Information Security Analyst Information Security Analyst Information Security Analyst - Innovation Power Technologies Alexandria, VA Dedicated and highly-driven Security Assessment and Authorization [A&A] professional, knowledgeable in Risk Management Framework (RMF), Systems Development Life Cycle (SDLC), Security Life Cycle and vulnerability management using applicable NIST standards. A proven goal-getter and team lead with strong positive customer service. Work Experience Information Security Analyst Innovation Power Technologies - Nokesville, VA March 2015 to Present Working with Management in determining and recommending Information assurance governance structure to protect IT resources. Developing, reviewing and updating information system policies and procedures governing security best practices for assigned systems. Reviewed completed security Policies and Procedures for completeness, accuracy, and quality. Support the review of all Cloud Service Provider and ATO package documentation for compliance with the agency and FedRAMP security requirements. Creating, reviewing and updating ATO package documents such as SSP, SAR, POA&M, IR, SAP, DRP, BIA, PTA, RA, ISCP, and CPT. Experience with conducting Risk Assessment (RA) and completing Risk Management Framework (RMF) process to obtain ATO. Performing security packages validation to ensure completeness on Risk Assessment, (RA), FIPS-199 Security Categorization, PTA, PIA, SORN, and E-authentication. Monitor controls post authorization to ensure continuous compliance with the security requirement Document and Review security plans (SP), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and risk assessment (RA) documents per NIST 800 guidelines for various government agencies. Work with ISSOs to ensure documenting and remediating audit findings, security planning and reporting, and mitigation of security vulnerabilities are completed in a timely manner. Assisted system owners on policies and procedures development. Ensures that systems stakeholders adhere strictly to the government regulatory standards and guidance such as FISMA. Perform risk assessments for on diverse application systems - including reviewing evidence, interviewing personnel, tests and inspections, producing assessment reports and recommendations. Evaluate security assessment documentation and provide written recommendations for security authorization to the AO. Conducting Vulnerability scanning and

assessment of report using tools such as Nessus HP WebInspect and HP Fortify. Experienced using centralized security document repository such as MS SharePoint, CFACTS, Modulo and DM 36O to manage deliverables. IT Security Analyst / Crest Consulting Group NIST SP - Rockville, MD July 2012 to March 2015 Conduct Assessment & Authorization (A&A) Kick-off Meetings. Conduct IT Controls risk assessment to identify system threats, vulnerabilities, risks, and generate reports. Develop and Conduct Security Test and Evaluation (ST&E) according to NIST SP 800-53A. Developed, reviewed and updated security Policies and Procedure. Monitor controls post authorization to ensure continuous compliance with the security requirements. Performed GAP analysis to identify controls changes from NIST-800 53 rev 3 to NIST-800 53 rev 4 and updated security plans and relevant documents to reflect the changes. Help facilitate and support the Ongoing Authorization Program for the organization. Reviewed completed security documentation for completeness, accuracy, and quality. Provide support to configuration management and control processes to integrate security and risk management. Conducted security impact analyses of security controls based on proposed system changes. Document the application level controls that include security controls in a narrative format. Support the preparation of security test plans, execute and assess the security control effectiveness using security control, test procedures, and create Security Assessment Reports (SAR) based on assessment findings. Familiar with NIST Publications SP 800-18, SP 800-30, SP 800-37 rev 1, SP 800-53 rev 4, SP 800-53A, SP 800-60 and FIPS 199 and FIPS 200. Assist the system owner with defining security objectives and system performance requirements. Works with the system administrators to examine and test the security posture of the systems and applications Conduct Security Assessment via document examination, interviews and manual assessments. Create, review and update POA&M documents Implementing, reviewing, maintaining and continuous monitoring for control systems in accordance to FISMA guidelines, NIST 800-137 Education Masters in Criminal Justice in Criminal Justice University of Phoenix 2012 Bachelors in Sociology in Sociology Alli Ambrose University 1999 Skills Life Cycle (2 years), Project Management (Less than 1 year), Risk Assessment (6 years), scanning (3 years), Security (6 years) Additional Information Areas of expertise include: Policies and

Procedures development Information Systems Security Plan Vulnerability scanning and assessment Privacy Impact Assessment Project Management and Support Business Impact Analysis Systems Risk Assessment Systems Development Life Cycle U.S Citizen and authorized to work for any employer

Name: Sherry Clarke

Email: benjaminmartinez@example.net

Phone: (311)624-1289x0674