DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

IT Staffing and Consulting, Inc. d.b.a. ISC
Florida State Contract No. 80101507-21-STC-ITSA

Lee County CISO and Cybersecurity Support Positions
Statement of Work

1. Scope of Work.

The Contractor shall provide information technology (IT) staff augmentation services in support of the Lee County's Office of Information Technology (OIT). The Contractor must provide the qualified Chief Information Security Officer (CISO) and Cybersecurity Support Positions of Security Manager and Security Specialist proposed in its Response, and selected by the County, who has the experience and ability to fulfill the requirements of this Statement of Work (SOW). The Contractor shall provide services in compliance with the terms of The Department of Management Services- Florida State Contract No. 80101507-21-STC-ITSA.

2. Definitions.

In this SOW, the following terms are defined as set forth below:

a. **Business Days** – Monday through Friday, inclusive, except for holidays identified in section 110.117, Florida Statutes (F.S.), or emergencies identified by the Department's Contract Manager.
b. **Contractor** – The entity selected to provide services pursuant to this Statement of Work (SOW). "Contractor" shall be defined as Contractor, its Affiliates, and its and their employees, directors, officers, agents, representatives, subcontractors, interconnection service Contractors and suppliers.
c. **County** –shall be defined as Department, You, Lee County, Florida, Office of Information Technology, Your Affiliates, and Your and their employees, directors, officers, agents, and representatives.
d. **Damages** - will refer collectively to all injury, damage, liability, loss, penalty, interest and expense incurred.
e. **Office of Information Technology (OIT)** – A unit of the Department that plans, manages, and maintains the IT resources for the County.
f. **Project Team** – A team whose members usually belong to different groups and are assigned to activities for the same project.

3. Purchase Order (PO) Duration.

a. Term. October 1th, 2023, until September 30th, 2024, unless otherwise terminated.
b. Renewals. The PO may be renewed if the underlying State Term Contract No. 80101507-21-STC-ITSA, Information Technology Staff Augmentation Services (Contract), (STC), is extended, but the renewal period will not exceed the expiration of the STC by more than twelve (12) months.

4. Payment Provisions.

a. Invoicing. The Contractor shall invoice the Department monthly by submitting invoices to:

Lee County Finance Department
Post Office Box 2238
Fort Myers, FL 33902-2238

b. Compensation. The Department will pay the fixed hourly rate of compensation proposed in the Contractor's Response for the services provided under the PO. All payments are subject to the acceptance of the deliverables through the process set forth in Section 5.d., Acceptance of Deliverables. The PO will not exceed the estimated total PO Amount in fiscal year 2023-2024 without modification and issuance of a change order to the PO. No costs or expenses, incurred by the Contractor for the services described herein will be reimbursed by the Department. Pre-approved travel expenses incurred by the Contractor will be reimbursed by the Department at cost to the contractor.

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

5. Contractor Responsibilities.

a. CISO and Support Personnel Task List. The Contractor, through the CISO and Cybersecurity Support Personnel it provides, shall perform the following tasks as assigned by the Department's Contract Manager:

Item #	Service
SC.1	Lead Cyber Governance, Risk, and Compliance (GRC) for the County.
SC.2	Assist and participate in communicating cybersecurity issues to County leadership.
SC.3	Work to reduce risk exposure to technology assets to acceptable levels defined by County leadership.
SC.4	Ensure Local, State, and Federal regulatory compliance as required by the County.
SC.5	Ensure compliance with industry regulations (e.g., PCI, HIPAA, etc.) as required by the County.
SC.6	Develop and maintain frameworks and processes to institutionalize cyber for the County.
ST.1	Conduct penetration testing, vulnerability assessment, and/or cybersecurity assessment services (up to three (3) tests or assessments for small projects or operational systems per contract year (up to one week of testing or assessment each)
ST.2	Find problems malicious actors would seek to exploit
ST.3	Provide neutral, third-party testing and evaluation
ST.4	Review effectiveness of the County's cyber posture, infrastructure, and provider support
SI.1	Provide strategies and plans to improve incident handling and response communication and coordination across the County
SI.2	Develop playbooks and processes to reduce downtime and remain in compliance
SI.3	Provide strategies for maintaining public trust
SO.1	Provide Virtual Security Operations Center (SOC) Analyst (aka SOC as a service)
SO.2	Identify threats before they become critical events
SO.3	Provide timely response and protection

