

Hicks@HicksZilla.com

(770) 307-8221

Bethlehem, Ga 30620

WWW: [Bold Profile](#)

## Skills

- Cyber Threats Intelligence Assessments and Reporting
- Security Operations Center (SOC) Blue Team
- Incident Response and reporting
- Security Information and Event Management (SIEM) Tools
- AWS Cloud Computing
- Programming - Java, C++, Python, SQL
- Web Development Technologies - HTML, CSS, JavaScript
- Operating Systems - Windows, Mac, Linux

## Education And Training

*Expected in 12/2024*

**Master Of Science:**

Information Security Management

**Augusta University**

Augusta, GA

*Expected in 12/2023*

**A.A.S Networking Specialist**

**Degree:**

**Cloud Computing Gwinnett**

**Technical College**

*Expected in 12/2023*

**Cisco Specialist Certificate**

**Gwinnett:**

**Technical College**

*01/2021*

**A.A.S:**

Computer Programming

**Gwinnett Technical College**

*01/2018*

**Bachelor Of Science:**

**American Military University**

Charleston, WV

# FRANKLIN HICKS

## Senior Cyber Security Analyst

Experienced Senior Cyber Security Analyst with over 12 years of service in the US Air Force, providing essential cyber security expertise to advance the missions of both the National Security Agency (NSA) and US Cyber Command (USCYBERCOM). Proven expertise in identifying and mitigating cyber threats, conducting incident response, and developing comprehensive threat assessments. Well-versed in the adversary Tactics, Techniques, and Procedures (TTPs). Skilled in metadata analysis, network flow analysis, and developing signatures for Advanced Persistent Threats (APTs). Strong analytical, reporting, and briefing abilities. Adept at collaborating with Cross-functional teams and providing critical insights to senior leadership. Complemented by a bachelor's degree in information systems security (INFOSEC) and ongoing professional development in AWS cloud computing, CISCO networking. Currently working towards a Masters Degree in Information Security Management

## Experience

**National Security Agency, NSA, National Cyber Threat Operations Center, NCTOC - SENIOR CYBER INTELLIGENCE ANALYST**

*Ft Meade, MD*

*02/2015 - 03/2019*

- Performed metadata and network flow analysis to identify and characterize malicious network intrusions
- Conducted in-depth analysis of cyber threat intelligence data from various sources, including open-source intelligence, dark web monitoring, and internal security logs, to identify emerging threats and potential vulnerabilities
- Leveraged MITRE ATT&CK Framework to develop comprehensive Cyber threat assessments
- Implemented automated reporting mechanisms that integrated Common vulnerabilities and Exposures (CVE) information, streamlining the reporting process, and ensuring accurate and timely delivery of vulnerability reports
- Analyzed anomalous traffic to develop signatures for Advanced Persistent Threats (APTs) and recommend mitigation strategies
- As an intrusion analyst, used multi-source information to conduct network protocol analysis and map networks of interest
- Conducted research and drafted products that enabled in-depth enemy target assessments & insight into adversary Tactics Techniques and Procedures (TTPs)

**US Cyber Command, USCYBERCOM - CYBER INTELLIGENCE ANALYST**

*Ft Meade, MD*

*11/2010 - 02/2015*

- Conducted full spectrum computer network operations (CNO) intelligence analysis within hi-level, short suspense, and dynamic Joint forces environments

## Certifications

- AWS Certified Solutions Architect - Associate (SAA-C03) (In Progress 14 August 2023)
- CompTIA Security+ (SY0-501)
- Microsoft Certified Application Specialist (MCAS) Access 2010

## Websites

- HicksZilla.com
- <https://bold.pro/my/franklin-hicks-230619163953>
- <https://www.linkedin.com/in/franklin-hicks-a8287b171/>

- to provide comprehensive assessments of threat actor's capabilities
- Responsible for all-source analysis and production of a broad scope of complex intelligence products supporting Computer Network Defense (CND) within the Department of Defense (DoD) information networks
- Designed and Maintained database that aided in analysis of Intrusion Set activity baseline which was utilized to develop a wide range of intelligence products that were provided to the Intelligence Community and briefed to senior leadership
- Performed Intelligence Preparation of the Cyber Environment (IPCE/CIPE) modeling for multiple targets.

## **USAF Distributed Common Grounds Systems - MISSION PLANNER/TECHNICAL REPORTER**

*Langley AFB, VA*

*09/2007 - 11/2010*

- Performed short suspense mission planning for Intelligence Surveillance and Reconnaissance (ISR) platforms
- Maintained communications with forward deployed units to facilitate dynamic tasking of air assets fulfilling collection for critical mission requirements
- Briefed Squadron/Wing leadership on Missions collection requirements
- Developed fused intelligence products by combining data from multiple intelligence disciplines
- Drafted time sensitive reports in accordance with established guidelines and provided this information to war fighters and national level decision makers.

## Professional Courses

- JNAC – Joint Network Attack Course, 160 hours – Corry station Pensacola, FL 2011
- Cyber 200 – Air Force continuing education course for Cyberspace professionals, 120 hours – (AFIT) Air Force Institute of Technology, Wright Patterson AFB Dayton, Ohio, 2012
- JIOPE – Joint Intelligence Preparation of the Operational Environment. 40 hours – Ft Meade, MD 2011
- NETA 1020 – Digital Network Intelligence Gateway Course. 40 hours – Ft Meade, MD 2011
- NETA 1021 – Internet Technologies. 16 hours - Ft Meade, MD 2011
- NETA1030 – Digital Network Intelligence Gateway Course. 24 hours – Ft Meade, MD 2011
- NETA2002 – Orientation to Applied Digital Network Analysis. 16 hours - Ft Meade, MD 2015
- NETA 2108 – Digital Network Intelligence Workshop. 80 hours – Ft Meade, MD 2015
- NETC 2101 – Cryptologic Access Management Fundamentals. 24 hours - Ft Meade, MD 2015
- NETW1051 – Wireless 1: Exploring Wireless Technologies, 40hours – Ft Meade, MD 2011
- RPTG 1012 – Basics of SIGINT Dissemination - Ft Meade, MD 2015
- RPTG 1500 – NTOC Cybersecurity Dissemination. 16 hours - Ft Meade, MD 2015
- RPTG 2500 – Cyber Incident Analysis and Reporting. 40 hours - Ft Meade, MD 2015
- RPTG 3222 – SIGINT Analysis and Report Writing. 80 hours - Ft Meade, MD 2011
- RPTG 3225 – Reporting Boot Camp. 80 hours - Ft Meade, MD 2015
- RPTG 4018 – USSID SP0018 For SIGINT Reporters - Ft Meade, MD 2015