February 27, 2025

Proposal to provide professional cybersecurity services to:

Pinellas County
Request for Proposal - #25-0238
Comprehensive Security Risk Assessment
Clearwater, FL

Prepared by:

David Scaffido, CISA, CISM, CDPSE, Principal
571-227-9668
David.Scaffido@CLAconnect.com

Section 6.3: RFP Submittal Requirements

Table of Contents

Cover Letter/Statement of Interest

CliftonLarsonAllen LLP
One Tampa City Center, 201 North Franklin St, Suite 2500
Tampa, FL 33602-5845

phone 813-384-2700 **fax** 813-384-2750
CLAconnect.com

February 27, 2025

Merry Celeste, CPPB
Division Director of Purchasing and Risk Management
Pinellas County
Pinellas County Courthouse Annex Bldg., Sixth Floor
Clearwater, FL 33765

RE: **Request for Proposal - #25-0238 Comprehensive Security Risk Assessment**

Dear Merry:

Thank you for inviting us to propose our services to you. CLA is active in the Florida state government community and looks forward to offering our expertise and security assessment services. We gladly welcome the opportunity to share our approach to helping Pinellas County (the County) meet its need for professional services. The enclosed proposal responds to your **Request for Proposal - #25-0238 Comprehensive Security Risk Assessment.**

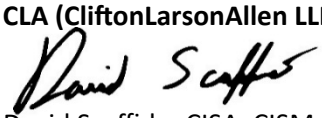
Our security assessment services practice relies on a combination of tools that are developed internally by CLA security professionals, as well as open-source and commercially available software. While the core tools used by our practice remain the same, our professionals are constantly on the lookout for new tools and utilities to continually enhance their capabilities. We have also developed, and continually update, comprehensive work programs that lead the way for the holistic and efficient approach to performing our risk and control review assessments, as well as our compliance assessments. Specific scope, approach and desired outcomes are defined in collaboration with clients. Our assessment model includes a dedicated project management approach.

CLA is focused on delivering an exceptional level of knowledge, insight, and industry experience. As our clients' most trusted business advisor, we:

- Take a genuine interest in your opportunities and challenges
- Proactively work with you to develop strategies based on a deep understanding of your business and industry
- Address your organization's financial challenges through our national and global resources
- Continually strive to better your organization, the government industry, the communities in which we work and live, the cybersecurity profession, and ourselves

We are eager to work with you and welcome the chance to present our proposal to the County's audit committee or entire management team. If you have any questions about our offerings, please do not hesitate to contact me.

CLA (CliftonLarsonAllen LLP)



David Scaffido, CISA, CISM, CDPSE
Principal
571-227-9668
David.Scaffido@CLAconnect.com

CLA Cybersecurity Services Team Resumes

Engagement team

The most important resource any business has is people — the right people.

An experienced engagement team has been aligned to provide the most value to your organization. The team consists of personnel with technical and business credentials, including CBA, CCSE, CCSFP, CEH, CFE, CHPS, CIA, CICA, CISA, CISM, CISSP, CITP, CPA, CPT, CRISC, CRMA, CTGA, FCSP, GCFA, GCIH, GSEC, GWAPT, HCISPP, ITIL, MCNE, MCP, MCSE-Security, OSCP, OSWP, PCI-QSA, PMP, WCNA and others. The team members have performed numerous engagements of this nature and will commit the resources necessary to provide top quality service throughout the engagement.

The core proposed management team members are listed below and will be supported by additional business, process, and technology professionals as needed.

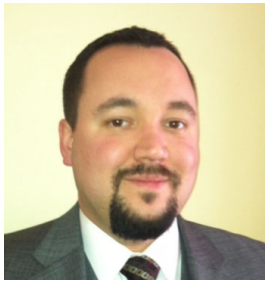
Resource	*Title*	*Role/Emphasis*
David Scaffido	*Principal*	*Engagement Leader – Cybersecurity, IT Audits, Risk Assessment*
Randy Romes	*Principal*	*Service Leadership – Cybersecurity, Health Care and Financial Industry, PCI*
David Anderson	*Principal*	*Service Leadership – Cybersecurity/IT*
Lindsay Timcke	*Director*	*Service Leadership – Cybersecurity, Business Risk/Internal Audit*
Sedric Louissaint	*Director*	*Engagement Mgmt. – IT Audit, Cybersecurity and Vulnerability Assmts.*
James Barton	*Director*	*Engagement Mgmt. – IT Audit, Network Management*
David Nowacki	*Director*	*Engagement Mgmt. – IT Audit, Cybersecurity and Vulnerability Assmts.*
Ryan O'Conor	*Manager*	*Engagement Mgmt. – IT Audits, Controls, State & Local Government*
Zoran Jovic	*Manager*	*Engagement Mgmt. – IT Audits, Cybersecurity and Vulnerability Assmts.*
RJ Stallkamp	*Manager*	*Engagement Mgmt. – IT Audits, Cybersecurity and Vulnerability Assmts.*
Andrew Petro	*Senior*	*Technical Analyst – IT Audits, Cybersecurity and Vulnerability Assmts.*
Gregory Kempf	*Senior*	*Technical Analyst – IT Audits, Cybersecurity and Vulnerability Assmts.*
Daniel Printke	*Senior*	*Technical Analyst - IT Audits, Cybersecurity and Vulnerability Assmts*

Resumes

Detailed biographies are available beginning on the next page.

David Scaffido, CISA, CISM, CDPSE

CLA (CliftonLarsonAllen LLP)



Principal
Arlington, Virginia

571-227-9668
David.Scaffido@CLAconnect.com

Profile

David is an Information Technology Principal specializing in information technology audits and security assessments. He has more than eighteen years of experience overseeing IT control reviews supporting financial statement audits and performing security assessments and compliance audits of public sector and governmental organizations. David has conducted an array of security, risk, vulnerability, and penetration testing assessments for government and commercial entities. David operates as the key security point of contact for large governmental audits and assessments. David has significant experience conducting evaluations of general and application controls to support the financial statement audits. He also has significant experience with Federal Information Security Management Act (FISMA) security control assessments based on National Institute of Standards and Technology (NIST) Special Publication 800-53.

Technical experience

- Information systems security reviews and audit of both general and application controls with an emphasis on public sector and governmental entities
- IT auditing and assessments focusing on COBIT, FISCAM, FISMA, NIST, OMB, CIS and other guidance
- Internal and external vulnerability assessments
- Penetration testing assessments
- Experience with network security and monitoring software

Education and professional involvement

- Bachelor of science, Management Information Systems, West Virginia University
- Information Systems Audit and Control Association (ISACA)
- Association of Government Accountants (AGA)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Data Privacy Solutions Engineer (CDPSE)
- CMMC Registered Practitioner – Advanced (RPA)

Randall J. Romes, CISSP, CRISC, CISA, MCP, PCI-QSA

CLA (CliftonLarsonAllen LLP)

Principal
Minneapolis, MN

612-397-3114
Randy.Romes@CLAconnect.com

Profile

Randy is a Principal in CLA's National Digital group and has been a consultant for more than 20 years with a strong background in computer technology, physics, and education. Randy leads a team of technology and industry professionals providing IT audits and security assessments for clients in a wide range of industries and diverse operating environments. He is responsible for the continuing development of the open-source, Unix, and Windows applications used in all the security audits.

