



Security Penetration Test

STATEMENT OF WORK

CITY OF NEW BRAUNFELS

28-Jul-2022



PROPOSAL TEAM

Name	Company/Function	Phone	Email
Jen Eckhardt	Presidio Senior Account Manager	210.245.3804	jeckhardt@presidio.com
Tim Nicolaou	Presidio Security Practice Lead	512.795.7180	tnicolaou@presidio.com
Adam Barber	Presidio Cybersecurity Consultant	512.795.7144	abarber@presidio.com

CHANGE REVISION RECORD

Revision	Date	Author	Notes
V0.1	21-Jul-2022	Adam Barber	First Client Release
V1.0	25-Jul-2022	Ted Kilgore	RAP Review & Approval
V1.1	28-Jul-2022	Tim Nicolaou	Corrected Client's Address for engagement

© 2022 Presidio. All Rights Reserved. This document and its contents are the confidential and proprietary intellectual property of PRESIDIO and may not be duplicated, redistributed or displayed to any third party without the express written consent of PRESIDIO.

Other product and company names mentioned herein may be the trademarks of their respective owners.

The scope and pricing are valid for 60 days unless otherwise noted.

1 EXECUTIVE SUMMARY

1.1 Background

City of New Braunfels (“Client”) is engaging Presidio to perform the assessments and related services outlined in §1.2 Scope of Services and §2 Methodology and Approach, and to produce for Client the deliverables outlined in §3 Deliverables.

1.2 Locations

Work will be done at the following locations. All work will be performed remotely unless otherwise specified.

Site Name	Address	City State ZIP	On-Site / Remote Services
Primary	550 Landa Street	New Braunfels TX 78130	Remote

1.3 Scope of Services

1.3.1 Engagement Management and Control

- **Engagement Management level**
 - Standard
 - Status meeting frequency – Weekly
 - Engagement Kickoff
 - Deliverable Presentation

1.3.2 Security Program Assessment

- Employee Count: 700
- Number of Business Units with Unique Staff: 1
- IT Staff (not including Developers): 5
- Dedicated Security Staff: 1
- Maturity: Low
- Regulated: Yes
- International IT Staff: No

1.3.3 External Vulnerability Assessment

- 26 active hosts
- Testing to be performed during business hours

1.3.4 Internal Vulnerability Assessment

- No. of Hosts – 222
- Network scanning location(s): 2
- Password strength analysis is included
- 4 AD domain(s), 4 forest(s)
- Testing to be performed during business hours

1.3.5 External Penetration Testing

- Up to 26 live external hosts to be tested
- Included Objectives
 - Password spraying with data gained via open source intelligence gathering (OSINT)
 - Attempt to gain access via remotely exposed web portals (like OWA, O365) and remove access methods
 - Attempt to gain access via other remotely exposed services
- Testing to be performed during business hours

1.3.6 Remote Access Assessment

- 1 - Sonicwall NSA
- 1 - NetMotion VPN

2 METHODOLOGY AND APPROACH

2.1 Engagement Management and Control

Detailed project planning is key to ensuring that the proposed engagement will meet requirements and help to reduce the risk of an ineffective project.

2.1.1 Standard

- Identify and schedule Presidio resources
 - Identify and schedule Presidio resources as appropriate to the engagement
- Hold kickoff meeting with key stakeholders
 - Review details of scope of work and methodology
 - Introduce key project team members and define roles and responsibilities
 - Review timelines, meetings, and additional requirements
 - Schedule implementation for discovery software
 - Schedule status meeting and other recurring touchpoints, as required
- Conduct status meetings at a frequency defined in this document
 - Review engagement progress
 - Identify engagement risks
 - Identify upcoming tasks
 - Request any additional customer or Presidio involvement
- Maintain and distribute engagement status report and schedule
 - All documents provided in Presidio formats
- Schedule Deliverable Presentation
 - Schedule mutually agreeable deliverable presentation

2.2 Security Program Assessment

The security program risk assessment looks at the structure, enforcement, and implementation of the information security management program. Presidio's Information Security Governance consultants and Cyber Security Architects will evaluate various program elements by reviewing the overall maturity of the documented practices and processes that are in place, the security of infrastructure architecture, and the potential risk to the organization resulting from the above as related to people, process, and technology.

