AGREEMENT

25-0238-RFP

Comprehensive Security Risk Assessment

This Agreement (the “agreement” or “contract”), is entered into on the date last executed below (“Effective Date”), by and between Pinellas County, a subdivision of the State of Florida whose primary address is 315 Court Street, Clearwater, Florida 33756 (“COUNTY”) and CliftonLarsonAllen, LLP whose primary address is 220 S 6th Street, Suite 300 Minneapolis, MN 55402 (hereinafter “CONTRACTOR”) (jointly, the “Parties”).

NOW THEREFORE, the Parties agree as follows:

A. **Documents Comprising Agreement**

1. This Agreement, including the Exhibits listed below, constitutes the entire agreement and understanding of the Parties with respect to the transactions and services contemplated hereby and supersedes all prior agreements, arrangements, and understandings relating to the subject matter of the Agreement. The documents listed below are hereby incorporated into and made a part of this Agreement:

    a. This Agreement

    b. Pinellas County Standard Terms & Conditions, located on Pinellas County Purchasing's website, effective 6/14/2023, posted at https://pinellas.gov/county-standard-terms-conditions/

    c. Solicitation Section 4, titled Special Conditions attached as Exhibit C.

    d. Solicitation Section 5, titled Insurance Requirements attached as Exhibit D.

    e. Contractor's response to Solicitation Section 6, titled Scope of Work / Specifications attached as Exhibit E.

    f. Contractor's response to Solicitation Section 9, titled Pricing Proposal attached as Exhibit F.

    g. Confidentiality Agreement attached as Exhibit G.

2. In the case of a conflict, the terms of this document govern, followed by the terms of the attached Exhibits, which control in the order listed above.

B. **Term**

1. The initial term of this Agreement is for twelve (12) months from the Effective Date ("Contract Term"). At the end of the initial term of this contract, this Agreement may be extended for one (1), additional twelve (12) month term, or such other renewal terms agreed to by the Parties.

C. **Expenditures Cap**

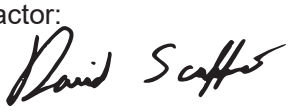
1. Payment and pricing terms for the initial and renewal terms are subject to the Pricing Proposals in Exhibit F. County expenditures under the Agreement will not exceed $499,325.00 for the Contract term without a written amendment to this Agreement.

D. **Entire Agreement**

1. This Agreement constitutes the entire agreement between the Parties.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their undersigned officials, who are duly authorized to bind the Parties to the Agreement.

For Contractor:

Signature: 

Print Name and Title: David Scaffido, Principal

Date: 4/18/2025

For County:

Signature: 

Print Name and Title: Brian Scott, Chair

Date: May 20, 2025.

ATTEST: KEN BURKE, CLERK

By: 

APPROVED AS TO FORM

By: *Keiah Townsend*

Office of the County Attorney

Exhibit C

Special Terms & Conditions

1.1. INTENT

It is the intent of Pinellas County to establish an Agreement for Comprehensive Security Risk Assessment to be ordered, as and when required.

1.2. NON-NEGOTIABLE TERMS

While the County prefers that no exceptions to its contract terms be taken, the solicitation does authorize respondent to take exception to terms as part of its submittal. The County has deemed the following contract terms in the County's Standard Terms & Conditions https://pinellas.gov/county-standard-terms-conditions/ to be non-negotiable:

Section 3: Compliance with Applicable Laws (all terms)

Section 7: Indemnification & Liability (all terms)

Section 8: Insurance & Conditions Precedent

Section 10(G): Governing Law & Venue

Section 12(A): Fiscal Non-Funding

Section 13: Confidential Records, Public Records, & Audit (all terms)

Section 19: Digital Content (all terms) (*if the Agreement includes software, online, or digital content services*)

Any terms required by law

1.3. PRICING/PERIOD OF CONTRACT

Unit prices submitted of listed items will be held firm for the duration of the Agreement. Duration of the Agreement shall be for a period of twelve (12) months. The Parties may extend the term of the Agreement for one (1) additional twelve (12) month period pursuant to the same terms, conditions, and pricing set forth in the Agreement.

1.4. PRE-COMMENCEMENT MEETING

Upon award of the Agreement, the County will coordinate a pre-commencement meeting with the successful Contractor. The meeting will require Contractor and the County Representative to review specific Agreement details and deliverable documents at this meeting to ensure the scope of work and work areas are understood.

1.5. ORDERS

Within the term of this Agreement, County may place one or more orders for goods and/or services at the prices listed on the Pricing Proposal section of this solicitation, which is incorporated by reference hereto.

1.6. ASBESTOS MATERIALS

The Contractor must perform all Work in compliance with Federal, State and local laws, statutes, rules, regulations and ordinances, including but not limited to the Department of Environmental Protection (DEP)'s asbestos requirements, 40 CFR Part 61, Subpart M, and OSHA Section 29 CFR 1926.58. Additionally, the Contractor must be properly licensed and/or certified for asbestos removal as required under Federal, State and local laws, statutes, rules, regulations and ordinances. The County is responsible for filing all DEP notifications and furnish a copy of the DEP notification and approval for demolition to the successful Contractor. The County will furnish a copy of the asbestos survey to the successful Contractor. The Contractor must keep this copy on site at all times during the actual demolition.

1.7. SERVICES

The terms below are applicable if the Solicitation includes the provision of SERVICES:

A. **ADD/DELETE LOCATIONS SERVICES** - The County reserves the right to unilaterally add or delete locations/services, either collectively or individually, at the County's sole option, at any time after award has been made as may be deemed necessary or in the best interests of the County. In such case, the Contractor(s) will be required to provide services to this agreement in accordance with the terms, conditions, and specifications.

