LanceSoft, Inc's Response

County of Hawaii

Professional Services

LanceSoft, Inc.
2121 Cooperative Way, Suite 130,
Herndon VA 20171
Phone: (+1) 914-217-9600
Fax: 703-889-6500

Point of Contact: Mr. Venkat Ramamohan
Phone: (+1) 914-217-9600
E-mail: marketing@lancesoft.com

CAGE Code: 4AUM9
DUNS: 154610971
TIN: 54-1974095

LanceSoft Inc. is Minority Owned Business Enterprise (MBE) and a Diversity Owned Company in the USA & Canada

http://www.lancesoft.com/

Table of Contents

1. COVER LETTER

Response to County of Hawaii – Professional Services

Dear Corey Stone,

On behalf of the entire team at LanceSoft, I am pleased to present our collective response to the County of Hawaii – Professional Services. We appreciate the opportunity to offer our services.

Our proposal in response to the above solicitation is 100 percent compliant with all requirements and in many cases, we exceed the requirements to provide County of Hawaii with a high-value solution to the requirement.

Established in 2000, LanceSoft is a privately-owned S corporation, headquartered at 2121 Cooperative Way, Suite 130, Herndon VA 20171 and with our regional headquarters in Richmond Hill, ON has over 25 years of experience in providing IT, engineering, scientific, and professional talent to companies across diverse domains and geographies worldwide. LanceSoft operates through a network of more than 28 offices throughout North America, including additional offices in Canada, India, Hong Kong, Mexico, the Philippines, and various European and Asian countries.

We take pride in our strong partnerships with top companies and our deep relationships with IT and non-IT consultants across the globe. Our extensive experience and global presence uniquely position us to deliver high-quality solutions tailored to meet the specific needs of our clients.

We appreciate the opportunity to submit our proposal and look forward to the possibility of partnering with you on this project.

CONTACT FOR THIS PROPOSAL

I, the undersigned, Mr. Venkat Ramamohan, of LanceSoft, INC will be the POC (Point of Contact) for the County of Hawaii during project execution. I am authorized to sign the enclosed offer and will be the designated authorized negotiator for a contract resulting from this offer. You may reach me (+1) 914-217-9600 via phone, or via e-mail at marketing@lancesoft.com

Respectfully,

For LanceSoft Inc.,

LANCESOFT, INC. CORPORATE SEAL 2000 VIRGINIA

Venkat Ramamohan

Senior VP & Global Head

2121 Cooperative Way | Suite 130 | Herndon | VA 20171 | 914-217-9600 Phone | 703-889-6500 Fax

2. EXECUTIVE SUMMARY

LanceSoft reiterates its gratitude to County of Hawaii for the opportunity to submit our response to its EOI for Professional Services. We appreciate the chance to showcase our capabilities and propose tailored solutions to meet your needs.

With an illustrious history spanning over 25 years, LanceSoft specializes in delivering exceptional Cybersecurity solutions, Infrastructure maintenance, Network support, and a myriad of other IT services. LanceSoft takes pride in its proven ability to provide scalable, high-quality solutions to esteemed clients worldwide.

Purpose, People, Performance and Partnerships: LanceSoft is built upon four pillars: Purpose, People, Performance and Partnerships. In undertaking these principles, we acknowledge our responsibility to adhere to them. These core pillars are who we are, and where we come from. They are what we base our decisions on. They frame how we interact with our clients, our vendors, our community, and ourselves. They form our culture and shape our relationships and our work.

LanceSoft, headquartered in Herndon, Virginia, with our regional headquarters in Richmond Hill, ON, offers global IT services to clients. We are uniquely positioned to collaborate with the County of Hawaii on this initiative. Our proposal reflects our dedication to establishing a lasting partnership with the County of Hawaii, focusing on process-oriented methodologies, optimization, automation, and service excellence.

With extensive experience serving clients globally across the USA and Canada. LanceSoft is confident that our approach will align with the objectives of the County of Hawaii. We are eager to engage with the County of Hawaii in a long-term strategic partnership. Through this proposal, LanceSoft aims to showcase our approach, governance practices, and process optimization capabilities, demonstrating how we can contribute to creating a resilient and scalable service delivery framework for the County of Hawaii.

