LEGEND **GLENN**

LinkedIn| legendglenn001@gmail.com |Portfolio

SUMMARY

Dedicated and results-oriented professional with a proven track record in seeking a federal position. Adept at navigating complex regulatory landscapes and leveraging analytical skills to drive strategic decision-making. Strong background as an IT Specialist, coupled with a commitment to excellence and attention to detail. Recognized for effective communication and collaboration in interdisciplinary teams. I have a proven ability to meet and exceed project milestones and deadlines. I am eager to contribute my expertise to state / federal/federal contract jobs in a role that demands both innovation and compliance with federal standards.
I look forward to providing my expertise to the state or federal government.

Tools

- Virus Total
- Talos File
- Malware Information Sharing Platforms
- Splunk
- Scapel
- Volality
- Wire Shark
- URL SCAN
- STIX
- Threat Connect
- SQL, C++,Python
- FTK IMAGER
- Windows Server 2016/2019
- SCCM
- NMAP
- The Cyber Kill Chain Framework
- Linux CLI
- Deep Blue CLI
- KAPE
- Windows Event Log
- Snort

SKILLS

- Cyber security
- Network Administration
- Risk Management
- Leadership and Team Management
- Cyber security Proficiency
- Project Planning and Execution
- Customer Service Excellence
- PowerShell
- ProcDump
- Splunk Administration
- SQL, C++,Python
- Technical Proficiency
- Network Administration
- Ticketing System Management
- IT Support
- KAPE
- Linux CLI
- MISP
- Azure AD
- Scalpel, Sigma
- Snort

EXPERIENCE

System Administrator **02/2022 to Current**
Norfolk State University **Norfolk, VA**
Dynamic system administrator with expertise in configuring secure servers, managing IAM duties, and implementing security procedures, ensuring compliance with VITA Sec 501. Documented processes, reduced downtime by 90%, and facilitated the successful migration from UNIDATA to SQL, enhancing cybersecurity. Proven ability to scope technical requirements, provide top-tier customer service, and architect efficient systems for federal entities.

- Documented system processes and technical SOPs, contributing to the creation of a comprehensive knowledge base for seamless transition and operational efficiency in federal roles.
- Works with stakeholders to identify and recommend methods for incorporating promising technologies to meet organizational IT requirements based on their ability to stay current on emerging technologies and their applications to current and emerging business processes (e.g., cloud, mobile).
- Builds practical solutions that fully consider the lifecycle of costs, acquisitions, programs and projects, management, and budget.
- Managed accounts, network rights, and system access, ensuring the implementation of security procedures and compliance with federal standards.
- Ensured all authorization documentation is current and accessible to properly authorized individuals
- Used query languages to maintain critical databases and provide reports to stakeholders.

- Architected and maintained critical systems and processes for a university, showcasing expertise in designing and implementing information technology solutions.
- Ensured that data ownership and responsibilities are established for each authorization boundary, to include accountability, access rights, and special handling requirements.
- Provided technical support for secure software development and integration tasks, including reviewing work products for correctness, and adhering to the design concept and to user standards.
- Scoped and analyzed technical requirements, demonstrating a keen understanding of federal standards and regulations to ensure compliance in collaborative environments.
- Provided responsive technical support, ensuring timely completion of IT tickets, and minimizing downtime. Maintained open tickets below five 90% of the time, emphasizing efficient problem resolution.
- Identified and evaluated complex business and technology risks to upgrade the enterprise environment
- Develop impactful reports and presentations that support the achievement of engagement goals and objectives.
- Possesses experience with software tool integrations, including REST APIs, SOAP, and APIs
- Coordinated the implementation of IT-focused technologies across Tier I, II, and III systems to ensure advancement of the organization
- Reviewed, advised on, and conducted complex analyses, evaluations, and investigations in support of organizational programs, systems, and processes where definitions, methods, and/or data are incomplete, controversial, or uncertain, with boundaries that were extremely broad and difficult to determine in advance to advise leadership about return on investment, and future technology needs.

Cyber Analyst Intern **05/2021 to 08/2021**
Canon Virginia, INC **Newport News, VA**

Adept at configuring and optimizing network servers, implementing robust security procedures through Active Directory, and monitoring suspicious activities using Elastic SIEM. Demonstrated proficiency in installing software across corporate networks and providing responsive technical support. Successfully established a Hyper V Test Lab and optimized resources, resulting in significant cost savings. Seeking to leverage this experience for a seamless transition into federal cyber security roles.

- Configured and optimized network servers, achieving a 15% increase in system efficiency.
- Implemented stringent security procedures via Active Directory, reducing potential vulnerabilities by 20%.
- Managed and upgraded Windows and Linux Systems.
- Evaluated threats and vulnerabilities to ascertain whether additional safeguards are needed
- Experience maintaining and providing security within an enterprise infrastructure and network.
- Defensive Cyber Operations analyst monitoring elastic stack SIEM for anomalous activity, creating monitoring queries, and initiating incident response activities upon detection of anomalies.
- Provided responsive technical support, ensuring timely completion of IT tickets and minimizing downtime to 99.5% uptime.
- Established a cost-effective MINIO storage system, resulting in $60,000 in organizational savings.
- Demonstrated expertise in cyber domains, including vulnerability assessment and scanning tools and assessing system compliance with security controls
- Ensured that system security requirements are addressed during all phases of the system life cycle
- Monitored and analyzed suspicious activities through Elastic SIEM, enhancing the company's cyber threat detection capabilities by 30%.
- Performed security reviews, identified gaps in security architecture, and developed security risk management for designated systems

IT Technician **03/2019 to 05/2021**
Old Dominion University **Norfolk, VA**

Results-driven and detail-oriented IT professional with a strong foundation in Cybersecurity, a graduate of Old Dominion University with minors in Information Technology and Risk Management. Over 2+ years of hands-on experience as an IT Technician and Help Desk Operator, successfully leading a team of student workers in network administration functions across a large campus serving over 24,000 users.

- Played a key role in onboarding and training new employees, reducing the learning curve by 30% and accelerating their integration into the work environment.
- Conducted comprehensive training sessions for 15+ new employees, ensuring proficiency in utilizing workstations and peripheral devices
- Managed the Service Now Ticketing System, focusing on meeting or exceeding service level agreements (SLAs) for issue resolution.
- Successfully submitted and tracked over 500 tickets, maintaining a 98% on-time resolution rate, showcasing a proactive problem-solving approach and effective stakeholder communication.
- Demonstrated proficiency in managing the Service Now Ticketing System, consistently meeting or exceeding service level agreements (SLAs) for issue resolution.

EDUCATION

Master of Science: **Cyber security** **Expected in 05/2026**
Norfolk State University

Bachelor of Science: **Cyber security Information Technology& Risk Management** **05/2021**
Old Dominion University

Certifications

- Splunk Core Certified User
- Blue Team Level 1
- CompTIA CYSA+CSO-003
- Certified in Cybersecurity (ISC2)
- CompTIA Security+ SY0-601
- CompTIA Network + N10-008