Senior Consultant Senior Consultant Senior Consultant - Coalfire Systems Inc Hanover, MD IT Security Professional with over 6 years of experience specialized in Security Assessment & Authorization (SA&A), CyberSecurity, Information Assurance (IA), Risk Management, System Continuous Monitoring, Regulatory Compliance, Vulnerability Management and Project Management. I possess strong managerial skills, expertise in FISMA compliance, highly adaptive and superior analytical and organizational skills. Self driven with the ability to build and work collaboratively in a team environment or independently with strong written and verbal communication skills. Work Experience Senior Consultant Coalfire Systems Inc - Washington, DC August 2018 to Present Assisted in developing FRTIB's security architecture Part of the Audit liaison support team, assisting with internal audits Helped identify performance improvement opportunities for FRTIB's Assisted with Audit walkthrough and audit status meetings Cyber Security Analyst PingWind Inc - Washington, DC April 2016 to August 2018 Conduct security control assessments for new client systems based on NIST SP 800-53A Rev4 and in accordance with client policies and procedures Leadership in utilizing Risk Management Framework process to enable successful approval to operate (ATO) Provided leadership and strategic guidance to teams during solution development process to ensure alignment with overall business strategy and effective use of AWS services. Ensure that security policies, procedures, and recommendations comply with NIST, FISMA, organizational guidelines, and technical practice. Analyze discovered infrastructure and software vulnerabilities obtained from scanning to determine risk, impact and remediation strategies. Prepare recommendation reports that are made available to system owners to remediate identified vulnerabilities during the risk assessment process. IT Security Analyst Ernst & Young - Washington, DC June 2015 to April 2016 Assisted in conducting FedRAMP Readiness Assessments and reviewed ATO packages for FedRAMP Cloud environments. Implemented NIST 800-53 security controls in a FedRAMP Cloud environment for the Federal Government. Provide expertise in vulnerability management processes and network vulnerability scanning using Tenable Security Center and/or Nessus. Responsible for the development of system security control test plan and in-depth security assessments of information

systems. Develop security baseline controls and test plans used to assess implemented security controls. Conduct interviews, test and examine organizational processes and policies for FISMA compliance. Assess system design and security posture as well as advise information security compliance with FISMA and NIST SP 800-53 rev 4 controls. Create Security Assessment Reports (SAR) identifying the results of the assessment along with Plan of Action and Milestone (POA&M). Perform and recommend maintenance and system configuration settings in order to protect systems from emerging cyber threats. Participate in CDM meetings to discuss vulnerabilities and potential remediation actions with system and application owners. Develop System Security Plans (SSP) to provide an overview of system security requirements and describe the controls in place or planned by information system owners to meet those requirements Conduct follow up meetings to assist ISSOs, System Owners and Authorizing Officials to close remediated POA&M items. Cyber Security Risk Consultant Deloitte Consulting - Washington, DC October 2013 to June 2015 Create and review System Security Plans compliance with FISMA and FISCAM. Conduct security control assessments for new client systems based on NIST SP 800-53A Rev4 and in accordance with client policies and procedures. Initiate kick-off meetings to collect system information to assist in the categorization phase using FIPS 199 and NIST SP 800-60. Develop System Security Plans (SSP) to provide an overview of system security requirements and describe the controls in place or planned by information system owners to meet those requirements. Assess security and privacy controls using NIST 800-53 Rev4 publication guideline. Review vulnerability management documents and provide remediation recommendations. Review contingency plan and disaster recovery operation policy and procedures for compliance. Manually reviewed logs and provided documentation guidelines to business process owners and management. IT Security Analyst Acentia LLC - Washington, DC September 2012 to October 2013 Provided expertise on technical services including all aspects of information security Conduct IT risk assessments to identify system threats 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 Performed maintenance and advanced configuration of systems in order to protect systems from emerging cyber threats. Conducted forensic traffic logs analysis to isolate issues and respond to analyst alerts Business Impact Analysis (BIA) to analyse mission-critical business functions, and identify and quantify the impact if these are lost (e.g., operational, financial). BIA helped to define the company's business continuity plan and IT internal control audit objective. Performed IT General Control Audits (ITGC) in relation to Sarbanes -Oxley (SOX) Section 404 framework. AWS Cloud Security Compliance- Proficient Federal ATO package development for Cloud based systems- Proficient Education Master of Science in Cybersecurity Management Kean University May 2017 Bachelor of Science in Information Technology University of Ghana - Accra, GH June 2008 Skills Cobit, Iso, Iso 27001, Itil, Nessus, Nist, Sox, Fisma, Security, Sas, Sarbanes-oxley, Sarbanes-oxley act Additional Information EXPERTISE: Security Assessment & Authorization (SA&A), OMB Circular A-130 Appendix III, NIST 800-53A, FIPS, FISMA, FedRAMP, AWS, COSO/COBIT, Sarbanes-Oxley Act, (SOX) SAS-70/SSAE 16, ITIL, ISO 27001, Privacy Act of 1974, Gramm-Leach-Bliley Act (GLB), Nessus.

Name: James Todd

Email: jenniferwilkins@example.com

Phone: 001-916-427-5873x673