Sandra Montiel

smontiel@actionet.com
703-731-7599

PROFESSIONAL HIGHLIGHTS:

Senior Information Security Professional with 14 years of experience specializing in Risk Management Framework (RMF) compliance, secure system design, and cybersecurity program development. Skilled in Assessment and Authorization (A&A), security control implementation, privacy compliance, disaster recovery, and business continuity. Proficient in frameworks including NIST 800-53, NIST 800-171, CMMC, FedRAMP, and ISO 27001, with extensive experience developing System Security and Privacy Plans (SSPP), POA&Ms, Risk Assessments, and Security Control Assessments. Proven ability to collaborate with diverse stakeholders and provide leadership with insights on organizational risk tolerance, enabling well-informed, strategic cybersecurity decisions.

EDUCATION/TRAINING:

- Northern Virginia Community College – Completed IT Coursework (2015–2017)
- The Volgenau School of Engineering at George Mason – Attended (2012)

CERTIFICATIONS:

- ISC² Certified Information Systems Security Professional (CISSP), Cert # 561712
- ISC² Certified Authorization Professional (CAP) (now known as CGRC) (Inactive)
- CompTIA Security+ (Inactive)

CITIZENSHIP STATUS

- United States U.S Citizen

ACTIVE CLEARANCE(S)

- Active Secret Clearance

TECHNICAL KNOWLEDGE:

Cloud Platforms	AWS, Azure, Appian, OutSystems, Salesforce (Foundational knowledge)
Operating Systems:	Windows, Linux (Basic familiarity)
Help Desk Applications:	ServiceNow, Remedy

Govt. Process/Policy Experience – NIST SP 800-53, SP 800-37 (RMF), SP 800-171, FISMA, FedRAMP, ITIL, CSAM

Membership Organization

- Women in Tech (WIT)
- Latinas in Tech (LIT)
-

WORK EXPERIENCE:

ActioNet, Inc., 6/24 - Present

Cybersecurity Architect/Engineer

Actionet Inovation Center (AIC)

- Represents the AIC as a solution architect and cybersecurity SME, providing input throughout the proposal development lifecycle, including compliance matrix reviews, technical scoping, and solution narratives.

- Supports the Marine Corps Installation Services Transport and Communications (ISTC) task orders by delivering cybersecurity-related deliverables, including identifying applicable security controls and documenting their implementation, determining relevant STIGs, documenting ports, protocols, and services in use, and providing input to the engineering design.
- Serves as the assigned ISSO for Actionet's IT Operations, collaborating with the IT Ops Manager to maintain the Actionet System Security Plan (SSP), develop security awareness training, and ensure audit readiness for ISO, CMMI, and CMMC assessments.
- Drives efforts toward organizational readiness for CMMC Level 2 and Commercial Solutions for Classified (CSfC) compliance by aligning security controls, documentation, and processes with DoD and NSA requirements.
- Participates in solutioning sessions to develop innovative technical strategies, contributing to proposals that addressed complex client requirements.
- Assists with development of technical responses for RFQs and RFPs, ensuring compliance with customer needs and emphasizing technical strengths.
- Serves as a proposal reviewer for Pink, Red and Gold team reviews, providing technical and strategic feedback to strengthen compliance, clarity, and alignment with customer requirements.
- Developed cybersecurity-focused articles for ActioNet's company-wide newsletters (Fall 2024, Spring 2025), promoting awareness during Cybersecurity Awareness Month and sharing practical strategies for building a security-conscious workplace.
- Drive AI adoption across proposal operations by implementing tools such as ChatGPT and CoPilot, developing internal playbooks, and aligning usage with the NIST AI Risk Management Framework (AI RMF).

ActioNet, Inc., 3/24 – 6/24

Senior Information System Security Officer (ISSO)

NOAA Office of Marine and Aviation (OMAO)

- Led the Internal Security Control Assessment (SCA) for Year 2, including the development of a Security Assessment Plan, CSAM control evaluation, results documentation, and Security Assessment Report (SAR). Drafted POA&Ms in CSAM, created briefing presentations, and presented findings to the MACC Director, Acting Deputy Director, CISO, and System Owner.
- Represented OMAO in the NOAA Risk Management Framework (RMF) Workgroup, contributing to the development of NOAA RMF templates (e.g., CP, BIA, SLA, ISA). Proposed revisions to the ISA template to align with departmental policies and NIST guidance (SP 800-47 Rev. 1).
- Provided support for the External Security Control Assessment which includes facilitating the weeklong interview sessions between the assessment team and system support team, and following up to ensure artifacts were provided.
- Performed an initial gap analysis of the High Value Asset (HVA) overlay controls implemented at OMAO to identify what controls are implemented and identify the POA&Ms that should be prioritized.

- Completed Cybersecurity Supply Chain Risk Analysis reviews (Tier 1 and Tier 2) for IT purchase requests identifying potential vulnerabilities and ensuring compliance with organizational and regulatory standards.
- Developed Acceptance of Risk (AOR)/Risk Waivers to formally document and approve residual risk, ensuring informed decision-making and accountability while maintaining compliance with organizational risk management policies.
- Reviewed open POA&Ms and worked with the CISO and System Owner to update milestone details, cost and planned finish dates.
- Tracked and followed up on all open security incidents ensuring timely resolution and closure by coordinating and following up with relevant teams.

