VILKAS
CYBERSECURITY

Security Assessment Proposal

2026 Network & Web Application Penetration Test

REVISION Rev1
DOCUMENT DATE July 20, 2026

PREPARED FOR

Prysm Medical, Inc.
1000 Example Plaza
Suite 600
Raleigh, NC 27601

Elena Marlowe
Chief Information Security Officer

PREPARED BY

Vilkas Cybersecurity & Risk LLC
7901 4th St N
Suite 300
St Petersburg, FL 33702

Ben Rollin
Founder & CEO

Table of Contents

Statement of Confidentiality

The contents of this document are proprietary and confidential information developed by Vilkas Cybersecurity & Risk LLC (“Vilkas”). This document may not be shared with vendors, business partners, or contractors without prior written consent from Vilkas. No portion of this document may be reproduced, distributed, or disclosed without the written consent of both Vilkas and the Client.

This document does not constitute legal advice. The services described herein are not intended to provide legal counsel and should not be interpreted as such. Clients requiring legal guidance should consult with qualified legal counsel.

Overview

Vilkas will conduct professional security assessment services to identify vulnerabilities and attack vectors across the in-scope assets of Prysm Medical, Inc. (“Client”). Using attack simulation and penetration testing techniques, Vilkas will evaluate the Client’s security controls, demonstrate real-world exploitation impact, and provide actionable remediation guidance.

The following security assessment services are considered in scope as part of this engagement:

Internal & External Infrastructure

- **External Penetration Test (EPT)** – Publicly accessible boundary devices, applications, and services.
- **Internal Penetration Test (IPT)** – Internal network, servers, workstations, and identity infrastructure.

Application & Data Security

- **Web Application Security Assessment (WASA)** – In-scope web applications and APIs.

The specific combination of services, test perspectives (for example, unauthenticated versus authenticated users), and environments (such as on-premises, cloud, and Active Directory) are defined in this Statement of Work and detailed in the Scope of Services Detail section.

Assessment Frameworks & Methodology

Assessment Frameworks

Vilkas aligns its testing approach with widely recognized security and penetration testing standards and frameworks, including:

- Open-Source Security Testing Methodology Manual (OSSTMM)
- OWASP Testing Guide and OWASP Application Security Verification Standard (ASVS)
- NIST SP 800-115 and the Penetration Testing Execution Standard (PTES)
- MITRE ATT&CK Framework and the Information Systems Security Assessment Framework (ISSAF)

Our approach mirrors that of real-world attackers by probing the Client attack surfaces, identifying vulnerabilities, and demonstrating their impact, while operating under strict Rules of Engagement agreed with the Client.

Four Phase Assessment Methodology

1. Information Gathering (Reconnaissance)

Vilkas performs reconnaissance and Open-Source Intelligence (OSINT) to identify in-scope assets, technologies, and potential attack vectors, then profiles the environment to prioritize targets and focuses effort on the highest-value areas.

2. Scanning & Enumeration (Automated Analysis)

Authenticated and unauthenticated scanning of networks, systems, web applications, and APIs is combined with targeted manual analysis to uncover vulnerabilities, configuration weaknesses, and gaps in security controls, while reducing false positives.

3. Exploitation & Testing (Manual Penetration Testing)

Vilkas executes controlled exploitation, privilege escalation, lateral movement, and attack chaining (across on-premises, cloud, identity, wireless, and segmentation controls where in scope) to show how weaknesses can be combined to affect the Client's operating environment and business functions.

4. Reporting & Validation

Confirmed findings are documented with evidence, reproduction steps, impact analysis, and prioritized remediation guidance, and post-remediation retesting is performed, when requested, to validate fixes and update the status of each issue.

> **Post-remediation Testing:** Post-remediation testing to confirm the effectiveness of the Client's corrective actions and updated security controls is included in all test scopes. Our team works side-by-side with your team to ensure remediation/mitigation actions are effective at breaking attack chains and reducing risk across the organization.

Senior-Led Manual Scoping & Testing

Vilkas conducts all assessments using an expert-led, manual-first approach, supported by carefully selected commercial, open-source, and proprietary tools where they add efficiency or coverage. Each engagement is scoped, planned, and executed by a senior penetration tester with more than ten years of hands-on experience, ensuring that testing goes beyond automated checks to uncover complex, real-world attack paths. Tools are used to augment deep manual analysis, custom attack chains, and professional judgment.

