Team lead/ Sr. IT Security Analyst Team lead/ Sr. IT Security Analyst Team lead/ Sr. IT Security Analyst - Coastal International Upper Marlboro, MD Over 7 years of experience in Information Technology services supporting security initiatives for government and commercial customers. Work experience encompasses threat analysis, incident response, network surveillance, Risk Management Framework (RMF), National Institute of Technology (NIST), System Development Life Cycle (SDLC), Information security documents, developing and promulgating Security Assessment Plans (SAP) and Security Assessment Reports (SARs). Work Experience Team lead/ Sr. IT Security Analyst Coastal International February 2015 to Present Team lead for A&A process responsible for program development, project planning, gap analysis and assigning systems and tasks to A&A team Apply appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53, FIPS 199, FIPS 200, and NIST SP 800-53A R4 Conduct IT risk assessment to identify system threats, vulnerabilities and risk, and generate reports. Maintain, review and update information security system documentations, including System Security Plan (SSP), Plan of Action & Milestone (POA&M), Risk Assessment (RA), policies and procedures, security control baselines in accordance with NIST guideline and security practices. Assess security controls and develop security assessment report (SAR) Support A&A activities (Categorize, Selection, Implement, Assessment, Authorize, Monitor) according to the A&A project plan. Developed system security plans (SSPs) under guidance of NIST. Managed from end to end FISMA Plan of Actions & Milestones (POAM) and associated activities Review authorization documentation for completeness and accuracy for compliance. Facilitate Security Control Assessment (SCA) and monitor activities. Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4. Ensure cyber security policies are adhered to and that required controls are implemented. Validated information system security plans to ensure NIST control requirements are met. Assist team members with proper artifact collection and detail to client's examples of artifacts that will satisfy assessment requirements. Review security logs to ensure compliance with policies and procedures and identifies potential anomalies. Update and review A&A Packages to include Core Docs, Policy & Procedures, Operations and Maintenance

Artifacts, SSP, SAR, FIPS 200, FIPS 199, and POA&M. Collect Operation and Maintenance artifacts on an ongoing basis so that Security Control Assessment (SCA) is seamless. Developed Continuous Diagnostics and Mitigation tasks through related security operational tasks, including capture and management of device baselines, configuration/hardening checklists and compliance monitoring activities, implementing a process to document and track deviations from approved configuration baselines. Upload supporting documentations into the Sharepoint, Google Docs, and CSAM Manage vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network. Deploying, managing, and operating scalable, highly available, and systems on AWS Proficient in an AGILE culture to develop and operate security services in a cloud environment. Proven capability to administrate, engineer, and operate a Splunk environment. Information Security Analyst Cyber Point - Baltimore, MD October 2012 to February 2015 Ensure proper system categorization using NIST 800-60 and FIPS 199; implement appropriate security controls for information system based on NIST 800-53 rev 4 and FIPS 200. ? Conduct security assessment interviews to determine the Security posture of the System and to ? Perform kick Off Meetings ? Conducted incident/event investigation and analysis. ? Maintained security system infrastructure and assesses technical engineering services for the support of integrated security systems and solutions. ? Apply appropriate information security control for Federal Information system based on NIST 800-37 Rev 1. ? Facilitate Security Control Assessment (SCA) and monitor activities. Develop a Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. ? Reviewing, maintaining, and ensuring all assessment and authorization (A&A) documentation is included in the system security package. ? Perform information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements. ? Work with system owners to develop, test, and train on contingency plans and incident response plans. ? Tests, assess, and document security control

effectiveness. Collect evidence, interview personnel, and examine records to evaluate effectiveness of controls. ? Review and update remediation on plan of action and milestones (POA&Ms), in organization's CSAM Work with system administrators to resolve POA&Ms, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M. Computer & Software Proficiencies Microsoft Office Suite Powerpoint CSAM Adobe Qualified Typist (70wpm) Nessus Vulnerability Scanner (SC-5) Splunk MS Project Education BA of Science in Communication Art St. Johns University Skills security

Name: Michael Berry

Email: qperez@example.net

Phone: 316.716.0618x071