**John Bradley Webb IV**

Clearance: **Active TS/SCI Clearance** 757.754.3080 | [john.b.webb4@gmail.com](mailto:john.b.webb4@gmail.com) | [www.linkedin.com/in/john-b-webb4](http://www.linkedin.com/in/john-b-webb4) **GitHub:** <https://github.com/jwbizz08>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**WHAT I CAN DO FOR YOU**

**Dynamic and skilled Cybersecurity Professional** with over 13 years of experience in intelligence operations, cyber threat analysis, cybersecurity defense, electronic warfare, and operations management. Currently serving as a Cyber Watch Analyst at Peraton, operating from the CISA Operations Center to oversee and respond to threats targeting national critical infrastructure. Proficient in triaging, creating, updating, and documenting tickets, leveraging an in-depth knowledge of computer and network architecture. Adept at utilizing open-source research, forensic analysis, log review, correlation, and packet capture (PCAP) analysis for comprehensive threat investigations. Known for exceptional communication skills, effective collaboration within enterprise teams, and a strategic approach to enhancing cybersecurity defenses. Committed to safeguarding critical infrastructure through continuous improvement and robust incident response strategies. Holds an **MBA in Cyber Forensics and Information Security Management** and a **CompTIA Security+ CE** certification.

**Core Competencies & Technical Credentials**

Tactical/Strategic Planning | Program Management | Software Testing | Personnel Management | Project Management | Target Development | Effective Communication | Information Security Quality Assurance | Vulnerability Assessment &amp; Tracking | Risk Evaluation | Agile | Intelligence Collection Management | Incident Response | Threat Intelligence | Electronic Warfare | Database Management | Team Enterprise Cohesion & Collaboration | Complex Problem Solving | Cyber Forensics | Intelligence Operations

**Intelligence Analysis Tools**: Gale | MIST | DEFSMAC | Widow| NASIC | CMD | | Analyst Notebook | JTT | TDL | ABMS | Thresher | Aspen | NCTC Online | Google Earth | ArcGIS | CED | IC Reach SIGINT database | CHROME | First Alert | Shodan | Virus Total | Alien Vault | Metasploit |

**Malware Analysis Tools:** Wireshark | Splunk (SIEM) **Languages:** Python | PowerShell | Bash | HTML

**Microsoft Applications:** Azure | WSUS | GPO | Windows Server 2019 | Microsoft System Center Configuration Management | Active Directory | Microsoft Office Suite Word, Excel, and PowerPoint

**Monitoring Tools:** | Remote Desktop Connection | NMAP | Tenable Nessus | Remedy | Service Now | JIRA | AN/ULQ-16 | SLQ-32 | GCCS-M | Splunk | Wireshark | Snort

**Vulnerability Assessments:** Nmap, Tenable Nessus

**Network Optimization**: Consolidated Afloat Networks and Enterprise Services (CANES) | Real-Time Spectrum Operations (RTSO)

**Operating Systems**: Ubuntu Linux, Kali Linux, Microsoft Windows **Virtualization**: VMware, Virtual Box

**Governance, Risk, and Compliance Tools**: eMASS | DISA STIG Viewer **Cloud Operating Platforms:** Azure, AWS

**Work Experience**

Peraton, Arlington, Virginia (06/2024–Present)

Cyber Watch Analyst, Cyber Intelligence Senior Associate 06/2024–Present

* Operate from the Cybersecurity Infrastructure Security Agency (CISA) Operations Center to oversee and respond to threats targeting national critical infrastructure, ensuring compliance with government directives and policies.
* Utilize open-source intelligence collection techniques to systematically gather and analyze critical data to enhance threat detection and situational awareness for critical infrastructure protection.
* Prioritize inquiries and security incident response events related to Critical Infrastructure (CI), leveraging expertise in troubleshooting and accountability to gather diverse, classified information for accurate, timely intelligence delivery.
* Analyze and draft investigation reports and articles on cyber threats, including Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs), disseminating findings to government leadership and law enforcement agencies.
* Maintain coordination of cyber reporting across federal agencies and industry partners triaging, creating, updating, and documenting tickets via Service Now and Remedy tracking systems, enhancing the collective response capability to cyber incidents impacting critical infrastructure.
* Collaborate with Communications and Physical teams during cyber incidents impacting CI sectors, identifying vulnerabilities, alert logic triage, and implementing procedures to enhance security posture for national customers.
* Manage cyber incidents by conducting root cause analysis, interpreting technical reports for non-technical audiences, and coordinating cyber reporting across federal agencies and industry partners.