Table 1 Services

Item #	Service Level	Measurement Period	Measure	Required Service Level (as calculated below)
MC.1	Provide cyber situation report	Monthly	1 per week	100%
MC.2	Review compliance	Quarterly	1 per month	100%
MC.3	Framework and process updates	Biannually	1 per quarter	100%
MT.1	Provide test report	As requested by Client	Within one week of testing cycle	100%
MI.1	Provide incident handling plan update	Biannually	1 per quarter	100%
MO.1	Provide alerting and guidance	Monthly	Within 24 hours	100%

Table 2 Service Level Agreement (SLA)

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

1. Deliverables. The Contractor shall perform the tasks listed in Section 5.a., as requested by the Department. The Contractor shall invoice these tasks to the Department in one-hour increments, at the fixed hourly rate specified in the PO. The Contractor shall provide evidence of performance by submitting the required documentation detailed in the list below to the Department's Contract Manager. Documentation shall be submitted in a format compatible with MS Office 2013, or newer.
2. Status Report. A report detailing the status of tasks, level of service provided to Department staff, and the projected completion date for each assigned task. The Contractor shall submit this report weekly on the day specified by the Department's Contract Manager.
3. Time Reports. A report detailing the tasks worked on each day and the hours spent on each task. The Contractor shall submit this report no later than the 5th day of the month that follows the month for which the total hours worked are being submitted, via the OIT Time Log (upon the start date of the Contractor Representative, as defined in Attachment 1, Standard Terms and Conditions, access to this log will be provided), using the agreed upon CCIDs for the work performed.
4. Technical Documentation. Documentation, identified in the SDF, that evidences all work performed complies with the OIT policies, procedures, and technical standards provided to the Contractor by the Department's Contract Manager. The information contained in the technical documentation must also facilitate the transfer of knowledge to the Department's staff that is necessary to maintain the system(s), application(s), or solution(s) that the Contractor Representative has worked on. The technical documentation must be satisfactorily completed within the response time specified by the Department's Contract Manager.
5. Additional Documentation. Any additional documentation required by the Department's Contract Manager, which must be submitted within the timeframe specified by the Department's Contract Manager.

b. Performance Measures. The Contractor shall provide the deliverables and required documentation in accordance with Sections 5.a. above.

c. Acceptance of Deliverables. The Contractor shall submit the required documentation evidencing the deliverables listed in Section 5.b., above, to the Department's Contract Manager for review and approval. Notwithstanding Section 5, Acceptance of Deliverables, of Attachment 1, Standard Terms and Conditions, failure to accept a deliverable within twenty (20) Business Days constitutes non-acceptance by the Department, unless provided otherwise by the Department's Contract Manager in writing. If subsequent work that is the responsibility of the Contractor invalidates some or all of the contents of a deliverable, the Department reserves the right to require the Contractor to revise deliverables previously approved at no additional cost to the Department or to reject current deliverables based on inconsistency with the SOW.

d. Facilities and Equipment. The Department will provide items such as working facilities, development and testing environments, equipment and software licenses, access to the Department's network, and internet connectivity, etc. **Note: A Contractor Representative with access to the Department's network is required to complete the Department's security awareness training. This training must be completed within fifteen (15) calendar days of the Contractor Representative's start date**. If the Contractor Representative uses his or her own computer laptop, the equipment must undergo a security review by the Department to ensure it is free of software viruses and does not otherwise pose a security threat prior to connection to the Department's network.

6. Qualification Requirements for Contractor Representative.

a. Professional Qualification Requirements.

