components with known vulnerabilities. Additional testing may include a review of multi-factor enforcement practices where possible and applicable.

5) **Password Spraying and Credential Stuffing** – As the threat landscape continues to change, so do threat actor tactics. Common attacks include password spraying, where adversaries guess a single password against a large number of probable users. These attacks are often hard to detect for several reasons. Credential stuffing will also be attempted, where permissible, to determine if breached credentials associated with an organization's domain and user population have been reused on corporate login portals.

BHIS Background with Network Assessments and Penetration Tests

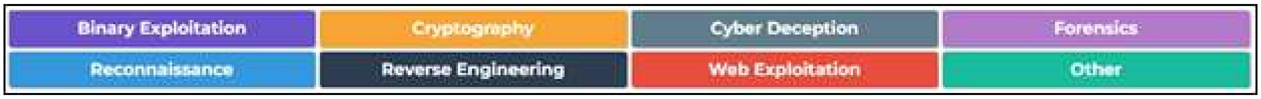
1. The staff at BHIS hold multiple certifications in the area of network assessment and network penetration testing. However, certifications often don't tell the whole story.
2. Our training organization, Antisyphon, also provides a broad spectrum of cybersecurity training that is written and delivered by industry practitioners. Many of our testers are also alums of the SANS Technology Institute, as instructors, course creators, or both.

Antisyphon Cyber Range

1. As part of this SOW, all Black Hills Information Security (BHIS) customers will gain access to an online cyber range for up to five people from their team. This environment contains over 100 different challenges ranging from network, active directory and host-based threat hunting, web application attacks and security, operating system security, and forensics. This SOW item is available upon request for up to one year after SOW start.

a. Challenges

i. After registration is complete and you've successfully logged into the Antisyphon Cyber Range Scoreboard, you will gain access to the Antisyphon Cyber Range challenges.



Antisyphon Cyber Range Challenge Types

b. There are seven different challenge types:

i. Cryptography
ii. Reconnaissance
iii. Web Exploitation
iv. Reverse Engineering
v. Forensics
vi. Penetration Testing
vii. Other

2. Many of these challenges have hints to help people through them.

3. The goal of any SOW with BHIS is to help wholly strengthen our customers' teams. We fundamentally believe that training should be part of any SOW we sign. Because of this, we make this cyber range available to all our customers.
4. ACE-T™ stands for "Antisyphon Cyber Education Testing." Individuals can get ACE-T™ certified by completing challenges in the Antisyphon Cyber Range, which contains a variety of challenges related to cryptography, forensics, penetration testing, reconnaissance, reverse engineering, and web exploitation. The Cyber Range currently has ten levels of ACE- T™ certification for users to work through.
   ACE-T™ certification allows users to demonstrate their infosec expertise to colleagues, management, and HR personnel alike. Users also share their ACE-T™ certification level with others by having them look up their name at the following URL: https://lookup.hackhills.com/.

Black Hills Information Security to Customer

1. Schedule and coordination
   a. Establishment of test dates
   b. Project plan
   c. Selection of tester(s)
2. Rules of Engagement call
   a. Review of scope
   b. Communication Protocol
   c. Confirmation of penetration testing start dates and times
3. Report Delivery and Review Process
   a. Report detailed testing results, as described in the Report Format section below:
   b. First copy will be considered "draft pending customer comments/input"
   c. The first copy will be issued no later than 10 business days from the completion of work. Customer then has 10 business days to review the report, add comments, and request changes. BHIS then has 5 business days to issue a response and deliver the final report. Further reasonable revisions are up to the discretion of the tester(s) yet, all reporting requests will not exceed 30 calendar days past initial report delivery.
   d. If no comments/input are received, the "Draft" will be considered "Final"
   e. BHIS will invoice upon report delivery.
4. Post-Engagement Support and Security Recommendations
   a. General recommendations for improvement of organizational security
   b. Customer's questions will be answered for 90 days following completion of work. BHIS cannot guarantee tester's continued availability after this point.
5. Security Assessment Report Structure
   a. Black Hills Information Security (BHIS) will compile each phase of the security assessment into a report containing the following:
      i. **Executive Summary** – A highlight of the major problems found and high-level recommendations that address the specific issues, tailored for an executive-level audience. An overall risk analysis rating relative to the discovered findings will also be assigned and described in this section.
      ii. **Methodology** – A complete description of all testing performed, including instructions for recreating the test scenarios so that the organization can re-test after mitigating controls have been implemented (as available).
      iii. **Findings** – A complete description of each major vulnerability found, including details on how it was exploited and what information or level of access was obtained as a result. This section will also contain:

1) DISCUSSION – A description of how the documented vulnerability could affect the organization if an attacker exploited it
2) RECOMMENDATIONS – A detailed description of how to fix the vulnerability (as available), including command and configuration examples. Also included are any organizational improvements to policy and/or processes that will help remediate the vulnerability
3) RESOURCES – Links to information about the vulnerabilities that were found and remediation guides (as available)

iv. **SUPPORTING DATA ARCHIVE** – An archive of all tool output and vulnerability scan reports. The archive will also include:

1) Listing of all open ports and likely services based upon fingerprinting and analysis techniques
    a) Results of Any Specific Testing (as applicable)
        i) For example, password cracking, wireless assessments, social engineering, and port scanning will be included. Each vulnerability or exposure will be documented in the format described above.

v. **REMEDIATION VALIDATION (OPTIONAL)**

1) This is also known as a remediation check of reported findings and can be added as an option as one day blocks of $2,500. Remediation validation must be completed within 30-60 days from the Initial Report. Ongoing remediation validations are limited to one validation. Remediation validations cannot be performed on Assumed Compromise, Red Team, Physical, and Wireless tests.

CUSTOMER TO BLACK HILLS INFORMATION SECURITY

1. Signed agreement (see separate MSA)
2. BHIS strongly suggests testing occur on non-production systems and databases (for web application penetration testing). When needed, we can accommodate two phase engagements, where testing occurs on non-production assets with some issues validated later on production.
3. Authentication credentials for the web application(s) to be tested
4. Remote access via VPN or other compatible remote access method
5. Scoping document with scope authorization. Generated with project management team following award of SOW.
6. BHIS will need access to customers testing environment for the 2 weeks of the reporting period
7. Primary Project Contact and Primary Technical Contact information:

Primary Project	**Primary Technical (if different)**
Name: Derek Gumaer	Name:
Title:	Title:
Email:	Email:

8. Please note, the project management team will generate a scoping checklist in conjunction with the BHIS customer during meetings, following the signing of the statement of work. Below is a breakdown of some of the items typically covered in the scope checklist.
    a. Targets or technical points of focus
    b. Primary and backup points of contact
    c. Notification procedures for critical findings
    d. Authorized testing timeframes
    e. Notification procedures and protocols for customer points of contact
    f. Meetings, notifications, and contact frequency and format
    g. Sensitive and/or prohibited ranges and systems
    h. Customer guidance to testers
    i. Etc.

PROJECT TIMING

1. The timing of this project will be determined following signature of SOW/statement of work. The schedule will be generated by the BHIS project team, following coordination with Customer regarding deadlines, tester availability, and customer enterprise environmental factors (e.g., remote access, test string availability, blackout dates, support personnel etc.). No guarantees on scheduling can be made that are not identified in this section.
2. BHIS has not preplanned this work.
3. Work that has not been preplanned may take 6-12 or more weeks to commence, starting from the date of a signed SOW/statement of work. This estimate is based on current workloads, resources, and projections.
4. Cancellation or rescheduling of work without four weeks prior notice will incur an additional charge.
5. The following schedule may be enforced if BHIS is not able to reschedule work to avoid idling a tester.
   a. Less than 4 weeks' notice incurs an additional 20% charge
   b. Less than 2 weeks' notice incurs an additional 50% charge
   c. Day of start or within testing time frame incurs an additional 100% charge
6. BHIS will make a reasonable effort to reschedule work for testers and avoid the additional charge. Additional charge shall be assessed only on the portion of a test that is delayed or cancelled.
7. The table below is listed for planning and estimation purposes. This reflects time on keyboard or on-site actively engaged in the testing methodology. It does not include planning, coordination, set up, reporting or debriefing the customer. As all BHIS engagements are timebound, proper guidance from Customer will result in optimal coverage within the time constraints.

Service	Estimated Active Tester Time for Planning Purposes
External Network Penetration Test <40 Live IPs	3 days
Antisyphon Cyber Range	Within a Year

8. Fee(s) include(s) project setup, coordination, test preparation, standard report production, report review, report editing, and comment resolution. Any work beyond this description and the work described in each section above should be discussed with the BHIS team prior to signing this SOW. All line items are timebound.

