

Brian David Kiehl

Baltimore, MD
brian.kiehl@gmail.com

CISSP Certificate #359348

Top Secret SCI (w/ CI Poly)

Summary

Brian is a highly accomplished technical leader with over 15 years of cyber security experience. Currently serving as a Cyber Intel Analyst with the Defense Information Systems Agency (DISA), he has also held senior information security engineer positions with Lockheed Martin and SafeNet, Inc. In addition to his civilian experience, Brian spent three years as an active duty military instructor at the United States Naval Academy, providing a combination of technical and theoretical instruction in all aspects of cyber security to the Brigade of Midshipmen.

Education

Master of Science in Information Assurance | Johns Hopkins University | May 2006

Bachelor of Science in Computer Science | Shepherd University | May 2003

Training & Certifications

- ISC² Certified Information Systems Security Professional (CISSP #359348)
- EC-Council Certified Ethical Hacker (CEH #03409049817)
- SANS SEC560 – Network Penetration Testing & Ethical Hacking
- National Security Telecommunications and Information Systems Security (NSTISSI 4011)

Professional Experience

United States Naval Academy

July 2018 – Present

Cyber Science Department - Annapolis, Maryland

Cyber Instructor

- Course Coordinator for SY110 - Intro to Cyber Security – managed the core cyber security course that is required by all students at USNA. Led the team of 30 faculty members that delivered the course to over 500 students during the spring 2015 semester. Developed new course curriculum and assisted in the management of the web/linux/virtual infrastructure utilized by faculty & students.

Defense Information Systems Agency

August 2016 – July 2018

DISA Command Center - Fort Meade, Maryland

Cyber Intel Analyst

- Lead the planning, coordination, implementation, validation, mitigation and compliance of cyber security tasks.
- Establish and lead Operational Planning Teams (OPT) in order to plan and execute DISA Cyber Missions.
- Issue orders in support of Defensive Cyber Operations (DCO) of the DoD Information Network (DODIN).
- Coordinate with mission partners to help shape DISA Network Assurance strategic alignment.
- Establish subordinate command reporting portals and provide status reporting to senior commanders.
- Serve as a Cyber Security Watch Officer and/or Special Projects Team Lead as required.

United States Naval Academy

July 2013 – July 2016

Center for Cyber Security Studies - Annapolis, Maryland

Cyber Instructor

- Course Coordinator for SI110 - Intro to Cyber Security – managed the core cyber security course that is required by all students at USNA. Led the team of 30 faculty members that delivered the course to over 500

students during the spring 2015 semester. Developed new course curriculum and assisted in the management of the web/linux/virtual infrastructure utilized by faculty & students.

- Provided a combination of technical and academic instruction to 300+ students on all aspects of cyber security, to include: Architecture & Operating Systems, Client/Server Hardening, Web Vulnerabilities, Scripting/Injection Attacks, Networking, Encryption/Digital Crypto, and Network Recon & Attack.
- Managed/Coordinated the USNA Cyber Center Lecture Series, a recurring series of cyber-related lectures from flag-level military officers and industry leaders, attended by over 1200 students & faculty members.
- Served as the senior Information Professional (IP) Officer at USNA. Provided leadership with future officer recommendations after conducting a highly competitive selection process.

Defense Information Systems Agency

October 2012 – July 2013

DISA Command Center - Fort Meade, Maryland

Principal Cyber Security Engineer

- Monitored the Defense Information Systems Network (DISN) to identify computer incidents, provide threat analysis and proactive response, and disseminate threat/incident reports.
- Analyzed results of Intrusion Assessments (i.e. Penetration Testing) to incorporate into DISA Defensive Cyber Operations (DCO) corrective actions and/or future mitigation strategies.
- Managed and coordinated DISA's Host Based Security System (HBSS) command and control operations. Configured and tuned global HBSS ePO reporting server. Identified and alerted on HBSS events.
- Briefed senior leadership on existing security posture and defensive cyber recommendations.

SafeNet, Inc.

December 2010 – July 2012

Corporate Headquarters, Belcamp, MD

Lead Information Security Engineer

- Managed the company's enterprise technical security solutions: global system patching, enterprise anti-virus, internal & external vulnerability scanning, and log management & correlation.
- Designated Information Systems Security Manager (ISSM) for SafeNet's cleared DoD spaces.
- Managed the company's LogRhythm SIEM log correlation system for alerting and forensic analysis.
- Developed the company's internal security policies, directives and standards (NIST/DoD).
- Developed and delivered information security awareness training program to SafeNet employees.

Lockheed Martin Corporation

March 2004 – December 2010

Corporate Information Security Team, Bethesda, MD

Information Assurance Engineer

- Conducted network architecture vulnerability analysis for Lockheed Martin's extranet environments.
- Assessed overall compliance with both corporate and federal policies and procedures.
- Designated Approver (DA) for external network connections to the Lockheed Martin intranet.
- Successfully balanced risk management and mission requirements while making final determinations.
- Conducted risk/vulnerability assessments and security audits, and implemented resulting mitigations.

US Navy Reserves

Defense Intelligence Agency | Lieutenant | 2016-Present

Washington, DC

- Executive Officer – Unit second-in-command, responsible for unit administration and operational readiness.
- Supervise unit members in daily operations, logistics, and maintenance of DIA IT/IA network systems.

Naval Criminal Investigative Service | Lieutenant | 2011-2013

Quantico, VA

- Cyber Division Officer–Provide Cyber Intelligence Analysis support for target investigations.

Naval Network Warfare Command | Ensign | 2008-2011**Norfolk, VA**

- Provided Information Security/Assurance expertise in support of the NETWARCOM mission.
- Terminal Fury Exercise 2011 – Observing, recording and reporting network attack and defense activities.

Applications | Environments | Frameworks

McAfee ePO (VSE, HIPS, PA), NeXpose, LogRhythm, Vulnerability Management System (VMS), WireShark, Snort, Nessus, Microsoft Windows/Office/SharePoint, BackTrack Linux (Kali), NMAP, Cascade Server Web Management System, DoD Info Assurance Certification & Accreditation Process (DIACAP), FISMA FIPS 199/200, NIST 800 Series, DISA/NSA Security Technical Implementation Guides (STIGs), Disaster Recovery/Continuity of Operations (COOP)