CISO (Chief Information Security Office) Senior Security Manager
- CISSP (Certified Information System Security Professional)
- GSLC (GAIC Security Leadership Certification)
- 10+ years' experience in technology
- 5+ Years' experience as CIO or CISO
- Experience in conducting NIST Experience in conducting NIST (National Institute of Standards and Technology) assessments

vSOC (Virtual Security Operations Center) Advanced Cybersecurity Specialist
- GIAC – Security Essentials
- Expertise with Palo Alto Cortex XDR

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

Degree in computer science, networks, or cyber security
3+ years' experience in technology, cyber security, or incident response/management

VA & PT (Vulnerability Assessment, Penetration Test)
Degree in computer science, networks, or cyber security
OSCP (offensive security certified professional) certification
5+ years' experience technology, cyber security, or incident response/management
Experience in conducting NIST (National Institute of Standards and Technology) assessments

Senior Cyber Security Engineer
(PCCSA) Palo Alto Certified Associate
MITRE Attack Defender (MAD) ATT&CK Cyber Threat Intelligence Certification
10+ years' experience in technology, cyber security, or incident response / management

IR (Incident Response) Planning
Expertise in Florida County level cyber incident response planning

Cybersecurity SME
CISSP (Certified Information System Security Professional)
10+ years' experience in cybersecurity

b. Educational Requirements. The Contractor Representative, and any subsequent Contractor Representative provided by the Contractor, must possess, at a minimum, a bachelor's degree in one of the computer sciences fields or in management information systems, or four (4) years of work experience in IT, systems analysis, management analysis, program planning, program research, or program evaluation.

7. MISCELLANEOUS PURCHASE ORDERS TERMS:

a. Termination for Convenience. The Department may, in its sole discretion, terminate the PO at any time by giving one (1) month's written notice to the Contractor.

b. Transition Plan. At the end of the PO term, or if the PO is otherwise terminated, the Contractor agrees to cooperate in the transition of PO services to the Department or a successor contractor. The transition will include, at a minimum, training, transfer of data, and transition period error correction.

c. Background Checks. The Contractor Representative provided to perform the work described herein must undergo a background check at the expense of the Contractor. Review and approval of a background check, which, at a minimum, is the equivalent of a Level 2 screening described in section 435.04, Florida Statutes, including fingerprinting, is required for each Contractor Representative before he or she will be allowed to perform work under the PO.

8. DEPARTMENT'S CONTRACT MANAGER.

The Department's Contract Manager for the PO is:
Ashley Mason, Director, Innovation and Technology

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

9. PERSONNEL MATRIX:

Position	Personnel	Job No.	Job Title
vCISO	Kevin O'Malley	6800	Security Manager
vSOC	John Henderson	6830	Network Security Specialist
VA and PT	John Henderson	6830	Network Security Specialist
Sr. Security Eng	Justin Frazier	6800	Security Manager
Sr. Security Eng	TBD	6800	Security Manager
IR Planning Expert	John Henderson/ Joe Petre	6830	Network Security Specialist
Cyber SME	Joe Petre	6800	Security Manager
NIST Eval	Benjamin Barnhill	6800	Security Manager

PRICING

Information Technology Staff Augmentation							
POSITIONS							
Position	**Unit of Measure**		**Job No.**	**Job Title**	**Estimated Hours / Month**	**Hourly Rate**	**Total (Est. Hr x Hr Rate)**
vCISO	Hourly	Kevin O'Malley	6800	Security Manager	163	154	25102
vSOC	Hourly	John Henderson	6830	Network Security Specialist	90	128	11520
VA and PT	Hourly	John Henderson	6830	Network Security Specialist	50	128	6400
Sr. Security Eng	Hourly	Justin Frazier	6800	Security Manager	163	154	25102
Sr. Security Eng	Hourly	TBD	6800	Security Manager	163	154	25102
IR Planning Expert	Hourly	John H /Joe P	6830	Network Security Specialist	13	128	1664
Cyber SME	Hourly	Joe Petre	6800	Security Manager	24	154	3696
NIST Eval	Hourly	Ben Barnhill	6800	Security Manager	14	154	2156
				Total Monthly			**$100,742**
				Total Annual			**$1,208,904**