County of Hawaii Needs and LanceSoft Selection of Professional Services:

Lancesoft, Inc. wishes to opt for the **Department of Information Technology's - Computer Engineering** category for proposing its expertise and area of interest.

3. APPENDIX: COMPANY OVERVIEW - LANCESOFT INC.

With a global workforce exceeding 6,500 employees and an annual revenue surpassing $400 million, LanceSoft is a premier provider of comprehensive IT Consulting, Solutions, Development, Cybersecurity Services, Infrastructure, and Support Services. Our commitment to excellence is reflected in our diverse portfolio of clients spanning various industries, including Public Sector, State and Federal Clients, Information Technology, Finance, Banking, Automotive, Engineering, Education, Oil & Gas, Petrochemicals, Energy, Aerospace, Semiconductor, Telecom, Retail, and more. LanceSoft specializes in comprehensive Cybersecurity Services, spanning various industries. Our offerings include proactive IT support, network management, cybersecurity, cloud computing, migration, and strategic consulting. With a dedicated team, we ensure seamless operations, proactive maintenance, and swift issue resolution, allowing businesses to focus on core objectives. Our tailored approach delivers scalable, reliable solutions for efficiency, security, and growth.

Local presence: LanceSoft has established itself as a leading accounting and consulting practice with a strong local presence. Our client base spans from Fortune 500 companies to ambitious startups, showcasing the diversity of our services. We take pride in serving a wide range of clients, from multinational corporations to middle-market enterprises. Our strength lies in our collaborative approach, bringing together diverse talents to deliver exceptional results.

In addition to our client-focused work, LanceSoft is deeply committed to serving the community and promoting diversity and inclusivity. Our TADAH (Together We Achieve Diversity and Harmony) program exemplifies this commitment by providing equal opportunities for individuals from various backgrounds.

Public sector presence: LanceSoft has maintained a strong presence in the public sector, providing cybersecurity services to federal, state, and local government entities for over 24 years. Our clientele includes cities, counties, states, federal organizations, mass transit authorities, airports, cultural complexes, housing authorities, school districts, workforce agencies, welfare agencies, colleges, and universities.

We are dedicated to addressing complex challenges and delivering high-quality service to enable our clients to enhance customer service for their constituents. With extensive experience in the public sector, we have developed a deep understanding of diverse management issues and government program requirements. Our track record reflects our commitment to excellence and our ability to navigate the unique landscape of public sector environments.

Global Footprint: Operating across the globe, LanceSoft has established a strong presence in numerous regions, allowing us to deliver tailored solutions to clients worldwide .We have an international footprint with 28 support offices throughout North America, Four (4) country offices in Canada, Eleven (11) in India, Three (3) in Philippines, Two (2) in Malaysia and one each in Hongkong, Mexico, UK, Ireland, Netherlands, Czech Republic, Hungary, Vietnam, Italy, France, Norway, Poland, Switzerland, Romania, Turkey, Estonia, Singapore, Thailand, Indonesia, Bangladesh, China, Lithuania, Japan, Ethiopia, UAE, Bulgaria, and Australia underscores our ability to provide “follow the sun” model support.

Quality and Certifications: LanceSoft's dedication to cybersecurity excellence is evident through its attainment of various industry-leading quality certifications. These include ISO certifications and SOC certifications, which validate our strict adherence to internationally recognized standards for information security management and assurance. These certifications serve as a testament to our unwavering commitment to upholding the highest standards of security and compliance across all facets of our operations. By obtaining these certifications, LanceSoft ensures that our clients can place their trust in the integrity and reliability of our cybersecurity solutions, providing them with the assurance and confidence they need in their data protection measures.

Among our notable certifications are ISO 27001 for Information Security Management Systems (ISMS), ISO 9001 for Quality Management Systems (QMS), and ISO 14001 for Environmental Management Systems. These ISO certifications underscore our dedication to maintaining superior standards in information security, quality, and environmental responsibility across our suite of cybersecurity solutions.
Furthermore, LanceSoft has also achieved SOC certification, which signifies our strict adherence to stringent security standards and practices in managing and safeguarding client data. This certification reinforces our commitment to delivering secure and reliable cybersecurity solutions, thereby bolstering trust and confidence in our services among our valued clients and partners.

