Assessment and Authorization Lead Assessor Assessment and Authorization Lead Assessor Laurel, MD Work Experience Assessment and Authorization Lead Assessor Arch Systems/ CMS April 2019 to Present Responsible for assuring the implementation of the Centers of Medicare & Medicaid Services (CMS) security controls for all systems. Assess security controls for various systems using automation procedure called the Adaptive Capability Test (ACT). Assess mainframe systems for security compliance. Assist in process improvement and automation for the assessment methodology. Conduct evaluations of information system components, management, and design, focusing on information security aspects and accreditation according to the NIST Risk Management Framework. Document control reviews and findings on time and as they occur according to client requirements. Utilize various information system inspection tools to audit systems, analyze potential vulnerabilities and identify mitigation approaches. Review program documentation such as Risk Assessments, Security Plans, and Contingency Plans. Conduct ongoing assessments of contractor facilities as needed to ensure compliance with security requirements tailoring requirements, as needed. Other project support, as needed. IT Security Analyst Montefiore Medical Center - Bronx, NY July 2016 to March 2019 Schedule, plan, and participate in internal auditing in accordance with HIPAA, NIST, and PCI standards Perform security assessments; design reviews; and provide guidance on new technologies for the customers. Develop POA&M (Plan of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation) Perform Assessment and Authorization (A&A) documentation in compliance with company standards Perform Security Categorization (FIPS 199 and NIST SP 800-60 vol 2), Privacy Threshold Analysis (PTA), e-Authentication with business owners and selected stakeholders Author or coordinate the development of other required system security plans: Configuration management (CM), Contingency Plan (CP), Continuity of Operations (COOP), Disaster Recovery Plan (DR) and Incident Response Plan (IRP). Conduct Systems Risk Assessment through Risk Analysis, assessed the various Assets within the systems boundaries and rigorously identifying all the possible vulnerabilities that exist within the system. Developed the audit plan and performed the General Computer Controls testing of Information Security, Business

Continuity Planning, and Relationship with Outsourced Vendors. Performing Vulnerability scanning using Nessus Ensure all security-related incidents are documented and reported to the ISSM and Security Officer Perform systems security audit on a weekly basis to detect unauthorized activities and ensure systems maintain security compliance. Perform Security Control Assessment (SCA) according to NIST SP 800-53A Document and conform to processes related to security monitoring, patching and incident response Manage the organization's RMF continuous monitoring tool and complete specific control activities, Maintain security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Upgrade security systems by monitoring security environment; identifying security gaps; evaluating and implementing enhancements. Perform security engineering analysis, risk and vulnerability assessment, etc. Monitor and analyze security functional tests. Prepare A&A documentation such as SSP, SCONOPS, ST&E reports, etc. Information Security Analyst, Sunrise The Fairfax - Fort Belvoir, VA November 2013 to November 2013 - July 16) Guided System Owners and ISSOs through the Certification and Accreditation (C&A) process, ensuring that management; operational and technical controls for securing either sensitive Security Systems or IT Systems are in place and are followed according to federal guidelines (NIST 800-53). Applied security risk assessment methodology to system development, including threat model development, vulnerability assessments and resulting security risk analysis Provided support and guidance through the phases of FISMA C&A, including monitoring of the C&A artifacts compliance, annual self-assessment (NIST SP 800-53A guidelines) and quarterly self-assessment completion using NIST SP 800-26 guidelines. Created or updated the System Security Plan and conducted an Annual Self-Assessment. Applied knowledge of C&A policies, guidelines, and regulations in the assessment of IT systems and the documentation and preparation of related documents Executed vulnerability assessment and vulnerability scanning tools such as Acas, Metasploit, on a challenging and complex systems-wide information assurance/ system security environment requiring analysis of user, operational, policy, regulatory, and resource demands Assesses and mitigates system security threats/risks throughout the program life cycle;