ISC accounting contact is as follows:
Jennifer Britt | Director of Accounting
Accounting@goisc.com
850-212-6977 JBritt@goisc.com

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

Personnel Resumes

Dr. Benjamin Barnhill

Education / Certifications:

● Doctor of Information Technology, 4.0 GPA, Cybersecurity, Capella University, 04/2023 Dissertation Topic: Federal agencies cyber threat indicator share programs
● Master of Science, Cybersecurity / Information Assurance, Western Governors University, 06/2017
● Bachelor of Science, Information Technology / Security, Western Governors University, 08/2016
● Certifications: CISSP, CHFI, A+, Net+, Sec+, Project+, Linux+, Linux Essentials, CCNA, CEH, Digital Forensic Investigator
● Programming Models & Languages: Agile & Waterfall, C++, Java, JavaScript
● Compliance Models: NIST, CMMC, CSF

Professional Experience:

Senior Security Consultant, PLEX Cyber, 03/22/2022 - Current

● Conducted physical and wireless red team assessments against commercial organizations. Leveraged Kali Linux and a variety of tools for penetration testing. Identified Security gaps in both physical and IT infrastructures. Provided detailed report on findings and potential mitigations.
● Performed NIST/CSF/CMMC assessments of commercial organizations. Reviewed documentation to ensure best practices were documented. Interviewed personnel to ensure documented practices were enforced; Drafted reports with recommendation to enhance or meet compliance requirements
● Developed portable wireless assessment platform to anonymously perform Man-In-The-Middle testing

Senior Systems Engineer – Level 3, PLEX Solutions LLC, National Security Agency, 04/01/2022 - Current

● Provided direct subject matter expertise to NSA Customer. Overhauled overarching Systems Engineering processes and procedures for entire directorate. Drafted 120-page Systems Engineering handbook and converted 15+ templates into directorate formatting. Leveraged resources from Systems Engineering frameworks such as: DoDAFv2.0, PMBok, SEBok, and RMF.
● Oversaw delivery of monthly status reporting. Ensured metrics, schedules, and status updates were accurately captured and disseminated. Participated in multiple cross organization working groups to enhance organizational business practices. Created collaboration sites on both SharePoint and Confluence. Authored organization project workflow.
● Coordinated publication of National level cybersecurity policy on behalf of NSA. Assisted with establishing Quantum Resistant security protocols for next-generation cybersecurity controls.

SkillBridge Intern / Cybersecurity Compliance Specialist, Applied Network Solutions, 09/01/2021 to 03/01/2022

● Enhanced small business cybersecurity program, established a road map to compliance with the Cybersecurity Maturity Model Certification (CMMC), solidified best practices, reviewed and recommended technology solutions, and drafted organization policies, procedures, and standards
● Authored and responded to request for proposals for Red Team / Blue Team exercises
● Defined and implemented business tools including Multi Factor Authentication (MFA), Mobile Device Management (MDM), Security Information and Event Management (SIEM) solutions

United States Air Force (USAF) 02/5/2002 to 03/01/2022
Mission Superintendent / SEL, 707th Communication Squadron, USAF, NSA MD, 11/2020 to Present

● Program manager for agency Robotic Process Automation (RPA) Center of Excellence (CoE)

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

initiative. Managed 25 personnel assigned to three teams of contractors, military, and civilian across a variety of geographically separated locations.
● Defined agency level policy for automation protocols. Leveraged Commercial-Off-The-Shelf software to develop automations saving personnel thousands of hours per year redirected to mission task.

