Carmeshia Miller
13711 Kotili Ln.
San Antonio, TX 78245
Phone: 512-466-2928
Carmeshia35@Gmail.com

****

SUMMARY

I have more than 20 years of experience in the information technology field serving in several capacities including Risk Manager, Information System Security Manager (ISSM), Cyber Security Analyst/Engineer, Instructor/Writer, and most recently a University Professor. I work well independently, as part of a team, or in a group setting. I have excellent leadership, communication, and presentation capabilities.

****

EXPERIENCE

Integrated Project Team (IPT) Cyber Security Assessment and Authorization (A&A) Program Support Team Manager, Defense Health Agency (DHA) Cyber Security Policy and Business Operations (CPBO) Team
December 2020 – Present 50 hours

- Manages multiple Cybersecurity Assessment and Authorization (A&A) Program Support Teams and Risk Management Program projects for the Defense Health Agency. Responsibilities include providing technical subject matter expert (SME) advice to stakeholders, addressing A&A business requirements, and managing the DHA Risk Management Framework (RMF) Portal Website.
- Evaluates RMF program needs and makes recommendations on required changes to ensure process is run in accordance with established Federal Information Processing Standards (FIPS), Federal Information Security Modernization Act (FISMA), and National Institute of Standards and Technology (NIST) Special Publication (SP) guidelines.
- Assigns, communicates, and plans work assignments with each team member, in conjunction with development of performance standards for essential program support team (PST) job elements.
- Configures and customizes Microsoft Windows SharePoint Services (WSS). Create and administer team sites, user administration, web parts creation etc. based on customer requirements.
- Provides technical expertise to the DHA RMF community and the A&A workforce to facilitate the rapid processing of customer artifact submissions.
- Responsible for the Configuration Management and Infrastructure Change Control facilitating health services to approximately 9.6 million beneficiaries, active-duty service members, military retirees, and their eligible family members and survivors.
- Facilitates and manages the A&A for over 50 military hospitals and over 600 clinics, as well as a supporting network of private sector providers.
- Interfaces daily with stakeholders, customers, project leads, and Security Control Assessor Representatives (SCAR) serving as the key Configuration Management point of contact and provides support for the project documentation and tracking of key deliverables.
- Educates end-users with online training sessions and provided test data and scenarios that reflected day-to-day activities, enhancing user knowledge and skill.

Cybersecurity Adjunct Instructor, Lone Star College – Houston, Department of Information Technology and Cybersecurity
January 2022 – Present 5 hours

- Teaches Cybersecurity courses for undergraduate level students with varied ages, nationalities, disabilities, and backgrounds.
- Mentors and provides guidance to Cybersecurity students entering the Information Security, Information Assurance, and Cybersecurity fields.
- Manages course content, student grades, and student progress using the Blackboard Learning System.
- Responsible for the design and implementation of four Certified Ethical Hacking lab experiments including: the choice of experiments, assessment of required materials, experimental optimization for both time and student learning opportunities, and the production of both the student lab and instructor solutions manuals.
- Lab instructor for multiple hands-on Certified Ethical Hacking (C|EH) assignments using Kali-Linux, which involved ensuring that proper laboratory procedures were followed, assessment of student work, and provision of feedback facilitating an understanding of the basics of ethical hacking.
- Creates intuitive quiz, mid-term, and final examination material for undergraduate and graduate level courses, which enable accurate assessments of student assignments, understanding of material, and check on learning.

Cybersecurity Lead Instructor, ThriveDX, Department of Cybersecurity
June 2021 – Present 25 hours

- Lead instructor at ThriveDX, formerly known as HackerU, responsible for teaching multiple cybersecurity courses as a member of the Cybersecurity Professional Bootcamp team.
- Instructs learners in Microsoft Security consisting of the management of networks and computers in an organization through the setup of domain environments using Active Directory, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) servers as well as other network services.
- Educates students in Computer Networking covering network devices, protocols, and layers of the Open Systems Interconnect (OSI) model.
- Teaches Cloud Security exploring cloud platforms and demonstrates ways to ensure data integrity in the longer term, while providing training applicable to the AWS Certified Cloud Practitioner exam.
- Instructs on the intricacies of the open-source Linux operating system, specifically the cybersecurity distribution known as Kali Linux.
- Teaches Network Security students how to manage, secure, and operate network communication equipment with a focus on security.
- Facilitates practical exercises and simulations through labs using virtual machines.