RapidAscent Cybersecurity Analyst Internship, Remote (DoD Skillbridge) (01/2024-06/2024)

Cybersecurity Analyst Intern 01/2024-06/2024

* Ensured security standards and compliance through STIG application and NIST framework assessments tracking in eMASS.
* Created PowerShell scripts for automated security log analysis, boosting threat detection.
* Established virtual environments with VMware, and VirtualBox for network scenario testing.
* Developed Python, and Bash scripts for system updates, reducing manual workload by 30%.
* Conducted network scans with Nmap/Nessus, host, and network forensics for vulnerability identification.
* Analyzed network traffic with Wireshark, and processed logs with a custom Splunk dashboard and alerts for monitoring.
* Proficient in Windows, Ubuntu, and Kali Linux; configures Windows Server 2019, and manages Active Directory.
* Conducted PCAP utilizing Wireshark for intrusion detection system anomalies.
* Hardened Unix, and Linux file systems for simulated user groups and databases.
* Executed cybersecurity defense operations in AWS, and Azure cloud environments to counter simulated adversary activities.
* Designed fortified network infrastructures; crafted segmentation plans to minimize ransomware impact.
* Implemented and managed WSUS for streamlined distribution of critical updates across the network, utilizing Group Policy Objects (GPOs) to enforce and automate update policies and configurations, ensuring compliance and minimizing system vulnerabilities.

United States Navy, Littoral Combat (LCS) Ship Squadron Two, Jacksonville, Florida (02/2021-06/2024)

Lead Intelligence Operations Assessment Specialist 12/2021-01/2024

* Orchestrated crisis management strategies, resource allocation, and inter-agency coordination during critical incidents. Managed incident command systems, conducted risk assessments, and facilitated joint exercises with military units.
* Oversaw system administration and information security assurance governance for the CHROME database, managing user access privileges, ensuring data security, and maintaining system integrity.
* Trained, assessed, and certified eight LCS in surface intelligence and visual information warfare operations for worldwide deployment missions.
* Provide daily and weekly intelligence updates on commands intelligence interest for executive leadership and department heads.
* Instituted training programs for unit intelligence personnel, ensuring 100% compliance with professional qualifications and enhancing team effectiveness.

Intelligence Oversight Officer 12/2021-12/2023

* Directed program governance for 15 Intelligence Oversight Officers, overseeing inspections and program integration. Prepared for Inspector General inspections, annual reviews, and quarterly reports for 15 IO programs, ensuring compliance and fostering a culture of excellence.
* Prioritized and conducted quarterly risk and compliance inspections for eight IT enterprises, ensuring 100% adherence to NIST, HIPAA, PII, cyber, and intelligence oversight regulations and government standards.
* Established and conducted multi-facility training programs for 300 personnel on information and government security standards.

United States Navy, Information Warfare Training Group Norfolk, Norfolk, Virginia (12/2017-02/2021)

Information Operations Watch Officer 12/2017-2/2021

* Managed 60 employees through 766 tactical vulnerability assessments and 74 defense equipment casualty remediations, focusing on inventory management, compliance, and security protocols for strike optimization.
* Developed, maintained, and executed information technology architecture design plans utilizing Real-Time Spectrum Operations (RTSO) for 38 signal detection systems on six ships.
* Coordinated Windows triage for IT issues in Consolidated Afloat Networks and Enterprise Services (CANES), applying command prompt/CLI troubleshooting techniques for user support networks.
* Directed defense cyber operations, utilizing archive management and MITRE ATT&CK framework to monitor, and analyze Wireshark network traffic, contributing to threat detection, anomaly identification, and cybersecurity risk mitigation.
* Worked with third-party vendors to address information operations security concerns and enhance cybersecurity measures. Conducted systems updates and patch management for radar spectrum management and coordination systems.
* Managed and created through HTML code for two Share Points on SIPR, and NIPR for daily data updates, user privileges, and directory management.
* As executive information operations analyst, led strike group signals intelligence operations for six operation centers, conducted scientific and technical studies against adversary technologies, and developed policies and instructions for SIGINT operations in various theaters.
* Oversaw all-source intelligence watch center monitoring and collection of real-time intelligence data, adversary IOC, TTPS, data logs, and technical reporting of critical adversary actions.
* Drove adversary incident response, and counter-targeting operations for six ships during enemy tactical engagements.

United States Navy, Naval Information Operations Center Colorado, Aurora, Colorado (12/2014-12/2017)

Blue Team Threat Analyst 10/2015-02/2016

* Monitored NCTC Online and ASAS global data sensors for target analysis and threat detection. Collaborated with cross-functional security teams to investigate 340 SIEM anomalies across various network systems. Analyzed 500 ELINT signatures and cross-referenced intelligence sources including Gale, MIST, DEFSMAC, Widow, NASIC, CMD, JWICS, and SIPR to produce detailed technical reports.