Project Manager, Detachment 1, 318 Information Operations Group, USAF, NSA MD, 08/2019 to 11/2020
● Managed working model of city infrastructure including multiple logical networks, physical Programmable Logic Controllers (PLCs), and Supervisory Control and Data Acquisition (SCADA) software supporting a realistic and responsive environment for Red Team / Blue Team events.
● Coordinated capture the flag events for federal agency and Department of Defense Personnel.
● Developed ElasticSearch log capture and monitoring system used to track Red Team actions and produce YARA signatures for Blue Team countermeasures.
● Liaison for Platform One, CYBERCOMM, and Defense Industrial Base (DIB) partners in the roll out of CMMC and threat sharing capabilities.

Mission Superintendent, DoD Cyber Crime Center (DC3), USAF, MD, 01/2014 to 08/2019
● Managed 50 military, civilian, and contract personnel in the Information Technology Division.
● Supported the Air Force Office of Special Investigations (AFOSI) cybercrime division by building and maintaining DC3 network infrastructure.
● Liaison with the Secretary of the Air Force/Chief Information Officer (SAF/CIO) secure coding working group (8570/8140). Researched and recommended updated validation tools for military and civilian secure software development certifications.
● Liaison with DHS FCIG (Formally ESSA). Identified processes, standards, procedures, and best practices for machine-to-machine sharing of threat indicators between federal agencies.

Mission Superintendent, 90th Information Operations Squadron, USAF, TX, 06/2008 to 01/2014
● Directed software development projects supporting 24th USAF requirements. Coordinated 5-7 contractor teams in creation of custom / novel software using Agile project development techniques.
● Managed the first USAF authored McAfee Host Based Security System module in support of DISA.
● Debuted cutting edge network defensive capabilities; participated in multiple USAF / Joint DoD cybersecurity exercises demonstrating defensive cyber tactics, techniques, and procedures.
● Developed training program supporting 688th Cyberspace Wing consisting of over 1,400 civilian and military personnel.

Mission Manager, Detachment 1, 23rd Information Operations Squadron, USAF, NSA MD, 03/2002 to 06/2008
● Maintained Joint Functional Component Command Network Warfare (JFCCNW) software repository; ensured proper storage and secure transmission of software.

Awards:
● Air Force Meritorious Service Medal 2019
● DoD SparkTank Innovation 2017, 2018, & 2019
● Air Force Information Dominance 2014 & 2016
● Air Force Commendation Medal 2008
● Capella University Presidents List Honoree 15 times between 2019 - 2023

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

Joe Petre

Certifications:

- CISSP – 2014 – 377292
- Security +

Education:

- Eastern Michigan University
  Bachelor of Arts *Organizational Communication*, 1998

Professional Experience:

PLEX Cyber May 2022 - Present

Vice President

- Consulting services leader for an NSA NSCAP accredited testing firm
- Plan, develop, and analyze service offerings for testing and governance risk & compliance offerings
- Direct technical activities and inspect client engagements to ensure alignment with client expectations
- Provide guidance to clients for "on the horizon" services to improve security posture
- Establish and maintain relationships with client and partner leaders

NTT Security 2019 – 2022

Vice President, Americas

- P&L owner for Americas consulting team
- Lead delivery and management of client engagements
- Coordinated with sales leaders for identification, pursuit and closure of deals
- Mentored team leadership to develop a team that provides a positive client experience
- Performed regular client experience calls with customer executives on quarterly schedule
- Regional leader for sales Opportunity Review Board
- Lead Application Security, Penetration Testing, Privacy, GRC, Architecture and Security Operations Consulting for Americas
- Developed global portfolio of 4 distinct offerings for Software Security Assurance
- Global leader for Application Security offerings and sales support functions
- Co-developed professional development program for Americas CS team
- Developed and delivered enhanced client engagement program for improved deal generation

Hewlett-Packard Enterprise/Micro Focus 2013 – 2019

Practice Principal, Cybersecurity Professional Services (3 years)