Technical experience

Randy has been involved in the development of numerous leading-edge hacking/testing methods and the development of numerous security service offerings including:

- Techniques for email Phishing that result in remote access to company networks, bypassing improperly configured firewalls and proxy systems.
- Social Engineering Techniques designed to assess all aspects of company security "People, Rules, and Tools."
- Techniques incorporating SSL encryption to evade commercial intrusion detection systems (IDS).
- Incident response and computer forensic services.
- Internal Vulnerability Assessment services for financial services industry.

Education and professional involvement

- Masters degree in educational technology from the University of Saint Thomas—St. Paul, MN
- Bachelor of science in education from the University of Wisconsin-Madison—Madison, WI
- Certified Information Systems Security Professional (CISSP)
- Certified in Risk and Information Systems Controls (CRISC)
- Certified Information Security Auditor (CISA)
- Microsoft Certified Professional (MCP)
- PCI Qualified Security Assessor (PCI-QSA)

Speaking engagements

Randy is an active member of the conference planning and selection committee for the Minnesota Government IT Symposium, the longest running government IT conference in the country. He also a regular speaker at the Florida Government Finance Officers Association.

He has been a featured speaker at national conferences and training sessions related to information and security management including topics related to:

- Identity Theft and On-line Security
- Email Phishing
- Social Engineering
- Securing Windows Operating Systems
- Incident Response, e-Discovery, and Computer Forensics
- Network and Wireless Security
- PCI Security

David Anderson, OSCP

CLA (CliftonLarsonAllen LLP)

Principal
Minneapolis, Minnesota

612-376-4699
David.Anderson@CLAconnect.com

Profile

David is a Principal and Cybersecurity Consultant in the CLA National Digital group with a strong focus on Offensive Cybersecurity. He has over 12 years of experience in the field, performing penetration testing, vulnerability assessments, and social engineering engagements. David's expertise also includes project management for cybersecurity engagements across a diverse range of industries.

Technical experience

David has firsthand knowledge and experience using leading edge hacking/testing methods:

- External and internal network penetration designed to gain access to high value targets
- Social engineering techniques designed to assess security related to the human element
- Techniques for email phishing that result in remote access to company networks, bypassing improperly configured firewalls and proxy systems
- Domain and network management

Education and professional involvement

- Bachelor of art, information technology with focus on networking and security, Minnesota State University – Mankato (MNSU)
- Offensive Security Certified Professional (OSCP)

Speaking engagements

David has been a featured speaker at national conferences and training sessions related to cybersecurity including topics related to:

- Penetration testing and vulnerability assessments
- Corporate account takeovers
- Email phishing
- Social engineering
- Network security

Lindsay Timcke, MBA

CLA (CliftonLarsonAllen LLP)

Director
Boston, MA

781-610-1249
Lindsay.Timcke@CLAconnect.com

Profile

Lindsay is a cybersecurity director in the CLA National Digital group with extensive experience spanning more than 25 years in providing risk assessment and data security services in a wide range of industries including bio tech and pharma, hi-tech, software, military vendors, and SaaS-based companies.

In his role, he conducts a wide array of IT-based reviews and assessments ranging from risk assessments, penetration testing, and vulnerability scans to interim-based CISO and CIO services.

Lindsay is also responsible for collaborating with the risk advisory group to guide teams in navigating both traditional technologies like mainframes and server farms, as well as advanced cloud-based environments that have been fully outsourced. Recently, he has focused on exploring cutting-edge technology in the areas of crypto currency/blockchain and military vendors.

Technical experience

- Cybersecurity
- SOX
- PCI
- SOC preparation
- IT risk assessments
- Crypto currency/Blockchain
- NIST 800 standards

Education and professional involvement

- Master of science in environmental education from Southern Connecticut State University, New Haven, Connecticut
- Master of business administration from Northeastern University, Boston, Massachusetts
- Bachelor of science in English from Boston University, Boston, Massachusetts
- ISICA (Information Systems Audit and Control Association)

Civic organizations

- Alpha Defense, *Board Member*

Sedric Louissaint, CISSP

CLA (CliftonLarsonAllen LLP)

Director
Orlando, FL

386-450-1293
Sedric.Louissant@CLAconnect.com

Profile

Sedric is a Director of Cybersecurity Penetration Testing in the CLA National Digital group. Sedric currently performs and manages IT and Cybersecurity testing and assessments within the healthcare and other industries served by CLA. Sedric has over 11 years of technical and management experience in providing IT solutions, security, customer service, and project management.

Technical Experience

- External / Internal Network Penetration Testing and Vulnerability Assessments
- Web and Mobile Application Penetration Testing
- IoT Penetration Testing
- Cloud Security Posture Management & Architecture
- Digital Forensics & Incident Response
- Threat Intelligence
- Threat Hunting
- Secure System Design and Software Development
- Governance, Risk Management, & Compliance

Education and Professional Involvement

- Bachelor of Science in Information Systems Technology (Specialization in Cybersecurity), Seminole State College
- Associate of Science in Information Systems Technology (Specialization in Cybersecurity), Seminole State College
- Technical Certificate in Information Technology Client Specialist, Seminole State College
- Certified Information Systems Security Professional (CISSP)
- CompTIA Security Analytics Expert (CSAE)
- CompTIA Secure Infrastructure Expert (CSIE)
- CompTIA Cloud Admin Professional (CCAP)
- Cisco Certified Networking Associate

James W. Barton, CISA, CISSP

CLA (CliftonLarsonAllen LLP)

Director
Tampa, Florida

813-384-2708
Jim.Barton@CLAconnect.com

Profile

Jim is a Cybersecurity Director in the CLA National Digital group with more than 15 years of experience in the IT profession. He has a strong background in network management and end user support, as well as extensive experience in project management, business management, and service delivery. Jim is well-versed in performing various IT-based reviews, including compliance assessments, penetration testing, and vulnerability scans.

Technical Experience

- Cybersecurity
- PCI
- SOC
- IT General Controls

Education and professional involvement

- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certifications previously held include PCI-QSA and CCSFP
- Member of West Florida Chapter of ISACA, a worldwide association of IS professionals
- Computer Electronics and Networking Technology Diploma, Florida Career Institute

David Nowacki, CISA, CIA

CLA (CliftonLarsonAllen LLP)

Manager
West Hartford, Connecticut

860-561-6811
david.nowacki@CLAconnect.com

Profile

Dave is a Manager with the CLA Cybersecurity group, with more than 23 years of combined experience in cybersecurity, IT controls, enterprise risk management, internal audit, and management consulting. He has worked with government entities, higher education, financial services, and various other private businesses in setting strategies, reviewing, and assessing operations, governance and enterprise risk management practices, project and program management practices; information security programs, and identifying process improvement opportunities.