1.8. GOODS & PRODUCTS

The terms below are applicable if the Solicitation includes the purchase of GOODS or PRODUCTS:

A. **DELIVERY/CLAIMS** - Prices quoted will be FOB Destination, freight included and unloaded to location(s) within Pinellas County. Actual delivery address(s) will be identified at time of order. Successful Contractor(s) will be responsible for making any and all claims against carriers for missing or damaged items.

1.9. QUANTITIES

Any quantities stated are an estimate only and no guarantee is given or implied as to quantities that will be used during the Agreement period. Estimated quantities are based upon previous use and/or anticipated needs.

1.10. PERFORMANCE SECURITY

Not Applicable

Exhibit D

Insurance Requirements

1.1. INSURANCE (General)

The Vendor must provide a certificate of insurance and endorsement in accordance with the insurance requirements listed below, prior to recommendation for award. The Vendor shall obtain and maintain, and require any subcontractor to obtain and maintain, at all times during its performance of the Agreement in Phase 1 insurance of the types and in the amounts set forth. For projects with a Completed Operations exposure, Vendor shall maintain coverage and provide evidence of insurance for 2 years beyond final acceptance. All insurance policies shall be from responsible companies duly authorized to do business in the State of Florida and have an AM Best rating of VIII or better.

1.2. INSURANCE (Requirements)

A. Submittals should include, the Vendor's current Certificate(s) of Insurance. If Vendor does not currently meet insurance requirements, Vendor shall also include verification from their broker or agent that any required insurance not provided at that time of submittal will be in place prior to the award of contract. Upon selection of Vendor for award, the selected Vendor shall email certificate that is compliant with the insurance requirements. If the certificate received is compliant, no further action may be necessary. The Certificate(s) of Insurance shall be signed by authorized representatives of the insurance companies shown on the Certificate(s).

B. **The Certificate holder section shall indicate Pinellas County, a Political Subdivision of the State of Florida, 400 S Fort Harrison Ave, Clearwater, FL 33756. Pinellas County, a Political Subdivision shall be named as an Additional Insured for General Liability. A Waiver of Subrogation for Workers Compensation shall be provided if Workers Compensation coverage is a requirement.**

C. Approval by the County of any Certificate(s) of Insurance does not constitute verification by the County that the insurance requirements have been satisfied or that the insurance policy shown on the Certificate(s) of Insurance is in compliance with the requirements of the Agreement. County reserves the right to require a certified copy of the entire insurance policy, including endorsement(s), at any time during the Bid and/or contract period.

D. If any insurance provided pursuant to the Agreement expires or cancels prior to the completion of the Work, you will be notified by CTrax, the authorized vendor of Pinellas County. Upon notification, renewal Certificate(s) of Insurance and endorsement(s) shall be furnished to Pinellas County Risk Management at InsuranceCerts@pinellascounty.org and to CTrax c/o JDi Data at PinellasSupport@ididata.com by the Vendor or their agent prior to the expiration date.

1. Vendor shall also notify County within twenty-four (24) hours after receipt, of any notices of expiration, cancellation, nonrenewal or adverse material change in coverage received by said Vendor from its insurer Notice shall be given by email to Pinellas County Risk

Management at InsuranceCerts@pinellascounty.org. Nothing contained herein shall absolve Vendor of this requirement to provide notice.

2. Should the Vendor, at any time, not maintain the insurance coverages required herein, the County may terminate the Agreement.

E. If subcontracting is allowed under this Bid, the Primary Vendor shall obtain and maintain, at all times during its performance of the Agreement, insurance of the types and in the amounts set forth; and require any subcontractors to obtain and maintain, at all times during its performance of the Agreement, insurance limits as it may apply to the portion of the Work performed by the subcontractor; but in no event will the insurance limits be less than $500,000 for Workers' Compensation/Employers' Liability, and $1,000,000 for General Liability and Auto Liability if required below.

1. All subcontracts between the Vendor and its Subcontractors shall be in writing and are subject to the County's prior written approval. Further, all subcontracts shall

   a. Require each Subcontractor to be bound to the Vendor to the same extent the Vendor is bound to the County by the terms of the Contract Documents, as those terms may apply to the portion of the Work to be performed by the Subcontractor;

   b. Provide for the assignment of the subcontracts from the Vendor to the County at the election of Owner upon termination of the Contract;

   c. Provide that County will be an additional indemnified party of the subcontract;

   d. Provide that the County will be an additional insured on all insurance policies required to be provided by the Subcontractor except workers compensation and professional liability;

   e. Provide a waiver of subrogation in favor of the County and other insurance terms and/or conditions

   f. Assign all warranties directly to the County; and

   g. Identify the County as an intended third-party beneficiary of the subcontract. The Vendor shall make available to each proposed Subcontractor, prior to the execution of the subcontract, copies of the Contract Documents to which the Subcontractor will be bound by this Section C and identify to the Subcontractor any terms and conditions of the proposed subcontract which may be at variance with the Contract Documents.

F. Each insurance policy and/or certificate shall include the following terms and/or conditions:

1. The Named Insured on the Certificate of Insurance and insurance policy must match the entity's name that responded to the solicitation and/or is signing the agreement with the County.

2. Companies issuing the insurance policy, or policies, shall have no recourse against County for payment of premiums or assessments for any deductibles which all are at the sole responsibility and risk of Vendor.

3. The term "County" or "Pinellas County" shall include all Authorities, Boards, Bureaus, Commissions, Divisions, Departments and Constitutional offices of County and individual members, employees thereof in their official capacities, and/or while acting on behalf of Pinellas County.