- Drove ArcSight SIEM and Fortify application security Professional Services business to revenue in excess $6M annually
- Developed service offering for OWASP SAMM client assessments
- Prepared quarterly and weekly deal and revenue forecast for 5 regions
- Presented at Executive Briefing Center for fortune 50 customer CIO, and CISO personnel
- Improved processes to increase accuracy of revenue forecasting and achieve

targets

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

- Managing Principal, Professional Services (3 years)

- Led ArcSight/Atalla/TippingPoint professional services team for US Central, LATAM and Canada
- Increased revenue from $300k per quarter to over $1M with many of the largest customer engagements and
- customers
- Decreased personnel attrition from 30% to 10% annually

IBM Security Services (MSS) 2007-2013

Manager, Client Services (2 years)

- Led team of 20+ global security service delivery managers
- Responsible for monthly recurring revenue stream of 1.5M
- Developed initiatives to drive renewals to 95% for participating customers
- Drove engagement and utilization of personnel from 65% to 100% in one

quarter Device Management Service Delivery Manager (2 years)

- Responsible for team management of health, policy, audit and compliance of infrastructure firewall clusters that service over 20,000 managed devices
- Architected procedural changes that allowed for operational deployments of over 200 policy changes per week for specialized customers
- Led project to consolidate 4 disparate information repositories into a single knowledge base for MSS engineers and customers
- Led large-scale projects to re-engineer MSS customer portal to allow for accurate ticket submissions and track customer service allocation

Senior Global Security Operations Manager & Senior Manager (2 years)

- Oversight of tactical delivery of portfolio services for the largest global clients
- Supported Executive briefings for top clients
- Service delivery leader for 6 global SOC locations
- Leader for global team of 30+ firewall security engineers and IDS analysts
- Senior escalation point for customer delivery issues
- Led development and implementation of priority support engagement
- Led device management group in engineering development projects
- Worked across functional teams to streamline device deployment processes and decreased QA time to less than 24 hours
- Provided training for customer relations personnel on SOC processes and procedures

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

John Henderson

Education / Certifications:

- Bachelor of Science, Computer Networks and Cybersecurity, University of Maryland 08/2022
- Offensive Security Web Expert (OSWE)
- Offensive Security Certified Professional (OSCP)
- eLearnSecurity Penetration Tester (eCPPT)
- eLearnSecurity Web Application Penetration Tester (eWPT)
- eLearnSecurity Junior Penetration Tester (eJPT)
- CompTIA Network +, Security +, CySA +
- Microsoft Certified Azure Fundamentals (AZ-900)
- Application Experience: AWS, VMWare, Kali Linux, Metasploit, Burp Suite Pro, Nessus, Palo Alto Cortex, GhostWriter, Packet Tracer

Professional Experience:

PLEX Cyber LLC Aug 2022 - Present

Principal Penetration Tester | July 2023 – Present

- Led and executed comprehensive penetration tests on diverse systems, networks, and applications, identifying and exploiting vulnerabilities to assess overall security posture.
- Conducted thorough analysis of penetration test results, delivering detailed reports outlining identified vulnerabilities, their severity ratings, and recommended remediation strategies
- Conducted extensive source code review as part of penetration testing engagements, meticulously analyzing software code to identify security vulnerabilities, potential logic flaws, and insecure coding practices.
- Performed comprehensive penetration testing on wireless networks, utilizing advanced techniques and tools to identify vulnerabilities, such as weak encryption, unauthorized access points, and misconfigurations, ensuring the overall security and integrity of WiFi infrastructures.

SOC Analyst | May 2023 – Present

- Demonstrated expertise in threat detection and response, effectively identifying and mitigating potential threats. Monitored network traffic, analyzed security logs and alerts, and collaborated with security team members to ensure timely incident resolution.
- Developed and implemented efficient incident response plans, enabling swift and effective responses to security incidents, and minimizing organizational impact.
- Ensured compliance with regulatory standards by staying informed of requirements, conducting assessments, and implementing necessary measures to maintain a compliant environment.
- Produced detailed reports and effectively communicated findings to diverse stakeholders, including executives, IT staff, and end users, facilitating informed decision-making and promoting a culture of security awareness throughout the organization.