Achievements and Awards: LanceSoft takes great pride in its achievements and recognition within the industry, showcasing our commitment to excellence and innovation. Over the years, we have garnered numerous awards and accolades, underscoring our leadership in providing cutting-edge IT solutions and services. Our dedication to delivering exceptional value to clients has been repeatedly acknowledged by esteemed organizations and industry bodies, further solidifying our reputation as a trusted partner in the technological landscape.

Among our notable achievements, LanceSoft has been honored with prestigious awards for excellence in areas such as cybersecurity, IT consulting, and workforce solutions. These accolades serve as a testament to our relentless pursuit of innovation, quality, and client satisfaction. Additionally, our commitment to fostering diversity and inclusion has been recognized through various awards, highlighting our efforts to create a workplace culture that celebrates and empowers individuals from diverse backgrounds.

Furthermore, LanceSoft's contributions to the community and corporate social responsibility initiatives have been applauded by various organizations, reflecting our commitment to making a positive impact beyond business boundaries. Through our dedication to excellence, innovation, and social responsibility, LanceSoft continues to set new benchmarks in the industry, driving positive change and delivering value to clients, employees, and communities alike.

Strategic Client Services Team: LanceSoft adheres to a meticulously structured and thoroughly documented approach to team management, ensuring uninterrupted business operations, transparency, and seamless communication between County of Hawaii and LanceSoft stakeholders throughout our collaboration. In line with our commitment to excellence, we are pleased to offer County of Hawaii the specialized support of our strategic client services team, dedicated to ensuring precise service delivery and exceeding all requirements with utmost professionalism.

4. APPENDIX : REFERENCES

For over twenty-four years, LanceSoft has demonstrated its professional commitment to providing Cybersecurity Services. The table below provides a broad overview of LanceSoft's experience in providing "Cybersecurity Services"

REFERENCE 1	
Name	Texas Community Health Choice
Address	Houston, TX
Telephone Number	+1 (713) 295-2313
Email	Richard.Hobbs@CommunityHealthChoice.org
Point of Contact	Richard Hobbs - Manager Information Security
Project Description	LanceSoft's team conducted a comprehensive grey box penetration testing, encompassing internal, external, and wireless networks, as well as social phishing tests and a thorough vulnerability assessment for all web applications, networks, systems, and workstations (over 20,000 in total). The objective of this testing was to identify and mitigate any vulnerabilities or weaknesses that could be exploited by malicious actors. Our team of cybersecurity experts simulated real-world attack scenarios to exploit these vulnerabilities from the perspective of potential attackers, ensuring a robust defense mechanism. Additionally, for workstations, LanceSoft performed a Remote User Security assessment. This assessment aimed to enhance data privacy and implement robust security controls for both office-based and remote workers. This dual focus on internal security and remote access ensures that all entry points are fortified, providing comprehensive protection for the organization's digital assets.

REFERENCE 2	
Name	Gwinnett County Government (Georgia)
Address	75 Langley Drive, Lawrenceville, GA 30046
Telephone Number	770-822-7905
Email	Melanie.Brooks@gwinnettcounty.com
Point of Contact	Melanie Brooks /IT Business Manager
Project Description	Gwinnett County Government in Georgia partnered with LanceSoft to enhance its cybersecurity posture through Managed Detection and Response (MDR), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) solutions. These services provided 24/7 monitoring, real-time threat detection, and automated incident response, significantly reducing successful cyber attacks and improving incident resolution times. The XDR solution offered comprehensive visibility across the IT environment, enabling proactive threat management and operational efficiency. LanceSoft's

	tailored security solutions ensured the protection of sensitive government data and critical infrastructure, demonstrating their expertise in meeting the unique needs of government clients.