Testing Tools

Vilkas uses a tailored combination of commercial, open-source, and proprietary security testing tools, supplemented by targeted manual techniques. Our proprietary tooling includes an in-house identity exposure and attack chain correlation engine, developed by our team from real-world engagement experience to map how misconfigurations across Active Directory, Entra ID, file shares, certificate services, and credential hygiene chain together into exploitable attack paths, surfacing risks that siloed commercial scanners often miss. The specific tools and configurations selected for an engagement depend on the Client environment, in-scope services, and agreed testing scenarios, ensuring accurate, repeatable, and high-value results.

Remediation & Next Steps

Following the completion of testing, Vilkas will provide a detailed report outlining all identified findings, prioritized by risk and exploitability, along with clear, actionable remediation guidance for each. Upon request, Vilkas offers a complimentary retest of critical and high-severity findings to validate remediation effectiveness.

Vilkas uses ForestGuardian, an in-house identity and attack-path exposure platform built by our engineering team and informed by patterns observed across real-world Active Directory and Entra ID assessments, to identify and validate findings during relevant engagements. Where traditional point-in-time testing captures a single snapshot, ForestGuardian is also available to Client as an ongoing option between engagements, continuously monitoring Active Directory, Entra ID, file shares, certificate services, and credential hygiene to flag new attack chains and misconfigurations as they emerge, rather than waiting for the next annual test to surface them. This is offered as an optional extension of your security program, not a required component of this assessment.

Testing Scenario Options

Vilkas offers flexible testing scenarios so the engagement can mirror the Client's desired balance between realism, efficiency, and operational risk. Two primary dimensions are defined: Information Disclosure and Evasiveness.

Information Disclosure Levels

These options define how much information the Client provides to Vilkas before testing begins, which directly affects realism, efficiency, and how quickly coverage can be achieved.

Full Disclosure

The Client provides detailed information about in-scope environments, such as architecture, diagrams, and target lists. This option maximizes efficiency and depth of coverage by allowing Vilkas to focus testing on known assets while collaborating closely with the Client's team.

Semi-Blind

The Client provides limited technical details (for example, IP ranges or application URLs) after initial discovery. This option balances realism and efficiency when the Client wants Vilkas to perform some discovery while still constraining scope and effort.

Blind

The Client provides little to no technical information before testing, and Vilkas relies primarily on publicly available information and testing-derived data to discover and profile targets. This option best simulates the reconnaissance phase of a real-world external attacker.

Hybrid

Vilkas begins with limited or no information and transitions to a more cooperative, full-disclosure posture once testing activity is identified by the Client's monitoring or incident response teams. This option is appropriate when the Client wants both realistic attacker behavior and comprehensive coverage once detection occurs.

Evasiveness Levels

Define how stealthy Vilkas will be in attempting to avoid detection during testing.

Non-Evasive

Testing is not intentionally concealed from the Client's monitoring, IDS/IPS, or service providers. This option is typically used alongside full-disclosure engagements to maximize coverage, speed, and visibility into findings.

Evasive

Vilkas uses techniques intended to avoid or delay detection by the Client's monitoring and security controls. This option is appropriate when the Client wants to validate the effectiveness of existing detection and response capabilities, such as an MSSP, SOC, or IDS/IPS deployment.

Hybrid-Evasive

Vilkas begins with evasive techniques and shifts to non-evasive operation once testing is detected or at a defined point in the engagement. This option provides a balance between assessing stealthy attack paths and ensuring comprehensive testing once coordination with the Client's team is established.

Scope of Services Detail

External Penetration Test (EPT) → [Selected]

Performed from the perspective of an unauthenticated attacker on the internet to identify vulnerabilities and misconfigurations in the Client's internet-facing infrastructure, services, and applications. This assessment focuses on gaining initial access, demonstrating realistic attack paths, and evaluating the potential business impact of a compromise originating from the public internet.

External Penetration Test Scope Summary	
Scope Detail	• Up to 50 external IP addresses (~35 live hosts expected) • Vilkas to perform external reconnaissance and Open-Source Intelligence Gathering (OSINT) to map out the Client's external footprint ◦ This data will be presented to Client to confirm ownership before external testing commences
Assessment Details	• Open-Source Intelligence Gathering (OSINT) to profile Client's external footprint (e.g., domains, subdomains, public code repositories, leaked credentials). • In-depth analysis of any in-scope web applications exposed externally. • Thorough testing of in-scope API and web service endpoints. • Testing of all in-scope, externally exposed services for known and emerging vulnerabilities.
Vulnerability Analysis	Automated external vulnerability scanning with manual validation and analysis of results.
Penetration Testing	Manual and automated external penetration testing to validate exploitability, lateral movement, and potential impact, subject to the agreed Rules of Engagement.
Compliance Requirements	Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA)
Testing Time Window	Business hours unless otherwise specified in the Rules of Engagement.
Assessment Location	Remote
Information Disclosure	Blind
Evasive Technique	Hybrid-Evasive
Flags/Objectives	Client will define any specific flags, objectives, or success criteria to be captured during testing and specified in the agreed Rules of Engagement.