Penetration Tester | Aug 2022 – July 2023

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

- Communicates, coordinates, and performs penetration tests and security assessments at application, system, and enterprise levels.
- Assists with reconnaissance, threat modeling, vulnerability identification, authorized exploitation, and post-exploitation cleanup.

U.S. Marine Corps Dec 2014 - Dec 2019

Signals Intelligence Collector

- Collected, analyzed, and integrated complex intelligence data from multiple sources for senior clients in the intelligence community, providing accurate information to key decision makers.
- Performed short and long-term SIGINT analysis and fused collected data with various intelligence disciplines into reports to be used by partnering intelligence organizations.

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

Justin Frazier

Education/Certifications:

- Master's, Business Administration, Liberty University, 2020
- Master's, Leadership, Liberty University, 2019
- Bachelor's, Business Communication, Liberty University, 2017
- Bachelor's, Cybersecurity, Western Governor's University, 2024
- Associate's, Human Resource Management, Community College of the Air Force, 2020
- Mitre ATT&CK Defender Cyber Threat Intelligence, Microsoft Data Analytics, ScrumMaster, ITIL4, A+

Professional Experience:

PLEX Cyber, Senior Cybersecurity Engineer, 01/2022 - Present

- Support organizational security with focus on vulnerabilities, patching, and risk management
- Develop processes for monitoring, detecting, managing, and analyzing security vulnerabilities and offer recommendations for mitigation
- Manage asset protection, incident response, security configurations and security reporting
- Partner with IT teams to enhance security posture of IT infrastructure

U.S. Air Force (ANG), Cyber Warfare Officer (Sr. Manager, Red Team Operations) 10/2020 - 04/2023

- Supervised 2 managers, 4 individual contributors conducting threat intelligence analysis, penetration testing, and security strategy
- Interpret and provide direction on Department of Defense policy changes and cybersecurity news/trends

Textron Aviation, Senior Cybersecurity Analyst, 03/2022 - 01/2023

- Responsible for cyber incident response, eDiscovery, continuous improvement, and cyber investigation programs
- Supervise 7 cybersecurity contractors, manage/prioritize projects
- Palo Alto firewall management ●AD, Azure/Intune asset

Textron Aviation, IT Business Intelligence/Advanced Analytics, 07/2020 - 03/2022

- Oversaw BI system reliability for all company departments
- Consulted internal depts on analytics development, data usage, insight extraction, and business decision making
- SME for Power BI report development and data manipulation (SQL)

U.S. Air Force (ANG), Human Resources Manager, 10/2017 - 10/2020

- Coordinated personnel actions (supervised 1 HR business partner)
- Counsel employees on training, promotions, contracts, career moves

Textron Aviation, Sales, Operations, and Pricing Analyst, 05/2019 - 07/2020

- Developed automated pricing strategy –featured in aviation magazine
- Used market/industry factors to create/adjust product pricing

Textron Aviation, Safety Engineer, 12/2017 - 05/2019

- Analyzed human factors, enhanced production/supply chain processes
- EHS compliance lead for 1300+ personnel, 20+ facilities, 8 countries

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

U.S. Air Force, Program Manager, 12/2016 - 10/2017

- ●Managed EHS, Fitness, and Facilities programs for 650 employees
- ●Ensured adherence of federal, state, and local policies

U.S. Air Force, Aircraft Maintenance Lead, 04/2012 - 12/2016

- ●Led repair teams for U-2/A-10 aircraft, +2 overseas tours

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

Kevin O'Malley

Certifications:

- CISSP (Certified Information System Security Professional) 2018

Professional Experience:

July 2019 – Present
CISO for Lee County Florida

Having three years' experience as a CISO in Lee County, I have a new perspective on security and the importance of human behavior. While it is important to have a holistic view of the technical side of security and be conversant with technical controls, understanding human behavior and the security culture of an organization are critical elements of security. With this new perspective, I have been able to implement a successful security training program for Lee County which has created a stronger security culture which is measurable and helps to convey to key stakeholders the incremental successes made at each new simulation.

