

Lead IV&V SCA Lead IV&V SCA Lead IV&V POAM Manager - MBL Technologies Woodbridge, VA
Currently have an active Secret Clearance Extensive knowledge of all common business-related IT functions XACTA Analyze Nessus and Web Inspect scans. Ability to identify potential online security risks Ability to compile daily database reports to ensure the security of the system
Demonstrated achiever with exceptional knowledge of organizational and customer service skills
Expert at utilizing MS Word, MS Excel, MS Power point, MS Outlook AND SharePoint. I have a very strong work ethic. Skilled at learning new concepts quickly, work well under pressure, communicating ideas clearly and effectively. Enthusiastic and experienced in overseas travel.

IV&V SME System Insepection Authorized to work in the US for any employer Work Experience

Lead IV&V SCA MBL Technologies - Washington, DC November 2017 to Present ? Supported the Security Assessment and Authorization process of the clients systems as a Security Analyst ? Worked in the development, documentation and completion of the SA&A. ? Supported the SDLC process from system review, to assessment of system using the NIST -800-53 guideline ? Worked on the Security Assessment Process from System Categorization using NIST 800-60 and FIPS 199 ? POAM management ? Reviewed technical security controls and provide implementation responses to meet requirements ? Provide continuous monitoring support for control systems in accordance to FISMA guidelines ? Document findings in the SAR and the POAM ? Documents and manage system artifacts using Archer as tool ? Meet with client to discuss findings and process of remediation ? Marquis supports the Security Assessment and Authorization process of the clients systems as a Security Analyst ? Marquis also works in 3PAO projects as well ? Marquis utilizes FedRAMP requirements to assess cloud systems to ensure the proper security requirements are satisfied. ? Reviewed technical security controls and provide implementation responses to meet requirements ? Document findings in the SAR ? Meet with client to discuss findings and process of remediation

IT Security Specialist Skyline Technology Solutions LLC June 2015 to November 2017 Update IT security policies, procedures, standards and guidelines according to department and federal requirements using steps of the SA&A (Security, Assessment and Authorization)(NIST 800-53/53ARisk Management Framework) RMF ? Perform risk assessments,

update and review System Security Plans (SSP) using NIST 800-18 (Guide for Developing Security Plans for federal information systems) Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Management Plans (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation. ? Perform vulnerabilities scan and monitor continuously using NIST 800-137 as a guide with the aid of Nessus ? Vulnerability Scanner to detect potential risks on a single or multiple assets across the company network IT security analyst Contingency Plans (CP) March 2013 to June 2015 Developed, reviewed and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices. ? Performed vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple assets across the enterprise network. ? Updated IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. ? Performed risk assessments, reviewed and updated, Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Management Plans (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation. (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). ? Monitored controls post authorization to ensure constant compliance with the security requirements Dispatcher/ It Intern Homeland Security Solutions Inc - Quantico, VA June 2007 to March 2013 Monitor personnel or equipment locations and utilization to coordinate service and schedules. ? Record facts to prepare reports that document incidents and activities. ? Relay complaint and emergency-request information to appropriate agency dispatchers. ? Question callers to determine their locations, and the nature of their problems to determine type of response needed. ? Receive incoming telephone or alarm system calls regarding emergency and non-emergency police and fire service, emergency ambulance service, information and after hours calls for departments within a city. ? Determine response requirements and relative priorities of situations, and dispatch units in accordance with established procedures. ? Record details of calls, dispatches, and messages. Enter, update, and retrieve information from teletype networks and

computerized data systems regarding such things as wanted persons, stolen property, vehicle registration, and stolen vehicles. ? Maintain access to, and security of, highly sensitive materials. ? Relay information and messages to and from emergency sites, to law enforcement agencies, and to all other individuals or groups requiring notification. ? Scan status charts and computer screens, and contact emergency response field units to determine emergency units available for dispatch. ? Observe alarm registers and scan maps to determine whether a specific emergency is in the dispatch service area. ? Maintain files of information relating to emergency calls such as personnel rosters, and emergency call-out and pager files. ? Monitor various radio frequencies such as those used by public works departments, school security, and civil defense to keep apprised of developing situations. ? Learn material and pass required tests for certification. ? Read and effectively interpret small-scale maps and information from a computer screen to determine locations and provide directions. ? Test and adjust communication and alarm systems, and report malfunctions to maintenance units ? Monitor alarm systems to detect emergencies such as fires and illegal entry into establishments. ? Interned as a security analyst as well as worked with different SIEM tools. Education Washington & Lee High School - Arlington, VA Certifications/Licenses CEH September 2018 to September 2021

Name: Ryan Mendoza

Email: danawright@example.org

Phone: +1-373-218-0350x310