REFERENCE 3	
Name	Commonwealth of Massachusetts
Address	Office of Financial Management – 7th 600 Washington Street, Boston, MA 02111
Telephone Number	617-348-5029
Email	Kara.Banderier@state.ma.us
Point of Contact	Kara Banderier/EOHHS IT Contractor Liaison
Project Description	LanceSoft provided a suite of advanced cybersecurity services to the Commonwealth of Massachusetts, significantly enhancing its IT security infrastructure. Our team conducted rigorous penetration testing to proactively identify vulnerabilities within databases and applications, addressing weaknesses before they could be exploited. Through red teaming exercises, we simulated sophisticated cyber-attacks, allowing the Commonwealth to refine its defensive strategies and improve its incident response capabilities. Our endpoint security services ensured robust protection for all devices, safeguarding sensitive information from unauthorized access and malware threats. Remote security monitoring provided continuous surveillance of the IT environment, allowing for real-time detection and response to potential security incidents. Additionally, we assisted in optimizing their cloud services, ensuring secure data storage and management while maintaining compliance with industry standards. These comprehensive efforts not only fortified the Commonwealth's security posture but also provided peace of mind, knowing that their critical systems and data were well-protected against evolving cyber threats.

REFERENCE 4	
Name	Alberta Blue Cross
Address	Edmonton, AB, Canada
Telephone Number	+1 (780) 498-8278
Email	kjaising@ab.bluecross.ca
Point of Contact	Kushal Jaisingh - Security Analyst
Project Description	LanceSoft team conducted comprehensive penetration testing on databases and applications to proactively identify and address security vulnerabilities. This testing aimed to prevent unauthorized access or disclosure of sensitive information, such as customer data, financial records, or intellectual property. The team meticulously

	examined potential weaknesses in software code, configuration settings, input validation, authentication mechanisms, and access controls. By identifying these vulnerabilities, LanceSoft ensured that critical security measures were reinforced, safeguarding the integrity and confidentiality of vital organizational information. This proactive approach not only enhances the overall security posture but also mitigates risks associated with data breaches and unauthorized access.

REFERENCE 5	
Name	Bell Canada
Address	Quebec, Canada
Telephone Number	+1 (613) 785-4016
Email	oksana.vassilieva@bell.ca
Point of Contact	Oksana Vassilieva - Senior Manager Cyber Security
Project Description	LanceSoft's team conducted a thorough annual penetration testing exercise on the network and devices with the primary objective of identifying potential vulnerabilities. Our skilled cybersecurity experts simulated real-world attack scenarios to rigorously assess the security posture of both the network and connected devices. This proactive initiative involved comprehensive testing methodologies, enabling us to uncover a wide range of potential weaknesses. The detailed findings from this penetration testing allowed the organization to prioritize and address vulnerabilities promptly. As a result, the organization benefited from enhanced security measures, ensuring a robust and secure operational environment. This exercise not only fortified the existing infrastructure but also prepared the organization to effectively mitigate future cyber threats.

5. APPENDIX: TECHNOLOGY EXPERIENCE

Use Case: Comprehensive Cybersecurity Assessment for a Power Utility Company

Overview of the Project:
We conducted a comprehensive cybersecurity assessment for a large power utility company. The scope included evaluating computer operating systems, network infrastructure equipment, network security devices, and EMS/SCADA systems. Additionally, the assessment covered models of Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Remote Terminal Automation Controllers (RTACs), and other Intelligent Electronic Devices (IEDs).

Challenges:
The power utility company faced several challenges, including outdated and misconfigured computer operating systems, lack of visibility into network infrastructure, inadequate security configurations of network devices, and potential vulnerabilities in EMS/SCADA systems. Furthermore, there was a need to ensure the security of various models of RTUs, PLCs, RTACs, and IEDs, which were critical for the utility's operations.

How We Overcame the Challenges:

- We performed detailed vulnerability scans and configuration audits on Windows and Linux systems, identifying outdated software and misconfigurations. We recommended and assisted in implementing security patches, strengthening access controls, and enhancing system monitoring.
- Using advanced network discovery tools, we mapped the network topology and identified unauthorized devices. We provided recommendations to improve network segmentation, upgrade firmware, and secure configuration settings.
- We reviewed the deployment and configuration of IDS/IPS, firewalls, and SIEM systems. Our team fine-tuned detection rules and enhanced logging capabilities to ensure effective threat detection and response.
- We evaluated the security of SCADA applications, focusing on communication protocols and data integrity measures. We addressed vulnerabilities related to outdated software and unpatched systems by providing a detailed remediation plan.
- We assessed the hardware and software configurations of various RTUs, PLCs, RTACs, and IEDs. Recommendations included firmware updates, enhanced security controls, and regular maintenance to prevent unauthorized access and tampering.