It has become very clear that a CISO in the public sector should have a close relationship with Emergency Management. The sharing of expertise and experience has been essential as the nexus between the cyber-physical world grows. The planning experience, co-presentations and the grant writing skills have been invaluable to the overall cybersecurity facet of the county. Monthly meetings along with sharing of resources has helped make a strong bridge between these two domains.

Chief Information Officer 2009 – June 2019 Jackson, MS

- Setup a Security Awareness program using Knowbe4.com
- Work with 3rd party vendor to get PCI DSS compliant
- Write IT security policies, procedures and guidelines
- Implemented a PII, CHD, and HITECH program to review and make changes to how sensitive data is retained and handled
- Work with facilities director and security consultant on physical security and ICS security
- Work with CFO and agent on cyber security insurance policy
- Work with 3rd party vendor to perform IT security audit
- Designed and implemented with HR a new onboarding process
- Moved LMS system from local to cloud (SaaS)
    - Work with senior management on communicating move
    - Worked with finance department on contracts
    - Work with vendor on timeline implementation
    - Work with system admin on exporting data
    - Coordinated and developed training of employees
- Approve all IT purchases and keep IT budget of accounts
- Manage technical staff

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

Formed technology consulting firm 2004 – 2009 ProData Tech Jackson, MS

- Network Design
- Trial Preparation of Exhibits
- In Trial Presentation

Director of Technology 1996 – 2004 St. Andrew's Episcopal School Jackson, MS

- Worked with Administration and staff on the implementation of new records management software
- Developed and implemented laptop program for grades 5-12th grade
- Designed and installed wireless infrastructure
- Designed network infrastructure and PC deployment
- Developed and implemented a faculty and staff training program

Interim Head of Middle School and AP Latin Instructor 1994 – 1996 St. Andrew's Episcopal School Jackson, MS

- Work with Board and Division Heads to implemented new policies and procedures to enhance communication and governance throughout the school
- Worked with Faculty and Student Handbook Committee to develop a more consistent set of rules to govern the school

Latin Instructor and Dean of Students 1991 – 1993 St. Andrew's Episcopal School Jackson, MS

- Taught all Middle School Latin, Latin IV, and AP Latin
- Scheduled all classes for Middle School
- Worked with parents, students, and faculty on disciplinary issues

1985 – 1990 St. Andrew's Episcopal School Jackson, MS

- Latin and Algebra 1 Instructor
- Assisted with Middle School scheduling

Education

1980–1984 Millsaps College Jackson, MS

- B.A., Latin.
- Minor in Music
- Graduated Magna Cum Laude

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

Resume TBD

DocuSign Envelope ID: 385F29BA-CBBC-4548-8DC9-ED0040795789

IN WITNESS WHEREOF, the parties have executed this Agreement for Piggyback Purchase as of the last date written below.

APPROVED as to Form for the Reliance of Lee County Only

BY: DocuSigned by: Andrea Fraser D7B0A432435E448...
County Attorney's Office

DATE: 9/18/2023 | 8:09 AM EDT

COUNTY: LEE COUNTY, FLORIDA
BOARD OF COUNTY COMMISSIONERS

BY: DocuSigned by: C95488F9BF0F428...
Chair
Board of County Commissioners of
Lee County, Florida

DATE: 9/19/2023 | 3:58 PM EDT

ATTEST:
CLERK OF THE CIRCUIT COURT

BY: DocuSigned by: Melissa Butler B72C163D219C464...
Deputy Clerk

DS

BOARD OF COUNTY COMMISSIONERS SEAL LEE COUNTY, FLORIDA

IT Staffing and Consulting, Inc. D/B/A ISC

BY: _____
Authorized Signature

Edwin Lott
Authorized Signature Printed Name

President
Authorized Signature Title

DATE: 7/21/2023