determines/analyzes and decomposes security requirements at the level of detail that can be implemented and tested; reviews and monitors security designs in hardware, software, data, and procedures, Worked with C&A team members and senior representatives to establish and define programs, resources, schedules, and risks. Developed Test Plans, testing procedures and documented test results and exceptions. Conducted the IT Risk Assessment and documented the controls. IT Security Analyst Speedway LLC - Baltimore, MD September 2011 to October 2013 Develops and implements new IT Security Policies to meet HIPAA and NIST standards for ensuring optimum compliance Perform vendor documentation review and analysis Assess current business practices and identify opportunities to promote effective third-party risk management Document and report risk to Vendor Assessment management team, business partners, and vendors Perform onsite assessments of vendor facilities Document risks and recommendations based on a vendor lack of controls Support and respond to audit procedures and findings. Works across the Global IT organization to ensure compliance activities are being performed as required by PCI-DSS 3.1 Works closely with team members, end users, and other departments to design, implement, support, and maintain application security and security policies that protects Speedway IT systems Reviews existing policies to meet HIPAA security and privacy rules. Conducts risk assessment and formulates a road map for risk remediation Works on risk remediation Analyzes Gap Analysis and prepares a roadmap for risk mitigation Analyzes the physical security environment and implemented policies to secure the overall security infrastructure Initiates and developed strong physical and technical security infrastructure from the scratch. Provides security training and awareness to the entire work force. Participates in the company's Technology Awareness forum Monitors the Network infrastructure for intrusion and vulnerabilities and applied update patches IT Help Desk Specialist FedEx - Alexandria, VA August 2010 to July 2011 Provided support for application software installation and use. Act as an advocate for the office in the resolution of any and all computer-related problems or issues. Assisted in the delivery, installation, and use of systems and services, (e.g., Washington to district office connectivity, Internet, remote access, etc.). Provided front line phone, Live Chat, and Remote Desktop support,

may be required to resolve requests via on-site visit(s). Provide Hardware/Software Installation and Setup support. Troubleshoot and solve common network issues using physical and logical diagnostic tools. Troubleshoot and solve common Microsoft based platforms (Windows XP, Windows 7, Microsoft Office Suite, Etc.) and common hardware used throughout FBCH (Dell, Lenovo, and HP) Troubleshoot basic technical issues over the phone or by logging in remotely to their computers Escalate serious technical issues to engineering staff by relaying information from customer to help diagnose the problem Provided second-tier support to end users for either PC, server, or mainframe applications or hardware. Actuarial Risk Analyst Vanguard Life Assurance Company June 2007 to May 2010 Responsible for assisting in pricing and product development Analyze historical claims data Responsible for monitoring high risk accounts Assist with internal and external reporting Assist in ad hoc requests from internal and external customers Assist with profit share calculations and reporting Assist with reinsurance reports for ceding Conducting Periodic Underwriting and Policy Management Audit Provision of information or report to all users of Underwriting, Claims, Policy Management and Actuarial Information Education BSc. in Actuarial Science University of Cape Coast August 2003 to May 2007 Certified Information Systems Auditor Bellevue University Skills HIPAA (4 years), NIST (5 years), PAYMENT CARD INDUSTRY (4 years), PCI (4 years), security (5 years) Additional Information TECHNICAL COMPETENCY Working knowledge of Risk Management Framework (RMF) for Assessment & Authorization process to obtain an ATO using federal security policies, standards and guidelines including NIST 800 SPs such as 800-18, 800-30, 800-37 rev 1, 800-60, 800- 53/53A rev 4) and FIPS 199 & 200. Experience in developing and reviewing security Authorization and Assessment (A&A) artifacts including, but not limited to Contingency Plans (CP), Incident Response Plans (IRP), Configuration Management Plans (CMP), Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA). Knowledge of Federal and international regulatory bodies such as Office of Management Budget (OMB), FISMA Reports, FedRAMP, PCI DSS , SOX, HIPAA and ISO. Experience in performing on-site security testing using vulnerability scanning tools such as Nessus and Penetrating testing using tool such as Nessus and Wireshark Experience in the development

of ATO Package Documents such as System Security Plans (SSP), Security Assessment Reports (SAR) and Plan of Action and Milestones (POA&M). Proficient in explaining technical information, resolutions, documentations, and presentations to clients and non-technical personnel at all levels of the organization or enterprise. Team oriented with the ability to work independently and proactively while prioritizing competing priorities, often under time constraints.

Name: Penny Cooper

Email: martinezsusan@example.org

Phone: (217)953-2933x032