4. All policies shall be written on a primary, non-contributory basis.

The minimum insurance requirements and limits for this Agreement, which shall remain in effect throughout its duration and for two (2) years beyond final acceptance for projects with a Completed Operations exposure, are as follows:

1.3. COMMERCIAL GENERAL LIABILITY INSURANCE

Includes, but not limited to, Independent Vendor, Contractual Liability Premises/Operations, Products/Completed Operations, and Personal Injury. No explosion, collapse, or underground damage exclusions allowed.

A. Limits

1. Combined Single Limit Per Occurrence $ 1,000,000

2. Products/Completed Operations Aggregate $ 2,000,000

3. Personal Injury and Advertising Injury $ 1,000,000

4. General Aggregate $ 2,000,000

1.4. CYBER RISK LIABILITY (NETWORK SECURITY/PRIVACY LIABILITY) INSURANCE

To include cloud computing and mobile devices, for protection of private or confidential information whether electronic or non- electronic, network security and privacy; privacy against liability for system attacks, digital asset loss, denial or loss of service, introduction, implantation or spread of malicious software code, security breach, unauthorized access and use; including regulatory action expenses; and notification and credit monitoring expenses with at least minimum limits as follows:

A. Limits

1. Each Occurrence $ 5,000,000

2. General Aggregate $ 5,000,000

B. For acceptance of Cyber Risk Liability coverage included within another policy required herein, a statement notifying the certificate holder must be included on the certificate of insurance and the total amount of said coverage per occurrence must be greater than or equal to the amount of Cyber Risk Liability and other coverage combined.

1.5. PROFESSIONAL LIABILITY (ERRORS AND OMISSIONS) INSURANCE

Minimum limits as follows. If “claims made” coverage is provided, “tail coverage” extending three (3) years beyond completion and acceptance of the project with proof of “tail coverage” to be submitted with the invoice for final payment. In lieu of “tail coverage”, Proposer may submit annually to the County, for a three (3) year period, a current certificate of insurance providing “claims made” insurance with prior acts coverage in force with a retroactive date no later than commencement date of this contract.

A. Limits

    1. Each Occurrence or Claim $ 5,000,000

    2. General Aggregate $ 5,000,000

B. For acceptance of Professional Liability coverage included within another policy required herein, a statement notifying the certificate holder must be included on the certificate of insurance and the total amount of said coverage per occurrence must be greater than or equal to the amount of Professional Liability and other coverage combined.

1.6. PROPERTY INSURANCE

Vendor will be responsible for all damage to its own property, equipment and/or materials.

Exhibit E

Scope of Work

Security Assessment

NIST Cybersecurity Framework Assessment

Introduction

To guide our efforts in conducting a holistic and comprehensive cybersecurity assessment, CLA relies upon guidance, control descriptions, and recommendations from industry-accepted, vendor neutral, best practice frameworks and standards from authoritative sources such as the National Institute of Standards and Technology (NIST), International Standards Organization (ISO), Center for Internet Security (CIS), among several others. For Pinellas, we will leverage the well-known NIST Cybersecurity Framework v2.0 (CSF) to review and assess Pinellas's overall alignment with the information security best practices detailed in the NIST CSF. Further, CLA will provide one overall CSF report for the county and 14 county agency reports for controls specific to the individual county agencies not managed by the county.

Objective

- Provide a thorough review and risk assessment of your cybersecurity practices and preparedness to adopt the NIST CSF as a framework to evolve and enhance the cybersecurity program. To include additional detailed review of AWS and Azure Security, Data Loss Prevention services, Inventory of Data Assets and Impact Analysis, and Ransomware Defense and Incident Readiness Analysis assessment.

- Provide advisory services as needed regarding the scoping of systems, selection of a maturity scale or implementation tiers identified in the NIST CSF that aligns with your risk appetite and burden of compliance.

- Recommend an approach to developing a sustainable cybersecurity roadmap that incorporates the NIST CSF functions, categories, subcategories, and controls at a pace consistent with objectives identified by management.

- Provide an independent gap assessment of your cybersecurity practices using either your selected maturity scale, or implementation tiers identified in NIST CSF, based upon the in-scope NIST CSF functions, categories, and subcategories of controls.

- Provide an independent assessment of your cybersecurity risks associated with NIST CSF, AWS and Azure risks, information security program risk, gaps in program documentation with PCI, CJIS, HIPAA, Data Loss Prevention risks, Data Asset risks, and Ransomware response readiness and Incident response readiness.

- Incorporate prioritized findings and recommendations from vulnerability assessments, penetration testing and application assessments into overall recommendations.

Approach

The scope of the assessment includes assessing controls identified to address the following functions and categories from the NIST CSF Framework Core. In all, there are six core functions, 22 control categories, and 106 sub-category controls that will be reviewed and assessed as part of our approach. A listing of the core functions and control categories is represented in the following table. We will further test key areas including AWS, Azure, Information Security Program and documentation gaps, and Data Loss Prevention services, Inventory of Data Assets and Impact Analysis, and Ransomware Defense and Incident Readiness.

Work Plan

Our work plan for assessing cybersecurity controls follows a four-phase approach detailed below. The phases are (1) Project Initiation and Management Activities, (2) Data Gathering, (3) Analysis and Assessment, and (4) Reporting.

Phase 1: Project Initiation and Management Activities

Task 1.1 - Conduct a Kick-Off Meeting

Task 1.2 - Develop and Distribute Documentation Request List (DRL)

Task 1.3 - Setup Client Access to Secure File Transfer Portal

Task 1.4 - Establish Ongoing Project Management and Status Reporting Schedule

Task 1.5 - Perform Ongoing Quality Assurance Reviews Over Deliverables and Engagement Execution

Phase 2: Data Gathering

Task 2.1 - Collect and Review Client-Provided Documentation (e.g., network diagrams, policy documents, incident response plans, etc.)

