Cyber security Analyst Cyber security Analyst Cyber security Analyst - Top Group Technologies Lanham, MD I have 5 years of experience as an Information Security Analyst, I am knowledgeable in Risk Management Framework (RMF), Security Life Cycle, Systems Development Life Cycle (SDLC), and vulnerabilities management using FISMA, and applicable NIST standards. Tools/Skills Nessus, Snort, Web Inspect, App Scan, Metasploit Authorized to work in the US for any employer Work Experience Cyber security Analyst Top Group Technologies June 2015 to Present Perform vulnerability assessment, ensuring risks are assessed and appropriate actions are taken to mitigate or resolve each. Conduct IT controls risk assessments including reviewing organizational policies, standards and procedures, as well as providing advice on their adequacy, accuracy and compliance with industry standards. Ensure all Security Authorization documentation for assigned systems remains accurate and up to date on a continuous basis, including, but not limited to, accurate and valid lists of assets (hardware/software), accurate boundary diagrams, accurate ports and protocols, etc. Compile, write, update, finalize, produce, and support activities for IT Security Common Control Catalogs and related documentation including, but not limited to, Security Plans or other documents required. Compile, write, update, finalize, and produce all FISMA documentation and associated artifacts as required by Client in a manner compliant with all Federal security requirements and policies. Ascertain all FISMA documents are updated within 6 months of a new policy release. Manage the Interconnection Security Agreements for all systems, including creation, tracking, and vetting. Review all ISSO provided documentation for accuracy and relevancy, provide follow-up to ISSOs to ensure documents are properly completed. Prepare Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. IT Security Specialist Smart Tech Inc January 2013 to June 2015 Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, Security Test and Evaluations (ST&Es), Risk Assessments (RAs), Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Plan of Action and Milestones (POAMs). Prepared Security Assessment and Authorization (SA&A) packages to

ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. Performed vulnerability assessment, making sure risks are assessed and proper, actions taken to mitigate them. Conduct IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. Conducted the IT Risk Assessment and documented key controls. Develop, review and evaluate Security Plan based on NIST Special Publications 800-18 Investigates possible security breaches identified through review of audit reports and follows up accordingly with departments / management Prepared and reviewed C&A package for Information Systems. Education Nursing RN associates Prince George's Community College Skills Cissp, Cyber Security, Nist, Siem, Information Security Certifications/Licenses Security + Present CAP Present

Name: Shelley Ferguson

Email: angela63@example.com

Phone: 446.510.4885x4000