Remote Testing	Estimated Active Tester Time for Planning Purposes
External Network Penetration Test <40 Live IPs	3 days
Onsite Testing	
NA	NA
Subtotal	
Assessment Total (not including any applicable travel expenses)	

Included Services	USD
5 Licenses for any John Strand On Demand or Live Classes	Included
Antisyphon Cyber Range	Included

9. There is no decrease in cost if the customer chooses not to select the included service. The included service is available upon customer request.
   a. NOTE: Daytime/business hours testing is assumed. Daytime/business hours are defined as 8am ET to 6pm PST, Monday through Friday. Automated scanning may be run off-hours but not penetration testing.
10. Remediation validation (remediation check of reported findings) can be added as an option as one day blocks. Remediation validation must be completed within 30-60 days from the Initial Report. Ongoing remediation

validations are limited to one validation. Remediation validations cannot be performed on Assumed Compromise, Red Team, Physical, and Wireless tests.

Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

GENERAL RESPONSIBILITIES AND ASSUMPTIONS

- Customer is responsible for providing all access that is reasonably necessary to assist and accommodate Seller's performance of the Services.
- Customer will provide in advance and in writing and Seller will follow, all applicable Customer's facility's safety and security rules and procedures.
- Customer is responsible for security at all Customer-Designated Locations; Seller is not responsible for lost or stolen equipment, other than solely as a result of Seller's gross negligence and willful misconduct.
- Customer acknowledges that in order to efficiently and effectively perform the Services CDW may need to collect information from Customer's systems by using software tools developed or used by CDW ("Tools"). In some cases, these Tools will need to be loaded onto the Customer's systems to gather necessary information, and CDW may also use them to make changes in the Customer's systems consistent with the agreed upon scope. Tools will be used only for purposes of performing the Services and will be removed or automatically deleted when CDW has completed use of them. Customer hereby consents to CDW's use of the Tools as set forth in this paragraph.
- Upon completion of the Services, Customer is responsible for disabling or deleting all CDW coworker access credentials and completing any other necessary steps to ensure that access to all of Customer's environments has been permanently terminated for all CDW coworkers and contractors that were part of this engagement.
- This SOW can be terminated by either party without cause upon at least fourteen (14) days' advance written notice.

CONTACT PERSONS

Each Party will appoint a person to act as that Party's point of contact ("**Contact Person**") as the time for performance nears and will communicate that person's name and information to the other Party's Contact Person.

Customer Contact Person is authorized to approve materials and Services provided by Seller, and Seller may rely on the decisions and approvals made by the Customer Contact Person (except that Seller understands that Customer may require a different person to sign any Change Orders amending this SOW). The Customer Contact Person will manage all communications with Seller, and when Services are performed at a Customer-Designated Location, the Customer Contact Person will be present or available. The Parties' Contact Persons shall be authorized to approve changes in personnel and associated rates for Services under this SOW.

CHANGE MANAGEMENT

This SOW may be modified or amended only in a writing signed by both Customer and Seller, generally in the form provided by Seller ("**Change Order**"). Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

In the event of a conflict between the terms and conditions set forth in a fully executed Change Order and those set forth in this SOW or a prior fully executed Change Order, the terms and conditions of the most recent fully executed Change Order shall prevail.

PROJECT SCHEDULING

Customer and Seller, who will jointly manage this project, will together develop timelines for an anticipated schedule ("**Anticipated Schedule**") based on Seller's project management methodology. Any dates, deadlines, timelines or schedules contained in the Anticipated Schedule, in this SOW or otherwise, are estimates only, and the Parties will not rely on them for purposes other than initial planning.

The following scheduling scenarios that trigger delays and durations to extend beyond what's been planned may require a Change Order:

- Site preparation, such as power, cabling, physical access, system access, hardware/software issues, etc. must be completed in a timely manner.
- Project tasks delegated to Customer PMs/Engineers/Techs/Management/Resources must be completed in a timely manner. For example, in the event a project 's prioritization is demoted, and Customer resources are reallocated causing the project's schedule to extend on account of experiencing interruptions to its momentum requiring complete stop(s) and start(s).
- External projects/dependencies that may have significant impact on the timeline, schedule and deliverables. It is Seller's assumption that every reasonable attempt will be made to mitigate such situations.

TOTAL FEES

The total fees due and payable under this SOW ("**Total Fees**") include both fees for Seller's performance of work ("**Services Fees**") and any other related costs and fees specified in the Expenses section ("**Expenses**").

Seller will invoice for Total Fees. Customer will pay invoices containing amounts authorized by this SOW in accordance with the terms of the Agreement. Unless otherwise specified, taxes will be invoiced but are not included in any numbers or calculations provided herein. The pricing included in this SOW expires and will be of no force or effect unless it is signed by Customer and Seller within thirty (30) days from the Date listed on the SOW, except as otherwise agreed by Seller. Any objections to an invoice must be communicated to the Seller Contact Person within fifteen (15) days after receipt of the invoice.
This SOW may include multiple types of Services Fees; please reference below Services Fees section(s) for further details.

