Information Security Analyst Information Security Analyst Information Security Analyst Bronx, NY An Information Security Analyst with experience in Risk Management and Compliance, Assessment & Authorization process, POA&M management, Vulnerability Assessment, Continuous Monitoring program, Security Control Assessment in accordance with NIST, FISMA, OMB, RMF, FedRAMP and industry best Security practices. Core Proficiencies / Technical Skills Risk Assessment & Management Microsoft Suite: Word, Excel, PowerPoint Assessment & Authorization process Operating Systems: Windows & Mac System Security Documentation A&A Tool: GRC RiskVision PO&AM Management & Mitigation Vulnerability Tool: Nessus Vulnerability Assessment Cloud Security Authorization-to-Operate (ATO) Documentation Authorized to work in the US for any employer Work Experience Information Security Analyst WeWork - New York, NY November 2016 to Present Develop and update Authorization to Operate (ATO) packages such as the SSPs, SARs and POA&Ms for information systems to ensure compliance with organization's information security requirements Create and maintain POA&Ms for discovered operational and technical vulnerabilities for all assigned systems as well as review security threats and provide recommendations for effective countermeasures. Develop and review system security artifacts such as contingency plan (CP), incident response plan (IRP), privacy impact assessment (PIA), MOU/ISA and risk assessment (RA) document for accuracy, currency, and compliance with NIST 800 guidelines and agency's security requirements. Monitor controls after authorization to ensure control effectiveness and continuous compliance with the system security requirements by evaluating threats and vulnerabilities through Nessus scan results and work with the IT staff for mitigation actions. Support the review of all Cloud Service Provider (CSP) documentation for compliance as well as work with stakeholders until the cloud system documentation meets FedRAMP A&A requirements. Conduct security control assessments for assigned systems using the steps outlines in NIST SP 800-53A to determine the effectiveness of the implemented controls. Review implementation statements and supporting evidence of security controls as to determine if a system currently meeting the requirements and provide findings/suggested mitigations to stakeholders. Coordinate with the ISOs and System Owners to review and complete the Customer

Responsibilities Security Plan for proper implementation details and documentation as part of FedRAMP ATO process. IT Security Compliance Analyst IRI - Queens, NY July 2013 to August 2016 Tracked and updated Plan of Action & Milestones (POA&Ms) for actions following assessment activities and in response to identified vulnerabilities for maintaining system ATO status.

Coordinated with system stakeholders to perform security categorization using NIST 800-60 and FIPS 199 as well as reviewed the PTA, PIA and E-Authentication for assigned systems. Participated as a member of Certification and Accreditation team; to perform risk assessment, update System Security Plan (SSP), Security Assessment Reports (SAR) and Plan of Actions and Milestones (POA&M). Interfaced with internal security personnel, system administrator, customers and management on the on the operational security posture for the systems assigned to me and on security related requirements. Supported the Information Systems Certification and Accreditation process as needed as well as responsible for implementing and maintaining security policies and procedures. Coordinated with the Vulnerability and Patch Management department to review vulnerability scan results, report findings and developed mitigation plans for corrective actions. Worked with system stakeholders to review and maintain security documents such as Configuration Management Plan (CMP), Contingency Plan (CP), Disaster Recovery Plan (DRP), Incident Response Plan (IRP), ISAs and PTA/PIA for compliance. Responsible for researching and evaluating relevant information security policies, guidance, and best industry practices, including NIST and FISMA for applicability to IT systems security. Facilities/Records Manager Utica College - New York, NY August 2009 to March 2013 Overseeing the switch from paper to electronic record-keeping. Ensuring that financial, legal or administrative requirements and regulations are complied with. Ensuring that data is protected, and classifying and indexing records Destroying or archiving finished data/records. Ensuring that records are easily accessible when needed. Education Bachelor's Degree Health Sciences/Information Technologies - Utica College of Syracuse University Skills Risk Assessment & Management Microsoft Suite: Word, Excel, PowerPoint Assessment & Authorization process Operating Systems: Windows & Mac System Security Documentation A&A Tool: GRC RiskVision PO&AM Management & Mitigation Vulnerability Tool:

Nessus Vulnerability Assessment Cloud Security Authorization-to-Operate (ATO) Documentation Work Experience (9 years), Information Security, Cyber Security Certifications/Licenses Certified ScrumMaster (CSM) Present A scrum master is the facilitator for an agile development team. Scrum is a methodology that allows a team to self-organize and make changes quickly, in accordance with agile principles. The scrum master manages the process for how information is exchanged.

Name: Kevin Bailey

Email: candicematthews@example.org

Phone: 780.908.7592