Customer Value Partner Customer Value Partner Customer Value Partner - CVP Silver Spring, MD Detailed knowledge of security tools, technologies and best practices with more emphasis on FISMA/NIST and FedRAMP. Over 7 years of experience in system security monitoring, auditing and evaluation, A&A and Risk Assessment of General Support Systems (GSS), Major System and Minor Application. Work Experience Customer Value Partner CVP - Fairfax, VA November 2017 to Present Information Systems Security Officer   Provide Information Assurance support to a key Government client.   Use Accreditation and Authorization (A&A) skills to work with various program and interagency personnel to strengthen organizational security posture.   Make sure the assigned systems continue to be FISMA/FedRAMP compliant   Make sure the Security Assessment Report (SAP) and the authorization to operate are within their life span   Categorize systems' C.I.A using FIPS 199 and NIST SP 800-60   Conduct Self-Annual Assessment (NIST SP 800-53A)   Perform Vulnerability Assessment and ensure that risks are assessed, evaluated and a proper actions have been taken to limit their impact on the Information and Information Systems   Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages Information Systems Security Officer BREWYN HEIGHTS, MD November 2014 to August 2018   Reviews and continuously monitors implemented security controls.   Creates and maintains security checklists, templates and other tools to aid in the A&A process. Performs security control assessment using NIST 800-53 guidance and as per continuous monitoring requirements.   Performs risk analyses to determine and recommends essential safeguards.   Proactively mitigates system vulnerabilities and recommends compensating controls.   Prepares security authorization packages in accordance with the client contractual requirements. Develops core documents such as System Security Plan, Contingency Plan, Incident Response Plan, Standard Operating Procedures, Plan of Actions and Milestones, Remediation Plans, Configuration Management Plan, etc.   Maintains client specific Plan of Action and Milestones and supports remediation activities. IT Security Analyst SMARTTHINK Ltd, MD December 2011 to November 2014   Assisted Business Owners and ISSOs in preparing Security Assessment and

Authorization (SA&A) packages for systems, ensuring management, operational and technical security controls are adhered to a formal and well-established security requirement authorized by NIST SP 800-53rev4   Provided support to external audit teams as required (Help with gathering/presentation of evidence to validate controls effectiveness and efficiency) Analyzed/reviewed and update System Security Plan (SSP), Information System Risk Assessment (ISRA)   Created and reviewed Privacy Impact Analysis (PIA) artifacts. This involved working closely with the Information System Security Officers (ISSOs), system administrators, application developers, and the Privacy Act Officer TRAINING/INTERNSHIP SMARTTHINK Ltd, MD October 2010 to August 2011   Certification and accreditation document review training   FISMA compliance training   FedRAMP training   Developing reviewing and evaluating System Security Plan Getting familiar with all NIST publications   RMF training   Information assurance awareness training Information systems security training Education Liberal Arts and Science Borough of Manhattan Community College January 2011 to February 2012 Bachelor of Science in Biological Science in Biological Science University of Ghana - Accra, GH August 2008 to May 2010 Computer science The City College of New York Skills MySQL, Office Management, Leadership Development, Excel, Visio, Word, Linux, Sharepoint, Powerpoint, Oracle, Microsoft Excel, Microsoft Office, Documentation, Organizational Skills, Management, training Certifications/Licenses CompTIA Security+ AWS Dev Certified Ethical Hacker (CEH) Additional Information   Perform Security Assessment and Authorization (SA&A) documentation   Develop, review and evaluate System Security Plan Develop and conduct SCA (Security Control Assessment) according to NIST SP 800-53A   Familiar with NIST publication; FIPS 199, SP 800-60, SP 800-53rev4, SP -800-137 Develop and update POA&Ms   MS Excel, Power Point, Visio, SharePoint, Windows   Ability to multi-task, work independently and as part of a team   Strong analytical and quantitative skills Effective interpersonal and verbal/written communication

Name: Peter Mcknight

Email: jacobmoore@example.org

Phone: 288.352.9482