Information Technology Security Analyst Information Technology Security Analyst Information Technology Security Analyst - Top Group Tech Boyds, MD I am a passionate and solutions-focused Cyber Security Analyst with over 5 years experience in the Information system field. Knowledgeable in Risk Management Framework (RMF), Systems Development Life Cycle (SDLC), and Vulnerabilities Management using FISMA, with in-depth understanding of numerous security tools. Work Experience Information Technology Security Analyst Top Group Tech - Largo, MD June 2016 to Present Update and analyze System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M) ? Support System Owners and ISSO in preparing Certification and Accreditation package for companies IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4 ? Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60 ? Perform Self-Annual Assessment (NIST SP 800-53A) ? Perform Vulnerability Assessment. Make sure that risks are assessed, evaluated and a proper action have been taken to limit their impact on the Information and Information Systems ? Create standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages ? Performing I.T controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard (PCI DSS) IT Security Analyst ProTech Inc - Baltimore, MD October 2014 to May 2016 Documented and managed Risks in accordance with SP 800-30 and SP 800-37 using nine steps to evaluate the threats, vulnerabilities and security controls surrounding the Information System as well as the likelihood of an exploit and the impact it will have to systems operations. ? Responsible for monitoring compliance with information security policies by coaching others within the organization on acceptable uses of information technology and how to protect organization systems ? Prepared and reviewed Authorization to Operate (ATO) packages (i.e. SSP, RA, CMP, ISCP, DRP, IRP and PIA) for over

1200 systems and facilities ? Collected and evaluated assessment artifacts in order to determine compliance with the NIST SP 800-53 rev 4 control requirements ? Participated in the FIPS 199 process in which security categorization takes place, and selecting the technical, operational and managerial controls using NIST SP 800-60 guidelines. ? Developed POA&M (Plan of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation) Education Bachelors of Science in Psychology University of MD Baltimore County - Baltimore, MD 2012 Associates of Arts in General Studies Montgomery College - Germantown, MD 2008 to 2010 Skills Hipaa (5 years), Life cycle (5 years), Risk assessment (5 years), Scanning (5 years), Security (5 years), Systems development (5 years), Vulnerability assessment. (5 years) Certifications/Licenses CAP Present

Name: Robert Morrison

Email: vparsons@example.net

Phone: (284)571-2732