
A. Vince Tolentino

U.S. Navy Veteran • Active TS/SCI CI POLY • Washington, DC • tolentino.anthonyv@gmail.com • (773)-308-5720

Education

American Military University

Bachelor of Science, Cybersecurity, GPA 3.7

Charles Town, WV

July 2024

Western Governors University

Master of Science, Cybersecurity Information Assurance, GPA 4.0

Millcreek, UT

May 2027

Certification

ISC2 Certified in Cybersecurity (ISC2 CC)

August 2026

CompTIA Security + CE

June 2024

Experience

King Cyber LLC

Washington, DC

Senior Information Systems Security Engineer

May 2025 – Present

- Lead cybersecurity strategy across multiple Navy Mission-critical systems, designing and implementing a standardized RMF process that improved Authority to Operate (ATO) readiness by 30% and reduced accreditation delays.
- Secured ATO for 6+ mission-critical systems by delivering complete RMF accreditation packages that meet DoD, NAVIFOR, and Navy cybersecurity standards.
- Cut High/Cat 1 vulnerabilities by 75% across mission-critical systems by driving coordinated remediation with system owners and engineering teams.
- Brief Navy leadership on cyber risk and system security status, turning technical findings into clear, actionable recommendations for decision-makers.
- Identify security architecture gaps and implement mitigations that reduce repeat POA&M findings and strengthen overall security posture.
- Automate compliance reporting, data collection, and security validation through scripting, reducing manual effort and improving report accuracy.
- Conduct vulnerability assessments across applications, systems, and cloud-hosted environments, and monitor results in ACAS to enforce DISA STIG and CSSP compliance.
- Sustain continuous FISMA and DoD compliance through annual reviews, security impact analyses of system changes, and artifact validation in eMASS, DITPR-DON, and VRAM.

Serco Inc

Washington, DC

Information Systems Security Engineer

August 2024 – May 2025

- Led development and submission of RMF accreditation packages, securing ATO for multiple Navy systems.
- Developed and implemented Navy cybersecurity policies and procedures, establishing compliance with DoD, NAVSEA, and SEA 05Q standards across all supported systems.
- Directed annual cybersecurity assessments for TEAM SUB systems, performing comprehensive reviews to ensure FISMA and DoD compliance.
- Managed cybersecurity posture for a diverse system portfolio, validating artifacts and tracking compliance in eMASS, DITPR-DON, and VRAM.

Apex Systems

Washington, DC

Cybersecurity Intern

April 2024 – August 2025

- Built an end-to-end Elastic Stack SIEM environment, deploying Elastic agents on a Kali Linux VM to collect and forward logs for centralized security monitoring.
- Designed custom Elastic SIEM dashboards and created and test alert rules for specific security events, enabling faster pattern recognition and proactive incident response.
- Simulated attack activity with Nmap and investigated the resulting events through SIEM queries,

strengthening threat detection and incident investigation skills.

- Configured and managed a pfSense firewall to enforce network security policies and detect potential threats through traffic monitoring.
- Performed network discovery and troubleshooting using Nmap, Wireshark, and TCP/IP analysis, identifying open ports, running services, and potential vulnerabilities.

U.S. Navy

Washington, DC

Chief of Operations, Senior Signals Analyst, Mission Manager

May 2013 – August 2024

- Led and managed teams of 45+ personnel on critical national missions, including civilians conducting highly sensitive intelligence operations, strengthening secure information handling and mission assurance practices.
- Conducted advanced technical analysis of foreign communications systems, identifying vulnerabilities, operational risks, and emerging threat patterns.
- Performed detection, acquisition, geolocation, and exploitation of signals using complex systems – skills directly aligned with cyber security threat analysis and incident investigation.
- Analyzed and reverse-engineered previously unseen microwave and RF signals, developing technical procedures for extracting and securing critical data.
- Producing intelligence reports and trend assessments that informed leadership of evolving threats, risk posture, and operational impacts.
- Optimized and maintained classified processing pipelines and mission systems, ensuring secure and reliable functionality across multiple domains.
- Managed secure data handling and system integrity as a Data Transfer Agent, protecting \$2 Million dollars in classified systems and equipment.
- Collaborated with U.S. and partner-nation intelligence/cyber units to identify and mitigate threats to friendly communications and network systems.

Skills & Interests

Technical: Windows, Linux, MacOS, SIEM Platforms, Wireshark, Pfsense, Nmap, Nessus, Snort, Microsoft Office, eMASSTER, Evaluate-STIG, SCAP, STIG Viewer

Language: English and Tagalog

Employment: My self-motivation, hard work, and dedication all contribute to the continuing success of my employer.

Technically competent. A natural leader and team player. Expertise in secure-system development, risk analysis, emerging technologies, and security best practices. Proven ability to manage complex projects, build practical solutions, and translate technical concepts for non-technical audiences. Skilled in collaboration, communication, and exceeding expectations.