SERVICES FEES

Services Fees hereunder are FIXED FEES, meaning that the amount invoiced for the Services will be $19,000.00.

The invoiced amount of Services Fees will equal the amount of fees applicable to each completed project milestone (see Table below).

Milestone	Percentage	Fee
Project Completion	100%	$19,000.00
Totals	**100%**	**$19,000.00**

Texas Prompt Payment Act Compliance: Payment for goods and services shall be governed by Chapter 2251 of the Texas Government Code. An invoice shall be deemed overdue the 31st day after the later of (1) the date Client receives the goods under the contract; (2) the date the performance of the service under the contract is completed; or (3) the date the Williamson County Auditor receives an invoice for the goods or services. Interest charges for any overdue payments shall be paid by Client in accordance with Texas Government Code Section 2251.025. More specifically, the rate of interest that shall accrue on a late payment is the rate in effect on September 1 of Client's fiscal year in which the payment becomes due. The said rate in effect on September 1 shall be equal to the sum of one percent (1%); and (2) the prime rate published in the Wall Street Journal on the first day of July of the preceding fiscal year that does not fall on a Saturday or Sunday.

The County is a political subdivision under the laws of the State of Texas and claims exemption from sales and use taxes. The County agrees to provide exemption certificates to Service Provider upon request.

EXPENSES

Neither travel time nor direct expenses will be billed for this project.

TRAVEL NOTICE

The Parties agree that there will be no travel required for this project. All services under this SOW will be performed remotely.

CUSTOMER-DESIGNATED LOCATIONS

Seller will provide Services benefiting the following locations ("**Customer-Designated Locations**")

Location	Address
Main	301 SE INNER LOOP STE 105, georgetown, TX 78626

SIGNATURES

In acknowledgement that the parties below have read and understood this Statement of Work and agree to be bound by it, each party has caused this Statement of Work to be signed and transferred by its respective authorized representative.

This SOW and any Change Order may be signed in separate counterparts, each of which shall be deemed an original and all of which together will be deemed to be one original. Electronic signatures on this SOW or on any Change Order (or copies of signatures sent via electronic means) are the equivalent of handwritten signatures.

CDW Government LLC	**WILLIAMSON COUNTY, TX**
By: Alexander M Goes Alexander M Goes (Mar 5, 2025 11:50 CST)	By:
Name: Services Contracts Manager	Name:
Title: Services Contract Manager	Title:
Date: Mar 5, 2025	Date:
Mailing Address:	Mailing Address:
200 N. Milwaukee Ave. Vernon Hills, IL 60061	301 SE INNER LOOP STE 105 GEORGETOWN, TX 78626-8207

Valerie Covey

Valerie Covey

Presiding Officer

Mar 28, 2025

Reviewed by General Counsel's Office
Jennifer Miller
General Counsel, Commissioners Court
Date: Mar 11 2025 Time: 12:41 pm

Reviewed by Contract Audit
SARA GREER, CGAP
Contract Auditor
Williamson County Auditor's Office
Date: Mar 11 2025 Time: 12:31 pm

SIGNATURES

In acknowledgement that the parties below have read and understood this Statement of Work and agree to be bound by it, each party has caused this Statement of Work to be signed and transferred by its respective authorized representative.

This SOW and any Change Order may be signed in separate counterparts, each of which shall be deemed an original and all of which together will be deemed to be one original. Electronic signatures on this SOW or on any Change Order (or copies of signatures sent via electronic means) are the equivalent of handwritten signatures.

CDW Government LLC	WILLIAMSON COUNTY, TX
By: Alexander M Goes Alexander M Goes (Mar 5, 2025 11:50 CST)	By:
Name: Services Contracts Manager	Name:
Title: Services Contract Manager	Title:
Date: Mar 5, 2025	Date:
Mailing Address:	Mailing Address:
200 N. Milwaukee Ave.	301 SE INNER LOOP STE 105
Vernon Hills, IL 60061	GEORGETOWN, TX 78626-8207

Reviewed by General Counsel's Office
Jennifer Miller
General Counsel, Commissioners Court
Date: Mar 11 2025 Time: 12:41 pm

Reviewed by Contract Audit
SARA GREER, CGAP
Contract Auditor
Williamson County Auditor's Office
Date: Mar 11 2025 Time: 12:31 pm