External Penetration Test Scope Summary	
Role-based Testing	Testing will be performed from the perspective of an unauthenticated user on the internet; additional authenticated roles (e.g., customer or partner portals) may be included where explicitly in scope.
Sensitive/Fragile Hosts	Client will provide a listing of any sensitive or fragile URLs, code packages, or application stack elements that require special handling as specified in the agreed Rules of Engagement.

Internal Penetration Test (IPT) → [Selected]

Performed from the perspective of an intruder or malicious insider on the Client's internal network. The objective is to determine the level of access an attacker may achieve once inside, including lateral movement, privilege escalation, and access to sensitive systems and data, given the Client's current security controls and configurations.

Internal Penetration Test Scope Summary	
Scope Detail	• Up to 1,000 internal hosts across the Client's corporate network environment • 1 Active Directory forest comprising 2 domains: 1 parent domain and 1 child domain • 1 Microsoft Entra ID and Microsoft 365 tenant connected to the on-premises environment • Testing will begin from an unauthenticated internal network position and transition to authenticated testing using a standard domain user account if an initial foothold is not achieved within the agreed testing window
Assessment Details	• Internal reconnaissance to map out the internal network, including accessible servers, workstations, network devices, services, and applications. • In-depth analysis of the Client's Active Directory and relevant internal identity infrastructure from both unauthenticated and authenticated perspectives. • Testing from the perspective of an unauthenticated internal user (e.g., rogue device or intruder) and, where appropriate, a standard domain user if Vilkas is unable to obtain a foothold via unauthenticated testing. • Attempts to bypass or evade endpoint and network security controls in accordance with the agreed Rules of Engagement.
Vulnerability Analysis	Automated internal vulnerability scanning with manual validation and analysis of results.
Penetration Testing	Manual and automated internal penetration testing to validate exploitability, lateral movement, and potential impact, subject to the agreed Rules of Engagement.
Compliance Requirements	Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS)
Testing Time Window	Business hours unless otherwise specified in the Rules of Engagement.
Assessment Location	Remote
Information Disclosure	Semi-Blind
Evasive Technique	Hybrid-Evasive

Internal Penetration Test Scope Summary	
Flags/Objectives	Client will define any specific flags, objectives, or success criteria to be captured during testing and specified in the agreed Rules of Engagement.
Role-based Testing	Testing will be performed from the perspective of an unauthenticated user on the internal network and a standard domain user.
Sensitive/Fragile Hosts	Client will provide Vilkas with a listing of any sensitive or fragile hosts as specified in Rules of Engagement.

Web Application Security Assessment (WASA) → [Selected]

Evaluates the security of in-scope web applications and their supporting components from both unauthenticated and authenticated perspectives. Testing focuses on application-layer vulnerabilities, configuration weaknesses, and business logic flaws, and includes scenario-based evaluation of role-based access controls (RBAC) for the Client's defined user roles.

Web Application Security Assessment (WASA) Scope Summary	

Scope Detail	• PrysmConnect Patient Portal and associated REST API
	  ◦ 1 externally accessible web application and its supporting API endpoints
	  ◦ Approximately 150 API endpoints
	• Testing of 3 user roles: Patient, Provider, and Billing

Assessment Details	• Testing will begin from the perspective of an unauthenticated remote user originating from the public internet or internal network, as applicable to the application's deployment. • Role-based testing will be performed for in-scope application roles (for example, standard user, administrator, and any additional claims-based roles) to validate authorization and access controls. • The assessment will evaluate the application, its supporting software stack, and interconnected components (such as databases, proxies, and load balancers) for vulnerabilities and misconfigurations.
Vulnerability Analysis	Automated vulnerability scanning with manual validation and analysis of results.
Penetration Testing	Manual and automated penetration testing to validate exploitability, lateral movement, and potential impact, subject to the agreed Rules of Engagement.
Compliance Requirements	Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS)
Testing Time Window	Business hours unless otherwise specified in the Rules of Engagement.
Assessment Location	Remote
Information Disclosure	Semi-Blind
Evasive Technique	Non-Evasive
Flags/Objectives	Client will define any specific flags, objectives, or success criteria to be captured during testing and specified in the agreed Rules of Engagement.