Technical experience

- Cybersecurity Program Development
- Department of Defense (DFARs) Cybersecurity Compliance (CMMC)
- NIST Cybersecurity Framework and NIST 800 Series
- GLBA and FFIEC Cybersecurity Frameworks
- IT General Controls
- IT Audit and Information Security
- Enterprise Risk Management
- Process Improvement
- Strategic Planning
- Organizational Transformation

Education and professional involvement

- Bachelor of Science, Information Systems from the University of Montana
- Certified Information Security Auditor (CISA)
- Information Systems Audit and Control Association
- The Institute of Internal Auditors

Speaking engagements

David is actively involved in speaking engagements and conferences throughout the New England region and has helped many organizations and associations raise awareness of cybersecurity and related topics such as:

- Cybersecurity Awareness
- Third Party Vendor Risk Management
- Organizational Cyber Hygiene
- Business Resiliency
- Leveraging SOC Reports and Independent Assessments
- Optimizing Policies, Procedures and Controls
- Incident Response

Ryan O’Conor, CISA

CLA (CliftonLarsonAllen LLP)

Manager
Baltimore, Maryland

301-902-8552
Ryan.Oconor@clconnect.com

Profile

Ryan is a manager within the Value and Risk Services group at CLA specializing in IT control and security assessments and audits. Ryan has over 14 years of experience performing IT security audits and evaluations of significant entities within the Federal government including agencies such as the Department of Veterans Affairs (VA), Department of Transportation (DOT), Housing and Urban Development (HUD), Library of Congress (LOC), Smithsonian Institute, and US Agency for International Development (USAID). He has performed IT assessments in support of Financial Statement audits as well as standalone security evaluations. Ryan has also performed consulting and audit services for other industries such as Health Care, Financial Institutions, and Manufacturing and Development.

Technical experience

- Audits and evaluations using Federal regulations and standards such as the Federal Information Security Modernization Act (FISMA), Government Accountability Office (GAO) Federal Information System Control Audit Manual (FISCAM), National Institute of Standards and Technology (NIST) Special Publications (SPs), as well as key and relevant Executive Orders (EO) and Office of Management and Budget (OMB) memorandum.
- Experience auditing and evaluating systems and applications leveraging various technology platforms including windows, Linux, Top Secret Mainframes, and Oracle SAP within traditional on-premises hosted environments as well as cloud enclaves.
- Evaluations and assessments over IT general and application controls in accordance with American Institute of Certified Public Accountants (AICPA) Generally Accepted Auditing Standards (GAAS) and the GAO Generally Accepted Government Auditing Standards (GAGAS/Yellow Book).
- Financial statement audit, performance audit, gap/readiness assessments, and remediation consulting services.

Education and professional involvement

- Bachelor of Science in Accounting and Information Systems from University of Maryland, College Park, Maryland
- Certified Information Systems Auditor (CISA)
- Information Systems Audit and Control Association (ISACA)
- Association of Government Accountants (AGA)

Zoran Jovic, GPEN, CCNA

CLA (CliftonLarsonAllen LLP)

Manager
Tampa, Florida

813-384-2728
Zoran.Jovic@CLAconnect.com

Profile

Zoran is a Cybersecurity Penetration Testing Manager in the National Digital group, focusing on Technical Assessments. Zoran currently performs network penetration testing, internal and external vulnerability assessments, social engineering assessments, and wireless network security assessments.

Prior to joining the firm, Zoran worked with a wide range of organizations, ranging from start-up, small businesses to Fortune 10 organizations. Zoran's experience includes technical assessments, project management and consulting. Zoran is also a United States Army Veteran.

Technical Experience

- Internal/External Network Penetration Testing
- Remote/On-Site Social Engineering
- Wireless Network Security Assessments

Education and Professional Involvement

- Bachelor of Science in Cybersecurity from Bellevue University - Bellevue, Nebraska
- Associates of Science in Computer Science from Onondaga Community College - Syracuse, New York
- GIAC Network Penetration Tester (GPEN)
- Cisco Certified Network Associate (CCNA)

RJ Stallkamp, OSCP

CLA (CliftonLarsonAllen LLP)

Manager
Minneapolis, MN

615-939-4723
Rick.Stallkamp@CLAconnect.com

Profile

RJ has 10+ years of experience and is a Penetration Testing Manager in CLA's national digital group. RJ currently performs cybersecurity and social engineering assessments within a wide range of industries including financial, manufacturing and distribution, healthcare, non-profit, insurance and government agencies.

Prior to joining CLA, RJ gained experience supporting the Department of Defense with a multitude of technological issues. Since RJ has joined CLA, he has spent his time providing penetration testing and social engineering assessments, discovering previously unknown exploits (aka Common Vulnerabilities & Exploits "CVE"), developing proprietary hacking tools, contributing to popular open-source hacking tools, and speaking at local, state, and national conferences.

Technical experience

- Internal/external network penetration testing
- Remote/on-site social engineering
- Web application penetration testing
- Wireless network security assessments

Education and professional involvement

- Offensive Security Certified Professional (OSCP)
- CVE-2023-27743
- CVE-2020-28004
- CVE-2019-16418

Andrew Petro, Sec+, CCNA, Net+, OSCP, CRTO, CHFI

CLA (CliftonLarsonAllen LLP)

Senior
Oak Brook, IL

312-343-3162
Andrew.Petro@CLAconnect.com

Profile

Andrew Petro is a Senior Cybersecurity Penetration Testing in CLA's National Digital group focused on Technical Assessments. Prior to CLA, Andrew worked as an Enterprise Networking and Security consultant for Sirius Computer Solutions. He has a B.A. in Mathematics and a M.S. in Computer Security.

Technical Experience

- Enterprise Networking and Security
- Internal Penetration Testing
- External Penetration Testing
- Firewall Reviews
- VMware Virtualization
- Software Defined Networking
- Red team Penetration Testing
- Purple team Exercises
- Active Directory
- Web Application Penetration test

Education and Professional Involvement

- CompTIA Security+
- CompTIA Network+
- Cisco CCNA-RS
- Offsec Offensive Security Certified Professional
- EC-Council Certified Hacking Forensic Investigator
- ZeroPoint Certified Red Team Operator

Gregory Kempf

CLA (CliftonLarsonAllen LLP)

Senior
Minneapolis, MN

612-256-8310
Gregory.Kempf@CLAconnect.com

Profile

Gregory is a Senior Cybersecurity Penetration Tester in CLA's National Digital group. Gregory performs penetration tests, social engineering engagements and network assessments for clients in the financial, manufacturing, retail, higher education, and healthcare industries. Gregory's focus is to provide maximum insight and value to clients, throughout their assessments.

Gregory has firsthand knowledge and experience using a large suite of security tools and software, with a focus on Active Directory and Windows exploitation.