Presidio will map all risks identified using NIST Cyber Security Framework (CSF) (or other customer defined framework as stated in the scope of services) and best practice as references. The security program assessment provides strategic guidance on areas of organizational risk, and information on compliance with stated standards in the context of the customer's business and security objectives, risk tolerance, and compliance objectives. This assessment evaluates

core security controls from the NIST CSF (or other specified framework); it does not assess every control and sub-control contained in the framework.

- Scoping
 - Identify stakeholders for interviews
 - Determine any applicable regulatory or compliance standards
 - Determine scoping inside Client's organization
 - Determine any Client security frameworks
 - Identify any key issues or challenges Client is facing
- Documentation Collection and Review
 - Collect existing information security policy documentation
 - Collect organizational charts
 - Determine security staffing
 - Determine security reporting
 - Review documentation
 - Review documentation structure
 - Review documentation for completeness
 - Review documentation for applicability
 - Review existing network, security, and systems documentation
 - Perform a high-level analysis of collected documentation
 - Compare documentation to standards and best practices
 - Review security staffing and reporting for capabilities and level of staffing
- Interviews
 - 1-2 hour Interviews or workshops with key stakeholders and process implementers
 - Business leadership
 - Security leadership (ex: CISO)
 - IT and IT Security staff, administrators, and implementers
 - Infrastructure Leadership and Architects
 - Systems Leadership and Architects
 - Security Leadership and Architects
 - Additional significant stakeholders as identified Client
 - Validate alignment of written documentation to business direction
 - Validate alignment of written documentation to actual practice
 - Determine any 'informal processes' being followed

- Review and analyze security program maturity, risk, and impact across 21 unique domains and over 70 discrete sub-domains:
 1. Security Governance
 2. Personnel Security
 3. Risk Management
 4. Vulnerability Management
 5. Security Incident Management
 6. Security Awareness and Education
 7. Secure Architecture
 8. Configuration Management
 9. Endpoint Security
 10. Data Security
 11. Identity Security
 12. Network Security
 13. Remote Access Security
 14. Application Security
 15. Email Security
 16. Encryption and Key Management
 17. Security Operations
 18. Business Resiliency
 19. Third Party Management
 20. IT Asset Management
 21. Physical Security
- Process Verification
 - Discover and review actual behaviors
 - Validate alignment of written documentation to actual practice
- Documentation
 - Create written report summarizing risks and recommended remediation efforts
 - Security roadmap based on business and IT initiatives
 - Strategic and Tactical
 - Prepare supporting spreadsheet
 - Processes reviewed with maturity and organizational risk
 - Alignment with NIST CSF or other specified framework

Alignment and summary of gaps with in-scope compliance standards

2.3 NIST CSF Assessment

The process risk and capabilities assessment looks at the structure and enforcement of the information security management program and evaluates it for both the maturity of the process and the risk to the organization. Presidio will map these levels using the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cyber Security Framework) to ensure that all key areas of information security are being considered and the policy, process and technical controls in place are appropriate to satisfy the organization's business objectives. This will provide strategic guidance on areas of organizational risk and information on compliance with stated standards.

This security assessment analyzes Client's alignment with the NIST CSF Framework.

- Framework Core: Identify, Protect, Detect, Respond and Recover functions
- Implementation Tiers: Partial, Risk Informed, Repeatable and Adaptive
- Framework Profile: Current Profile vs. Target Profile

2.4 External Vulnerability Assessment

Presidio will review the external security of Client network, including data collection from publicly available sources (OSINT), scanning of in-scope networks, and vulnerability collation and validation. This process provides a clear picture of the risk from an external attacker (with the exception of detailed attacks into the structure of web applications), as well as a picture of data intentionally or unintentionally exposed on the public Internet.