Web Application Security Assessment (WASA) Scope Summary	
Role-based Testing (WASA)	Up to 3 roles in a staging environment that mirrors production.
Sensitive/Fragile Hosts	Client will provide Vilkas with a listing of any sensitive or fragile URLs, code packages, or application stack elements.

Wireless Penetration Test → [Not Selected]

Assesses the security of the Client's wireless infrastructure, including identification of known and rogue SSIDs, weaknesses in encryption and authentication, and opportunities for unauthorized network access. Where in scope, wireless segmentation between guest and corporate networks is validated to confirm that untrusted wireless zones cannot be used to pivot into sensitive environments.

Vulnerability Assessment (VA) → [Not Selected]

Performed from the perspective of an unauthenticated or authenticated user on internal or external networks, using automated scanning and targeted manual validation to identify known weaknesses in the Client's systems and applications. No exploitation, lateral movement, or privilege escalation is performed; the primary focus is on comprehensive identification and confirmation of vulnerabilities rather than full attack chaining.

Compliance Network Segmentation Checks → [Not Selected]

Evaluates the effectiveness of network segmentation controls used to isolate regulated or sensitive environments (for example, PCI CDE, HIPAA systems, or other compliance-scoped networks) from less-trusted zones. Assessments validate that access between segments is appropriately restricted and that out-of-scope systems cannot communicate with, access, or impact in-scope systems, in alignment with applicable regulatory and security requirements.

Social Engineering Assessment → [Not Selected]

Evaluates the effectiveness of the Client's security awareness controls and related processes by simulating phishing, vishing, and/or physical social engineering attacks under controlled conditions. The objective is to measure user susceptibility, validate existing training and processes, and identify opportunities to strengthen the Client's human-centric defenses.

"Stolen" Laptop Security Assessment → [Not Selected]

Evaluates the level of access an unauthenticated attacker may achieve if they obtain a locked standard corporate laptop assigned to a Client's employee. Testing focuses on bypassing local protections, accessing stored data and credentials, and assessing the risk of lateral movement into the Client's broader environment.

Cloud Security Audit → [Not Selected]

Automated and manual review of in-scope cloud resources to compare current configurations against Center for Internet Security (CIS) Benchmarks hardening recommendations. Unlike a penetration test, this assessment focuses on configuration alignment and identifying risks from misconfigurations, rather than simulating an attacker attempting to exploit vulnerabilities.

Mobile Application Security Assessment (MASA) → [Not Selected]

Evaluation of the security of an organization's Android and/or iOS application(s), combining static testing (analysis of the application/binary and key configuration files) with dynamic testing (execution of the application and observation of its behavior while simulating the workflow of a real user). Mobile testing is aligned with the OWASP Mobile Top 10 Risk Categories and will help determine how the application protects sensitive data; specifically, what data the application stores on the device, how the data is stored on the device and what is being sent to and from backend services.

Application Programming Interface (API) Assessment → [Not Selected]

Evaluation of security risks of API endpoints for stand-alone integrations and back-end services (commonly REST/RESTful and GraphQL and other applicable API interfaces) including those supporting mobile and modern web applications with respect to API risk areas which are in alignment with the OWASP API Security Top 10 (e.g., authorization failures, authentication weaknesses, excessive data exposure, and security misconfigurations).

Cloud Penetration Test → [Not Selected]

Comprehensive assessment of an organization's cloud environment(s). It involves evaluating identity and access controls for in-scope systems, network boundaries, exposed services, and deployed workloads (for example, containers, serverless, storage, and managed databases). It also identifies weaknesses that could allow unauthorized access, elevation of privileges, lateral movement, or sensitive data exposure.

Physical Security Assessment → [Not Selected]

Physical walkthrough of the organization's building(s) to assess access controls, data center security controls, and surveillance system capabilities. Can be performed from an evasive perspective (during or outside of business hours) to attempt to bypass physical security controls to gain unauthorized access to office(s), data center, or other sensitive areas. A non-evasive assessment consists of a walkthrough of physical security controls based upon NIST SP 800-12 "Physical and Environmental Security" controls.

Red Team Assessment → [Not Selected]

Goes beyond traditional penetration testing by emulating advanced persistent threats (APTs) to evaluate your organization's detection and response capabilities under realistic attack conditions. Scenario-based testing including assumed breach, phishing campaigns, perimeter testing, and custom exercises tailored to your organization's structure, tools, and concerns. Reports highlight exploited paths, missed detections, and actionable improvements.