Technical Experience

- Internal and external network penetration testing and vulnerability assessments
- Wireless network security assessments
- Social engineering testing, both remote and on-site
- Email phishing testing
- Physical security assessments
- Collaborative "purple team" and monitoring effectiveness exercises
- Password hash cracking
- Domain and network management

Education and Professional Involvement

- Bachelor of science in Information Technology and Security with a focus in Cyber Defense, Baker College- Flint, MI
- Currently pursuing the Offensive Security Certified Professional (OSCP) certification

Daniel Printke

CLA (CliftonLarsonAllen LLP)

Senior
Minneapolis, MN

612-256-8314
Daniel.Printke@CLAconnect.com

Profile

Daniel is a Senior Cybersecurity Penetration Tester in CLA's National Digital group. Daniel currently performs penetration tests to identify cybersecurity risks on a client's production environment and their external perimeter. Daniel also performs social engineering engagements both remote and on location to evaluate a client's employees. Testing their ability to not fall victim to specially crafted phishing emails, deceitful phone calls, and in-person masquerading attempts to gain unauthorized access. Daniel has performed engagements for financial, government, healthcare, education, automotive, and non-profit institutions to identify and present recommendations to executive management. Daniel develops custom exploitation tools to improve the internal toolset that can be leveraged by other CLA team members.

Technical experience

- Conduct internal and external penetration testing and vulnerability assessments in client production environments, including collaborative purple team testing.
- Perform remote and on-site social engineering engagements including email phishing, phone calls, and in-person masquerading from both a white box and black-box approach.
- Evaluate physical security using various tools and techniques in order to gain unauthorized access to locations and facilities.
- Evaluate physical security using various tools and techniques in order to gain unauthorized access to locations and facilities.
- Laterally move, escalate privileges, and identify access to confidential information within Active Directory environments utilizing discovered misconfigurations, and vulnerabilities.
- Develop and leverage custom exploitation tools to further improve the team's internal toolset.

Education and professional involvement

- Bachelor of Information Technology and Security, Cyber Defense from Baker College of Flint
- Currently pursuing Offensive Security Certified Professional (OSCP)

Executive Summary

You deserve to work with people whose values match your own. Our values drive our behavior and lead to service delivery that exceeds expectations and provides you with the CLA client experience.

What does that mean? It means you'll work with a team with the resources to support the whole of your organization. You can count on industry specialized professionals who bring ideas and strategies that are relevant and actionable. Quite simply, you'll encounter value beyond the expected.

We put relationships first. Our family culture is at the center of our success, and we invite different beliefs and perspectives to the table, so we can truly know and help our clients, our communities, and each other. Here's what you can experience.

Your time is valuable: *We know how to deliver quality; timely work and we take care of the details so you can focus on what really matters: the important decisions that drive your success.*

CLA's Experience

CLA has a long history of serving state and local governments of Florida. We provide the knowledge unique to your community with experienced cybersecurity professionals locally accessible while bringing the depth of knowledge of almost 9,000 professionals from across the country. In addition, CLA professionals regularly present to Florida government associations such as the Florida Government Finance Officers Association (FGFOA). CLA brings a depth of government and related cybersecurity experience including exceptional knowledge of National Institute of Standards and Technology, Payment Card Industry Data Security Standard, Criminal Justice Information Services, and Health Insurance Portability and Accountability Act standards.

CLA's Comprehensive Information Security Risk Assessment Approach

Our approach will provide Pinellas County's management the opportunity to build a relationship with our team through the Security Assessment process and provides us with the opportunity to gain a thorough understanding of your information security operations and culture. This approach focuses security and risk posture of your organization and can be modified to more specific risk if Pinellas County management desires. Our assessment approach includes four phases for assessment Project Initiation and Management Activities, Data Gathering, Analysis and Assessment, and Reporting. The resulting assessment reports will include guidance to remediate identified gaps and weaknesses.

CLA's Understanding of Project Scope and Purpose

Understanding The Project

Pinellas County, Florida seeks to procure a comprehensive security risk assessment. The scope of the assessment includes include the following key areas:

1. NIST CSF 2.0 Assessment
2. Security Assessment
3. Vulnerability Assessment
4. Penetration Testing
5. Cloud Security Assessment
6. Application Assessments
7. Information Security Program Review
8. Security Architecture Analysis
9. Data Loss Prevention (DLP) Services Assessment
10. Inventory of Data Assets and Impact Analysis
11. Ransomware Defense & Incident Readiness Analysis
12. Security Policy Review and Modernization

To meet these requirements, CliftonLarsonAllen LLP (CLA) is proposing conduct a comprehensive information security risk assessment as outlined in the RFP scope:

- CLA will conduct a county level NIST CSF 2.0 assessment and assessments of the 14 agencies as indicated in the question and answers addendum to the RFP. This assessment is outlined in the NIST Cybersecurity Framework Assessment section of our proposal. (page 19)
- CLA will address the Security Assessment requirements will encompass our NIST CSF 2.0 assessment as well as the additional tiers of testing requested by the county. (page 19)
- CLA will address vulnerability assessment, penetration testing, and security architecture analysis requirements as part of our Internal, External, Wireless, and Web Application Penetration testing. (page 21-27)
- CLA will address the Application Assessment as part of our overall security assessment (page 19) and the Web Application Penetration testing. (page 26)
- CLA will address the Information Security Program Review and Security Policy Review and modernization as part of our overall security assessment. (page 19)
- CLA will address the Cloud Security Assessment for 4 AWS and Azure environments as part of additional testing under the overall security assessment. (page 19)
- CLA will address Data Loss Prevention services, Inventory of Data Assets and Impact Analysis, and Ransomware Defense and Incident Readiness Analysis assessment as part of additional testing under the overall security assessment. (page 19)

CLA will provide the expertise, technical knowledge, staff support, and other related resources necessary to achieve the objectives of the comprehensive security assessment. CLA will provide services, personnel and materials necessary to perform the work described by the Request of Proposal (RFP).

Experience

General background and experience

CLA's Cybersecurity Services Group is the information security assessment and consulting arm of CLA's National Digital group, and is led by a team of seven principals, 18 directors and managers, and resources of over 80 professionals. We are a full-service consulting group with a depth of talent with specific experience with a number of enterprise data processing systems, operating systems and network protocols.

CLA has been performing a wide range of cybersecurity assessment services for over 25 years, including those requested by the County for this proposal. In this time, we have performed more than 4,500 penetration tests, and thousands of IT audits and vulnerability assessments. Our core leadership team has been in place at CLA since the inception of the security services group as a standalone service line in 1999. Senior personnel have upwards of 25 years of experience in the information security and assessment field. We specialize in professional penetration testing, vulnerability assessment, IT and enterprise risk assessment, independent network security consulting, physical access controls and social engineering assessments, security incident response and computer forensics, and IT/security compliance against all major governance and compliance frameworks. We have client references for whom we have provided these services continuously for 10 or more years. CLA does not client names without authorization, please see our references on page 32.

We have been providing PCI gap assessments and the underlying testing requirements (External and Internal Penetration Testing, Vulnerability Scanning and Assessment, Wireless Testing, and Social Engineering Assessments) for clients since the inception of the PCI DSS. Clients include financial institutions; non-profits and foundations; government agencies, counties, and municipalities; restaurant and retail; transportation; manufacturing; and higher education. CLA has been a certified QSA firm since 2011. CLA has developed a standard process/methodology that is mapped directly to the requirements set forth by the PCI Security Council.