Adjunct Professor, Texas A&M University – San Antonio, Department of Computing and Cyber Security
August 2018 – Present 5 hours

- Teaches Penetration Testing (PENTEST), Computer Forensics, Security Risk Analysis, Incident Response, and Information Systems Management Principles at Texas A&M University – San Antonio for undergraduate and graduate level students; with an average class size of 36 diverse students ranging a myriad of different ages, nationalities, disabilities, and backgrounds.
- Mentors and provides guidance to Cyber Security students entering the Information Security, Information Assurance, and Cyber Security fields.
- Manages course content, student grades, and student progress using the Blackboard Learning System.
- Responsible for the design and implementation of four Certified Ethical Hacking lab experiments including: the choice of experiments, assessment of required materials, experimental optimization for both time and student learning opportunities, and the production of both the student lab and instructor solutions manuals.

- Lab instructor for multiple hands-on Certified Ethical Hacking (C|EH) assignments using Kali-Linux, which involved ensuring that proper laboratory procedures were followed, assessment of student work, and provision of feedback facilitating an understanding of the basics of ethical hacking.
- Creates intuitive quiz, mid-term, and final examination material for undergraduate and graduate level courses, which enable accurate assessments of student assignments, understanding of material, and check on learning.

Senior Cyber Security Assessment and Authorization (A&A) Engineer/Analyst, Defense Health Agency (DHA) Independent Verification & Validation (IV&V) Team
May 2018 – December 2020 50 hours

- Assessed and supported the Defense Health Agency's (DHA) Independent Verification & Validation (IV&V) Assessment and Authorization (A&A) process through Risk Management Framework (RMF).
- Validated requirements, risks, and controls for the Defense Health Agency's (DHA) medical enclave systems and subsystems.
- Evaluated security control compliance via Enterprise Mission Assurance Support Service (eMASS) to obtain initial and subsequent system accreditations and Authority to Operate (ATO).
- Ensured the implementation of Security Technical Implementation Guides (STIGs) and Information Assurance Vulnerability Alert (IAVA).
- Reviewed Assured Client Assessment Solution (ACAS) system scans to accurately determine security posture.
- Advised customer on implementation and enforcement of all DoD Information Systems (IS) and IT cyber security policies and procedures as defined by cyber security related documentation.
- Analyzed the IA program plan, strategy, integrated baselines, and guidance and standards.
- Participated in meetings and working groups to provide recommendations and provide summary reports of briefings with result of findings.
- Monitored compliance with cyber security policy, as appropriate and review the results of such monitoring.
- Tracked and identified vulnerabilities via the Plans of Actions and Milestones (POA&M) of assigned systems from creation to remediation.

Senior Cyber Security Analyst/Engineer, Defense Information Systems Agency (DISA), National Leadership Command Division, Crisis Management System (CMS) Program Office
GS-13
October 2016 – May 2018 50 hours

- Performed assessment and authorization (A&A) duties for the CMS program office's Nuclear Command, Control, and Communication (NC3) accredited Voice over Secure Internet Protocol (IP) – Top Secret (VoSIP-TS), and Secure Video Teleconferencing System (SVTS).
- Developed and managed documentation for the security authorization package/certification packages: documentation includes System Security Plans (SSP), Concept of Operations (CONOPS), the Plans of Actions and Milestones (POA&M), and Security Requirements Traceability Matrices (SRTM).
- Facilitated the program office's Engineering Change Proposal (ECP) and Configuration Management Plan agendas to plan for future requirements and lifecycle replacement priorities.
- Managed and updated the POA&M to ensure identified risks are remediated or mitigated in a timely manner.
- Managed the CMS Continuous Monitoring program by continually addressing the security and privacy controls outlined in NIST SP 800-53 revision 4: enabling the organization's re-accreditation process to flow smoothly and expeditiously.
- Conducted Continuous Monitoring of all CMS assets: ensuring any unauthorized change to the network is quickly discovered, addressed, and documented using tools like Splunk and SolarWinds.

- Constructed a detailed information CMS information security site acceptance checklist to ensure all CMS installations are performed according to the CMS' SSP, NIST standards, National Security Agency (NSA) standards, and organizational policies and procedures.
- Established and manages the CMS Network Operation Center (NOC) Training Plan ensuring all current and new employees receive proper training as well as refresher training.
- Ensured Configuration Management is being performed by reviewing network scans and directs the remediation and/or mitigation of all vulnerabilities and updates of any outdated software or hardware.
- **Received Civilian Time-Off Award for two consecutive years for outstanding performance.**

Information System Security Manager (ISSM), US Army Cyber Brigade, GISA Detachment Fort Gordon, Information Assurance (IA) Division
GG-12
December 2014 - October 2016 40 hours

