IT Security Analyst IT Security Analyst Seasoned Accredidation and Authorization Analyst Ashburn, VA Security Assessment and Authorization (A&A/C&A) professional, knowledgeable in risk management framework (RMF), systems development life cycle (SDLC), security life cycle and vulnerability management using FISMA, and applicable NIST standards. Solutions-focused, team oriented, work well independently, or in team providing all facets of computer supports with in-depth knowledge and understanding of numerous software packages and operating systems Authorized to work in the US for any employer Work Experience IT Security Analyst Small Business Administration - Washington, DC August 2014 to Present ? Develop and updated system security plan (SSP), plan of action and milestone (POA&M) in CSAM ? Review security logs to ensure compliance with policies and procedures and identifies potential anomalies ? Ensure cyber security policies are followed to and required controls are implemented ? Reviewed SAR post assessment; created and completed POAM's milestones to remediate findings and vulnerabilities ? Validate information system security plans to ensure NIST control requirements are met ? Developed and reviewed various artifacts including SSP, SAR, PTA, and PIA ? Developed, 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 ? Uploaded supporting docs in the System s Artifact Libraries, Google Docs, and CSAM ? Monitored security controls post authorization to ensure continuous compliance with the security requirements ? Performs all activities of certification and accreditation (C&A) effort for information systems as well as site accreditations. ? Perform Federal Information Security Management Act (FISMA) audit reviews using NIST 800-37 rev 1. ? Update IT security policies, procedures, standards, and guidelines according to private and federal requirements. ? Hold kick-off meetings with system owners prior to assessment engagements ? Prepare and submit Security Assessment Plan (SAP) to ISO for approval IT Audit Security Analyst Wells Fargo - Charlotte, NC July 2011 to August 2014 ? Provided information security, compliance, risk advisory, and risk management services. Primary responsibilities included: ? Assisted business units with understanding the risks associated with using a particular vendor and recommending solutions to reduce or eliminate risk. ? Prepared

written reports after the completion of the assessment ? Categorized systems based on SP -800-60 in order to select the appropriate NIST recommended control SP 800-53. ? Performed audit of IT general and application controls, information security, systems development, change management, business continuity, disaster recovery and computer operations. ? Developed, reviewed and updated Information Security System Policies and System Security Plans (SSP) in accordance with NIST, FISMA and industry best security practices. ? Assist in the development of audit objectives and detailed test procedures that effectively address key controls and risks ? Develop audit report and findings, issues and recommendations for improvement. ? Performs Assessment and Authorization in compliance with FISMA/NIST Standards. ? Identified vulnerabilities, recommend corrective measures and ensure the adequacy of existing information security controls ? Reviewed Rules of Behavior (RoB), Interconnection Security Agreement (ISA) and Memorandum of Understanding (MoU) for clients using NIST SP 800-47 Information Security Analyst Paychex, Inc. - Garden City, NY May 2010 to July 2011 ? Performed IT risk assessment and document the system security keys controls. ? Meet with IT team to gather evidence, develop test plans, testing procedures and document test results and exceptions. ? Designed and Conducted walkthroughs, formulate test plans, test results and develop remediation plans for each area of the testing. ? Managed and coordinated Plan of Action and Milestone (POA&Ms) for DSS accredited approved classified systems. ? Conducted IT controls risk assessments (NIST 800-53A) including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with NIST standards ? Reviewed and revised System Security Plan (SSP), System Security test and Evaluation (ST&E) Risk Assessment (RA), Privacy Impact Assessment (PIA), and the Plan Of Actions and Milestones (POA&M) Technical Support Representative INOVA Health Systems - Leesburg, VA September 2009 to April 2010 ? Installed software and resolved technical issues ? Displayed courtesy and strong interpersonal skills with all customer interactions ? Resolved customer complaints and concerns with strong verbal and negotiation skills ? Resolved Remedy tickets on a daily basis ? Coordinated with other IT groups for remediation of complex issues. Education Bachelor of Science in Health Science Mercy College - Dobbs Ferry, NY

September 2005 to May 2010 Skills CSAM (1 year), SSP (4 years), Microsoft Office Suite (10+ years), QRadar (Less than 1 year) Certifications/Licenses Certified Six Sigma Black Belt Present Certified Six Sigma Green Belt Present Additional Information MS Office (Word, Excel, PowerPoint, Access, Outlook), MS Project, CSAM, FIPS 199, SORN, E-Authentication, PTA, PIA, RA, SSP, CP, CIPT, ST&E, SAR, POA&M, ATO, 800-53A, ISA, MOU, CSAM.

Name: Tricia Allen

Email: jenniferbutler@example.net

Phone: +1-800-392-4414