We have been providing HIPAA Security readiness and compliance assessments and the underlying testing requirements (External and Internal Penetration Testing, Vulnerability Scanning and Assessment, Wireless Testing, and Social Engineering Assessments) for clients since the Security Rule was announced in 2005. Clients include nearly all the sub-industries within health care, as well as public agencies, and private companies required to be in compliance. CLA has developed a standard process/methodology that is mapped directly to the requirements set forth by the HIPAA Security Rule and the underlying NIST standards framework.

On an annual basis, CLA's cybersecurity professionals present at seminars and teach hands on classes focused on IT audit techniques, vulnerability assessment, and penetration testing. These seminars are offered through CLA directly several times per year, as well as our teaming with national, regional, state and local associations such as ISACA, the Minnesota Government IT Symposium, the Florida Government Finance Officers Association, the Independent Community Bankers of America, and many others. Our professionals are active in a variety of associations, and we actively sponsor Cyber Collegiate Defense competitions and Cyber Security training institutes in conjunction with the Minnesota Cyber Security Careers Consortium (*mnc3.advanceitmn.org)*. They are actively sought out as instructors for the services we provide, including penetration testing, IT auditing, SOC assessments and PCI-DSS.

Our professionals are people with character who invest their emotional capital in a vision they understand and adopt as their own to provide CLA's competitive advantage—emotional ownership. They want to succeed personally, they want our Firm to succeed, and above all, they want those they are serving to succeed.

Technical qualifications

Following is a listing of the information management systems and security tools that CLA has experience with as a result of previous projects.

Security Tools: Our security assessment services rely on a combination of tools that are developed internally by CLA security professionals, as well as open-source and commercially available software. While the core tools used by our practice remain the same, our professionals are constantly on the lookout for new tools and utilities to continually enhance their capabilities.

- **Internally developed tools to perform the following:**
  - *Audit scripts for various database applications*
  - *Automated drive mapping utility*
  - *Keystroke loggers for remote monitoring*
  - *Password changing utility*
  - *Remote access command prompt management tool*
  - *Remote host configuration auditing tool*
  - *Various wireless attack programs and scripts*

- **Free / Open Source Tools:**
  - Aircrack Suite
  - AirSnort
  - Autopsy Forensic Browser
  - CAIN
  - CIS software & benchmarks:
    - RAT
    - OS benchmarks
  - Dictgen
  - DumpACL
  - Hydra
  - John the Ripper
  - Kismet
  - Metasploit Framework
  - Zed Attack Proxy
  - Visual Studio
  - MBSA
  - BeEF
  - W3af
  - Nikto
  - SET
  - Dsniff
  - Wireshark
  - VirtualBox
  - SQLmap
  - Medusa
  - THCSSLCheck
  - NBTEnum
  - Netcat
  - Netstumbler
  - Nmap
  - pwdump2
  - Sleuthkit
  - VNC
  - SQLPing3
  - Mana Toolkit
  - libesedb
  - rcracki
  - DNSenum
  - DirBuster
  - DNSRecon
  - IKEScan
  - RAWR
  - Sysinternals Suite
  - LdapAdmin
  - Maltego
  - Recon-ng
  - Impacket
  - Responder
  - Mimikatz
  - OllyDbg
  - PowerSploit
  - PowerShell Empire
  - Veil Framework
  - Windows Credential Editor

- **Commercial Tools:**
  - EnCase Forensic Edition
  - LC5
  - Microsoft OS & apps
    - Resource kits
    - Enterprise Manager
    - Query Analyzer
  - Nessus
  - pcAnywhere
  - Sandstorm PhoneSweep
  - Silent Watch
  - SolarWinds
  - SpyTech
  - VMware Fusion
  - Burp Suite
  - IDA Pro
  - Hyena
  - SAINT
  - Qualys Guard

Scope of work – Exhibit E

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.

Tast 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.

References

We are pleased to provide you with the following references, who have used our cybersecurity assessment and consulting services. Please do not hesitate to contact any of the individuals listed regarding the value provided by CLA's Cybersecurity Services Group.

Client	Contact Name	Contact Telephone/Email
Sarasota County *Sarasota, FL*	Scott Gibbs Enterprise Systems Architect	941/861-2130 sgibbs@scgov.net
Services performed: External and internal network penetration testing, internal vulnerability assessment, web application testing, wireless assessment, PCI gap assessment and vulnerability scanning, other audit and accounting services		
City of Safety Harbor *Safety Harbor, FL*	June Solanes Finance Director	727/724-1555 x1222 jsolanes@cityofsafetyharbor.com
Services performed: External and internal penetration testing, internal vulnerability assessment, and PCI compliance		
Lake County *Lake County, FL*	Terri Freeman Inspector General	352/253-4937 tfreeman@lakecountycleak.org
Services performed: Data governance and HIPAA security risk assessment, general controls review, vendor management assessment, external and internal network penetration testing, internal vulnerability assessment, web application testing, and wireless assessment.		
Polk County Florida BOCC *Bartow, FL*	Phil Lambert Security Administrator	863/534-7564 phillambert@polk-county.net
Services performed: External Penetration Testing, Web Application Penetration Testing, Internal Vulnerability Assessment, Wireless Assessment, Social Engineering Assessments, and IT General Controls Reviews.		
City of Phoenix *Phoenix, AZ*	Shannon Lawson CISO/ACIO	480/536-3018 Shannon.Lawson@phoenix.gov
Services performed: PCI Compliance Assessment, IT Risk Assessment, Web Application Penetration, External and Internal Penetration Testing		
Pinellas Suncoast Transit Authority	Kessia Harris Director of Information Technology	727/540.1982 KHarris@psta.net
Services performed: External and Internal Penetration Testing		

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 March 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 June 30, 2025

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

Mitigation – Expected July 2025 through September 2025

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

Follow-up Assessment – Expected October 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-November 2025

- 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.

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
Total Estimate	**$334,325**

***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

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

Our last word on fees – we are committed to serving you. Therefore, if fees are a deciding factor in your selection of a professional services firm, we would appreciate the opportunity to discuss with you the scope of our audit plan.

At CLA, it's more than just getting the job done…

Quality control procedures and peer review report

In the most recent peer review report, dated November 2022, we received a rating of ***pass***, which is the most positive report a firm can receive. We are proud of this accomplishment and its strong evidence of our commitment to technical excellence and quality service.

In addition to an external peer review, we have implemented an intensive internal quality control system to provide reasonable assurance that the firm and our personnel comply with professional standards and applicable legal and regulatory requirements. Our quality control system includes the following:

- A quality control document that dictates the quality control policies of our firm. In many cases, these policies exceed the requirements of standard setters and regulatory bodies. Firm leadership promotes and demonstrates a culture of quality that is pervasive throughout the firm's operations. To monitor our adherence to our policies and procedures, and to foster quality and accuracy in our services, internal inspections are performed annually.
- Quality control standards as prescribed by the AICPA. The engagement principal is involved in the planning, fieldwork, and post-fieldwork review. In addition, an appropriately experienced professional performs a risk-based second review of the engagement prior to issuance of the reports.
- Hiring decisions and professional development programs designed so personnel possess the competence, capabilities, and commitment to ethical principles, including independence, integrity, and objectivity, to perform our services with due professional care.
- An annual internal inspection program to monitor compliance with CLA's quality control policies. Workpapers from a representative sample of engagements are reviewed and improvements to our practices and processes are made, if necessary, based on the results of the internal inspection.
- Strict adherence to the AICPA's rules of professional conduct, which specifically require maintaining the confidentiality of client records and information. Privacy and trust are implicit in the accounting profession, and CLA strives to act in a way that will honor the public trust.
- A requirement that all single audit engagements be reviewed by a designated single audit reviewer, thereby confirming we are in compliance with the standards set forth in the *Uniform Guidance*.

