Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - PingWind Inc Woodbridge, VA IT Security professional with a 6 years' experience with proven hands-on project experience using the Risk Management Framework (RMF); who possess the knowledge to Categorize, Select, Implement, Assess, Authorize, and Monitoring; to integrate information security, and risk management activities into organizational enterprise architecture, and System Development Lifecycle (SDLC), using applicable FIPS, FISMA, and NIST standards and guidelines. With the ability and knowledge to facilitate strategic best practices in utilizing security controls to mitigate vulnerabilities to achieve confidentiality, integrity, and availability of organizational information, and information systems. Hold strong work ethics and maintains an effective devotion to customer service delivery. Work Experience Cyber Security Analyst PingWind Inc - Washington, DC June 2016 to Present Perform security categorization using FIPS 199 and NIST SP 800-60, reviewed Privacy Threshold Analysis (PTA), and E-Authentication with system stakeholders. Prepare, update and maintain RMF documentation, but does not limit to ATO packages such as the SSPs, SARs, POA&Ms and Security Control Traceability Matrix (SCTM) for all networks and systems. Participate as a member of Certification and Accreditation team; to perform risk assessment, update System Security Plan (SSP), Contingency Plan (CP), and Plan of Actions and Milestones (POA&M). Perform threat vulnerability assessments and provided security test and evaluation support. Ensure that security policies, procedures, and recommendations comply with NIST, FISMA, organizational guidelines, standards, and technical practice. Work with the Security Control Assessors (SCA) team to uncover the effective of current security controls and a path to implement future security controls, where potential weaknesses may exist. Review implementation statements and supporting evidence of security controls to determine if the systems are currently meeting the requirements and provide findings/suggested mitigations to the system stakeholders. IT Security Analyst Acentia LLC - Washington, DC October 2013 to June 2016 Worked with business process owners to ensure timely identification and remediation of jointly-owned risk related issues and action plans. Ensured system security authorization controls contain accurate implementation statements and appropriate security documents as evidence to support implementations.

Assessed system design and security posture as well as advising information security compliance with FISMA and NIST SP 800-53 controls.   Conducted security control assessments to assess the adequacy of management, operation privacy, and technical security controls implemented.   Reviewed Nessus and Database vulnerability scan results for mitigation actions and help the ISOs to create and maintain POA&Ms for the deficiencies identified in the scan results.   Provided continuous monitoring activities after authorization to ensure control effectiveness and continuous compliance.   Applied current technologies, information security policies, guidance, and best practices to systems and networks to maintain an acceptable system security posture throughout the life cycle of systems.   Stayed abreast of current applicable federal and organization security laws/policies as well as developed and presented information security awareness and security trainings on various corporate policies. Data Center Site Officer Amazon - Manassas, VA March 2011 to October 2013   Maintained report and document safety concerns, policy violations, and maintenance issues.   Educated vendors, contractors, and employees on the data center badging policies.   Monitored the data center CCTV cameras for incoming and outgoing traffic activities, including fire alarm panels and other life safety equipment.   Responded to alarms, emergencies and other incidents as needed to preserve life and protect property.   Created reports, presentations and communicated with management on the status of physical security operations.   Ensured that all operational standards and requirements were adhered to for complete security of the infrastructures under my purview.   Contributed to team effort by accomplishing related results as needed. Education Bachelor of Arts in Human Services and Social Justice in Public Health George Washington University - Washington, DC Associate Degree in Cybersecurity in Cybersecurity Northern Virginia Community College - Springfield, VA Skills Security, Sharepoint, Nist, Fisma, Life cycle, Ms office, Security documentation, System security, Vulnerability assessment, Documentation Additional Information CORE COMPETENCIES   System Life Cycle Project Management MS Office Suite   Security Assessment & Authorization Windows Operating Systems   System Security Documentation GRC RiskVision   Vulnerability Assessment and Management SharePoint Application   POA&M Management McAfee Virus Scan Enterprise   Cloud Computing Security

NIST, FISMA, FedRAMP, OMB

Name: Dominique Tran

Email: rebeccawu@example.net

Phone: (665)528-9875