

**FIRST AMENDMENT TO THE LEE COUNTY CISO AND CYBERSECURITY
SUPPORT POSITIONS STATEMENT OF WORK**

THIS FIRST AMENDMENT TO THE LEE COUNTY CISO AND CYBERSECURITY SUPPORT POSITIONS STATEMENT OF WORK, is made by and between the Lee County Board of County Commissioners, a political subdivision of the State of Florida ("County") and IT Staffing and Consulting, Inc. dba ISC ("Contractor"), collectively, the "Parties."

WHEREAS, the County agreed to a Statement of Work with the Contractor, resulting from the Piggybacking of Florida State Contract No. 80101507-21-STC-ITSA through PB220535KLB, on the 19th day of September, 2023, to provide a qualified Chief Information Security Officer (CISO) and Cybersecurity Support Positions of Security Manager and Security Specialist ("Agreement"); and,

WHEREAS, specific personnel, namely Nick Jones, Nick Reichley, and Brian Antic were not listed within the Personnel Matrix in Section 9 of the Agreement; and,

WHEREAS, the Parties desire to modify the "PERSONNEL MATRIX" section of the Agreement, pursuant to Section 13.08 "Entire Agreement" of the Agreement.

NOW, THEREFORE, IN CONSIDERATION OF THE FOREGOING AND THE MUTUAL COVENANTS CONTAINED HEREIN, IT IS AGREED AS FOLLOWS:

1. The Parties agree that Section 9. PERSONNEL MATRIX of the Agreement shall be superseded by the following:

PERSONNEL MATRIX:

Position	Personnel	Job Number	Job Title
vCISO	Kevin O'Malley	6800	Security Manager
vCISO	John Henderson	6810	Security Analyst
VA and PT	John Henderson	6830	Network Security Specialist
VA and PT	Nick Reichley	6830	Network Security Specialist
Sr. Security ENG.	Justin Frazier	6799	Security Manager
Sr. Security ENG.	Nick Jones	6800	Security Manager
IR planning Expert	John Henderson/ Joe Petre/ Brian Antic	6830	Network Security Specialist
Cyber SME	Joe Petre	6800	Security Manager
NIST Eval	Benjamin Barnhill	6800	Security Manager

2. The Parties agree that the Personnel Resumes section of the Agreement shall be supplemented by the following:

Brian Antic

Wilmington, NC • (910) 473-8408

mail@brianantic.us • linkedin.com/bmantic

PROFESSIONAL SUMMARY

Passionate Cybersecurity Engineer with 12+ years of experience in the Department of Defense Cyberspace, and 5+ years of experience in Defensive Cyberspace Operations (DCO); Background in enterprise networking, threat hunting, Digital Forensics and Incident Response (DFIR), and detection engineering. Firm believer in automating *everything*.

COMPETENCIES & SKILLS

Technical: Threat hunting, DFIR, detection engineering, cyber threat intelligence, malware reverse-engineering, scripting and automation, log management and SIEM, cloud infrastructure, red/purple team operations, training and cyber range development, MITRE ATT&CK® framework, Cyber Kill Chain® framework, enterprise networking, network security, endpoint security, vulnerability management, identity and access management, NIST/CIS/ISO frameworks **Tools:** AWS, Azure, Cortex XDR, Splunk, ELK Stack, Zeek, Regex, Ansible, Python and various third-party modules (Plaso, Impacket, PExpect, Scapy, Requests, etc.), SQL, Git, Snort, Suricata, YARA, Sigma, SIFT Workstation, Winpmem, Linpmem, Volatility, Velociraptor, Ghidra, Regshot, Sysinternals, Cuckoo Sandbox, Autopsy, Magnet ACQUIRE, iLEAPP, ALEAPP, DeepBlueCLI, SRUM-Dump, CyberChef, Active Directory, PowerShell, Bash, Wireshark, TCPdump, Nmap, Metasploit, Burp Suite, Nessus, Docker, Kubernetes, VMware vSphere, Proxmox

Hardware/OS: Cisco/Juniper/MikroTik/VyOS routers and switches, Arista/Palo Alto/Sophos/Cisco next-generation firewalls, Windows, macOS, Unix/Linux, FreeBSD

Functional: Oral and written communication, documentation, complex analysis and problem-solving, attention to detail, team player, project management, quickly grasp new concepts

