Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Top Group Technologies An exceptional and detail-oriented Information Security professional with over seven (7+) years of experience in Risk Management and Cyber Threat Intelligence Analysis with great skills in the Information Assurance, Risk Assessor & Cyber Security subject matter. Expert in IT security governance implementing standards, policies, guidelines and best practices, create and generate reports for KPIs. Experience in utilizing automated security compliance tools. Experience with Certification & Accreditation, FIPS, FISMA and NIST using Cybersecurity, Risk Management Framework, FedRAMP, NIST Family of Security Control, POA&M, Contingency Planning, Incident Response, utilizing cyber security tools and configuration using security software tools on systems network. Knowledgeable in implementing IPS/IDS (Metasploit, Snort, Burp Suite), Nessus, Nmap, Wireshark, SIEM tools such as ArcSight, SPLUNK, as well as development of custom IDS signatures and SIEM use cases. WORK AUTHORIZATION STATUS U.S. Citizen Work Experience Cyber Security Analyst Top Group Technologies - Largo, MD April 2014 to Present Knowledge of Risk Management Framework (RMF) using NIST SP 800-37 as a guide in Categorizing a system, conduct a kick off meeting to Categorize a system according to NIST requirement of Confidentiality, Integrity & Availability (Low, Moderate, or High), and security baseline controls. Excellent verbal/written communication skill. Proficient in updating and reviewing A&A package which includes SSP, PII, PIA, PTA, by working closely with (ISSO) Information System Security Officer. Assist in the development of an Information Security and continuous monitoring in the company. Review SAR Post Assessment, create and completed POA&M remediation and preparing and reporting SSP, PTA, PIA, and ST&E. Work with ISSO and security team to Assess Security Controls in updating SAP, Rules of Engagement (ROE). Participate in security team meetings and rendered other support to IT Security office, which included ensuring appropriate steps are taken to implement information security requirements for all IT systems. Additional responsibilities include assurance of vulnerability mitigation, training on C&A tool Adhere to client security standards and industry best practices. Perform Categorization and classification of a system using NIST SP 800-60 VOL 1 and FIPS 199 as my guide base on the (CIA Triad)

Confidentiality, integrity and Availability of the system policy and procedure. Conduct Security Assessment interviews to determine the STE Security Test Evaluation. Work with my system engineer in implementing controls. Involve in reviewing, maintaining and ensuring all Assessment and Authorization process. Assist in the development of rules of engagement document to facilitate the scanning of Agency network and vulnerabilities. Establish an E-authentication report to provide technical guidance in implementation of electronic authentication. IT Security Analyst Pinnacle Solutions January 2012 to March 2014 Developed System Security Plan SSP to provide an overview of system requirements. Ensured that Security Authorization Package such as SSP, POA&M and SAR Security Assessment Reports are maintained, reviewed and updated in accordance with the guideline. 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. Assisted Senior Information Security Officer in the conduct of Information Security Assurance roles and ensuring system safety. Conducted time to time risk assessment and reviewed controls for any deficiencies, and the deficiencies where reported to the ISSO for complete mitigation actions. Involved in drafting Contingency Plan recommendations for system owners. Checked events logs for irregularities, identified regularities are then reported as incidents. Contributed in weekly changes, management meetings to evaluate changes. Performed cyber security risk and regulatory compliance assessments. Provided technical and operational leadership for cyber- security incident response Implemented IT security process using Risk Management Framework NIST 800-37, Certification & Accreditation, and Assessment & Authorization document from categorization of information system to monitoring security control Designed a Performance and security monitoring system, risk assessment report, incident response, vulnerability assessment and risk mitigation Education BS in Computer Science University of Maryland Skills Aws (Less than 1 year), Risk management (7 years), Sap (4 years), Security (7 years), Trading (7 years), Cyber Security, Information Security, Siem, Information Assurance, Comptia Additional Information AREAS OF EXPERTISE Superior ability to support and develop data analysis solutions, data transformations and reporting solutions Experience with

Cloud Platform AWS, Azure, Salesforce, Google drive, and Microsoft OneDrive Knowledge of the System & Software Development Life Cycle (SDLC), Risk Management Framework (RMF) Great skill sets such as Written, Verbal, Oral Communication, Interpersonal & Problem-Solving, Software Agile Methodologies, Security Assessment & Authorization (A&A) Involve with FISMA Compliance, Security Control Assessment (SCA); FIPS 199 and FIPS 200, SSP, Security Assessment Plan; Plan of Action and Milestones (POA&M) & ATO Packages (SAP), Security Assessment Report

Name: Phillip Davis

Email: sullivanderek@example.net

Phone: 675-766-1280