Results:
The comprehensive assessment led to significant improvements in the utility’s cybersecurity posture. Outdated systems were patched, network segmentation was enhanced, and security configurations of critical devices were strengthened. The client achieved compliance with industry standards and regulatory requirements, ensuring a more secure and resilient infrastructure.

The proposed tools for facilitating the work also includes the following:

Technical Security Assessment Tools	Description
Wikto / Nikto	Web application vulnerability scanner
W3AF	Web Application Attack and Audit Framework
IronWASP	Web application vulnerability scanner
Brutus	Password brute forcing tool
Grendel Scan	Web application vulnerability scanner
Httprint	Webserver fingerprinting
Amap , ID Serv	Application Enumeration, Banner Grabbing
SSLscan	SSL/TLS identification
Burp-Suite	Web application vulnerability scanner and browser proxy
ZAP Proxy	Web application vulnerability scanner
SQLmap	Database security
Skip fish	Web application security reconnaussance tool
Wapiti	Black-box application security auditors with fuzzer injecting scripts
Back Track R5 / Kali linux	Penetration testing framework, Used for build and configuration reviews
Nmap,Amap,Megaping	Network Port Scanning and Reconnaissance
Nessus	Network Vulnerability Scanner
Nexpose	Network Vulnerability Scanner
Ncrack	Password brute forcing tool
Metasploit	Network Exploitation Framework with mulltiple exploits and payloads
Snmpcheck	Snmo Enumeration tool
Enum4linux	Linus Enumeration tool
Super Scan	Windows Enumeration tools
nslookup	Dns Enumeration tool
Cain and Abel	Password cracking, ARP poisoning DNS poisoning
Yersinia, Gobbler	DHCP Starvation attack tools
LOIC, DosHTTP	Denial of service attack tools
Ettercap, Wireshark	Sniffer
OpenVas	Vulnerability scanner, uncovering potential weaknesses in various software, including those overlooked by other tools
Wireshark	Network packet analyzer used to capture and analyze traffic, identifying vulnerabilities and tracking security incidents in the target network

6. APPENDIX: PROJECT TEAM STAFFING

6.1 The Right team - LanceSoft's proposed Key Personnels

Selecting the right professionals is the most important engagement decision for LanceSoft. We have assembled a talented and specialized team of individuals to serve you, who will deliver the value of their experience and knowledge of state and local governments. Accordingly, our team members provide a strong blend of relevant industry experience, technical proficiency, and understanding of your operations. Our flexibility and scalability allow us to provide a significant talent pool to extract resources, allowing for the appropriate fit per requirements.

In the below table we have provided our key personnels proposed for this project:

#	Role	Skill Set	Certifications
1	Security Analyst	• Security strategy and transformation • Security assessment and advisory • Security Engineering and Automation	CEH, CHFI, CPISI PCI DSS, ISO27001
2	Vulnerability Analyst	• Infrastructure Vulnerability Assessment • System testing	CEH, CPISI, MCP, MCSA
3	Penetration Tester	• Penetration testing of web applications, network devices, cloud implementations, and APIs • Vulnerability scanning • Creating penetration testing reports	Offensive Security Certified Professional, CISSP, AWS Certified, Microsoft Certified
4	Cloud Security Specialist	• Conduct cloud security assessments and risk assessments to identify potential vulnerabilities. • Monitor compliance with industry • standards and regulatory requirements in cloud environments.	Azure Security Engineer Associate
5	Security Architect	• Develop and implement security architectures and solutions to protect IT systems. • Conduct risk assessments to identify potential threats and vulnerabilities.	CISSP, CISM, CISA, CCSP, TOGAF (The Open Group Architecture Framework) Certification

