Mark Anthony Munoz
Commercial: 512-271-3555
Austin, TX
Email: mrmunoz@tamusa.edu

OBJECTIVE: Provide excellent service and produce graduates to be the preferred industry provider of IT professionals and cyber defenders.

EDUCATION:
Saint Mary's University of Minnesota with a Masters in CIS.

CERTIFICATIONS:
Certified Information Systems Security Professional (CISSP), ID# 469777, Expire Nov 2026

SKILLS:

- Microsoft Endpoint Configuration Manager (MECM)
- Tanium
- VMware vSphere infrastructure
- Security Technical Implementation Guides (STIG) Viewer
- Languages: Powershell, Python, SQL
- Red Hat Enterprise Linux (RHEL) 6
- Microsoft Active Directory
- Enterprise Mission Assurance Support Service (eMASS)/Risk Management Framework (RMF)
- Microsoft Windows Server 2022
- Project Management
- Microsoft SQL Server
- Assured Compliance Assessment Solution (ACAS)/Nessus
- Security Content Automation Protocol (SCAP)
- Microsoft Azure/Amazon Web Services
- Microsoft Teams, Zoom, Google Classroom
- Blackboard and Canvas Learning management system

EMPLOYMENT HISTORY:

Security Operations and Team Lead, GS-12, 07/22 — present, 40 hours per week
Employer: United States Air Force (USAF)
Supervisor: Mr. William Zoyd, william.zoyd.33@us.af.mil, DSN 314-480-1876

Built MAJCOM Security Operation Center processes and procedures which monitored, analyzed and protected 65 mission systems' vital security operations from various security threats such as

cyber-attacks, data threats, viruses, malware, etc. Led a team of 12 personnel; under leadership, the team performed immediate incident response activities such as host triage and retrieval, malware analysis, remote system analysis, end-user interviews, and remediation efforts. Work and collaborate with HQ AETC/A2O, A6C, A6F, and 16 AF to assess their needs, provide information or assistance, resolve their problems, or satisfy their expectations in security threat intelligence using big data platform ELICSAR, ARAD Tanium, ACAS, SCORE, and Forescout. Gather and analyze customers' functional requirements and translate these requirements into technical solutions and costings for Mission Defense Operations Cell. Advises and counsels enlisted, civilians, and contractors on the continually changing needs of the security operations program. Serve as a functional expert at the senior experience level on cyberspace protection conducting cyber defense analysis and security investigations on complex networks and system architectures on AETC MAJCOM. Provided crew leads and team members direction and expert advice on proper techniques and methodologies for in-depth analysis of malicious activity. Utilized experience and skill in applying cyber security principles to develop new methods, approaches, and procedures for conducting research, acquiring data, and engaging threats in a constantly changing environment. Identified system vulnerabilities, discovered inadequate protection mechanisms, assessed the security posture of mission partner terrain, and determined the effectiveness of response operations. Conducted missions to detect and remove unauthorized, malicious, or adversary presence from operational systems, networks, or enclaves to ensure the reliability and availability of mission-critical capabilities. Performed mission activities within established timelines as determined by mission/unit requirements and utilized unit Standard Operating Procedures (SOPs) and guidance.

Information Systems Security Manager (ISSM), GS-13, 08/18 — 07/22, 40 hours per week
Employer: United States Army Medical Command
Regional Health Command Europe (RHCE)/G6 Cyber Security Division (CSD)
Sembach Kaserne, Germany
Supervisor: Mr. William Zoyd, william.zoyd.33@us.af.mil, DSN 314-480-1876

Provided advice and direction to user and management on systems management technology for region. Served as senior technical expert on all matters of managing cyber security, compliance and mission assurance using SCCM, eMASS, HBSS, ACAS, Tanium, group policy, etc. Facilitated Risk Management Framework (RMF) for Regional Health Command Europe (RHCE) systems. Served as the command focal point for all Cyber Security, Risk Management and Compliance issues for the region of Europe subordinate commands such as Dental Health Command Europe, Landsthul Regional Medical Command, Bavaria Medical Command, Public Health Command Europe, and US Army Medical Materiel Center. Plan, develop, implement, and sustain secure automated systems in support of a network. Create Microsoft System Center Configuration Manager (SCCM) Operating System (OS) Deployment packages to be deployed to centrally managed workstations and servers. Conduct risk/vulnerability assessments and detection/analysis to ensure compliance with Information Assurance Vulnerability Alerts (IAVA). Develop best practices for imaging, IAVA patching, OS deployment, and customer development in support of OS deployment packages. Write SCCM test plans and test cases for the maintenance of desktops and servers. Analyze, evaluate, and make recommendations in response to requests for development, implementation, and installation of new automated information systems. Experience in installing, testing, operating, troubleshooting, and maintaining of hardware and software systems for operating system deployment. Develop and implement a plan rolling out new Windows 10 releases such as 1709, 1809, and 1909 to 5,000 end user devices across different parts of Europe.

Information Systems Security Manager (ISSM), GS-12, 08/17 — 08/18, 40 hours per week
Employer: United States Army
509th Signal Battalion/Cyber Security Division (CSD)
Caserma Ederle; Vicenza, Italy

Supervisor: Mr. William Zoyd, william.zoyd.33@us.af.mil, DSN 314-480-1876

Ensured protective measures designed to prevent unauthorized access. Worked with the Division Chief in planning, organizing, and overseeing the activities of the Cyber Security Division. Administer and coordinate operational network security to include analysis, tests and evaluations over 17 tenant units using DISA Assured Compliance Assessment Solution (ACAS). Established Plans of Action & Milestones (POA&M) for improving the efficiency of IT applications on six Risk Management Framework (RMF) packages and closed over 100 POAM items. Performed security requirements for certification and accreditation by provided performance management methods sufficient to plan and conduct security accreditation reviews for installed systems or networks and assess and advice on new or revised security measures and countermeasures based on the results of accreditation reviews. Utilize Enterprise Mission Assurance Support Service (eMASS) to track security controls on six packages and maintain artifacts to support controls. Developed and implemented programs to ensure that systems, network, and data users are aware of, understand, and follow IA policies and procedures. Conducted risk/vulnerability assessments and detection/analysis to ensure compliance with Information Assurance Vulnerability Alerts (IAVA).