Datawiz Corp. 11/2022-3/2024

Senior Cybersecurity Consultant/ISSO

Department of Labor (DOL)/ Office of the Chief Information Officer (OCIO)

- Team lead overseeing continuous monitoring activities for DSAM managed systems providing guidance to other Information System Security Officers (ISSOs) to help ensure system compliance against FISMA requirements and organizational policies.
- Designated as the primary ISSO for over ten major information systems, regularly engaging with System Owners to ensure ongoing security compliance and manage critical deliverables.
- Served as a member of the DSAM System Security Specialist group. This group is responsible for standardizing and reviewing control tailoring across all DOL systems and supporting OCIO with evaluating new technical solutions for security risk and impact.
- Developed and reviewed Information System security package documentation including but not limited to FIPS 199, Digital Identity Risk Assessment, Contingency Plan, Configuration Management Plan, Incident Response Plan, PTA/PIA, etc.
- Extensive experience using Cyber Security Assessment and Management (CSAM) tool to perform security self-assessments, Risk Assessment, Security Categorization of information systems, Assessment and Authorization (A&A), Plan of Action and Milestones (POA&Ms) and updating System Security Plan (SSP).
- Developed and presented a Cloud System Contingency Plan and Incident Response Test/Training presentation to system support personnel for all DOL cloud systems. Approximately 70 participants comprised of System Owners, Program/Project Managers, Human Resource personnel, System Administrators, Developers, and other ISSO were in attendance.
- Prepared authorization packages and briefings to present to leadership
- Effectively worked with the OCIO audit team with Office of Inspector General (OIG) audit activities and provides responses to Notification of Finding & Recommendations (NOFR).
- Monitored implementation of corrective actions to appropriately address identified security vulnerabilities resulting from GAO engagement, OIG FISMA audits etc.
- Provided technical advice and guidance to senior management making recommendations on a variety of information system designs, system software, and/or equipment configuration, IT security principles, techniques, requirements and ensuring the confidentiality, integrity, availability, and authentication of applications

Datawiz Corp. 12/2019-11/2022

ISSO

Department of Labor (DOL)/ Office of the Chief Information Officer (OCIO)

- Served as the Information System Security Officer (ISSO) responsible for continuous monitoring activities for three major information systems to ensure system compliance against FISMA requirements and organizational policies.
- Performed gap analysis between FISMA and FedRAMP controls and provided guidance to System Owner and technical team with implementing new policies to comply with NIST 800-53 rev. 5 requirements.
- Led the Security Authorization Boundary Structure and Standardization for an information system. This included the development of an Authorization Playbook and checklist for new systems undergoing initial Authority to Operate (ATO) certification. Received recognition from the Director of DSAM for my contribution towards the DSAM Priority Project.
- Developed a Contingency Plan and Incident Response Test/Training presentation and presented training to System support personnel.

Datawiz Corp. 4/2011-12/2019
Security Analyst
Department of Labor (DOL) /Mine Safety and Health Administration (MSHA)

- Worked with a team of Information Security Specialists with performing information security compliance audits, developing and implementing information security policies, procedures, standards and guidelines, performing gap analysis, implementing new NIST guidelines as they become available, and oversees end user's security awareness and training.
- Provided guidance to users on DOL's IT security guidelines, directives, and procedural initiatives.
- Led MSHA to exceed the Department's goal of 97% completion for the mandatory annual Information System Security and Privacy Awareness (ISSPA) training and consistently exceeded this requirement for eight consecutive years.
- Managed the Role-Based Security Training (RBT) activities at MSHA and ensures employees with IT Security Responsibilities complete Role-Based Security training annually and maintains tracking records for each employee. Prepared and presented several Role-Based trainings via WebEx to contractors and MSHA IT Specialists. Presented RBT briefing to the Assistant Secretary and Deputy Assistant Secretary.
- Coordinated with the MSHA Office of the Assistant Secretary to post information for National Cyber Security Awareness Month and drafted articles and information for each weekly theme. Information was posted on MSHA's Intranet and PEIR's Quarterly Newsletter.
- Served as Information Security Representative for the agency's Configuration Control Board (CCB) responsible for reviewing and reporting on configuration change requests, performing security impact analysis, and ensuring that only organization-approved changes were implemented.
- Creates and tracks POA&Ms using the Department's Cyber Security Assessment and Management tool and uploads security documentation/artifacts.
- Supports team of Information Security specialists and System Owner with performing A&A activities for MSHA's major information system.

- Trained new contractor staff in the performance of tasks such as creating POA&Ms and following security incident response procedures. Provided guidance to IT Specialists/Helpdesk on what to do in the event of a security incident.
- Participates and coordinates activities for the Department's Quarterly Cybersecurity exercise. Presented a phishing awareness briefing to Program Area Administrative Officers to encourage discussing security awareness with users in staff meetings.
- Served on the Program Evaluation and Information Resources (PEIR) Newsletter Editorial Board and was responsible for providing topics on Information Security initiatives.
- Assisted with Agency-wide implementation of two-factor authentication for over 2,400 end users using Personal Identity Verification (PIV) cards.