CYBER SECURITY ANALYST CYBER SECURITY ANALYST CYBER SECURITY ANALYST - V-TECH SOLUTIONS ? Proactive and goal oriented IT Analyst professional with over 5 years of successful experience, seeking a position in growth and work on FISMA, system security monitoring, and auditing; risk assessments; audit engagements, testing information technology controls and developing security policies, procedures, and guidelines. Am a great team player with a fast learning curve. I can work perfectly and effectively under stressful conditions where speed and accuracy are necessary for mission critical situations. My attention to detail and the ability to maximize system resources can be beneficial to your company. CORE QUALIFICATIONS Performing daily ongoing (A&A) Assessment and Authorization projects in support of client security system. Conducting kick off meeting in order to categorize agency's systems according to NIST requirements of Low, Moderate or High system. Conducting IT controls risk assessments that include reviewing organizational polices, standards, procedures and guidelines. Reviewing and update of the System Security Plan (SSP) using NIST SP 800-18 guidelines. Knowledge of the entire RMF process and its compliance using NIST publications and standards. Supporting client with creating SOP as evidence in ongoing POA&M remediation process. Experience in system classification and categorization using RMF process to ensure system CIA. This ensures complaint security control selections and implementation for continuous system protection. Supporting client in creating findings for POA&Ms as part of ongoing remediation process. Supporting client in creating memos for POAMs that past Scheduled Completion Dates. ? Instrumental in developing and completing system authorization (ATO) packages/artifacts including System Security Plan (SSP), Security Assessment Report (SAR), Contingency plan (CP), Privacy Threshold and Impact Analysis (PTA & PIA), Security Assessment Plan (SAP), Plan of Action and Milestones (POAM). ? Extensive knowledge of FIPS 199, 200 NIST SP 800- [ ] 37, 60 Vol 1&2,53 rev4, 18, 53A rev 1, 30, 34, 137, guidelines to comply with FISMA. ? Providing ongoing gap analysis of current policies, practices, and procedures as they relate to established guidelines outlined by NIST, OMB, FISMA related Federal IT security mandates and best practices; and agency specific policies and directives. ? Highly acquainted with FedRAMP compliance and Cloud Computing services, ? Document

residual risks by conducting a thorough review of all the vulnerabilities, architecture and defense in depth and provide the IA risk analysis and mitigation determination results for the Test Report. ? Manage vulnerabilities with the aid of NESSUS and Microsoft Baseline Security Analyzer (MBSA 2.3) Vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network. ? Knowledge of IT security architecture and design (firewalls, Intrusion Detection Systems, Virtual Private Networking, and virus protection technologies), LAN/WAN design and general internetworking technologies. ? Communicates effectively through written and verbal means to co-workers, subordinates and senior leadership. ? Possess a strong work ethic, positive attitude, great analytical skills, and team player. Work Experience CYBER SECURITY ANALYST V-TECH SOLUTIONS November 2014 to Present Determining information system categorizations using the FIPS 199 and NIST 800-60 Vol 2 as a guide respectively. Reviewing Privacy Threshold Analysis (PTA), and E-Authentication with business owners and selected stakeholders. ? Specialized in the entire FISMA RMF, SA&A/C&A and system control, assessment processes using FIPS 199/NIST SP 800-60, NIST SP 800-53r4/53A, preparing and reporting SSP, SAP, ST&E, SAR, POAM, as well as the FedRAMP Frameworks. ? Work with Certification and Accreditation team (C&A); Spearhead team to develop and complete system ATO packages including System Security Plan (SSP), Security Assessment Report (SAR), Contingency plan (CP), Privacy Threshold and Impact Analyses (PTA & PIA), Security Assessment Plan (SAP), POAM. ? Supported client with creating SOP as evidence in ongoing POAM remediation process in accordance with Federal, Agency and Organizational policy, to include FISMA, NIST, OMB, FIPS instructions ? Supported client in creating findings for POAM as part of ongoing remediation process. ? Provided ongoing gap analysis of current policies, practices, and procedures as they relate to established guidelines outlined by NIST, OMB and FISMA ? Utilizes the Cyber Security Assessments and Management (CSAM) to record, manage, and assess common threats and vulnerabilities. ? Support client in creating Risk Based Decisions as part of pre- OIG audit. IT SECURITY ANALYST AMERICAN SYSTEMS February 2012 to November 2014 Developed and maintained artifacts supporting the Risk Profile SP, PTA, PIA, SAR, SSP, SAP CP, CM, IR and POAM. ? Provided subject matter

expertise with the development of security policy documentation that follows FISMA requirements, NIST 800 Series.  ? Performed periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk.  ? Developed the audit plan and Performed the general computer controls testing of Information Security, Business Continuity planning, and built professional relationships with outsourced Vendors.  ? Researched and communicated how vulnerabilities can be exploited within technology and the Client environment in a manner that resonates with the business areas.  ? Planned and conducted meetings with stakeholders to discuss and analyze system weakness and vulnerabilities and potential remediation actions  ? Conducted authorization and accreditation (A&A) through the RMF process for all system in the organization. This included developing a security plan, performing a complete risk assessment, identifying and implementing security controls. Education Bachelor's in Medical Technology University of Buea Skills FEDERAL INFORMATION SECURITY MANAGEMENT ACT (5 years), FISMA (5 years), NIST (5 years), FIREWALLS (Less than 1 year), IDS (Less than 1 year) Additional Information TECHNOLOGIES  ? Software: MS Office, Microsoft Windows, Linux/Unix.  Networking: LANs, WANs, VPNs, Routers, Firewalls, TCP/IP. IDS/IPS: ISS.  Standards: DIACAP, NIST, FISMA, FedRAMP.

Name: Tracy Marshall

Email: dayrobert@example.net

Phone: 001-482-570-7412