- Managed a large team of contractors and civilian technical professionals in the DoD intelligence community in the management of the organization's cybersecurity program.
- Ensured users' Cybersecurity training remains current and all users are aware of their responsibilities for protecting sensitive information systems and data; lead to the organization's ability to maintain a 95% to 98% compliance standard for annual user awareness training. The continued enforcement of the awareness program resulted in the organization having only two Unauthorized Disclosure of Classified Information (UDCI) incidents in the last fiscal year.
- Ensured users' Cybersecurity training remains current and all users are aware of their responsibilities for protecting sensitive information systems and data; lead to the organization's ability to maintain a 95% to 98% compliance standard for annual user awareness training. The continued enforcement of the awareness program resulted in the organization having only two Unauthorized Disclosure of Classified Information (UDCI) incidents in the last fiscal year.
- Advised senior staff and subordinates on authorized devices, systems, and software allowed in the current environment. As a member of the change management (CM) team, conducts risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, rules, and protection needs. Advises the command on systems that will introduce vulnerabilities to the existing network.
- Provided guidance to the director on any required or necessary security controls, performed ongoing maintenance, and prevented, detected, analyzed, and responded to security incidents through collaboration with customers, the Integrated Network Operations and Security Center (INOSC), and the 2nd Regional Cyber Center (2RCC).
- Created information security Standard Operating Procedures (SOP) and security policies for the Information Assurance branch for the United States Army Cyber Brigade and GISA-C Detachment Fort Gordon. Creates and continuously updates Incident Handling, Data Transfer, Video Teleconference, Hard Drive Destruction, and Portable Electronic Devices policies to guide users and information technology staff on the proper operating procedures and practices as it relates to information assurance and security.
- **Received Civilian Time-Off Award for outstanding performance.**

Computer Network Defense Technician/Information Assurance Technician, US Army, 1st Cavalry Division Information Assurance (IA) G6
January 2013- December 2014 50 hours

- Managed a diverse military team of more than 10 soldiers to ensure the organization's assets were protected and properly secured to prevent unauthorized access.
- Assisted in the development of security policies and operating procedures to ensure the reliability and accessibility to all networks/systems. Enforced security policy to prevent and defend against any unauthorized access to 1st Cavalry Division's information systems.

- Created and oversaw the user training program concerning information security policies and procedures regarding the 1st Cavalry Division information systems and networks.
- Monitored network security and applied patches and updates to systems.
- Administered the Windows Server Update Server (WSUS).
- Provided core services by designing, configuring, installing, and managing data services at the operating system and server application level. Provided directory services utilizing dynamically assigned IP addresses, domain name servers, storage area networks, and electronic messaging resources.

Information Assurance Technician, US Army, 1st Cavalry Division Information Assurance (IA) G6
March 2010-January 2013 50 hours

- Performed duties as Information Assurance Security Officer (IASO)
- Developed and implemented information security disaster recovery procedures and continuity of operations (COOP) plan.
- Conducted system security audits and reviewed vulnerability assessments and performed Information Assurance Vulnerability Management (IAVM). Ensured information system computers, printers, and multifunction devices were Security Technical Implementation Guide (STIG) compliant.

Windows System Administrator & Backup Administrator, US Army, 1st Cavalry Division, Division Automation Management Office (DAMO) G6
January 2009-March 2010 50 hours

- Installed, configured, managed, and troubleshot information systems for over 40 physical servers supporting over 6,000 clients on the Multinational Division- Baghdad (MND-B) Divisions Local Area Network.
- Used Systems Center Configuration Manager (SCCM) to remotely administer systems and deploy operating systems, software updates, patches, and software applications.
- Coordinated and integrated technical aspects of computer work, to include, utilizing Microsoft Windows Server and Microsoft Exchange systems.
- Extensive experience with Active Directory, Domain Name System, Windows Internet Naming Service, and Microsoft Exchange using virtual servers.
- Performed troubleshooting and diagnosis of hardware/software network failures and provided resolutions ensuring all mission critical servers for the organization were continuously available. Problem-solved hardware issues with fault-tolerant hard drives.

Combat Service Support Automated Management (CSSAMO) Supervisor, US Army, 82nd Combat Aviation Brigade, CSSAMO
June 2006-January 2009 55 hours

- Provided a single point of support for STAMIS hardware, software, communication devices, local area networks, and wide area networks and configured and managed Combat Automated Information Systems Interface (CAISI) and Very Small Aperture Terminal (VSAT) communications equipment.
- Ensured information assurance compliance, integrating databases for new units, coordinating signal support requirements with the signal officer, assisting supported units with STAMIS continuity of operations planning, recording, and reviewing system problem report. Prepared an Engineering Change Proposals-Software form for common problems and provided user-level support training.