Command Assistant Operations Security Manager 04/2016-10/2017

* Remediated 230 non-compliance vulnerabilities and improved security resiliency as an operational security manager with information systems, business operations, physical security program, and information security, ensuring adherence to regulatory NIST, NSA, DoD, PII, requirements and enhancing overall security posture.

Intermediate TECHELINT Analyst: 02/2016-06/2016

* Monitored 30 global data sensors for 400 target analysis missions, conducting threat analysis and implementing archive interfaces with Analyst Notebook to safeguard critical information.
* Utilized Aspen to research signal characterization and radar system identification for 130 disruptive technologies. Analyzed threat intelligence, metadata, telemetry, IMINT, OPIR, OSINT, and ELINT data sources for credibility and reliability,

All Source lead Intelligence Analyst 06/2016-12/2017

* Managed eight intelligence analysts to produce 2,200 national-level reports for POTUS, CIA, FBI, FAA, and JCOS. Utilized ArcGIS to handle complex customer requests for information (RFIs) and delivered concise, clear reporting of findings. Employed Google Earth to collaborate with interagency partners on complex R&D requests concerning analog and digital device applications.
* Oversaw complex civil air analysis projects, driving innovation through the creation of data mining tools and advanced flight schedule analysis techniques. Achieved significant operational efficiencies, including a 430% reduction in daily embedded man-hours, a 4,200% increase in automation analytics, and $486K in cost savings through strategic process improvements and automation initiatives.
* Administered the Thresher intelligence database, ensuring data accessibility, security, and user privilege integrity. Conducted operational testing and intelligence integration throughout the software development lifecycle.

United States Navy, USS Theodore Roosevelt (CVN-71), Norfolk, Virginia (03/2012-12/2014)

Electronic Warfare Operator 07/2011-12/2014

* Conducted routine maintenance and critical troubleshooting on electronic warfare computer systems using Ivanti Patch Management, maintained SLQ-32 information assurance requirements and server administration standards with ANLQ-16 for fleet operations, and conducted incident investigations, risk assessments, and published audit reports in compliance with government regulations.
* Provided continuous monitoring of threat detection and anomaly discoveries within ship security operations and combat information centers, conducted threat hunting, and extracted threat intelligence data utilizing intelligence databases, open source, GALE, MIST, GCCS-M, JTT, DCGS-N, CMD, CED, and NIODB.
* Assessed 135 system vulnerabilities and prioritized corrective measures for remediation using Nessus, conducted operations tasks including scanning, log monitoring, and responding to 120 incident response events, and analyzed 620 ELINT signatures.
* Implemented shipboard emission control plans for 20 radar systems to manage electromagnetic emissions and signatures, and designed fortified network infrastructures with segmentation plans using SolarWinds to enhance system architecture and security.

C4I Engineering System Administrator 02/2013-10/2014

* Designed, developed, and integrated C4I systems for naval operations using GCCS-M and Aegis Combat System, conducted system testing, managed incidents with Remedy, and provided technical support and training. Collaborated with Navy teams and vendors via JIRA and Microsoft Exchange 2010, ensuring alignment with mission objectives and minimal operational disruption.

**Education**

Perdue University Northwest Campus *Cybersecurity Workforce Certification Training* Present

City University of Seattle *RapidAscent Cybersecurity Program (DoD Skillbridge)* 06/2024

Coursera *Google Cybersecurity Analyst Professional Certificate* 12/2023

American Military University *Masters of Business Administration-Cyber Forensics & INFOCSEC Management* 06/2023

Strayer University *Bachelors of Business Administration-Healthcare Service Administration* 03/2011

Centura College *Associate Degree of Science-Business Management* 09/2007

**National Security Agency Specialized Training**

*Signal Analysis Development Pipeline* 02/2016

**U.S. Navy Specialized Training**

*AN/USQ-151 Joint Tactical Terminal- Maritime (JTT-M) Operations (Operator)* 11/2018

*Information Operations Watch Officer* 11/2018

*Surface Electronic Warfare Operations-Journeyman* 05/2018

*Navy Information Operations Planning Course (NIOPC) (Planner)* 04/2018

*Surface Electronic Warfare Threat Recognition* 03/2018

*Electronic Warfare Applications (Advanced) (Coordinator)* 02/2018

*Intermediate Technical ELINT Analysis Sige3810 (Signals Analysis-ELINT)* 03/2015

*Command/Control/Communications/Computers and Intelligence (C4I) System Engineering (Administrator)* 02/2013

*Navy Operational Security Staff Planner* 09/12

*Intermediate National Operational (OPELINT) ELINT Analysis (Analyst)* 03/2012

**Industry Certifications**

CySA+ CE | CompTIA | Estimated 08/2024

Certified Scrum Master | Scrum Alliance | 04/2024

Security+ CE | CompTIA | 02/2024

Certified in Cybersecurity | ISC2 | 02/2024