EDUCATION/CERTIFICATIONS

GIAC – Certified Python Coder (GPYC) –

In-progress Certified Incident Handler (GCIH)

Security Essentials Certification (GSEC)

Information Security Fundamentals (GISF)

Foundational Cybersecurity Technologies (GFACT)

Cisco – Cisco Certified Network Associate (CCNA)

NSA – Joint Cyber Analysis Course (JCAC)

Intermediate Cyber Core (ICC)

USMC – Red Team Certified Professional

Network Operators Course

Network Specialist Course

US Army – Title 10 Interactive On-Net Operator

CompTIA – Security+

SANS Technology Institute December 2024 Bachelor of Applied Cybersecurity

EXPERIENCE

Cybersecurity Engineer, USMC – Defensive Cyberspace Operations January 2020 – November 2023

- As a tier 3 SOC analyst, proactively and aggressively conducted internal threat hunting operations within the Marine Corps tactical cyberspace to identify any advanced and/or persistent threats, as well as the follow-on triage activities as required based on hunt findings.
- Investigated and reported on cyber threat hunt findings and provided recommendations to both technical and non-technical key leadership on ways to improve visibility and security posture across detective and preventive controls.
- Identified and tracked threat actor TTPs to conduct TTP-based hunting activity and gap remediation.
- Participated in Purple Team exercises to analyze and evaluate the effectiveness of existing security controls against identified TTPs.
- Emulated attack techniques in a lab environment to conduct research on artifacts, as well as test/validate search queries and ensure detections fire as expected.
- Coached and mentored junior engineers to enhance and mature our teams' capabilities and processes.

Enterprise Operations Chief, USMC – Cyberspace Command January 2019 – December 2019

- Served on the Marine Cyberspace Command's Cyber Security Incident Response Team (CSIRT) and was responsible for the planning, coordination, and direction of subordinate commands to complete incident response actions, tracking relevant task completion, providing a clear line of communication between USMC DCO Forces and Higher Headquarters, and assisting in the planning, deployment, and battle tracking of multiple Cyber Protection Teams.
- Worked with Joint Force Headquarters-Department of Defense Information Network, the Marine Corps Cyber Operations Group, and site owners to lead the effort in mitigating three critical vulnerabilities that were identified on USMC cyber infrastructure, as well as 32 medium and high-level vulnerabilities.
- Developed Marine cyberspace operations plans and orders in response to joint operations and service identified cyberspace events.

Special Operations Communicator, USMC – MARSOC July 2015 – December 2018

- Performed the installation, configuration, and maintenance of all data communications systems and network services.
- Planned, designed, and implemented local area, wide area, and linked heterogeneous networks through the application of appropriate data and telecommunications hardware and software.
- Employed advanced long-range voice and data communications, to include HF, VHF, UHF, TACSAT, SDN, and low visibility communication capabilities.
- Maintained accurate accountability of all Controlled Cryptographic Items (CCI) held within the Electronic Key Management System storage facility.
- Responsible for Communications Security key material and CCI preparation, configuration, security, and implementation.

Network Engineer, USMC – MARSOC December 2011 – June 2015

- Installed, configured, and managed all data network systems in an enterprise environment that supported thousands of users daily.
- Installed, configured, and maintained all network services, both hardware and software.
- Planned and executed the integration of multiple information systems.
- Evaluated and resolved customer information system problems.
- Performed required hardware upgrades.

Nicholas D. Jones

(316)519-1529 |

nick.jones2@yahoo.com

Objective Dedicated and highly skilled Information System Security Manager with a proven track record of safeguarding critical assets, mitigating risks, and ensuring compliance with industry standards and regulations. Seeking to leverage my experience in cybersecurity, leadership, and strategic planning to contribute to the success of a forward-thinking organization.

Work Experience Contract Operations Lead *CDO Technologies, Wichita, KS (December 2022 – Present)*

- Provide administrative oversight for a team of 24 contractor employees.
- Gather and analyze performance metrics to ensure compliance with performance work statement.
- Identify areas for improvement and recommend strategies for optimization.
- Facilitate monthly program management reviews with stakeholders ensuring effective communication among internal and external teams.
- Conduct onboarding and off boarding processes for all contract personnel.
- Act as primary point of contact between customer and program manager, facilitating strong communication and alignment.
- Effectively convey customer requirements, expectations, and feedback to internal team to ensure customer satisfaction.