- OSINT
 - Search common sources for Client data
 - Identify any customer networks not identified in scope
 - Identify any sensitive customer data available publicly
- Scheduling and target validation
 - Review target networks from scope and validate
 - Review additional networks from OSINT and verify testing
 - Testing of additional networks may incur a project change
 - Determine scheduled testing windows
 - Validate customer and tester contact information
- Network Scanning
 - Perform any required customization of scanning tools
 - Perform a tool-based scan of in-scope networks
- Vulnerability Validation
 - Review discovered vulnerabilities and validate as appropriate
- Documentation

- Prepare written report
 - Vulnerability
 - Risk Score
 - Suggested remediation
- Prepare a spreadsheet-based summary of vulnerabilities

2.5 Internal Vulnerability Assessment

Presidio will review the security of Client's network from inside the Internet perimeter. This will include basic validation of Active Directory (or other identity management platform) as well as both authenticated and unauthenticated scanning of in-scope hosts as defined in the scope of services. This will enable Presidio to provide a view of the risks based on privileged and service accounts, patching levels, as well as vulnerabilities with a high degree of confidence. Client will be able to clearly understand the risk should their perimeter protection be bypassed as is common in many current attack scenarios.

- Scheduling and target validation
 - Review target networks from scoping and discovery and validate
 - Determine scheduled testing windows
 - Validate customer and tester contact information
- Credentialed Network Scanning
 - Scan network with automated tools and customer-supplied administrative credentials
 - Determine vulnerabilities and patching status on all systems
- Active Directory Validation
 - Review existing accounts
 - Determine number and type of stale accounts
 - Review status of privileged accounts
 - Review password policy
- Password Strength Analysis
 - Securely obtain Active Directory passwords
 - Perform off-site analysis of passwords
 - Validate password complexity in use
 - Validate passwords meet written password standards
 - Determine any default or common passwords
 - Ensure all privileged accounts are correctly protected
- Vulnerability Validation
 - Review vulnerabilities and recommend priorities as appropriate

- Documentation
 - Prepare written report
 - Vulnerability
 - Risk Score
 - Suggested remediation
 - If applicable, password strength statistics and weak password details will be provided
 - Prepare spreadsheet-based summary of vulnerabilities

2.6 External Penetration Testing

Penetration testing focuses on assessing an organization's current security posture by simulating avenues of approach an attacker might take and determining the effectiveness of in-place security controls. During the penetration testing phase, Presidio will perform a testing cycle consisting of reconnaissance, initial compromise, privilege escalation, lateral movement, and achievement of targeted objectives. External Penetration Testing is conducted from a source coming from the Internet.

Client has elected the following:

- As defined in the scope section of the document

The following tasks are performed as part of this phase, as defined in the Scope of Services:

- Scoping
 - Validate systems for testing
 - Validate testing windows
 - Validate contacts
 - Validate starting scenario and targeted objectives
 - Define rules of engagement
- Reconnaissance
 - Open source intelligence (OSINT) reconnaissance
 - Enumerate hosts and services
 - Perform additional reconnaissance as required
- Initial Compromise
 - Attempt to obtain initial access to systems through methods like:
 - Direct exploitation
 - Misconfigured services and permissions
 - Weak security practices
 - Default or easily guessable credentials

- Sensitive file exposure
- Password spraying
- Additional methods as appropriate. The above list is a sample of techniques; Presidio will expand on this list as required to achieve appropriate results.
- Escalation
 - Continue testing cycle to achieve target objectives
- Clean-up
 - Remove any testing artifacts
 - Ensure any tools and access methods are removed
- Documentation
 - Prepare written report
 - Defined attack path
 - Systems and users compromised, and methods used
 - Suggested remediation/mitigation steps
 - List of any artifacts, tools, or access that couldn't be removed

2.7 Remote Access Assessment

Remote access systems present additional external risk since they are always accessible by external third parties. The purpose of this phase is to review the technical configurations and associated aspects of all remote access systems in order to identify and analyze risks associated with same.