Task 2.2 - Run Automated Data Collection Tools on Network to Gather Information on Physical and Logical Network Design and Security Mechanisms. It is anticipated that this task will leverage outputs from vulnerability assessment and penetration testing services running concurrently.

Task 2.3 - Conduct Interviews with Select IT Staff

Task 2.4 - Conduct Interview with Select Department Staff and Management Representatives

Task 2.5 - Perform a Walkthrough of Technology Environment and IT Operations to Obtain an Overview and Understanding of Technical, Administrative, and Physical and Environmental Security Controls

Phase 3: Analysis and Assessment

Task 3.1 - Compare the Existing Technology Environment Controls and Cybersecurity Posture with the NIST CSF's Six Core Functions, 22 Control Categories, and 106 Sub-Category Controls

Task 3.2 - Evaluate Each Control Category and Define Overall Implementation Tier (Implementation tiers described in the section below.)

Task 3.3 - Information Security Program and documentation gaps and crosswalk policies with PCI, CJIS, and HIPAA standards

Task 3.4 – Evaluate Data Loss Prevention services, including consideration of risks related to the following areas: ingress and egress network traffic, application and data transport traffic, email traffic, and foundational controls in Active Directory and Azure, such as digital rights management and conditional access which may limit opportunities for data loss.

Task 3.5 – Evaluate Inventory of Data Assets and Impact Analysis, including the county's creation of a comprehensive inventory of data, classification and labeling standards, and default protections and digital rights for data in storage and data in-use.
Task 3.6 – Evaluate Ransomware Defense and Incident Readiness against best practice guidelines, including but not limited to ransomware defense guides created by Joint Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing & Analysis Center (MS-ISAC).
Task 3.7 – Evaluate Cloud Security controls for AWS, Azure and Microsoft 365, evaluating platform security for parent accounts and subscriptions, and a sampling of critical accounts, subscriptions and tenants against manufacturer guides, CIS benchmarks and other authoritative hardening guides using a combination of automated tools and manual validation procedures.
Task 3.8 – Identify Opportunities for Improvement and Develop Practical and Cost-Effective Recommendations for Each

Phase 4: Reporting
Task 4.1 – Prepare an overall security assessment draft report for the county.
Task 4.2 - Prepare a Succinct NIST CSF Draft Report for the county and each of the 14 agencies in scope (Report will consist of an executive summary, including overall implementation tier rating, scope description and methodology, findings and recommendations, and an appendix for any supporting documentation.)
Task 4.3 - Review Reports with the Client's Project Team
Task 4.4 - Incorporate Feedback and Input from the Client's Project Team
Task 4.5 – Follow-up with the County's remediation activities
Task 4.6 - Revise and Deliver Final Report

Vulnerability Assessment and Penetration Testing:

External Penetration Test and Vulnerability Assessment

Overview

The External Penetration Test and Vulnerability Assessment is designed to aggressively test your network perimeter to identify exposure to security breaches from outside your network. Completeness is a critical objective when securing the network perimeter, therefore our testing approach is designed to test your entire infrastructure to identify rogue gateway entry points, and test systems that interact with the outside including: Internet gateways, VPN, routers and firewalls, email infrastructure, remote access, and application interfaces.

Objective

Identify potential vulnerabilities outside the network that might be used to:

- Gain unauthorized access to sensitive confidential information.
- Modify or destroy data.
- Operate trusted business systems for non-business purposes.

Benchmarks

We will rely on the organization's policies, procedures, and documented standards to define accepted standards of operation. In the absence of such documentation, we will utilize generally accepted industry best practices and our own skills and knowledge specializing in the area of Cybersecurity. If the organization possesses reports from previous penetration tests, we will verify that any previous findings have been adequately addressed.

Approach

CLA Cybersecurity Services will use a variety of manual and automated tools to test the configuration of Internet gateway connections. Our testing will identify and test such gateway connections in place on your current network configuration. We will then obtain appropriate documentation to verify that our activity was properly detected and logged.

The complete network penetration test occurs in four very distinct phases:

Phase 1 – Discovery

Discovery identifies Internet points of presence (potential entry points). In this phase, completeness is critical - entry points need to be identified and tested. We actively interrogate DNS to determine "where you are" on the Internet. The Discovery phase includes "Google Hacking" designed to gather information about your organization, your people, and whatever might be "out there" on social media sites, blog sites, etc.

Phase 2 – Reconnaissance

Hosts identified in the discovery stage are analyzed to determine:

- Type of host (i.e. router, firewall, web server, etc.).
- Operating system in use (including version and patch level).
- Services available and listening.

Phase 3 – Automated Vulnerability Scanning

Nessus and other automated scanning tools are used to determine potential vulnerabilities available to be exploited. Information developed from the discovery and reconnaissance stages is used to "tune" the scanner to focus its effort, improve its feedback, and eliminate unnecessary scanning.

Phase 4 – Analysis, Penetration, and Privilege Escalation

This phase typically represents 85% of our level of effort in a penetration test. We analyze the results of the first three phases ***to prepare a hacking plan***. We verify the results of the automated scanning to validate that we do not present "false positives" in our report. ***We perform numerous manual tests that cannot be accomplished with automated scanning techniques***. If we are "successful" in breaching your perimeter defense, we will quantify the extent of exposure in order to accomplish our critical objective of completeness.

We perform a penetration test in the same way a malicious hacker will exploit your network. This is accomplished by not only performing a basic vulnerability scan but by also analyzing the results of the scan and building a plan of attack. ***Simple vulnerability scans cannot apply intelligence to the task of finding chains of risks and vulnerabilities on disparate systems that can be used to compromise the network.*** They often reveal numerous "low risk" vulnerabilities disclosed within the automated reports that commercial scanning tools produce. However, these "low risk" vulnerabilities can sometimes be used in concert, like piecing together a jigsaw puzzle, to produce a plan of attack that can create "very high risk" results.