Purple Team Assessment → [Not Selected]

Involves coordinated offensive testing and defensive validation to assess how effectively the Client's security monitoring and response capabilities detect and respond to real-world attack techniques. Testing is performed in collaboration with defensive teams and focuses on executing targeted attack actions against in-scope systems while observing detection, alerting, and response behavior. The objective is to identify gaps in visibility, improve defensive coverage, and strengthen the organization's ability to identify and respond to malicious activities.

Active Directory (AD) Security Assessment → [Not Selected]

Evaluates all AD components including group membership, administrative access, Group Policy Objects (GPOs), access control lists (ACLs), trusts, remote access permissions, file shares, authentication mechanisms, legacy configurations, Active Directory Certificate Services (AD CS) implementations, and more. Assessments are tailored to both on-prem and hybrid environments.

Custom Assessment → [Not Selected]

A tailored assessment whose objectives, methodology, and deliverables are defined collaboratively with the Client and documented in this statement of work. Scope, testing approach, and reporting formats are aligned to the Client's risk priorities, technical environment, and compliance or assurance needs.

Deliverables

Vilkas delivers clear, actionable reporting tailored for both executive decision makers and technical implementers, so the Client can quickly understand risk, prioritize remediation, and demonstrate due diligence.

Executive Reporting

- Concise executive summary describing the services performed, overall testing approach, and the Client's security posture at a business and risk level.
- High-level view of key findings, business impact, and prioritized remediation themes, with an optional sanitized executive summary suitable for third-party distribution at the Client's request.

Technical Reporting

- Draft technical report provided for review prior to finalization, giving the Client an opportunity to validate context, add mitigating details, and clarify any questions before the report is finalized.
- Detailed findings list with severity ratings, affected assets, evidence, and step-by-step reproduction guidance for each issue.
- Specific remediation recommendations, including configuration changes, design improvements, or process updates, with mapping to relevant standards or best practices where applicable.

Attestation Report

- Formal attestation letter or summary report confirming that the agreed security assessment activities were performed over the stated period, scope, and environments.
- Summary of services completed, high-level testing coverage, and the overall status of identified findings and remediation at the time of reporting, suitable for sharing with auditors, insurers, and other external stakeholders.

Project Meetings, Status Updates & Timeline

Meetings

Key touchpoints to align on scope, communicate progress, and review results with the Client

Kickoff Meeting

Introduce project stakeholders, confirm objectives and success criteria, review the agreed upon scope and Rules of Engagement, and finalize logistics such as timelines, communication channels, and points of contact.

Status Touchpoints (as needed)

Brief check-ins during the engagement, when requested or appropriate, to share high-level progress, clarify questions, and address any emerging risks or constraints.

Report review meeting

Present the draft report, walk through key findings and their impact, discuss remediation priorities, and capture the Client's feedback and clarifications for inclusion in the final deliverables.

Status Updates

Ongoing Status Updates

Provided at key milestones and, where requested, through brief check-ins and weekly status reports to keep the Client informed of progress, risks, and any required decisions.

Weekly Status Reports (optional)

At Client's request, Vilkas will provide weekly status reports for each engagement at a day and time agreed upon by Vilkas and the Client per the Rules of Engagement. These reports include overall engagement progress and any risks or issues that may impact timelines or scope.

Vulnerability Notification Reports

Vilkas will issue an immediate vulnerability notification report to the Client, via email and a follow-up phone call to the technical point of contact defined in the Rules of Engagement, for any findings that require prompt attention.

Project Timeline

The project is expected to take approximately 4 weeks (20 business days) from the start of testing to delivery of the Draft Report, assuming timely access, approvals, and feedback from the Client throughout the engagement. Upon proposal acceptance, Vilkas can begin onboarding and scheduling immediately and will finalize specific testing windows and milestones in coordination with the Client's stakeholders.

Change Order Process

During the engagement, the Client may request changes to the project scope, schedule, or deliverables. Any material change will be documented in a written change order that describes the revised scope, assumptions, timeline, and associated fees, and must be approved by both Vilkas and the Client's designated representative before the additional work begins. Day-to-day clarifications that do not expand effort, scope, or risk will be handled through normal project communications and status updates.

Best Practices – Before You Test

Coordinate Internally

- Identify key internal contacts (for example, SOC, IT, and application owners) and ensure they understand the test window, scope, and Rules of Engagement.
- Decide whether your SOC will be fully blind or informed at a high level to balance realism with operational risk and contractual obligations.

Third-Party SOC / MDR / MSSP

- Review contracts for any required notification to external monitoring or managed security providers before testing.
- For realistic exercises, limit advance detail; if they block Vilkas traffic, treat that as a success, then proceed later with allowlisted tester IPs as needed.