- Scoping
 - Identify key stakeholders for interviews
 - Schedule discovery activities
- Data Collection and Analysis
 - Collection Information around remote access
 - Policies
 - Drawings
 - In-scope remote access solution configurations
 - Perform analysis of collected data
- Interview
 - Conduct interview around remote access
 - Remote Access Governance
 - Remote Access Architecture

- Remote Access Operations
- Remote Access Authentication and Authorization
- Remote Access Endpoint and Teleworker security
- Document
 - Prepare assessment results and recommendations

3 DELIVERABLES

Deliverable	Description	Format
Status Report	Artifact which depicts key task areas, actions, owners, estimated completion dates, task status, and overall project status and delivered following each status meeting.	PDF
Executive Summary and Security Assessment Report	This report is made up of two sections. The first, an Executive Summary, will include summary of findings for all phases of the project and include a risk profile, high-level recommendations, and roadmap. The second section will be Detailed Findings. This section will show all findings from the project by phase with suggested remediations and references.	PDF
Vulnerability Registers	Sortable list of discovered vulnerabilities from external and internal vulnerability scanning activities.	Excel
SPA Spreadsheet	Collated process summary showing processes and associated capabilities as well as staff requirements for key security functions. Spreadsheet will show mappings from processes to key security frameworks and regulatory standards as appropriate.	Excel
Executive Presentation (optional)	At the customer's discretion, Presidio can conduct an executive presentation that will provide an overview of the assessment for all phases including approach, methodology, summary of findings, and summary of recommendations. The format will be appropriate for a non-technical, executive audience. A copy of the executive presentation will be provided.	PPT
Stakeholder Q&A (optional)	Prior to the optional executive presentation and at the customer's discretion, Presidio will hold a Q&A session with the project stakeholders to discuss the report and preview the Executive Presentation. This Q&A will occur after the customer's review of the document, and will not be a risk-by-risk review of the published report	None

Deliverables will be released via secure exchange only to the Client project sponsor or to others with written permission from the project sponsor.

Final presentations and closeout must be completed within thirty (30) days after the day the original documentation deliverable is released to Client. If the deliverable presentations are not completed in this timeframe, Presidio will consider this phase completed and will invoice accordingly.

4 ASSUMPTIONS

Presidio made the following assumptions when developing this Statement of Work. These assumptions serve as the foundation to which the project estimate, approach, and timeline were developed. Any changes to the following assumptions must be processed using the procedures the section titled “Project Change Request Process.”

4.1 General

The following project assumptions are made and will be verified as part of the engagement:

- All Presidio activities will take place during normal working hours (Monday through Friday, 8:00 a.m. to 5:00 p.m., excluding holidays) unless noted as “Off Hours” in this SOW.
- Any items or tasks not explicitly listed as in-scope within this SOW are considered to be outside of the scope and not associated with this SOW and price.
- If integration of the product is performed at a Presidio facility, then transfer of ownership (acceptance) occurs upon the receipt and integration of goods at Presidio, regardless of shipment, as manufacturers will not accept returns of opened products.
- Changes to the Design, Equipment List, or proposed timeline presented to Client in this SOW will require a Project Change Request. A Project Change Request could impact the cost of the project
- Presidio will not be held responsible for troubleshooting networks, applications and/or hardware if Client has no formal change management documented processes and policies
- Presidio may engage subcontractors and third parties in performing a portion of this work.
- Some activities included in this project may be performed on Presidio’s premises.
- Additional required tasks discovered after the execution of this SOW that are not mentioned in this SOW will require a Project Change Request.
 - Presidio will provide clear guidance on the changes required to ensure optimal deployment.

4.2 General Client Responsibilities

The following items are listed as responsibilities of Client for this engagement. Client is responsible for performing the items and activities listed in this section or arranging for them to be performed by a third-party if appropriate.

- Provide a single Client point of contact with the authority and the responsibility of issue resolution and the identification, coordination, and scheduling of Client personnel to participate in the implementation of the SOW.
- Participate in any required design sessions or workshops.