Cherry Bekaert LLP
Your Guide Forward

Report on the Firm's System of Quality Control

To the Principals of CliftonLarsonAllen LLP
and the National Peer Review Committee

We have reviewed the system of quality control for the accounting and auditing practice of CliftonLarsonAllen LLP (the "Firm") applicable to engagements not subject to PCAOB permanent inspection in effect for the year ended May 31, 2022. Our peer review was conducted in accordance with the Standards for Performing and Reporting on Peer Reviews established by the Peer Review Board of the American Institute of Certified Public Accountants ("Standards").

A summary of the nature, objectives, scope, limitations of, and the procedures performed in a System Review as described in the Standards, may be found at www.aicpa.org/prsummary. The summary also includes an explanation of how engagements identified as not performed or reported on in conformity with applicable professional standards, if any, are evaluated by a peer reviewer to determine a peer review rating.

Firm's Responsibility

The Firm is responsible for designing and complying with a system of quality control to provide the Firm with reasonable assurance of performing and reporting in conformity with the requirements of applicable professional standards in all material respects. The Firm is also responsible for evaluating actions to promptly remediate engagements deemed as not performed or reported on in conformity with the requirements of applicable professional standards, when appropriate, and for remediating weaknesses in its system of quality control, if any.

Peer Reviewer's Responsibility

Our responsibility is to express an opinion on the design of and compliance with the Firm's system of quality control based on our review.

Required Selections and Considerations

Engagements selected for review included engagements performed under *Government Auditing Standards*, including compliance audits under the Single Audit Act; audits of employee benefit plans; audits performed under FDICIA; and examinations of service organizations (SOC 1® and SOC 2® engagements).

As a part of our peer review, we considered reviews by regulatory entities as communicated by the Firm, if applicable, in determining the nature and extent of our procedures.

Opinion

In our opinion, the system of quality control for the accounting and auditing practice of CliftonLarsonAllen LLP applicable to engagements not subject to PCAOB permanent inspection in effect for the year ended May 31, 2022, has been suitably designed and complied with to provide the Firm with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. Firms can receive a rating of *pass*, *pass with deficiency(ies)* or *fail*. CliftonLarsonAllen LLP has received a peer review rating of *pass*.

Cherry Bekaert LLP

Cherry Bekaert LLP
Charlotte, North Carolina
November 18, 2022

cbh.com

Appendices

Appendix A: Section 8.1.1. Contractor Acceptance Form and W-9

Appendix B: Section 8.1.2. OPENGOV Electronic Pricing Proposal and Delivery Days

Appendix C: Section 9. Pricing Proposal

Appendix D: Section 10. Sample Agreement

Appendix E: Disclaimer

Appendix A: Section 8.1.1 Contractor Acceptance Form

VENDOR SUBMITTAL ACKNOWLEDGEMENT FORM

It is the policy of Pinellas County, Board of County Commissioners, to accept the lowest responsive and responsible or highest ranked submittal received meeting specifications. No changes requested by a vendor due to an error in pricing will be considered after the advertised solicitation opening date. By signing this Vendor Submittal Acknowledgment Form, vendors are attesting to their awareness and acceptance of this policy and agreeing to all solicitation of terms and conditions, including any insurance requirements.

Vendor Name (as shown on W-9): **CliftonLarsonAllen, LLP**

Doing Business As (DBA) (if applicable):

Mailing Address (as shown on W-9): **220 S 6th Street, Ste 300**

City, State, Zip (as shown on W-9): **Minneapolis, MN 55402**

Vendor Email (primary company email): N/A

Remit to address (as shown on vendor invoice): **CliftonLarsonAllen LLP P.O. Box 740863 Atlanta, GA 30374-0863**

Federal Tax ID (FEIN) **#: 41-0746749**

SAM.gov UEID No**.: DJH5STL3MUK7**

Dun & Bradstreet D-U-N-S® UEID No. (if applicable): **077633311**

Vendor Contact Information

Contact Name: **David Scaffido**

Phone Number: **571-227-9668**

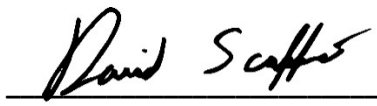
Email Address: David.Scaffido@CLAconnect.com

Payment Terms: Net 45 (per Florida Statute F.S. 218.73)	N/A**%**	N/A	**Days**
Deposit (if required) has been paid in the amount of $	N/A		

Proper Corporate Identity is needed for a firm registered with the Florida Division of Corporations. Please visit *dos.myflorida.com/sunbiz/* for this information. It is essential to return a copy of your W-9 with your submittal.

Please see on following page CliftonLarsonAllen, LLP W-9.

I hereby agree to abide by all terms and conditions of this solicitation, including all insurance requirements, and certify that I am authorized to sign this solicitation for the vendor.

Authorized Signature: 

Print Name: _David Scaffido_____

Title: __Principal_____

THIS FORM MUST BE RETURNED WITH YOUR RESPONSE

Form **W-9**
(Rev. March 2024)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

Go to *www.irs.gov/FormW9* for instructions and the latest information.

Give form to the requester. Do not send to the IRS.

Before you begin. For guidance related to the purpose of Form W-9, see *Purpose of Form*, below.

Print or type. See *Specific Instructions* on page 3.

1 Name of entity/individual. An entry is required. (For a sole proprietor or disregarded entity, enter the owner's name on line 1, and enter the business/disregarded entity's name on line 2.)

CliftonLarsonAllen LLP

2 Business name/disregarded entity name, if different from above.

3a Check the appropriate box for federal tax classification of the entity/individual whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor ☐ C corporation ☐ S corporation ☑ Partnership ☐ Trust/estate

☐ LLC. Enter the tax classification (C = C corporation, S = S corporation, P = Partnership) . . . . .

Note: Check the "LLC" box above and, in the entry space, enter the appropriate code (C, S, or P) for the tax classification of the LLC, unless it is a disregarded entity. A disregarded entity should instead check the appropriate box for the tax classification of its owner.

☐ Other (see instructions)

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any)

Exemption from Foreign Account Tax Compliance Act (FATCA) reporting code (if any)

(Applies to accounts maintained outside the United States.)