Alerts and Evidence

- Ask monitoring teams to export alerts, cases, or tickets related to test activity and to share them with Vilkas.
- These artifacts can be referenced in the report and, where appropriate, included as an appendix to show which activities were detected or missed.

Cloud Providers (AWS, Azure, GCP)

- Confirm in-scope assets are under your control and that testing remains within your tenancy, following each provider's current penetration testing and acceptable use guidance.
- Avoid prohibited activities (for example, DoS or large-scale stress tests) unless explicitly approved by the provider.

Other Hosting and Third Parties

- Check any additional hosting, SaaS, or data-center providers for formal penetration testing approval or notification requirements and obtain required approvals.
- Keep a record of approvals and abuse/incident contacts in case providers observe or escalate test traffic.

Professional Services Pricing

Service Description	Selection
• External Penetration Test	☑
• Internal Penetration Test	☑
• Web Application Security Assessment	☑
Total Investment for Selected Services	**$30,000**

Approval Signatures

Once signed by both parties, this Proposal, including this Statement of Work (“SoW”), constitutes the entire agreement governing the services to be provided by Vilkas Cybersecurity & Risk LLC (“Vilkas”). The parties acknowledge that they have read, understood, and agree to be bound by the terms and conditions set forth herein, and have caused this SoW to be executed by their duly authorized representatives as of the dates indicated below.

Payment Terms:

- 50% of the total professional services fee is due upon execution of this SoW in order to confirm scheduling and reserve project resources.
- The remaining 50% is due upon delivery of the Draft Report, with payment due within thirty (30) calendar days of the invoice date (NET 30).

Please sign and return an executed copy of this Statement of Work to Vilkas Cybersecurity. Electronic signatures and counterparts shall be deemed valid and binding for all purposes.

Accepted and agreed by:

Vilkas Cybersecurity & Risk LLC

By: _____

Date: _____

Name: Ben Rollin
Title: Founder & CEO

Prysm Medical, Inc.

By: _____

Date: _____

Name: Elena Marlowe
Title: Chief Information Security Officer

Appendix A – Terms and Conditions

This is a Service Agreement ("Agreement") dated **July 20, 2026** (the "Effective Date") between Vilkas Cybersecurity & Risk LLC ("Company"), a limited liability company organized pursuant to the laws of the state of Florida, and Prysm Medical, Inc. ("Client"). In consideration of the premises and of the mutual covenants and agreements contained herein, and intending to be legally bound, the parties hereby agree as follows:

Proprietary Information

(a) This provision is subject to the terms of a separate Confidentiality Agreement between the parties. During performance of this Agreement, each party may be provided information (including information that Client considers confidential) by the other which the other considers confidential and proprietary. The parties agree that all financial, statistical, marketing and personnel data relating to Client's business, and other information identified as confidential by Client, are confidential information of Client ("Confidential Information"). The parties agree that any security vulnerabilities found during this work order, the details behind these vulnerabilities and even the existence of these vulnerabilities are Confidential Information. Each party shall use Confidential Information of the other party which is disclosed to it only for the purposes of this Agreement and shall not disclose such Confidential Information to any third party, without the other party's prior written consent, other than to Client's other subcontractors, Client and its employees, and to each other's employees on a need-to-know basis. Each party agrees to take reasonable measures to protect the confidentiality of the other party's Confidential Information that, in the aggregate, are no less protective than those measures it uses to protect the confidentiality of its own Confidential Information, but at a minimum, each party shall take reasonable steps to advise their employees of the confidential nature of the Confidential Information and of the prohibitions on copying or revealing such Confidential Information contained herein. Client and the Company each agree to require that the other party's Confidential Information be kept in a reasonably secure location. Notwithstanding anything to the contrary contained in this Agreement, neither party shall be obligated to treat as confidential, or otherwise be subject to the restrictions on use, disclosure or treatment contained in this Agreement for, any information disclosed by the other party (the "Disclosing Party") which: (1) is rightfully known to the recipient prior to its disclosure by the Disclosing Party; (2) is generally known or easily ascertainable by nonparties of ordinary skill in computer or process design or programming or in the business of Client; (3) is released by the Disclosing Party to any other person, firm or entity (including governmental agencies or bureaus) without restriction; (4) is independently developed by the recipient without any reliance on Confidential Information; or (5) is or later becomes publicly available without violation of this Agreement or may be lawfully obtained by a party from any nonparty. Neither party will be liable to the other for inadvertent or accidental disclosure of Confidential Information (1) provided the disclosure occurs notwithstanding the party's exercise of the same level of protection and care that such party customarily uses in safeguarding its own confidential information, (2) immediate notification is given concerning the inadvertent disclosure and (3) best efforts are used to have the inadvertent disclosure information returned or destroyed.

