Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - V-Tech Solutions Work Experience Cyber Security Analyst V-Tech Solutions April 2016 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. ? A 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 the 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 System, Virginia February 2013 to March 2016 Developed and maintained artifacts such as 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. 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, Jira, rally. Networking: LANs, WANs, VPNs, Routers, Firewalls, TCP/IP. IDS/IPS: ISS. Standards: DIACAP, NIST, FISMA, FedRAMP.

Name: Patrick Bowen

Email: jsantiago@example.org

Phone: 001-373-293-1641