Information Security Engineer / Information System Security Manager *CDO Technologies, Wichita, KS (May 2022 – Present)*

- Aid in the development and implementation of comprehensive information security strategy, policies, and procedures to protect the organization's digital assets from threats and vulnerabilities. • Primary technical advisor to PM and Information System Owner (ISO).
 - Oversees day-to-day Risk Management (RMF) process.
 - Manages cybersecurity-related documentation.
 - Maintains Authority to Operate (ATO) via eMASS/Authority to Connect (ATC) via SNAP
 - Develops continuous monitoring strategy and validates implementation.
 - Coordinates with the Wing Cybersecurity Office (WCO) on incident handling.
 - Collaborate with cross-functional teams to ensure security considerations are integrated into the implementation of new systems and applications.
 - Oversee hardware and software (HW/SW) approval.
 - Provides guidance and assistance to Information System Security Officer(s) (ISSO).
 - Collaborate with external auditors and regulatory bodies to ensure compliance with relevant laws, regulations, and standards.

IT Specialist (Network Services) *Kansas Air National Guard, Wichita, KS (April 2020 – Present)*

- Leverage SolarWinds Network Monitoring System to administer and analyze the base Local Area Network (LAN) utilization to ensure the smooth, reliable, and robust operation of classified and unclassified networks.
 - Coordinate maintenance and troubleshooting activities, including reviewing, evaluating, and fine-tuning components such as physical and virtual servers to achieve peak network efficiency.
 - Implements new network operating systems hardware and software and develops base wide network operating procedures. • Identifies and documents network requirements for specific needs of customers. • Plans for current and future technology integration and works issues for compatibility and standardization based on current and projected customer needs.
 - Serve as a network security administrator by implementing technical solutions required to bring the network into compliance with current network and/or operating system security measures.
 - Maintains user access controls (physical, personnel, software, and information security) using applicable security policies and regulations while assisting IT security specialists with applicable security policies and regulations.
 - Conduct risk analyses and security tests and evaluations.
 - Track network security patches and ensures completion.

Cyber Security *Kansas Air National Guard, Wichita, KS (October 2019 – April 2020)*

- Developed network security policy and objectives for Network Operations, Infrastructure, Client Systems, and other work centers to follow.
- Implemented policy to enforce DoD directives, regulations, and vulnerability management procedures to over 1300 users.
- Conducted research of new vulnerabilities in operating systems, application software, infrastructure, and boundary protection devices through the use of Assured Compliance Assessment System and Host Based Security System compliance reporting tools.
- Coordinated with Information Systems Manager to accomplish network vulnerability assessments, accomplish network accreditation, and conduct risk mitigation activities.
- Monitored enterprise IA policy compliance and provided recommendations for effective implementation of IT security controls.
- Conducted audits and enforced the compliance of IA procedures and investigates security-related incidents.

Occupational Safety and Health NCO *Kansas Air National Guard, Wichita, KS (January 2013 – October 2019)*

- Developed and administered organizational SharePoint site to communicate current and future technology integrations for OHS objectives.
- Developed and maintained records database to track all mishaps for trend analysis to identify ineffective practices or procedures, and equipment shortcomings.
- Develop safety training guidance based on Federal Regulations, National Consensus Standards, and Air Force Instructions.
- Conduct facility inspections and program assessments utilizing Federal Regulations, National Consensus Standards, and Air Force Instructions.
- Perform investigations on all mishaps and potential hazards and maintained findings in the Air Force Safety Automated System (AFSAS) database.
- Develop and provide safety training for over 100 safety representatives and supervisors.
- Conduct Environmental, Safety and Occupational Health Safety Councils to inform leadership on issues relating to the overall status of the safety program.
- Conduct monthly spot inspections and suggest corrective actions in support of mishap prevention.

Customer Service Representative (Technical Support) *Cox Communications, Wichita, KS. (May 2018 – November 2018)*

- Monitored Local and Wide Area Networks (LAN/WAN) to ensure service availability in designated regions.
- Answer inbound customer calls providing evaluation and consultation on Internet Service Provider (ISP) telephone, cable, and internet products and services.
- Utilized troubleshooting tools to diagnose the root cause of customer problems and develop mitigation steps to resolve the issue.
- Tested and evaluated emerging technologies to provide quick response to customer concerns and maintain service connectivity.
- Utilized ticketing system to track status of work in progress and provide timely updates as requested.
- Consulted with field technicians to ensure proper application of hardware solutions and equipment placement.