(b) The provisions of this Section shall survive termination or expiration of this Agreement for any reason.

Place of Performance

When performing Services at Client facilities, the Company shall abide by all regulations for personnel identification, access and work at Client sites, and for safeguarding classified information.

Rights in Patents, Works of Authorship and Proprietary Data

(a) All work (including the Report and any other deliverable) produced under this Agreement shall be considered "works for hire." the Company agrees to promptly disclose and assign to Client all right, title and interest in all works of authorship, inventions and other proprietary data including

copyrights, patents, trade secrets and similar rights attendant thereto, conceived, authored, developed or reduced to practice by the Company, its employees, either solely or working jointly with others, during and in connection with the performance of Services under this Agreement. For the purposes of this Agreement, “works for hire” shall not include programs, designs, plans, inventions and the like which are developed by the Company for its own benefit or for the benefit of other Clients. The Company agrees that it will not seek to obtain, nor will its employees seek to obtain copyright, trademark or patent protection for any rights in any such works of authorship, inventions or proprietary data. The Company shall have no right to disclose or use any such works of authorship, inventions or proprietary data for any purpose whatsoever and shall not disclose to any Third Party Client the nature of or any details relating to such works of authorship, inventions, or proprietary data. For the purposes of this Agreement, a Third-Party Client shall be defined as any entity other than the parties to this Agreement. Nothing herein shall prevent the Company from working directly for Client or any other Client after the termination of this Agreement. The Company agrees that it and its employees shall, at Client’s expense, do everything necessary to vest in Client or its nominees, evidence or defend the rights referred to herein and to secure for Client or its nominees all copyright, trademark or patent protection.

(b) The provisions of this Section shall survive termination or expiration of this Agreement for any reason.

Termination for Convenience

The performance of work and Services under this Agreement may be terminated in whole or in part for its convenience by either party upon 15 days’ notice; provided however, that if the Company terminates this Agreement for its convenience, then upon such termination, or at the expiration of this Agreement, Client shall only be liable for payment of any work and services performed prior to such notification of termination or expiration.

Termination for Default

A party (the “Non-breaching Party”) may terminate the whole or any part of this Agreement if the other party (the “Breaching Party”) breaches any of the covenants or terms and conditions set forth in this Agreement or fails to perform any of the other provisions of this Agreement or so fails to make progress as to endanger performance of this Agreement in accordance with its terms, and in any of these circumstances, does not cure such breach or failure to the reasonable satisfaction of the Non-Breaching Party within a period of 10 days after receipt of notice from the Non-Breaching party of such breach or failure. Upon such termination, or at the expiration of this Agreement, if Client is the Breaching Party, then Client shall be liable to the Company for payment for all work and services performed under this Agreement prior to its termination or expiration.

Indemnification

(a) If, after termination, it is determined for any reason whatsoever that the Breaching Party was not in default, or that the default was excusable, then the rights and obligations of the parties shall be the same as if the termination had been issued for the convenience of the Non-Breaching Party. The provisions of this Section shall survive termination or expiration of this Agreement for any reason.

(b) The rights given to the parties herein are in addition to any rights that may be conferred by any statute or otherwise. Each party shall be liable for and shall indemnify and hold the other party harmless against any loss or damage arising from the fault or negligence of such party, its officers, employees, agents, and representatives. Each party agrees to indemnify, defend, and hold the other party harmless against any and all liability or claim, whatever kind or nature, including but not limited to all losses, costs, claims, liabilities, fines, penalties, judgments, awards, damages, and expenses (including costs of investigation and defense and reasonable attorneys’ fees and expenses), to the extent arising from the indemnifying party’s own acts, omissions, fault, negligence, or misconduct, including those of its officers, employees, agents, and representatives. This indemnity includes out-of-pocket expenses (including travel costs and attorneys’ fees) and

payment for staff members' time at standard hourly rates in effect at the time rendered to the extent such staff attend, prepare for, or participate in meetings, hearings, depositions, trials, and other proceedings, including travel time. If either party must bring legal action to enforce this Section, the prevailing party shall be entitled to recover its reasonable attorneys' fees and costs.

Limitation of Liability

To the extent permitted by applicable law, in no event shall the Company be liable under any legal theory for any special, indirect, consequential, exemplary or incidental damages, including but not limited to loss of profits, however caused, arising out of or relating to this Agreement, even if the Company has been advised of the possibility of such damages.

