John Haverly

www.greatresumesfast.com | 800.991.5187 | info@greatresumesfast.com | https://www.linkedin.com/in/jessicaholbrook/

Cybersecurity & Intelligence Executive

Solving our nation's complex technical challenges and protecting critical assets through focused leadership and expertise

IT Cyber Operations leader drives effective systems planning, engineering, and operations, ensuring security and readiness of network infrastructure and all elements of the end-to-end service chain.

Career Highlights

- *Fathoms organization threat impact from 20,000-ft. level*, maintaining team focus on optimizing capabilities while differentiating between perceived and actual threats as trusted advisor to C-suite.
- *Turned around major DoD contract* by assessing client needs, rebuilding trust, and properly utilizing existing technology inventory to secure and defend essential cyber assets.
- *Advanced from Air Force aviator to Command Chief Master Sergeant* (top 1% of top 1% of USAF) through work ethic, exceptional leadership of skilled teams, strategic planning and execution delivery, and technical expertise.
- *Propelled innovation and game-changing technological advances* to enable offensive posture of US in cyber warfare. Key player in developing all aspects of cyber operator and cyber analyst career fields within military.
- *Delivered 500+ global cyber infrastructure projects* on time/ahead of schedule, with cost savings of up to $1.2M.
- *Leverages vast network* of IT and cyber operations leaders across government, military, and private sectors.

MS in Cyber Intelligence | Active TS/SCI Security Clearance | "Best in Class" Cyber Operations Leader

Cybersecurity | Intelligence Operations | Thought Leadership | Consensus Building & Team Leadership | Budget Management | Lean Operations | Vulnerability Management | Cyber Forensics | Training & Professional Development | Technical Solution Delivery | Threat Assessment | Project Management | Incident Response | Risk Management | Network Defense | Penetration Testing | Multi-Source Fusion Reporting | Cross-Functional Collaboration | Vendor Relations

PROFESSIONAL HISTORY

XYZ, Arlington, VA, October 2017 to Present
Senior Manager for Computer Network Defense

Recruited to lead Computer Network Defense for major DoD client engagement supporting 1,700 users. Tapped for additional leadership roles including Senior Cyber SME, large-scale Problem Management, and PMO. Oversee 14 direct reports including 4 division managers executing vulnerability management, cyber protection, incident response, and cyber forensics analysis as well as protection management, cyber intelligence and reporting, and pen-testing. Senior advisor to CIO and government leaders on cyber risk to secure and defend essential cyber assets.

- Rebuilt client trust and course-corrected program after winning mismanaged DoD contract. Developed key relationships, assessed client needs, identified pain points and replaced incorrectly utilized technology in existing inventory, and assembled high-performing team to earn client praise for program turnaround.
- Spearheaded development of advanced cyber forensics capability, pinpointing appropriate technology and integrating technology into enclave, resulting in profound surge of in-house detection of cyber incidents across 42 national field sites and a secure evidence chain of custody.
- Entrusted with large-scale Problem Management oversight role, pulling from pool of 196 employees to drive end-to-end leadership from discovery to problem resolution for cross-functional problems related to vulnerability management, data management, cybersecurity, application management, customer service, hardware/software.
- Selected as keynote speaker for Southern Cyber Summit with 1,500+ attendees. Presented actionable insights related to human cyber risk measures to audience of security professionals.
- Supervise PMO including implementation of $30M budget to operate and defend three unique networks for DoD client engagement in accordance with SOW, exceeding KPIs.

UNITED STATES AIR FORCE (USAF), Various Locations, November 1990 to October 2017
Senior Cyber Operations Leader (June 2015 to October 2017)

Promoted to Command Chief Master Sergeant due to exceptional track record of leadership, results delivery, and expertise. Directed all operational, development, and utilization matters affecting 2,100+ cybersecurity personnel across 3 agencies, 13 branches, and 9 sections within the DoD and Intelligence Community (IC).

- **Cyber Defense Organization**: Played key role in strategic planning, development, launch, and optimization of USAF's first global cyber defense organization, meeting all goals under congressional scrutiny. Within 2 years, organization produced 996 highly trained cybersecurity employees and 80 technical weapons capabilities.
- Standardized Knowledge, Skills, and Abilities (KSAs) and industry-recognized certification training curriculum while developing cyber training and learning environment to meet DoD requirements.
- **CYBERCOM Cyber Mission Force** (CMF): Marshaled development of strategy, capabilities, and resources to meet vision for U.S. Cyber Command in DoD. Orchestrated 18 Cyber Protection Teams (CPT) of 64 people each and implemented $600M budget to build, test, and deploy cyber-mission systems, complete global CPT missions, and structure technical training of 1,300+ cyber operators.
- Heighted capabilities to defend critical cyber infrastructure across the U.S. through development and deployment of massive Cyber Vulnerability Assessment and Hunt weapon system and suite of tools utilized by CPT to analyze data and identify key indicators of compromised security.
- Modernized capabilities within organization across training, weapons system development, and program management, including budget and resource allocation management to ensure organization success.
- Propelled revolutionary advances in cyberspace operations capabilities through leadership of innovative technical team, development of 5 cyberspace weapon system qualification courses and introduction of Cyberspace Intelligence formal training component. Partnered with federal law enforcement agencies to share adversary cyberspace tactics, techniques, and procedures, enabling counter-intel operations to mitigate threats.
- Delivered 500+ worldwide critical infrastructure projects with $100M value 100% ahead of schedule and on-budget through supervision of multiple engineering and installation teams.

Senior Intelligence Leader (June 2014 to June 2015)

Promoted to Combatant Command, highest level of DoD operations, in joint position managing 370 military, civilian, and contract intelligence staff in supporting homeland defense. Senior advisor to intelligence director, provided data-driven intelligence to secure ports, airports, and airspace over and across homeland.

- Overcame intelligence ownership disputes between military and law enforcement by building consensus around priority of optimizing intelligence in support of homeland security.
- Broadened and enhanced intelligence community, facilitating intelligence sharing with El Paso Intelligence Center and optimizing allocation of manpower and resources across EPIC and Joint Task Force North, resulting in 40% increase in actionable intel and directly contributing to $240M narcotics seizure.
- Doubled intelligence production to IC partners and law enforcement through airborne ISR team.
- Enabled true multi-source fusion reporting from Signal Intelligence (SIGINT), Imagery Intelligence (IMINT), Open Source Intelligence (OSINT), and Geo-Location Intelligence (GEOINT) by coordinating intelligence sharing agreements among multiple IC partners.
- Upgraded intelligence watch center, integrating SIGINT and IMINT data for real-time updates.
- Led development of direct intelligence support to Joint Cyber Center, improving cross-agency protection of nation's critical infrastructure and key cyber terrain.

Senior Cybersecurity & Intelligence Leader (July 2011 to June 2014)

Directed 1,000+ staff in executing cyber operations and national intelligence missions, supervised resource allocation across eight global sites, and advised executive leadership on all operational issues.

- **Doubled organization's budget, manpower, and capabilities in 1.5 years,** setting 3-, 5-, and 7-year strategic plans that laid groundwork for future growth and direction of intelligence and cybersecurity functions.

Senior Cybersecurity & Intelligence Leader (*Continued---*)

- Surged network availability and response times 40% through integration of cyber infrastructure and customer support operations and shift into lean operations.
- Drove development of the first USAF Cybersecurity Intelligence Analyst career field, devised training roadmap with KSAs, justified need for analysts to executive leadership, and earned congressional funding of $14M to implement training program, yielding 1,100 analysts in 3 years.
- Streamlined integration of commercial education material into military curriculum by aligning military positions with standard industry job descriptions in collaboration with SME committee.
- Saved $1.2M through management of 37 global cyber infrastructure projects and $17.4M budget supporting multiple IC customers—on average, completed projects 3 months ahead of schedule.
- Accelerated $6M ISR weapons systems install and operator training with first-ever flexible SIGINT and IMINT collection capabilities to multiple entities for 6 months ahead of schedule ISR operation.
- Managed development, construction, and implementation of Security Operations Center, ensuring cyber mission assurance for global operations.
- Prioritized first-ever national tactical-level intel capability for localized, rapid communications to USAF pilots.

Senior Cyber Operations Leader (September 2007 to July 2011)

Guided shift from defensive to offensive posture through creation and development of USAF's first Offensive Cyber Operations unit, including management of budget, personnel, training, and equipment within NSA and CYBERCOM.

- Jump-started creation of new cybersecurity operators career field by briefing congressional delegation that gained approval for career field focused on cyber warfare.
- Strategized and conducted Computer Network Operations exploitation activities by developing technical products and solutions for deployment in support of NSA and CYBERCOM requirements.
- Created curriculum to educate and inform senior military leaders on cybersecurity capabilities and the future of the cybersecurity workforce.
- Forged 67-person team that directly supported the capture/kill of hundreds of enemy combatants through 7,000+ cyber operations supporting national security. Steered development of Tactics, Techniques, and Procedures for operational preparation related to cyber targets of interest.

Prior Roles within USAF

Lead Cyber Threat Intelligence Analyst, National Cyber Threat Operations Center, Fort Meade, MD (2004-2007)
Lead IT Lifecycle Budget Analyst, 354 Communications Squadron, Fairbanks, AK (2003-2004)
Lead Manager IT Customer Service Center, 354 Communications Squadron, Fairbanks, AK (2001-2003)
Senior Windows Server Systems Administrator, HQ NATO South, Izmir, Turkey (1999-2001)
Early USAF career positions of increasing responsibility (1990-1999)

EDUCATION & CREDENTIALS

Master of Science in Cyber Intelligence Studies, American Military University, 2017
Bachelor of Science in Intelligence Studies, American Military University, 2011
AAS in IT & Information Resource Management, Community College of the Air Force

Active DoD Top Secret/SCI Clearance with CI Poly, adjudicated 4/1/2014
CompTIA Security+ (IAT Level II) | Certified Ethical Hacker (CEH) | Certified Network Defense Architect (CNDA)

Project Management Professional Certification, PMI, Expected November 2018
Executive Leadership Program, University of North Carolina, Chapel Hill, NC, 2016
Smart Operations for Executive Leaders, University of Tennessee, Knoxville, TN, 2015
Leadership Development Program, Creative Center of Leadership, Greensboro, NC, 2015