- Supply current equipment configuration for review if applicable.
- Provide all required physical access to Client's facility (identification badge, escort, parking decal, etc.), as required by Client's policies; and provide all required functional access (passwords, IP address information, etc.), as required for Presidio to complete the tasks.
- Provide to Presidio all required IP addresses, passwords, system names, and aliases.
- Validate the site readiness prior to the dispatch of Presidio personnel to perform the services being contracted.
- Provide adequate facilities for the installation of the hardware. This includes all necessary peripheral hardware (KVM ports or monitors, keyboards, mice, network access, etc.) as well as electrical and spatial needs and required antivirus software.
- Provide Presidio administrator access on appropriate devices for the completion of the engagement.
- Provide requested documentation or information needed for the project within two (2) business days, unless otherwise agreed to by all parties.
- Provide to Presidio all relevant Client information security and information technology policies and procedures.
- Provide to Presidio all requested information about and administrative access to Client's technical infrastructure for the duration of the project, including, but not limited to, each technology component described in each phase listed above.
 - For phases that include a Technical Configuration Review activity, remote access is required, AND administrative access must be sufficient to analyze the configurations of each technology component.
- Provide a work area and network connectivity for Presidio consultants for on-site work when needed.
- Client will make all network and endpoint changes and configurations as required to integrate Presidio's tools.

4.3 Travel

Presidio has made the following assumptions for travel:

- Presidio assumes all work will be performed remotely

4.4 Internal Vulnerability Assessment

- Customer will provision a virtual host to Presidio's specifications or will provide connectivity and power for a Presidio-provided system. Customer will allow Presidio remote access to these systems to allow for internal scanning.
- Customer will provide VPN-based remote access to the provisioned virtual host or will allow other remote access as determined during the kickoff meeting
- The following specifications are required to run the necessary software during this phase

- Windows Server 2012, 2016, 2019
- (4) >= 2.4G vCPU
- (16) GB RAM
- (40) GB Hard Drive
- Local admin rights

5 PRICING

Presidio is providing a Fixed Fee Price as part of this Statement of Work. Presidio will invoice Client based on the project milestone(s) listed below:

Milestone Name	Amount
Project Initiation	\$ 2,000.00
External Vuln Assessment	\$ 4,350.00
Internal Vuln Assessment	\$ 10,850.00
External Pen Test	\$ 5,800.00
Remote Access	\$ 6,740.00
Security Program Assessment	\$ 39,760.00
Project Closure	\$ 2,110.00
Total	\$ 71,610.00

Presidio will bill Client upon completion of each Milestone. Invoices may contain multiple Milestones.

If Client requires a change in the scope of work, the parties will negotiate in good faith to generate a written change order documenting the additional labor and requirements that will be mutually agreed upon by the parties prior to onset of the additional work.

If, in Presidio's reasonable discretion, completion of one or more of a project's milestones are subject to a material delay due to factors outside of Presidio's control, Presidio may invoice Client a prorated amount for work performed which reflects Presidio's current progress toward completing the milestone(s) at the time of any such delay.

Payment terms are subject to credit department approval and will be negotiated and documented on a valid purchase order or other financial document. Presidio payment terms are Net-30. If Client fails to provide a notice of acceptance or a statement of issues to be resolved within ten (10) business days of project conclusion, the project will be deemed accepted and Client will be invoiced.

5.1 Expenses

There are no anticipated travel or incidental expenses to be incurred by Presidio in association with the execution of this Statement of Work and therefore no expenses will be billed to Client.

5.2 Travel Time

Travel to and from the work site(s) by Presidio resources in association with the execution of this Statement of Work will not be charged to Client.

6 TERMS AND CONDITIONS

6.1 General

This statement of work is governed by DIR Contract Number DIR-TSO-4254 between PRESIDIO and the Texas Department of Information Resources and the City of New Braunfels.

6.2 Authorization for Scanning/Testing Activities

Presidio is authorized to perform vulnerability, web application, penetration testing, and social engineering activities for the services performed in this Statement of Work (SOW). Such activities shall be confined to the infrastructure described in the SOW under Section 1.2. Presidio is not authorized to assess any other networks under this agreement. The security assessment involves the use of network tools and techniques designed to detect security vulnerabilities, and it is impossible to identify and eliminate all the risks involved with the use of these tools and techniques. Client understands that penetration testing may be disruptive and explicitly accepts the risk of such disruption. Presidio will take all reasonable precautions to minimize any impact. Client hereby authorizes employees of Presidio to conduct penetration testing activities of the application(s) and system(s) described in this SOW. This authorization shall be in effect from the day of the engagement kickoff meeting to the day the final deliverable from the engagement is provided to Client.