Very often, we are successful in putting together a plan of attack that can result in root or administrator level compromise of every host on the client's network ***through a firewall, even though the initial scan results listed only low or medium risk vulnerabilities.***

Our service verifies the results of the scan, so your people do not have to chase false positives often caused by many scanning tools*.* This eliminates the need for your IT personnel to devote time and effort to this process.

For each vulnerability, or perhaps more importantly for each chain of vulnerabilities, we do our homework and present a best practice set of solutions. Sometimes a simple patch download will suffice, but more often than not, the solution is more complex.

Our developers keep us on the cutting edge. They are constantly producing proprietary tools to test for the presence of emerging vulnerabilities, often before tools such as Nessus have scripts available to test for them. Email Spear Phishing is the #1 attack and delivery mechanism today for hackers. We perform email infrastructure testing procedures unlike anyone else, to verify the effectiveness of your email security and thoroughly define what types of messages can be slipped in past the organization's spam and antivirus filters.

We then test systems and users with targeted email messages designed to convince the user to bypass controls and/or test the underlying systems (browser, email client, and operating system) for exploitable vulnerabilities and weak security configurations (i.e. end users with local administrator rights).

Finally, our security auditors have the skills and knowledge specializing in the area of Cybersecurity to test for the presence of known and unknown vulnerabilities in web-based applications and the back end databases that support the websites operations, including buffer overflows, cross-site scripting attacks, and SQL injection. Our developers and security auditors have discovered and documented the presence of previously unknown vulnerabilities in numerous on-line banking, e-commerce, and vendor supplied web-based administrative applications. More complex web facing application infrastructure testing (*i.e.* e-commerce sites, extensive Share Point, electronic business to business interchanges, etc.) is addressed by our independent Web/Application Penetration testing.

Outcome

The external penetration test and vulnerability assessment may be used as an "audit" of the organization's incident response capabilities: does the organization have the right tools and processes in place to "Recognize, React, and Respond" to an actual attack or breach attempt?

Our deliverable report will provide your network administrators with detailed recommendations for how to address specific findings. Successive tests will include findings in a table format that track remediation of previous findings, and identification of new risks.

Internal Penetration Test and Vulnerability Assessment

Overview

The Internal Penetration Test and Vulnerability Assessment will be a technical evaluation of the key devices (*file servers, mail servers, production servers, routers, switches, etc.*) that reside on your trusted business network.

The Computer Security Institute estimates that only 3% of businesses have the appropriate security patches and configurations in place to protect their network from an internal breach or a successful perimeter breach.

Annual breach analysis reports from Trustwave and Verizon Business Services conclude that the majority of breaches have root causes related to:

- Weak/default administrator and vendor credentials
- Unsecured network shares
- Vendor supplied/managed systems
- Weak or poor patch/update management – especially for non-operating system applications.

The Internal Penetration Test and Vulnerability Assessment is designed to confirm that your network is reasonably protected from these types of threats, which can be more disruptive and more expensive.

Objective

Identify potential vulnerabilities inside the network that might be used to:

- Gain unauthorized access to sensitive confidential information.
- Modify or destroy data.
- Operate trusted business systems for non-business purposes.

Benchmarks

Benchmark measurement for this network security assessment will be your security policy and configuration standards. In the absence of these standards, CLA will use a combination of industry-specific best practices and vendor-specific best practices related to security for the specific devices deployed in your network.

Approach

The Internal Penetration Test and Vulnerability Assessment occurs in two distinct phases:

Phase 1 - Internal Penetration Testing

Beginning with very limited privileges, (*typically only a data port connection in a conference room*) CLA Cybersecurity Services will use automated and manual techniques to identify significant network hosts and routing devices. We will then review their configuration using a combination of automated tools and manual information security checklists (*i.e. hardening checklists*). The Internal Penetration Testing includes the following:

- Identify live hosts and services available on the network.
- Perform automated vulnerability assessments using up-to-date open source and custom developed proprietary tools.
- Manual testing of the results from automated scan to eliminate false positives
- Exploit vulnerabilities to demonstrate possible privilege escalation scenarios.

Phase 2 - Configuration Audit and Process Review

During the configuration audit we will review key systems and processes to document current configurations:

- Perform service pack/security patch/hot-fix scanning to identify currently level up update on key systems on the network (MS Windows operating systems, UNIX systems, Novell systems, etc.).
- Configuration audits of key servers and routing devices against industry standard benchmarks.
- User account and password auditing to validate compliance with information security policies.
- Review configuration of user account and group policy and auditing settings with Active Directory.
- Review end point protections for workstations and mobile devices, including anti-virus, anti-malware, encryption, etc.
- Review configuration of 3rd party vendor installed/maintained systems.
- Review network/system security architecture.

Outcome

Our deliverable report will provide your network administrators with detailed recommendations for how to address specific findings. Your network will be secured *(hardened)* from the inside to protect against malicious insiders, intruders who may gain physical access to network resources, or external hackers who successfully breach perimeter defenses.

The internal penetration test and vulnerability assessment can be used as an "audit" of the organization's incident response capabilities: does the organization have the right tools and processes in place to "Recognize, React, and Respond" to activities associated with an actual intrusion?

Web/Application Penetration Test

Objective

CLA will assessment up to 12 web applications/sites in order to verify that applications are configured and operating in a secure manner. The test focuses on publicly accessible profiles and limited credentialed access testing to assess that appropriate Confidentiality, Integrity, and Availability are maintained. Application inputs, processing, and functionality are assessed. The goal is to identify potential vulnerabilities within the application that might be used to:

- Gain unauthorized access to sensitive confidential information.
- Modify or destroy data.
- Operate trusted business systems for non-business purposes.

