Mark Ricard Munoz
Commercial: 210-271-3555
Austin, TX
Email: mrmunoz@tamusa.edu

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

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

CERTIFICATIONS:
Certified Information Systems Security Professional (CISSP), ID# 469777, Expire Nov 2025

SKILLS:

- Microsoft Endpoint Configuration Manager (MECM)
- Tanium
- Big Data Platform BDP Elicsar
- 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 2016/2019
- 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 Boyd, william.boyd.20@us.af.mil, DSN 314-480-1974

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 Boyd, william.boyd.20@us.af.mil, DSN 314-480-1974

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 Boyd, william.boyd.20@us.af.mil, DSN 314-480-1974

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).

System/Application Administrator, GS-12, 07/15 — 08/17, 40 hours per week
Employer: United States Air Force (USAF)
Supervisor: Mr. William Boyd, william.boyd.20@us.af.mil, DSN 314-480-1974

Implemented policies and procedures needed to effectively implement a central scheme for AETC CSS systems management and control. Sustained a secured SCCM environment for AETC networks. Used SMS Installer and PowerShell App Deployment Toolkit to create installer packages and deploy to 1,000 workstations using SCCM. Controlled user access and password generation and distribution process. Develop and maintain applications on SharePoint and mission operations using SharePoint Designer, InfoPath, and Visual Studio. Served as the preliminary technician for IT technical issues and challenges within AETC. Planned coordinated, and installed applications software and hardware for operating systems Windows Server 2008 R2 and 2012 R2. Coordinate activities related to all phases of Microsoft server operating systems, server virtualization technologies, collaboration applications, and server monitoring tools. Developed, reviewed, and modified changes to schedule of operations for successful day-to-day operations. Used STIG/SCAP tools to ensure servers are compliant to DISA standards. Provided technical guidance and instruction to AETC users. Troubleshoot complex problems and provided support that minimizes interruptions in the customers' ability to carry out business objectives by monitoring servers performance using IBM NetCool and SolarWinds. Provided technical support to team members to facilitate performance of IT support functions. Served as a senior technical advisor to management and maintain liaison with DISA, manufacturers such as Dell and HP, professional organizations, and counterparts at other installation services regarding available products and state-of-the-art technologies and advancements. Performed and coordinated the implementation of information processing standards as they relate to system security/Information Assurance. Developed and documented local systems administration standard operating procedures (SOP). Monitor system usage and the performance of production processors, modifying hardware and executive software configurations using SCCM, NetCool, SolarWinds, etc. Provided ongoing monitoring and problem resolution to VMware vSphere infrastructure to support functions of AETC CSS. Assisted in technical systems architecture and provided system analysis to determine proper performance of production processors to ensure the correct operation of systems. Managed and supported server-based applications such as SharePoint and MS SQL Server. Implemented DISA ACAS 5.3 on Randolph AFB scanning critical servers and mitigating vulnerabilities ensuring mission operations. Managed accounts and access to systems and equipment to ensure consistent application of established policies and procedures.

Information Assurance/Unit Security Manager, GS-11, 03/13 — 07/15, 40 hours per week
Employer: United States Air Force (USAF)
1st Air and Space Communications Operations Squadron (ACOS)
Ramstein AB, Germany
Supervisor: Mr. William Boyd, william.boyd.20@us.af.mil, DSN 314-480-1974

Program and Resource Manager for 1 ACOS AF JWICS security information technology (IT) assets. Maintained JWICS security across 1 ACOS and implemented JWICS resources. Oversaw IA activities, such as communication-computer security (COMPUSEC) and emission security (EMSEC) program, Air Force Electronic Key Management System (AFEKMS), Emission Security, and Information Assurance Awareness Program. Assisted GCCS in deciding which processes to automate on how to select equipment and software, and how best to use available technology. Monitored GCCS system using DISA Assured Compliance Assessment Solution (ACAS) by reviewing security configuration and security engineering assessments of vulnerabilities. Developed and assisted in the development and implementation of DISA ACAS procedures for GCCS. Trouble shoot deficiencies to identify and isolate sources and root causes. Prepared recommendations, justification, and specifications for GCCS equipment for end of year buys. Managed and directed control and oversight of 1 ACOS Information Assurance (IA) program as primary IA Officer by providing policy and procedural guidance for all assigned GCCS systems. Performed security and network event analysis to identify and mitigating network or system security incidents, breaches and malware outbreaks. Contributed to Ramstein AB, Germany reducing 29,000 client vulnerabilities for command cyber readiness inspection (CCRI), achieving the installation's lowest GCCS risk-factor to-date, providing vital contributions to the success of Ramstein's 2014 CCRI "Excellent" rating for SIPRNet. Carried out special projects and assignments designed specifically to meet the GCCS mission. Served as the unit Cybersecurity Liaison to the Wing Cybersecurity Office on day-to-day IA operations.

Client/Server Administrator, GS-11, 03/12 — 03/13, 40 hours per week
Employer: United States Air Force (USAF)
21st Operations Weather Squadron (OWS)
Kapaun Air Station, Germany
Supervisor: Mr. William Boyd, william.boyd.20@us.af.mil, DSN 314-480-1974

Worked with the 21st OWS with their communications systems using Windows 2008 Server and Ramstein AB network architecture. Planned and executed the installation of new or modified hardware, operating systems, and application software. Resolved AtHoc CAC reader dilemma; researched and implemented validation error fix action, 185 Windows 7 workstations brought online. Standardized Squadron Windows 7 workstation hard drive image, nailed TCNO compliance and accreditation requirements. Resolved recurring SIPRNet Token reader issue, timely response ensured timely weather forecast for Operations in 3 AORs. Performed Tech Refresh duties, inspected 85 Windows 7 unit workstations/20 COOP laptops, guaranteed unit readiness for AFNET migration. Oversaw monthly/bi-weekly TCNO compliance checks for NIPR/SIPRNet COOP systems, contingency mission capability guaranteed. Coordinated Hurrevac change request with INOSC East Change Management, AORs provided first ever Hurricane warning capability. Installed Cisco IP Phones on Windows 7 COOP laptops, reduced COOP footprint and equipment requirements, recognized as "best practice". Primary ADPE Equipment Custodian, eliminated outdated unit equipment holdings, brought Squadron in line with AF Standards. Award for civilian achievement for contributing to 21st OWS relocation from Sembach Kaserne, Germany to Kapaun Air Station, Germany, which resulted in seamless support to Department of Defense, Department of State, and North Atlantic Treaty Organization operations in the European Command and Africa Command Areas of Responsibility.