Information Security Engineer Information Security Engineer Information Security Engineer - Bic Line Technologies US Authorized to work in the US for any employer Work Experience Information Security Engineer Bic Line Technologies - Houston, TX November 2015 to Present Compile, write, update, finalize, and produce all FISMA documentation and associated artifacts as required by Client in a manner compliant with all Federal security requirements and policies. Ensure all Security Authorization documentation for assigned systems remains accurate and up to date on a continuous basis, including, but not limited to, accurate and valid lists of assets (hardware/software), accurate boundary diagrams, accurate ports and protocols, etc. Ensure all FISMA documentation is updated within 6 months following a new policy release. Participate in meetings related to SAP and OA. Compile, write, update, finalize, produce, and support activities for IT Security Common Control Catalogs and related documentation including, but not limited to, Security Plans or other documents required. Manage the Interconnection Security Agreements for all systems, including creation, tracking, and vetting. Review all ISSO provided documentation for accuracy and relevancy, provide follow-up to ISSOs to ensure documents are properly completed. Prepared Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. Performed vulnerability assessment, making sure risks are assessed and proper, actions taken to mitigate them. Conduct IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. Developed risk assessment reports. These reports identified threats and vulnerabilities. In addition, it also evaluates the likelihood that vulnerabilities can be exploited, assess the impact associated with these threats and vulnerabilities, and identified the overall risk level. IT Security Analyst Harris Health Systems January 2010 to November 2015 Analyze and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan Of Actions and Milestones (POA&M) Assist System Owners and ISSO in preparing Security Assessment and Authorization package for companies IT systems, making sure that management, operational and technical security controls adhere to a

formal and well-established security requirement authorized by NIST SP 800-53 R4 Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60 Conduct Annual Self-Assessment (ASA) (NIST SP 800-53A) Perform Vulnerability Assessment. Make sure 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 Ensured Systems' Plan of Action & Milestone (POA&Ms) are closed or update in a timely manner using a tracking tool CSAM Manages Systems' Accounts to ensure Privilege Users Accounts are Re-certified twice a year. Ensured Separation of Duties is enforced by reviewing all Accounts in the Windows Server Admins and Domain Admins. Created reports detailing identified vulnerabilities and the steps to remediate them. Tested and document comprehensive security assessment results that include a full description of the weakness and deficiencies discovered during assessment information System Security controls per the NIST 800-53A Revision 4 guidelines. Assisted in identifying and communicating application control deficiencies and the associated risks. Assisted with the development and maintenance of plan of action and milestones (POA&Ms) to document security vulnerabilities and mitigation strategies. Monitored controls post-authorization to ensure continuous compliance with security requirements. Provided expertise and assistance in the development of continuous monitoring programs and plans Education High School Diploma HND Automobile Engineering Polytechnic Ibadan - Houston, TX Skills RISK ASSESSMENT (8 years), SECURITY (8 years), VULNERABILITY ASSESSMENT (8 years), INFORMATION ASSURANCE (Less than 1 year), LIFE CYCLE (Less than 1 year) Additional Information Area Of Expertise Assessment and Authorization (A&A) IT Security Compliance Vulnerability Assessment Network Vulnerability Scanning Information Assurance Systems Risk Assessment Systems Development Life Cycle Technical Writing Project Management and Support Authorized to work in United States for any employer

Name: Christian Palmer

Email: lgarner@example.com

Phone: (471)512-8132x2109