Instructor/Writer, US Army, School of Information Technology
March 2005-September 2005 40 hours

- Instructed A+, Networking Essentials, Computer Security, Computer Troubleshooting, UNIX, Web Design, and Solaris.

- Maintained, administrated, and upgraded equipment, wrote course lesson plans, modified examinations, and ensured all Training Support Packages (TSPs) were current.
- Provided computer help desk support and technical training on hardware/software to end users at the School of Information Technology.

Joint Command Information System Activity (JCISA), US Army, Information Management Office (IMO)
March 2004-March 2005 40 hours

- Acted as the liaison between the unit and the installation Director of Information Management (DOIM). Interfaced with the DOIM for security, software and equipment upgrades and requests for repair.
- Evaluated manpower and personnel issues, developed life cycle replacement plans, and established and enforced policies internal to the organization.
- Ensured all required training was budgeted, scheduled, and conducted.
- Maintained, monitored, and troubleshot the Global Command and Control System (GCCS), Global Command and Control System-Korea (GCCS-K).

Instructor/Writer, US Army, School of Information Technology
June 2001-March 2004 40 hours

- Instructed A+, Networking Essentials, Computer Security, Computer Troubleshooting, Windows 2000 Professional, Windows 2000 Server, UNIX, Web Design, and Solaris.
- Maintained and upgraded equipment, wrote course lesson plans, modified examinations, and ensured all Training Support Packages (TSPs) were current.
- Integral member of an eight-person instructional team that developed course curriculum for the Army's information Systems Technician Course. Orchestrated multi-media presentations and technical training sessions for fellow instructors.
- Gathered feedback from over 5,000 students to provide vital feedback on course deficiencies.
- **Received the Instructor of the Month title four times.**

****

PRIVATE TUTORING

- I conduct private tutoring for Cybersecurity and Information Technology high school and college students.

****

EDUCATION

Trident University International, Cypress, California 2013
* **Master of Science in Information Technology Management with Major in Information Security/Assurance and Digital Forensics**

University of Maryland University College, Adelphi, Maryland 2012
* **Bachelor of Science with Major in Computer Studies**

Warrant Officer Basic Course Fort Gordon, GA 2006
* Awarded the Information Systems Technician military occupational specialty

****

PROFESSIONAL AFFILIATIONS

*** Information Systems Audit and Control Association (ISACA)**
Active Member 2015 – present
Director at Large – Technology and Engagements

- Research emerging technologies to advise board on possible use for chapter.
- Support the Chapter's various engagements as they relate to technology needs.
- Responsible for maintaining and keeping an inventory of the Chapter's equipment.

*** International Society of Female Professionals (ISFP)**

****

COMMUNITY INVOLVEMENT

Achievement Initiative for Minority Males (A.I.M.M.) Mentor
Texas A&M University-San Antonio
August 2021 to Present

CASA Volunteer
Court Appointed Special Advocate (CASA) Bell County
February 2014 to Present

Habitat for Humanity Habitat for Humanity
Deconstruction Crew, Build Crew, & Services Assistant
May 2021 – Present

****

PROFESSIONAL PROFILE LINKS

LinkedIn: Carmeshia Miller LinkedIn Profile

****

PROFESSIONAL CERTIFICATIONS

- Certified Information System Security Professional (CISSP) 2022
- CompTIA Network + CE 2017
- CompTIA Secure Infrastructure Specialist (CSIS) 2017
- CompTIA IT Operations Specialist (CIOS) 2017
- Global Information Assurance Certification (GIAC) Information Security Professional (GISP) 2016
- Certified Information Security Manager (CISM) 2015
- CompTIA Advanced Security Practitioner (CASP) (CE) 2014
- Certified Ethical Hacker (C|EH) 2014
- ITIL v3 Foundation 2013
- CompTIA Security + CE 2010
- CompTIA A+ CE 2009

****

RECENT COURSES

- Information Security Risk Assessment through Data Collection & Analysis (32 hours) 2019

- Defending Critical Infrastructure from Cyber Attacks (40 hours) 2018
- Network Forensics (40 hours) 2018
- EC-Council Certified Security Analyst (ECSA) Penetration Testing (40 hours) 2017
- Project Management Professional (PMP) Training & Certification Boot Camp (35 hours) 2017