IT Security Analyst IT Security Analyst IT Security Analyst - Maximus Laurel, MD Security Assessment and Authorization (SA&A) professional with 5 years of experience in Risk Management Framework (RMF) Develop, review and evaluated System Security Plan based NIST Special Publications Perform comprehensive assessments and write reviews of management, operational and technical security controls for audited applications and information systems Develop and conduct ST&E (Security Test and Evaluation) according to NIST SP 800-53A and NIST SP 800-53R4 Compile data to complete Residual Risk Report and to insert contents into the POA&M Ability to multi-task, work independently and as part of a team Strong analytical and quantitative skills Effective interpersonal and verbal/written communication skills Work Experience IT Security Analyst Maximus - Washington, DC October 2016 to Present As an IT Security Analyst, I support the FISMA compliance Security Assessment & Authorization services in support of the Department of Labor (DOL) Office of the Chief Information Officer (OCIO) Enterprise Security and Authorization Management (ESAM) mission of providing independent Security assessment &Authorization and FISMA compliance services to DOL Reviewed, and updated Information Security System Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices. Created and updated enterprise security policies Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53 rev4, FIPS 199, FIPS 200, FedRAMP and OMB A-130 Appendix III. Provided security expertise and guidance in support of security assessments. Participated in weekly IT Security Team meetings to provide guidance and support for the development of enterprise security architecture. Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4. Ensured cyber security policies are adhered to and that required controls are implemented. Validated information system security plans to ensure NIST control requirements are met. Developed resultant ST&E or SCA documentation, including but not limited to the Security Assessment Report (SAR). Assisted team members with proper artifact collection and detail to clients' examples of artifacts that will satisfy assessment requirements. Reviewed security logs to ensure compliance with policies and procedures and identifies potential

anomalies. Made input in data calls to ensure IT security projects are on track. Worked with systems and network administrators to develop implementation statement for security controls. Uploaded supporting docs in SharePoint and CSAM. Reviewed SAR post assessment; and worked with System Owners and ISSO to request and examine artifacts for POAM remediation. Reviewed system-specific Standard Operating Procedures, Rules of Behavior, Contingency Plan, Incidence Response Plan, Configuration Management Plan, Service Level Agreement, and Memorandum of Understanding to aid security assessment and authorization efforts. IT Compliance Analyst Federal Integrated Systems Corporation December 2014 to October 2016 Hold kick-off and weekly meetings with system owners prior to assessment engagements and weekly activities relating to CSAM Collected, reviewed and analyzed audit logs for anomalies Managed vulnerabilities using Nessus vulnerability scanners to detect potential risks on a single and multiple assets across the Enterprise Network. 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. Education BA in Information Technology Methodist University College - Accra, GH 2008 Skills Security, testing, access Certifications/Licenses CompTIA Security+

Name: Lori Ayala

Email: zrussell@example.com

Phone: 434.994.9139x1810