Pursuant to granting this authorization, Client declares that:

- Client owns the systems to be tested and the undersigned has the proper authority to allow Presidio to perform vulnerability, web application, and penetration testing security activities.
- Client has created a full backup of all systems to be tested and has verified that the backup procedure will enable Client to restore systems to their pretest state.

6.3 Deliverable Review and Acceptance

With the exception of Project Status Reports, each deliverable material, as defined in this Statement of Work, will be approved in accordance with the following procedure.

Within 5 business days of receipt, Customer will either accept the deliverable material or provide the Presidio project manager a written list of requested changes. If no written response, either accepting or requesting changes, is received from Customer within 5 business days, then the deliverable material shall be deemed accepted.

If a written list of requested changes is received within 5 business days, the Presidio project team will review and ensure that these changes do not impact the accuracy or veracity of the report and other deliverables. If this is the case, Presidio will make the appropriate revisions and will, within 5 business days, re-submit the updated version to Customer.

Once the updated version is received, Customer has 5 further business days to review and request changes for the final document. If no written response, either accepting or requesting changes, is received from Customer within five (5) business days, then the deliverable material shall be deemed accepted.

No further modifications of the document will be performed after these two (2) revisions without written approval from the Presidio account team. Additional revisions and changes may incur additional effort and charges at the discretion of the Presidio account team.

6.4 Project Change Request Process

In the event that both Presidio and Client agree to a change in this Statement of Work, a written description of the agreed upon change will be prepared using a Project Change Request (PCR) form, which both parties must sign. The PCR form will be used to describe

the change, the rationale for the change, and to specify any change in the charges, estimated schedule, or other terms. Depending on the extent and complexity of the requested changes, Presidio may charge for the effort required to analyze it. When charges are necessary to analyze a change, Presidio will provide a written estimate and begin the analysis upon written authorization from Client. The terms of a mutually agreed upon Change Authorization will prevail over those of this Statement of Work or any previous Change Authorization.

7 AUTHORIZATION TO PROCEED

The use of signatures on this Statement of Work is to ensure agreement on project objectives and the work to be performed by Presidio.

Presidio signature signifies our commitment to proceed with the project as described in this document. Please review this document thoroughly, as it will be the basis for all work performed by Presidio on this project.

This Statement of Work is valid for a period of sixty (60) days from the date that this Statement of Work is provided by Presidio to Client unless otherwise agreed to by both parties.


City of New Braunfels

Signature

Date

Printed Name

Presidio


Edward Kilgore (Jul 28, 2022 12:45 CDT)

Jul 28, 2022

Signature

Date

Edward Kilgore

Director of Professional Services

Printed Name & Title

APPENDIX A – PROCESSES AND GUIDELINES

Presidio Process for Network Degradation or Outage

Presidio and Client will exchange specific contact information (including cell phone numbers) prior to starting any scanning or testing activities. Either party observing a service disruption will contact the other party. Presidio will stop running the scan tool and work with Client to determine why the disruption occurred and how to successfully complete the assessment without causing any further disruption. No denial-of-service (DoS) attacks will be intentionally initiated against any Client assets.

Process to Report Observed Incidents or Critical Risks

Presidio will contact the Client contact immediately if any critical risks are identified (those which present sufficient risk to warrant immediate remediation), including any observed incidents of attempted intrusion (from a party other than the authorized Presidio consultant[s]), while executing this engagement. Presidio will immediately provide to Client all information gathered relevant to the critical risk(s) identified.

Engagement Data Management

The deliverables produced from this engagement should be managed with strict policies and procedures due to the sensitive nature of the raw data collected during the engagement, and the associated findings Client's policies should specify which person(s) in an organization should have access to the data. Presidio consultants will store and transmit engagement-related data using appropriate encryption.