3b If on line 3a you checked "Partnership" or "Trust/estate," or checked "LLC" and entered "P" as its tax classification, and you are providing this form to a partnership, trust, or estate in which you have an ownership interest, check this box if you have any foreign partners, owners, or beneficiaries. See instructions . . . . . ☐

5 Address (number, street, and apt. or suite no.). See instructions.

220 S 6th St, Ste 300

Requester's name and address (optional)

6 City, state, and ZIP code

Minneapolis MN 55402

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. See also *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

			–			–				

or

Employer identification number

4	1	–	0	7	4	6	7	4	9

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and, generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here | **Signature of U.S. person** Marta Vogel | **Date** 1-2-25

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

What's New

Line 3a has been modified to clarify how a disregarded entity completes this line. An LLC that is a disregarded entity should check the appropriate box for the tax classification of its owner. Otherwise, it should check the "LLC" box and enter its appropriate tax classification.

New line 3b has been added to this form. A flow-through entity is required to complete this line to indicate that it has direct or indirect foreign partners, owners, or beneficiaries when it provides the Form W-9 to another flow-through entity in which it has an ownership interest. This change is intended to provide a flow-through entity with information regarding the status of its indirect foreign partners, owners, or beneficiaries, so that it can satisfy any applicable reporting requirements. For example, a partnership that has any indirect foreign partners may be required to complete Schedules K-2 and K-3. See the Partnership Instructions for Schedules K-2 and K-3 (Form 1065).

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS is giving you this form because they

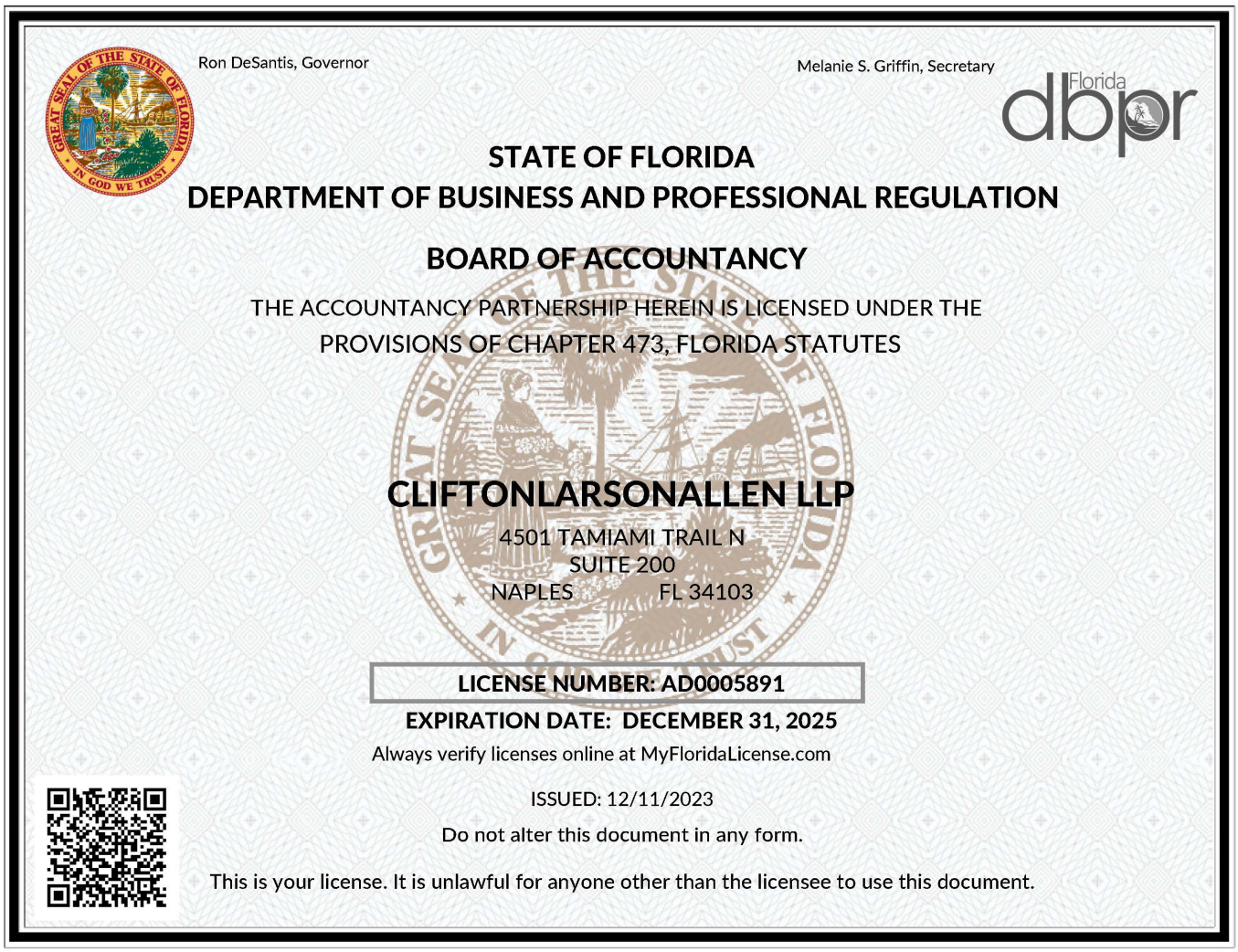
Appendix B: Section 8.1.2. OPENGOV Electronic Pricing Proposal and Delivery Days

PRICING PROPSAL

Line Item	Description	Quantity	Unit of Measure	Unit Cost	Total
1	Lump Sum	1	each	$**334,325**	$**334,325**
	Total				$**334,325**

DELIVERY 30 DAYS AFTER RECEIPT OF ORDER
An award may not be issued without proof that your firm is registered with the Florida Division of Corporations, as per Florida Statute §607.1501 www.flsenate.gov/Laws/Statutes/2011/607.1501.
A foreign corporation (foreign to the State of Florida) may not transact business in this state until it obtains a certificate of authority from the Department of State. Please visit dos.myflorida.com/sunbiz/ for this information on how to become registered.

See following page for CliftonLarsonAllen, LLP Certificate to do business in the state of Florida.



Ron DeSantis, Governor

Melanie S. Griffin, Secretary

Florida dbpr

STATE OF FLORIDA
DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

BOARD OF ACCOUNTANCY

THE ACCOUNTANCY PARTNERSHIP HEREIN IS LICENSED UNDER THE
PROVISIONS OF CHAPTER 473, FLORIDA STATUTES

CLIFTONLARSONALLEN LLP

4501 TAMIAMI TRAIL N
SUITE 200
NAPLES FL 34103

LICENSE NUMBER: AD0005891

EXPIRATION DATE: DECEMBER 31, 2025

Always verify licenses online at MyFloridaLicense.com

ISSUED: 12/11/2023

Do not alter this document in any form.

This is your license. It is unlawful for anyone other than the licensee to use this document.

Appendix C: Section 9. Pricing Proposal

Line Item	Description	Quantity	Unit of Measure	Unit Cost	Total
1	Lump Sum	1	each	$**334,325**	$**334,325**
	Total				$**334,325**

Appendix E: Section 10. Sample Agreement

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 [Contractor Legal Name] whose primary address is [Contractor Legal Address] (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.