Approach

A variety of manual and automated tools are used to test the application interfaces. Our testing is modeled after the industry accepted Open Web Application Security Project (OWASP) framework. The complete Web/Application Penetration test occurs in the following phases:

- Information Gathering
- Configuration Management Testing
- Business logic testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Data Validation Testing
- Web Services Testing

Testing is conducted without credentials followed by testing with credentials to validate that application functionality “behind” the authentication prompt is operating in a secure manner. We test the interfaces presented by the application through a combination of direct manual testing of inputs, as well as review, analysis and testing of data captured via proxy that is being transmitted between the browser/you and receiving web application service.

Wireless Network Security Assessment

Objective

Assess the configuration and security of existing wireless networks, evaluate segmentation controls to protect the internal, corporate network from less-secure wireless networks, and scan for rogue devices within your trusted infrastructure.

Approach

We will begin by documenting the external visibility of any 802.11 wireless signals within your facility. Our scanning tools identify wireless (802.11) devices within range. This includes your organization's access points, as well as any neighboring company's devices. For the organization's wireless networks, CLA identifies the security measures in place (encryption, cloaking, and existence of default configurations).

Each identified device is then be subjected to penetration testing using manual and automated techniques to gain access to the network. These techniques include attempts to break encryption, perform password guessing attacks, monitor traffic through "man in the middle" attacks, and take control of access points or your devices. Lastly, we test segmentation controls.

We will be responsible for the means and methods of providing our services and perform the engagement in a professional and workmanlike manner. We will not perform management functions or make management decisions on behalf of the County. However, we will provide advice and recommendations to assist the County in performing its functions and making decisions.

Project Management Approach

General Project Administration

We will assign a Principal and a Project Manager as your direct liaisons. These individuals will work with the County's designated project manager to oversee that the various components of the project are managed in a manner the meets everyone's expectations. We will work with your designated project manager to establish project timelines and deadlines, and communication protocols. These communication protocols will include formally scheduled project status meetings, as well as ongoing updates via phone and/or email. The exact timing and frequency for meetings and communication updates will be established as part of an initial kick off meeting between CLA and the County. We will keep you informed throughout all stages of the assessments. Any concerns or problems will be discussed with the client within 24 hours and resolved within a reasonable time relative to the issue. We welcome job shadowing as a means of knowledge transfer and are happy to openly share our processes and testing methodologies.

Quality Control Standards

We have undertaken an intensive internal quality control program to foster that professional standards are maintained in our work. This program is designed to provide reasonable assurance that our personnel will be competent and objective and will exercise due professional care. Included in that program are the following:

- A quality control manual to dictate the quality control standards and policies of our firm. These standards often exceed requirements set forth by professional standards and governmental guidelines. To monitor the adherence to policies and procedures, and to oversee that the quality and accuracy of services provided meet our standards of client services, each office must have a regular internal examination performed by professionals from other firm offices.
- Quality control standards as prescribed by the American Institute of Certified Public Accountants (AICPA) are maintained. A principal-in-charge is involved in the planning, fieldwork and post-fieldwork review.

Our reports are issued promptly after the completion of our fieldwork. CLA's communication framework is set up to foster value-driven results. We require our auditors to prioritize their findings and discuss drafts of reports with the appropriate Pinellas County and staff prior to issuance.

We believe this approach accomplishes the following:

- Confirms the information contained in the report.
- May foster a lesser reaction to significant findings.
- Encourages buy-in from the process owners.
- Increases likelihood of implementation of recommendations (if any).

We realize and appreciate that audit results and recommendations cannot be "textbook" responses. We work with our clients to assess and determine pragmatic recommendations based on cost-effectiveness, staffing and resource considerations, system limitations, and compliance considerations. This results in a collaborative effort to arrive at "real world" practical strategies and responses for executive management to consider and evaluate in managing IT risks.

Upon approval of the draft report, final reports will be issued to the County's senior management, and formally presented if requested. The final reports will consist of:

1) Executive Summary Report suitable for the County's senior management; summarizing the scope, approach, and findings; and
2) Detailed Report designed for the County's information technology staff which will include methodology employed, detailed information technology findings with a risk rating for each and detailed exhibit if appropriate, and detailed remediation steps.

Follow up calls after the completion of the final deliverable to discuss observations and recommendations are expected, and this is included in the fee quote – we believe it fosters a sound working relationship between our technical professionals and yours that leads to better outcomes.

A more detailed outline of our project management approach is set forth below.

Project Management Approach (Detailed Outline)

CLA will approach this project as a collaborative effort. CLA professionals will work closely with your team to achieve and satisfy the project objectives.

Project Planning Meeting

The major objectives of the initial meeting will be to validate the overall goals of the projects including definition of specific objectives and timelines. We will review the organization's organization structure, policies and procedures and any existing business and technology plans containing information that may impact the project.

Project Teams

Determine appropriate personnel who will participate in the project and have overall "ownership" from a strategic and day-to-day perspective.

Specific activities will vary but typical responsibilities include understanding the overall business and technology goals of the County, defining and monitoring the project schedule, and keeping appropriate staff (and external business partners) informed on the status of the project.

Decision-Making Authority

Throughout the project various decisions will need to be made. CLA will work with you to determine who must be involved in various evaluation and selection activities and who must be involved in the approval process and decisions.

Communication Strategy

CLA and the County will jointly determine the best method for communicating project-related information including but not limited to:

- On-site Meetings
- Teleconferences
- Email communication
- Protocol for communicating audit findings
- Other

Project Plan

As a result of the information obtained during the project planning meeting, establish a project plan that will identify the following:

- Specific project tasks
- Anticipated start/completion date for tasks
- Individual(s) responsible for completion of tasks

Throughout the life of the project, CLA will facilitate periodic project status meetings to identify task status including those that need specific attention to maintain the project objectives and related schedule.