		• Implement and manage security controls and countermeasures. • Oversee the continuous monitoring of the IT environment to detect and respond to security incidents.	
6	Operation Technology Security Engineer	• Conduct security assessments and vulnerability analyses of OT environments. • Design and implement security architectures tailored to OT environments. • Monitor OT networks and systems for security threats and anomalies. • Develop and maintain incident response plans for OT environments.	CISSP, GICSP, CSSA, ISA/IEC 62443 Cybersecurity Certifications (e.g., ISA/IEC 62443 Cybersecurity Fundamentals Specialist)
7	DFIR Specialist	• Monitor and analyze security alerts and logs to detect potential security incidents. • Perform digital forensics investigations to collect, preserve, and analyze evidence related to cyber incidents. • Conduct thorough analysis of security incidents to understand the attack vector, tactics, techniques, and procedures (TTPs) used by threat actors. • Identify the root cause of security incidents and provide insights to prevent future occurrences.	GCFE, GCIH, EnCE, CCE, CFCE
8	Incident Response Analyst	• Monitor security information and event management (SIEM) systems and other security tools to identify potential security incidents. • Perform initial triage to determine the severity and scope of detected incidents. • Conduct in-depth investigations of security incidents to identify the	GCIH, CISSP, CEH, CompTIA Security+, GCFA, ECIH

		attack vector, methods used, and extent of the compromise. • Implement immediate containment measures to prevent the spread of the incident. • Identify the root cause of security incidents and provide recommendations to prevent future occurrences.	
9	Blue team expert	• Analyze logs, network traffic, and other data to identify anomalies and potential threats. • Quickly respond to security incidents to contain and mitigate the impact. • Conduct regular vulnerability assessments and penetration testing to identify weaknesses. • Continuously monitor networks, systems, and applications for security breaches.	CISSP, CompTIA Security+, GSEC, CISM, CEH, CCNA
10	Red team expert	• Conduct thorough penetration tests on networks, systems, applications, and physical security controls. • Simulate advanced persistent threats (APTs) and other sophisticated attack scenarios to mimic real-world adversaries. • Perform vulnerability assessments to identify security weaknesses and provide recommendations for remediation. • Conduct social engineering attacks, such as phishing, pretexting, and baiting, to test employee awareness and response.	OSCP, CEH, GPEN, CRTOP, Offensive Security Certified Expert
11	Purple team expert	• Act as a bridge between Red and Blue Teams to ensure effective communication and cooperation.	CEH, CompTIA Security+, CISSP, OSCP, CISM, CISA

		• Work with Red Team to design and execute realistic attack scenarios. • Analyze the results of Red Team activities and Blue Team defenses to identify gaps and areas for improvement. • Provide training to Blue Team members based on Red Team findings and tactics. • Develop metrics to measure the effectiveness of security controls and response efforts.	
12	Data Protection Architect	• Develop and implement comprehensive data protection strategies and policies. • Conduct risk assessments to identify vulnerabilities and threats to data. • Design and implement access control mechanisms to ensure that only authorized personnel can access sensitive data. • Deploy and manage DLP solutions to monitor and prevent unauthorized data exfiltration. • Ensure compliance with data protection regulations such as GDPR, CCPA, HIPAA, and others.	CISSP, CIPP, CISM, CISA, CDPSE, CCSP
13	Network Analyst	• Network design, implementation, and troubleshooting • Network traffic monitoring and analysis • Incident response and root cause investigation • Firewall, IDS/IPS, and VPN configuration • Performance optimization and capacity planning • Log correlation and packet analysis (Wireshark, NetFlow, etc.)	CCNA / CCNP (Cisco), CompTIA Network+, Fortinet NSE (Network Security Expert), Palo Alto Networks PCNSA / PCNSE, Juniper JNCIA / JNCIS

14	Hardware Specialist (Installation, Analysis & Maintenance)	• Installation, configuration, and testing of servers, desktops, and peripheral devices • Preventive and corrective hardware maintenance • Troubleshooting system performance and diagnosing hardware failures • Firmware and driver updates • Hardware capacity planning and lifecycle management • Asset inventory, documentation, and vendor coordination	CompTIA A+, CompTIA Server+, Microsoft Certified: Windows Server / Hardware Support Specialist, Dell / HP / Lenovo Hardware Support Certifications, OEM-specific certifications (Cisco UCS, IBM, etc.)