Notice Under 18 USC 1030 & Notice Regarding Criminal Charges

Client agrees to inform all proper parties and authorities [including any and all third parties who may be affected] as required in order to conduct services as outlined in this SOW including but not limited to penetration tests and agrees not to file a complaint with legal or public authorities for the penetration testing. Furthermore, Client agrees to come to the aid of the Company if the local police, sheriff, FBI, FTC, or other governmental agency should detain or question them in any manner during the course of services being provided under this SOW. The Client agrees to defend and hold the Company harmless from any civil or criminal liability or damage arising from the performance of services under this SOW including but not limited to claims for violations of property trespass, breaking and entering, privacy laws, and criminal computer laws including but not limited to 18 USC 1030 and any federal, state or local laws. Furthermore, Client shall indemnify and hold the Company harmless for any and all claims, damages, expenses and liabilities to any third party which may arise as a result of such services being performed under this SOW.

Client understands that a breach of this provision may result in criminal charges being filed against the Company, and therefore agrees, if Client, directly or indirectly, fails to properly inform all necessary parties and authorities in violation of this section, Client will pay to the Company $25,000 for each one of the Company's employees/contractors/agents that have criminal charges brought against them, as liquidated damages, plus all reasonable costs that the Company incurs in providing a qualified legal defense, including, but not limited to all reasonable legal fees. Client and the Company agree that this amount represents the best estimate of the Company's expected actual losses and damages including, but not limited to, foregone business opportunities, loss of reputation and other incidental and consequential damages. Client acknowledges that this amount is not a penalty. This section survives the termination of this SOW.

Amendments

No amendment, waiver or discharge shall be valid unless in writing and signed by both parties.

Assignments and Delegation

No right or interest in this Agreement shall be assigned by either party without the prior written permission of the other and no delegation or subcontracting of services or other obligations of either party under this Agreement shall be made without prior written permission of the other party hereto. Any attempt to assign or otherwise transfer this Agreement in violation of this Section shall be void and of no force and effect.

Waiver

No delay or omission in exercising any right or powers shall impair such right or power or be construed to be a waiver. No provision of this Agreement will be waived, and no breach excused unless the waiver or consent is in writing and is signed by the party that is claimed to have waived or consented.

Severability

If any provision of this Agreement is declared or found to be illegal, unenforceable or void, then both parties shall be relieved of all obligations arising under such provision, but if the remainder of this Agreement shall not be affected by such declaration or finding and is capable of substantial performance, then each provision not so affected shall be enforced to the extent permitted by law.

Dispute Resolution

It is the intent of the parties that any disputes arising under this Agreement be resolved expeditiously, amicably, and at the level within each party's organization that is most knowledgeable about the relevant issues. The parties understand and agree that the procedures outlined in this Section are not intended to supplant the routine handling of inquiries and complaints through informal contact of the parties. Accordingly, for purposes of the procedures set forth in this Section, a "dispute" is a disagreement that the parties have been unable to resolve by the normal and routine channels ordinarily used for resolving problems. Pending the final disposition of a dispute other than a dispute arising out of the termination of this Agreement, the parties shall, at all times, proceed diligently with the performance of this Agreement. Before either party seeks any remedies available at law, the parties shall sequentially follow the procedures set forth below:

The complaining party will notify the other party in writing of the reasons for the dispute, and the parties will work together to resolve the matter as expeditiously as possible. A formal written response will not be required, but the responding party may put its position in writing in order to clarify the issues or suggest possible solutions. (b) If the dispute remains unresolved fifteen (15) days after the delivery of the complaining party's written notice, representatives of Client and the Company who have authority to act to resolve the dispute shall meet or participate in a telephone conference call within ten (10) business days of a request for the meeting or conference call by either party to resolve the dispute. If the parties are unable to reach a resolution of the dispute after following these procedures, or if either party fails to participate when requested, then the parties may pursue any remedies available under this Agreement. (c) The Parties accept and acknowledge that any legal proceedings arising from or in connection with this Agreement must be commenced within one year from the date the aggrieved party becomes aware or ought reasonably to have become aware of the facts which give rise to the alleged liability and in any event no later than two years after any such cause of action accrued. (d) IN THE EVENT OF LITIGATION BETWEEN THE PARTIES ARISING OUT OF THIS AGREEMENT, THE PARTIES HEREBY AGREE THAT, IN ADDITION TO ANY OTHER DAMAGES OR RELIEF WHICH IT MAY BE OBLIGATED TO PAY OR AFFORD, THE PARTY WHICH FAILS TO PREVAIL SHALL ALSO BE LIABLE TO PAY THE OTHER PARTY'S COURT COSTS, ATTORNEYS FEES AND ALL OTHER COSTS OF LITIGATION.