Production Recruiter & Retainer *Kansas Air National Guard, Wichita, KS (January 2016 – May 2017)*

- Managed recruiting program responsible for interviewing, screening, and evaluating applicants to achieve recruiting goals.
- Maintained records database to enable follow-up contacts with prospective enlistees.
- Established and maintained contact with high school, college, business and industry officials through the deployment of electronic communication campaigns.

- Presented Air National Guard orientations to civic, social, educational and student organizations.
- Coordinate and participate in special events such as state and municipal ceremonies, exhibits, fairs, parades, and sporting events.
- Planned and coordinated sales promotional projects using media such as direct mail, press, radio, television, and social media.
- Evaluated and coordinated the purchase and use of information technology assets in support recruiting efforts.
- Administered and trained users on the use of the Air Force Recruiting Information Support System – Total Force (AFRISS-TF) to meet production goals.

Sr. Environmental Health & Safety Manager *Exacta Aerospace, Inc., & Weaver Manufacturing, Inc., Wichita, KS. (October 2014 – June 2015)*

- Managed the development, implementation and administration of environmental, health, and safety (EHS) programs.
- Scheduled, coordinated, and conducted evaluations of programs to determine compliance with occupational safety and health regulations.
- Advised management of actions impacting facility operations, work processes, and environmental conditions which affect the safety of over 500 personnel.
- Reviewed health and safety programs to establish technical and administrative safety and occupational health requirements for industrial, construction, and transportation activities.
- Lead all environmental compliance (hazardous waste, air emissions, water) programs.
- Conducted various site Environmental Health and Safety spot and annual inspections required for compliance.
- Investigated all safety accidents and environmental incidents through root cause analysis and implement corrective actions.
- Conducted witness interviews and gathered supporting documentation to include photographs and written statements to provide a formal incident report to top management.
- Maintained records database to track all injuries for trend analysis and preventative measures.
- Reported and maintained all required Occupational Safety and Health Administration documentation in digital format.

Facility/ Safety & Compliance Coordinator *Exacta Aerospace, Inc., Wichita, KS (September 2012 – October 2014)*

- Utilized ticketing information system to coordinate the scheduling of preventative maintenance and upkeep on facility and grounds.
- Maintained the min/max database to ensure appropriate level of office supplies to support day to day organizational needs.
- Served as a liaison for federal agencies as the sites only Environmental Health & Safety contact.
- Conducted monthly and annual facility inspections to ensure safe and healthful work conditions.
- Provided annual safety training required per job hazard analysis.
- Lead 5S Lean Manufacturing activities and quarterly audits reporting findings and corrective actions to top management.

Educational and Professional Development:


- Bachelor of Science, Information Systems Management from Southwestern College
- Bachelor of Science, Security Management from Southwestern College
- CompTIA Security Plus Certification
- (ISC)² Certified in Governance, Risk, and Compliance Certification
- Top Secret Security Clearance

PB230550KLB - PB220535KLB
Lee County CISO and Cybersecurity Support Positions Statement of Work
Florida State Contract No. 80101507-21-STC-ITSA
IT Staffing and Consulting, Inc. dba ISC- Amendment No. 1


IN WITNESS WHEREOF, this First Amendment of the Municipal Rental Agreement has been signed and sealed, in duplicate, by the respective parties hereto.

DATED this 7/18/2024 | 2:11 PM EDT by the Lee County Board of County Commissioners.

COUNTY: LEE COUNTY, FLORIDA

Signed by:

BY: 123346F3B767465...
Ashley Mason
Chief Information Officer, on behalf of the Board of County Commissioners


APPROVED as to Form for the Reliance of Lee County Only

Signed by:

BY: D7B0A432435E448...
County Attorney's Office

DATED this 11th day of July, 2024 by IT Staffing and Consulting, Inc. dba ISC.

ATTEST:

BY: 
Authorized Signature



(Witness)
Eric H. Lott

Edwin E. Lott

Authorized Signature Printed Name

President

Authorized Signature Title

CORPORATE SEAL: