**Maria Bowser**

DevSecOps Engineer. Reverse Engineer Full-Stack Developer

Reston, VA  **TS/SCI + CI Poly**  [m.sbk@icloud.com](mailto:m.sbk@icloud.com) 7037279977

PROFESSIONAL SUMMARY

DevSecOps Engineer with 5+ years of experience designing, securing, and deploying mission-critical systems across Intelligence Community environments. Combines deep expertise in reverse engineering, cybersecurity, and full-stack software development to deliver high-assurance solutions in air-gapped and zero-trust infrastructures. Skilled at transforming low-level technical insights into scalable automation pipelines that strengthen software supply chains and threat resilience.

Known for calm execution under pressure, exceptional technical clarity, and the ability to align diverse engineering, security, and operations teams toward shared mission goals. Multilingual in Russian and Japanese, supporting international collaboration and technical translation in cross-cultural security contexts.

CORE STRENGTHS

Engineering & Architecture

* Full-Stack Software Development (Java, Python, C/C++, Go)
* Distributed Systems & High-Performance Computing
* Secure Systems Design, Air-Gapped Deployments, Zero-Trust Architecture

DevSecOps & Automation

* CI/CD Pipeline Design (GitLab, Jenkins, Gradle, Docker, Kubernetes)
* Infrastructure Hardening, Supply-Chain Security, Automated Testing
* Observability, Lockfile Management, and Cloud-Native Resilience

Cybersecurity & Reverse Engineering

* Binary Analysis, Vulnerability Research, Threat Intelligence
* Dynamic & Static Analysis (Ghidra, gdb, Valgrind, Wireshark)
* OSINT Methodologies, Network Intrusion Detection, Secure Coding

Approaches & Methodologies

* Agile / SAFe, DevSecOps, Threat Modeling, Security-First Development
* Human-Centered UI/UX Engineering and Cross-Functional Collaboration

PROFESSIONAL EXPERIENCE

**DevOps Engineer | Praxis Engineering *–*** [*Chantilly*](https://www.google.com/maps/place/Chantilly/data=!4m2!3m1!19sChIJGXJnGVZBtokRg60WQ_zwQUA) *| May 5, 2025 – Present*

Lead DevSecOps initiatives within a classified, globally distributed system-of-systems, integrating secure automation across air-gapped and cross-domain environments.

Architect and maintain CI/CD pipelines leveraging GitLab CI, Gradle, RenovateBot, and Selenium to deliver mission-critical software with full artifact traceability.

Engineer hardened build and test infrastructure for virtualized and ISO-based deployments, addressing container escape, image provenance, and secret isolation at every stage.

Develop custom Python and Bash frameworks to automate dependency intelligence, vulnerability scanning, and compliance reporting—enhancing software supply-chain assurance.

Partner across development, infrastructure, and cyber divisions to align automation practices with Zero-Trust and DoD DevSecOps reference architectures. Provide hands-on Linux systems engineering and forensic support, optimizing build performance and validating release integrity under live operational constraints.

**Reverse Engineer & Vulnerability Researcher | Verite Group Inc –**[*Dulles*](https://www.google.com/maps/place/Dulles/data=!4m2!3m1!19sChIJuc_EVAw2tokRvPJtxs0zbpI) *| May 2025 – Present*

Led reverse engineering and vulnerability research efforts against complex foreign binaries and embedded systems, turning raw code artifacts into prioritized operational intelligence.

Designed and implemented a scalable, headless Ghidra-based pipeline for bulk decompilation and control-flow mapping across hundreds of executables, cutting manual analysis effort >60%.

Directed multi-layer triage workflows spanning kernel, API, and network stacks to expose high-impact privilege escalation and RCE vectors and recommend mitigation paths.

Designed and built automated Python toolchains for binary extraction, metadata enrichment, and anomaly detection to standardize reproducible analysis.

Drove secure integration of an air-gapped ML/AI analysis system to correlate observed binary patterns with vulnerability databases and accelerate vulnerability classification for mission customers.

