Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst Great Falls, VA Work Experience Cyber Security Analyst Northern Virginia Community College November 2017 to Present Responsible for creating and updating Policy and Procedures, System Security Plan, Contingency Plan, Contingency Plan Test, Risk Assessment Report, System Categorization, Privacy Threshold Assessment, Privacy Impact Analysis, Security Assessment Report, Security Impact Analysis, and the Security Risk Traceability Matrix. Recommend changes to the current strategy on external threat factors and known good cyber protection initiatives. Provide recommended optimization of applications, hardware and components expediently or via user story escalation to the appropriate stakeholders Create detailed remediation reports and recommendations for compliance and security improvements across systems based on constant changing threats. Perform Vulnerability and Compliance scans via Nessus and WebInspect whilst mapping each finding to the NIST SP 800-53 Revision 4. Worked directly with the network administrators for applying the approved patches and validate all patches are deployed on every device Creating, updating, and maintaining the associated Plan of Action and Milestones (POAM) via CSAM. Facilitate the configuration control board (CCB) meeting; create the meeting agenda and meeting minutes on a weekly basis, close change management requests in a timely manner Up to date with the latest FISMA, NIST standards, and RMF. Familiar with AWS Cloud Security Security Analyst Altruista Health April 2015 to October 2017 Develop and implement documentation outlining system operating environment to include hardware configuration, software, and type of information processed. Manage Plan of Action & Milestones (POA&Ms) Ensure HIPAA compliance is met within the environment Assisted in vulnerability and compliance remediation by analyzing quarterly scan results via Nessus, AppDetective, and NetSparker. Implement the latest revisions of NIST SP 800-53 Rev. 4, and NIST SP 800-37 Rev. 1. Create and complete all the documents that are applied in the Security Authorization package. Perform and complete the Contingency Plan Testing (CPT), and ensured all points-of-contact were aware of their duties and responsibilities. Set up meetings and conference calls with all appropriate Points-of-Contact. Serve as lead analyst on multiple projects and packages, worked as a team with other security analysts and initiated peer

review sessions on A&A documents. Complete System Security Plan (SSP), Information Technology Contingency Plan (CP), Disaster Recovery Plan (DRP), Risk Assessment (RA), Rules of Behavior, Privacy Impact Assessment (PIA), Privacy Threshold Assessment (PTA), and Plan of Action and Milestones (POA&M) Report. IT Security Associate Sprint March 2013 to February 2015

Managed all aspects of cyber security documentation for all internal systems. Briefed senior management on all aspects of security. Developed required security assessment documentations using the Risk Management Framework (RMF). Identified security findings from the vulnerability reports, mapped each finding to a NIST control and tracked findings as needed. Reviewed and continuously monitored implemented security controls. Created and maintained security checklists, templates and other tools. Briefed new employees on security policies and procedures

Responsible for conducting and maintaining up to date security trainings for all employees and vendors. Education High school or equivalent Skills Nist (5 years), Data analytics, SDLC (5 years), Documentation (5 years), Audit (5 years), Customer service (10+ years), Information Security (5 years), Comptia, It Security (5 years), Cyber Security (5 years), Cybersecurity, Information Assurance, Network Security Certifications/Licenses CompTIA Security+ AWS Certified Developer

Name: Gina Rivera

Email: sallyhaney@example.net

Phone: 001-256-925-9003x61587