Information Security Analyst Information Security Analyst Information Security Analyst - AISEC GROUP Grayson, GA Dedicated and highly driven Security Assessment and Authorization [A&A] professional, knowledgeable in Risk Management Framework (RMF), Systems Development Life Cycle (SDLC), and vulnerability management using applicable NIST standards. A proven goal-getter and team lead with strong positive customer service. Work Experience Information Security Analyst AISEC GROUP - Philadelphia, PA January 2018 to Present Supports and maintains Identity Access Management tools. Support the review of all ATO package documentation for compliance with the agency and FedRAMP security requirements Develop, review and update Security plans (SP), Contingency plans (CP), Contingency plan tests (CPT), Privacy Impact Assessments (PIA), and Risk Assessment (RA) documents per NIST 800 guidelines. Updating systems baseline controls to align with NIST 800-53 security requirements. Reviewed analysis on NIST 1800-12 Derived Personal Identity Verification (PIV) Credentials-Draft publication. Develop and update all Contingency Planning Training and Testing related documents including completing After-Action Report. Conducting Risk Assessment (RA) and completing NIST 800-37 Risk Management Framework (RMF) process to obtain ATO Updating applicable RMF documents to ensure they comply with newly upgraded NIST 800-37r2 Document the application level controls that include security controls implementation statements. Ensures that systems security requirements comply with FISMA standards. 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 4 SQUARE IT CONSULTING - Houston, TX July 2014 to January 2018 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 Master in IT in IT/CYBER SECURITY Florida Institute of Technology Bachelor of Arts Ahmadu Bello University Zaria Skills Security, Life cycle, Sdlc, Systems development, Risk assessment, Security plan, Systems security, testing, Microsoft Office Certifications/Licenses Certified ScrumMaster (CSM) July 2019 to Present Additional Information Areas of expertise include: Risk and Management Compliance Cloud Security Information Systems Security Plan Vulnerability Review and Analysis Privacy Impact Assessment POA&M Management Business Impact Analysis Systems Risk Assessment Systems Development Life Cycle (SDLC) Identity Access Management (SCA) Security Control Assessment Web Application Security and Penetration Testing Authorization and Assessment (A&A Package)

Name: Henry Campbell

Email: amanda94@example.net

Phone: 499-869-4694