Advanced Preparation

CLA may request information to be provided in advance of any on-site or in-person interviews to conduct a thorough and effective assessment analysis. The information will be reviewed prior to any additional staff meetings. Specifically, the information that should be provided includes, but is not limited to, the following:

- Organization Structure (IT and Entity)
- Network Architecture Diagrams
- Application Inventory
- Information Security Policies and Procedures
- Key Vendor Relationships / Dependencies

This advanced preparation allows the audit professionals to more effectively use the time spent with your personnel. The CLA consulting team will review the information prior to the strategic planning meeting and summarize what factors are critical to the decision making process.

Pinellas County Interaction

We can perform most of our testing in either an informed (white box) or uninformed (black box) manner. We prefer that most or all testing will be done in an informed manner. This allows us to:

- Be efficient with our time and your resources
- Focus our efforts on testing controls as opposed to discovering controls
- Work collaboratively with your IT administration and security staff to understand what is being observed, develop accurate observations, and meaningful recommendations

We will expect the County to provide documentation related to the testing that may include: network and application diagrams; system and asset inventories; policies, procedures, and standards; and previous assessment reports. This approach allows us to focus on thorough testing of controls as opposed to spending time on discovery of controls.

During assessments we will expect to be able to interact with the County staff to discuss the status of testing results in order to refine and focus our testing and collaborate on observations, issues and possible recommendations. We encourage the County staff to spend time with our testing professionals during the course of the assessments (i.e. job shadowing) as time allows.

For a successful engagement, support from the County resources is necessary. Our anticipated needs for support are approximated below:

1. Sponsors/Management: 4 - 8 hours for initial planning phase
2. Periodic meetings (15-30 minutes) throughout the engagement for project meetings and updates
3. Subject Matter Experts: 1-4 hours per week in support of testing

As part of the planning phase, it will be the responsibility of the County to specifically identify all sponsors / management and subject matter professionals who will be supporting this engagement.

Project Schedule

Project Timeline

We will work with the County's management team to formally establish project timelines and deadlines. Below is the expected timing of each segment of this engagement.

Initial Assessment – Expected start May 2025

- Project Updates and Meetings
- Project Planning Meeting and Deliver Fieldwork Plan
    - Security Assessment
        - NIST CSF Assessment
        - Cloud Security Assessment
        - Information Security Program Review and Information Policy Review and Modernization
        - DLP Analysis, Inventory of Data Assets and Impact Analysis, Ransomware Defense & Incident Readiness Analysis
    - Vulnerability Assessment and Penetration Testing
        - Vulnerability Assessment
        - Penetration Testing
        - Application Assessments
        - Security Architecture Analysis
- Complete Fieldwork
- Deliverables Preparation and Review

Initial Reports – Expected August 30, 2025

- CLA typical provides initial report drafts within four weeks of fieldwork conclusion

Mitigation – Expected September 2025 through November 2025

- During this phase County management will have the opportunity to correct

Follow-up Assessment – Expected December 2025

- During this phase CLA will conduct review of remediation activities regarding initial report recommendations from our security assessment and NIST CSF assessments. In addition, CLA will conduct limited vulnerability scanning and penetration testing to determine in remediation activities have resolved weaknesses identified during the initial testing.

Deliver Final Report – Expected – Mid-January 2026

- CLA expects the final reports within two weeks of follow-up assessment conclusion.

Reports

Security Assessment Report

Our security assessment report will include an executive summary with highlighted NIST CFS results, findings and recommendations associated with the Cloud Security Assessment procedures, Information Security Program Review and Information Policy Review and Modernization Assessment procedures, and DLP Analysis, Inventory of Data Assets and Impact Analysis, Ransomware Defense & Incident Readiness Analysis procedures and high-level vulnerability and penetration testing results.

Draft reports are expected to be provided with four weeks of concluding fieldwork and will be finalized following management feedback and follow-up assessment activities. Reports will be provided in PDF format.

NIST Cybersecurity Framework Reports

Our county report will consist of an executive summary, including overall implementation tier rating, scope description and methodology, findings and recommendations for the county, and an appendix for any supporting documentation.

Our 14 agency level reports will consist of an executive summary, implementation tier rating, scope description and methodology, findings and recommendations specific to the agency. Scope of the agency level reports will be specific to controls and implementations unique to the agency that are not inherited from the county.

Draft reports are expected to be provided with four weeks of concluding fieldwork and will be finalized following management feedback and follow-up assessment activities. Reports will be provided in PDF format.

Vulnerability Assessment and Penetration Testing Reports

Our vulnerability assessment and penetration testing reports will include detailed recommendations for how to address specific findings and the risk associated with these findings. The detailed recommendations will be designed to assist network administrators with remediation efforts.

This report will be provided as a draft at the conclusion of fieldwork and will be finalized after the follow-up vulnerability and penetration testing. Reports will be provided in PDF format.

Exhibit F – Pricing Proposal

Professional Fees & Expenditures

Assumptions. Onsite review will be limited to the facility housing the data center, and CLA anticipates being on-site at Pinellas County for up to five weeks.

- Internal vulnerability assessment and penetration testing is expected focus on servers and sampling of other networked devices.
- Web application testing will primarily include unauthenticated testing and authenticated testing up to one role per application.
- Wireless assessment will be conducted from a central location with up to 4 SSIDs included in scope.

Schedule. CLA is prepared to begin the project within eight (8) to twelve (12) weeks of your notification to proceed, or as agreed upon with the County. The duration of fieldwork will be coordinated with management to align with expectations outlined in the RFP.