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 shall be for a period of twelve (12) months. The Parties may extend the term of this Agreement for one (1) additional twelve (12) month period pursuant to the same terms, conditions, and pricing set forth in the Agreement.

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 $334,325 for 12 months without a written amendment to this Agreement.

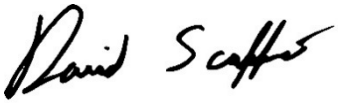
2. In no event will annual expenditures exceed $334,325 within any given fiscal year without a written amendment to the Agreement.

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: CliftonLarsonAllen, LLP

Signature: 

Print Name and Title: David Scaffido, Principal

Date: February 27, 2025

For County:

Signature:

Print Name and Title:

Date:

Disclaimer

CONTRACTOR's services cannot be relied upon to disclose all errors, fraud, or noncompliance with laws and regulations. Except as described in this Agreement or any applicable SOW, CONTRACTOR has no responsibility to identify and communicate deficiencies in COUNTY'S internal controls as part of any services.

Limitation of remedies
These limitation of remedies provisions are not applicable for any audit or examination services provided to COUNTY.

Contractor's role is strictly limited to the services described in an SOW, and Contractor offers no assurance as to the results or ultimate outcomes of any services or of any decisions that COUNTY may make based on our communications with Contractor. COUNTY agrees that it is appropriate to limit the liability of Contractor, its partners, principals, directors, officers, employees, and agents (each a "Contractor party").

COUNTY further agrees that COUNTY will not hold Contractor or any other Contractor party liable for any claim, cost, or damage, whether based on warranty, tort, contract, or other law, arising from or related to this MSA, the services provided under an SOW, the work product, or for any plans, actions, or results of an SOW, except to the extent authorized by this Contract. In no event shall any Contractor party be liable to COUNTY for any indirect, special, incidental, consequential, punitive, or exemplary damages, or for loss of profits or loss of goodwill, costs, or attorney fees.

The exclusive remedy available to COUNTY shall be the right to pursue claims for actual damages that are directly caused by acts or omissions that are breaches by a Contractor party of Contractor's duties owed under this Contract and the specific SOW thereunder, but any recovery on any such claims shall not exceed the fees actually paid by COUNTY to Contractor pursuant to the SOW that gives rise to the claim.

Time limitations
The nature of CONTRACTOR's services makes it difficult, with the passage of time, to gather and present evidence that fully and fairly establishes the facts underlying any dispute that may arise between COUNTY and CONTRACTOR. The parties agree that, notwithstanding any statute or law of limitations that might otherwise apply to a dispute, including one arising out of this Agreement or the services performed under an SOW, for breach of contract or fiduciary duty, tort, fraud, misrepresentation or any other cause of action or remedy, any action or legal proceeding by COUNTY against CONTRACTOR must be commenced as provided below, or COUNTY shall be forever barred from commencing a lawsuit or obtaining any legal or equitable relief or recovery. An action to recover on a dispute shall be commenced within these periods ("Limitation Period"), which vary based on the services provided, and may be modified as described in the following paragraph:

Service	Time after the date CONTRACTOR delivers the services or work product*
Tax Consulting Services	36 months
Tax Return Preparation	36 months
Examination, compilation, and preparation services related to prospective financial statements	12 months
Audit, review, examination, agreed-upon procedures, compilation, and preparation services other than those related to prospective financial information	24 months
All Other Services	12 months

* pursuant to the SOW on which the dispute is based

If this Agreement is terminated or COUNTY'S ongoing relationship with CONTRACTOR is terminated, then the applicable Limitation Period is the lesser of the above periods or 12 months after termination of this Agreement or COUNTY'S ongoing relationship with CONTRACTOR. The applicable Limitation Period applies and begins to run even if COUNTY has not suffered any damage or loss, or have not become aware of the existence or possible existence of a dispute.

CONTRACTOR will not disclose any of COUNTY'S confidential, proprietary, or privileged information to any person or party, unless COUNTY authorizes CONTRACTOR to do so, it is published or released by COUNTY, it becomes publicly known or available other than through disclosure by CONTRACTOR, or disclosure is required by law, regulation or professional standard. This confidentiality provision does not prohibit CONTRACTOR from disclosing COUNTY's information to one or more of CONTRACTOR's affiliated companies in order to provide services that COUNTY has requested from CONTRACTOR or from any such affiliated COUNTY. Any such affiliated COUNTY shall be subject to the same restrictions on the use and disclosure of COUNTY's information as apply to CONTRACTOR. COUNTY also consents to CONTRACTOR's disclosure of information regarding the nature of services CONTRACTOR provide to COUNTY to another independent network member of CLA Global, for the limited purpose of complying with professional obligations regarding independence and conflicts of interest.

The workpapers and files supporting the services CONTRACTOR performs are the sole and exclusive property of CONTRACTOR and constitute confidential and proprietary information. CONTRACTOR does not provide access to its workpapers and files to COUNTY or anyone else in the normal course of CONTRACTOR. Unless required by law or regulation to the contrary, CONTRACTOR retain its workpapers and files in accordance with its record retention policy that typically provides for a retention period of seven years. After this period expires, CONTRACTOR's workpapers and files will be destroyed. Furthermore, physical deterioration or catastrophic events may shorten the time CONTRACTOR's records are available. The workpapers and files of CONTRACTOR are not a substitute for COUNTY's records.

Pursuant to authority given by law, regulation or professional standards CONTRACTOR may be requested to make certain workpapers and files available to a regulator for its regulatory oversight purposes. CONTRACTOR will notify COUNTY of any such request, if permitted by law. Access to the requested workpapers and files will be provided to the regulator under the supervision of CONTRACTOR personnel

and at a location designated by CONTRACTOR. Furthermore, upon request, CONTRACTOR may provide copies of selected workpapers and files to such regulator. The regulator may intend, or decide, to distribute the copies or information contained therein to others, including other governmental agencies.

CONTRACTOR may, at times, utilize external web applications to receive and process information from its clients; however, any sensitive data, including protected health information and personally identifiable information, must be redacted by COUNTY to the maximum extent possible prior to uploading the document or file. In the event that COUNTY is unable to remove or obscure all sensitive data, please contact CONTRACTOR to discuss other potential options for transmitting the document or file.

CONTRACTOR and certain owners of CONTRACTOR are licensed by the California Board of Accountancy. However, CONTRACTOR has owners not licensed by the California Board of Accountancy who may provide services under this Agreement. If COUNTY has any questions regarding licensure of the personnel performing services under this Agreement, please do not hesitate to contact CONTRACTOR.

CONTRACTOR regularly aggregates anonymized client data and perform a variety of analyses using that aggregated data. Some of these analyses are published to clients or released publicly. However, CONTRACTOR is always careful to preserve the confidentiality of the separate information that CONTRACTOR obtains from each client, as required by the AICPA Code of Professional Conduct and various laws. COUNTY's acceptance of this Agreement will serve as COUNTY's consent to CONTRACTOR's use of anonymized data in performing and reporting on these cost comparison, performance indicator and/or benchmarking analyses.

CONTRACTOR may, at times, use third-party software applications to perform services under this Agreement. COUNTY acknowledges the software Contractor may have access to its data.