Presented technical findings and mitigation guidance to government stakeholders and engineering teams in classified and controlled environments.

**Software Engineering Consultant | Deloitte Consulting** *–* [*Washington D.C.*](https://www.google.com/maps/place/Washington+D.C./data=!4m2!3m1!19sChIJW-T2Wt7Gt4kRKl2I1CJFUsI) *| Jun 2021 – Jun 2024*

Delivered full-stack and DevSecOps engineering solutions for defense and intelligence clients operating in secure, air-gapped environments. Combined system-level awareness with scalable design to produce performance-critical applications and CI/CD pipelines.

Delivered secure full-stack and **DevSecOps** solutions for defense clients in classified environments.

Modernized legacy systems, improving throughput by 700% through microservice orchestration and parallelized processing.

Built **CI/CD pipelines** (Jenkins + Kubernetes + SonarQube) with automated code-quality enforcement and container-security scanning.

Developed **Python-based C2 servers** for Red-Team operations, enabling automated payload management and telemetry collection.

Performed **network packet analysis** using Wireshark to detect intrusions and guide defensive countermeasures.

**Winner, Deloitte OSINT Cybersecurity Capture-the-Flag (2023)**.

**Software Engineer | PioneerTech –**[*Fairfax*](https://www.google.com/maps/place/Fairfax/data=!4m2!3m1!19sChIJzZFLOZZOtokRQIZEhecmIwc) *| Jan 2021 – Jun 2021*

Built and optimized enterprise Java applications under stringent federal compliance requirements, combining performance engineering with deep database and security knowledge.

Engineered secure multi-tier **Java Enterprise** systems (Spring + JPA + Oracle DB) under OCA and FIPS 140-2 compliance.

Refactored legacy codebases and optimized SQL, cutting query latency by 65%.

Containerized legacy apps and implemented microservice architecture with 99.99% uptime handling 3 TB+ daily data.

Built caching and pooling strategies supporting 10 000+ concurrent transactions.

**Software Engineer | Concept Plus LLC –**[*Fairfax*](https://www.google.com/maps/place/Fairfax/data=!4m2!3m1!19sChIJzZFLOZZOtokRQIZEhecmIwc) *| Mar 2020 – Aug 2020*

Architected secure back-end systems for the Department of Defense’s DOEHRS-HC platform, ensuring real-time operational readiness data for 100,000+ service members.

Developed secure back-end **Spring Boot + Hibernate microservices** for the DoD DOEHRS-HC program, processing health data for 100 000+ service members.

Built encrypted, high-throughput data pipelines compliant with **HIPAA / DoD** standards.

Increased processing efficiency 40% through concurrency and queue optimization.

Modernized monolithic apps into containerized RESTful services.

**Systems Engineer | Perspecta Inc** *–* [*Chantilly*](https://www.google.com/maps/place/Chantilly/data=!4m2!3m1!19sChIJGXJnGVZBtokRg60WQ_zwQUA) *| Summer 2018 & Jan 2019 – Jun 2019*

Led exploratory analysis correlating **mobile application telemetry and geospatial data** with the **National Time Use Survey**, revealing novel methods for digital fingerprinting and behavioral attribution.

**Reverse-engineered proprietary mobile data formats** to extract unique identifiers and build high-fidelity movement profiles for activity-based intelligence models.

Supported **R&D for blockchain-backed secure data architectures**, applying distributed ledger concepts to protect mission datasets and enhance auditability.  
Delivered **briefings** translating complex signal patterns and data vulnerabilities into actionable insights for intelligence operations.

EDUCATION & CERTIFICATIONS

Education

* **B.A. in Economics** (Concentration: Computer Science, Minor: Statistics) – *Virginia Tech, Class of 2019*

Certifications

* CompTIA Security+
* Udacity Full-Stack Developer Nanodegree
* Deloitte Cybersecurity Software Engineering (Date)