Professional fees. Our professional fees for these services will be based on the time involved and the degree of responsibility and skills required, number of systems, and system complexity. The fees contained in this proposal are valid for ninety (90) days from the proposal date. Fees for each individual component are presented below:

Services	Professional fees
Security Assessment - NIST Cybersecurity Framework (Overall County Report + 14 Department Reports)	$120,000
External Penetration Testing and Vulnerability Assessment with Email Phishing	$19,000
Internal Penetration Test and Vulnerability Assessment	$100,000
Web/Application Penetration Testing (12 Applications)	$40,000
Wireless Assessment	$7,500
Follow-up Assessment	$10,000
Total for Services	**$296,500**
Travel Cost Estimate for up to 5 weeks onsite	$23,000
Technology and Client Support Fee (5% of Professional Fees billed)*	$14,825
Optional Additional Services – billed hourly	**$165,000**
Grand Total	**$499,325**

****Like most firms, we are investing heavily in technology to enhance the client experience, protect our data environment, and deliver quality services. We believe our clients deserve clarity around fees, and we will continue to be transparent with our fee structure.***

Reimbursable expenditures. Reimbursable expenditures made by CLA, **separate** from the professional fees, **include travel time and the following expenses**:

- Airfare / Mileage / Transportation / Parking
- Living expenses at project location (hotel, meals, rental car)
- Shipping and delivery of hardware related to execution of the engagement

Travel expenses will not exceed $23,000.00 during the Contract Term. All bills for any authorized travel expenses will be submitted and paid in accordance with the rates and procedures specified in Section 112.061, Florida Statutes, and in compliance with the COUNTY's policy for travel expenses.

All expenses are billed at actual cost with no markup of charges.

Optional Hourly rates for additional services are documented in the chart below:

Role	Hourly Rate
Controls Associate	$195
Controls Senior	$250
Tech Associate	$195
Tech Senior	$290
Manager	$470
Principal	$550

Optional additional services and any travel associated with the additional services must be approved in writing in advance by the BTS Project Manager and will not exceed $165,000.00 during the Contract Term.

Exhibit G

CONFIDENTIALITY AGREEMENT

Pinellas County, Florida ("Pinellas County") and CliftonLarsonAllen LLP ("CLA") wish to discuss matters pertaining to their prospective business/consulting relationship. For such discussions to be meaningful, it will be necessary for Pinellas County to provide to CLA certain proprietary and confidential information relating to Pinellas County's business.

As consideration for Pinellas County agreeing to disclose such information to CLA, and for other good and mutual consideration, the receipt and sufficiency of which are hereby acknowledged:

1. CLA agrees that all confidential information ("Confidential Information") regarding Pinellas County's business provided by Pinellas County to CLA shall remain the property of Pinellas County. CLA agrees to maintain the confidentiality of all such Confidential Information provided by Pinellas County to CLA. CLA's confidentiality obligation applies whether the information was provided orally, in writing, or in electronic form. However, "Confidential Information" does not include information that:

(a) is already known to CLA at the time it was disclosed by Pinellas County;

(b) was independently developed by CLA;

(c) became or has become publicly known through no wrongful act of any party;

(d) has been properly received by CLA from a third party without any restriction on disclosure; or

(e) is required by law, court order, subpoena or regulatory requirement to be disclosed.

2. CLA shall retain all Confidential Information in strict confidence to prevent the disclosure of Confidential Information to any third party. In doing so, CLA will exercise the same standard of care it uses to protect its own confidential and proprietary information and the confidential information of CLA's other clients. CLA shall not use, and shall not copy or reproduce, such Confidential Information at any time for any reason other than in furtherance of the purpose described in the introductory paragraph of this Agreement. CLA represents and warrants that each of its employees and agents to whom Confidential Information is disclosed shall have a need to know such information for the purposes contemplated by this Agreement.

CLA shall adopt procedures to reasonably ensure that the provisions of this Agreement are enforced and respected, such as requiring all employees to sign confidentiality agreements, and shall instruct its employees and agents who are provided access to Confidential Information that such information shall not be discussed with or disseminated to anyone who is not directly involved in these discussions.

3. In the event disclosure of Confidential Information is sought under subpoena, or required under provisions of any law or court or regulatory order, CLA will use all reasonable efforts to notify Pinellas County of the request to make such disclosure sufficiently in advance of the disclosure that Pinellas County will have a reasonable opportunity to intervene and object.

4. CLA's confidentiality obligations under this Agreement shall survive for the duration of discussions or negotiations regarding the proposed services. Further, if a business relationship is not consummated between CLA and Pinellas County, CLA's confidentiality obligations will continue to survive for the period of time set forth in CLA's record retention policy.

If the business relationship is consummated, this Agreement shall terminate and be of no further force or effect; instead, in that event CLA's confidentiality obligations shall be governed by the engagement letter or other agreement whereby CLA is engaged to provide professional services to Pinellas County and by the statutes and professional regulations that prohibit CLA from disclosing confidential client information.

5. If CLA violates this Agreement, Pinellas County shall be entitled, if it so elects, to institute and prosecute proceedings in any court of competent jurisdiction to obtain relief by way of injunction to enforce its rights hereunder.

6. Any waiver, modification, or amendment of any provision of this Agreement shall be effective only if in writing in a document signed by both parties that specifically refers to this Agreement.

7. This Agreement constitutes the full and complete understanding and agreement of the parties hereto with respect to the subject matter covered herein and supersedes all prior and contemporaneous oral or written understandings and agreements with respect thereto.

8. If any provision of this Agreement is found to be unenforceable by a court of competent jurisdiction, such provision shall be amended under the court's supervision so as to be enforceable to the fullest extent permitted by such court, and the remaining provisions shall nevertheless remain in full force and effect.

9. This Agreement shall be governed by and construed in accordance with the laws of the State of Florida, without regard to that State's choice of law provisions.