SHAWN WALSH

Cybersecurity Consultant | Cyber Risk & Threat Intelligence SME

207-610-4712 | shwnwalsh@gmail.com | linkedin.com/in/shawnpatrickwalsh | shawnpatrickwalsh.com

PROFESSIONAL SUMMARY

Cybersecurity leader with 11+ years of experience spanning high-stakes cyber operations, threat intelligence, and cyber risk assessments across national-security and enterprise environments. Combines operational experience supporting NSA and Joint Special Operations Command (JSOC) cyber missions including planning and executing complex cyber operations with current work leading mission-based cyber resiliency assessments and cyber test strategy for complex, billion-dollar Department of War acquisition programs. Serves as a cyber risk assessment subject-matter expert supporting a 23-program portfolio, helping program stakeholders identify exploitable conditions, shape risk-informed test approaches, and prioritize actions that strengthen system resilience and survivability. Proven leader of diverse technical teams, cross-functional initiatives, and executive-level engagements, translating complex cyber findings into clear, actionable recommendations. Special Operations Marine veteran.

CORE SKILLS

- Cyber Risk & Resiliency Assessment
- Cyber Operations Planning & Execution
- Vulnerability & Attack-Path Analysis
- Program & Portfolio Management
- Cross-Functional Team Leadership
- Technical Training & Mentorship
- Cybersecurity Test Strategy & Evaluation
- Threat Intelligence & Adversary Analysis
- Risk Mitigation Strategy
- Executive Advisory & Technical Briefing
- Stakeholder Engagement
- Mission-Critical Systems Resilience

PROFESSIONAL EXPERIENCE

ASTRION **Eglin AFB, Florida**

Cybersecurity Risk Assessment SME *2025–Present*

- Serving as a Mission-based Risk Assessment Process for Cyber (MRAP-C) Subject Matter Expert for the 48th Cyber Test Squadron, executed multiple assessments, highlighted by directing and leading the first-ever multi-national MRAP-C in the Department of War (DoW). This historic event integrated a Five Eyes (FVEY) international partner, delivering a landmark evaluation that validated joint-coalition cyber resilience and established the technical framework for future collaborative international test operations across the defense enterprise.
- As lead contractor for the DoW's Cross Service Working Group (XSWG) efforts, spearheaded the planning and end-to-end execution of CyberDT XSWG-19, a TEMS-style conference managing 28 speakers across classified and unclassified settings and hosting 200+ hybrid attendees. Fostered critical inter-agency networking and secured strategic alignment across the test and evaluation enterprise.
- As 48th CTS lead for the DTE&A DoW-directed CROC effort, directed a 10+ person joint team that produced 13 enterprise-level exemplar documents, including the primary TES and DT Test Plan templates. Facilitated a high-visibility, hybrid MRAP-C event for 40+ attendees in-person and virtually, bridging technical communication gaps and solidifying baseline test compliance across the test and evaluation community.
- Named Contractor of the Quarter for the 48th CTS in both Q2 and Q3 FY26 (out of 200 contractors) for leadership on the XSWG-19 conference and DTE&A CROC standardization effort.
- Achieved the "Advanced" qualification tier in DCWF WRC 671 (System Test and Evaluation Specialist) and WRC 752 (Cyber Policy and Strategy Planner), bringing immediate workforce compliance to the squadron and applying advanced cyber knowledge to strengthen 48th CTS efforts.

NATIONAL SECURITY AGENCY **Fort Meade, MD / Augusta, GA**

Note: the roles below reflect concurrent and successive duties across NSA-supported assignments, including operational control through the U.S. Marine Corps.

Cyber Exploitation Analyst / Threat Intelligence & Operations Lead *Fort Meade, MD | 2020–2025*

- Conducted in-depth cyber network analysis and capability pairing, identifying vulnerabilities and collaborating with developers to create new capabilities for cybersecurity projects and organizations.

- Gathered and synthesized cyber threat intelligence to identify adversary tactics, techniques, and procedures (TTPs), delivering actionable insights that shaped strategic security decisions and operational priorities.
- Leveraged packet capture and native log analysis to uncover indicators of compromise (IOCs), trace adversary activity, and support remediation of sophisticated threats, including profiling APTs and state-sponsored actors.
- Delivered executive briefings and clear, actionable reports to leadership, translating complex technical findings into strategic recommendations.
- Supervised and directed a cross-functional team as a senior Exploitation Analysts and Threat Intelligence Analysts, directing targeted operations that neutralized a top-priority threat to national and partner security.

Program Manager / Trainer *Fort Meade, MD | 2018–2025*

- Oversaw strategic planning, execution, and coordination as Program Manager for a national-level cybersecurity program, supporting cyber operational objectives and threat intelligence initiatives across four national-level projects; recognized with the Defense Meritorious Service Medal for exceptionally meritorious service in a position of great responsibility.
- Scoped and launched three cybersecurity projects, expanding mission coverage and directing daily activities of analysts and operators to achieve strategic collection and vulnerability assessment objectives.
- Trained and evaluated 40+ analysts and operators as an Exploitation Analyst Trainer, developing cross-functional team proficiency in malware analysis, phishing campaign detection, and threat actor profiling across multiple organizations and toolsets.
- Briefed executive leadership and program managers daily on ongoing operations, translating complex technical findings into actionable solutions to mitigate emerging threats and support informed decision-making.
- Directed multiple operational surges with joint military and special operations teams, enabling full access to adversary networks and pioneering innovative approaches to high-value targets within sophisticated threat landscapes.

Threat Intelligence Analyst / Threat Hunter *Augusta, GA | 2015–2020*

- Supervised and directed a multidisciplinary team in executing advanced cyber threat assessments, proactively identifying and mitigating high-priority risks to national and partner security; recognized with a Joint Commendation Medal for exemplary leadership and analysis.
- Interpreted complex threat data to reveal patterns in attacker methodology using frameworks comparable to MITRE ATT&CK, such as the Cyber Kill Chain, equipping decision-makers with insights that shaped organizational security strategies.

Transition Program Manager / Career Development Advisor *Augusta, GA | 2017–2019*

- Managed career development and transition processes for 100+ personnel, ensuring smooth workforce continuity and retention.
- Revitalized a struggling military transition program, elevating it to the highest performance rating within one year; recognized with a military commendation for outstanding achievement.

EDUCATION

Master of Science, Cybersecurity Technologies — University of Maryland Global Campus
Bachelor of Science, Computer Networks and Cybersecurity — University of Maryland Global Campus
Associate of Arts, Computer Studies — University of Maryland Global Campus

CERTIFICATIONS & TRAINING

- **Certificate** CompTIA SecurityX (estimated completion 11/2026)
- **Certificate** CompTIA Cloud+ (estimated completion 10/2026)
- **Certificate** CompTIA Security+
- **Certificate** NSA Core Exploitation Analyst (CEA)
- **Certificate** NSA Apprentice Exploitation Analyst (AEA)
- **Certificate** NSA Apprentice Exploitation Analyst Trainer (AEAt)
- **Certificate** GIAC Open Source Intelligence (GOSI) SEC487
- **Training** Holistic Analytic Mastery and Refinement (HAMR) (320 Hours)
- **Training** Senior Joint Force Leader Development Course (SEJPME 80 hours)
- **Training** Intermediate Cyber Course (ICC) (360 Hours)
- **Training** Joint Cyber Analysis Course (JCAC) (1008 Hours)