Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - NCI Systems Bethesda, MD An organized and analytical Information Assurance professional with superior goal setting, decision-making, problem solving skills with a solid reputation for having positive impact on both internal and external support and overall productivity. Experienced in providing services as a security assessment and authorization analyst (SA&A) and perform as an integral part of the Assessment and Authorization process to include A&A, documentation, reporting, reviewing and analysis requirements in accordance with NIST, FISMA and organizational security standards. Work Experience Cyber Security Analyst NCI Systems - Marietta, GA November 2016 to Present Provide services as a security assessment and authorization analyst (SA&A Analyst) and perform Certification and Accreditation documentation in compliance with company standards. As a team we determined security Categorizations using the FIPS 199 as a guide, review, update and develop Privacy Impact Assessment (PIA), Privacy Threshold Analysis (PTA), System security plan (SSP) and System of Record Notice (SORN). Work with ISSO, AO and security team to assess security control selected and assess the weaknesses and produce a Security Test and Evaluation Report (ST&E) with all findings reported in our Security Assessment Report (SAR). Review and document Contingency Plans (CP), Privacy Impact Assessment (PIA), and Risk Assessment (RA) documents per NIST 800 guidelines. Experience in developing and updating System Security Plans (SSP), Contingency Plan, Disaster Recovery Plan, Incident Response Plans and Configuration Management Plan. Apply appropriate information security control for Federal Information System as specified by NIST 800-37, SP 800-53 rev4 and FIPS 199. Specialize in the entire FISMA Risk Management Framework (RMF), and system control assessment processes using NIST SP 800-60, NIST SP 800-53A, preparing and reporting SSP, SAP, PTA, PIA, E-Authentication ST&E, POA&M. Information Security Analyst InAlfa Systems - Acworth, GA May 2014 to September 2016 Analyzed and updated System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Analysis (PIA), System Security Test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M). Assisted System Owners and ISSOs in preparing system packages, ensuring that management, operational, and technical controls are implemented adequately as specified in NIST SP 800-53

Rev4. Ensured that risks are assessed, evaluated and proper actions are taken to limit their impact on the Data and Information Systems. Developed templates for required security A&A documents: including risk assessments, security plans, Security Assessment Plans and Reports, Contingency Plans, and Security Authorization Packages. Conducted IT controls risk assessments that included reviewing organizational policies/procedures and provided advice on their adequacy, accuracy and compliance. Involved in security awareness training program to educate employees and managers on current threat and vulnerabilities. Updated IT Security policies, procedures, standards and guidelines according to department and federal requirements. Reviewed SAR at post assessment, created and completed POA&M's milestones to remediate findings and vulnerabilities. FISMA/SA&A Analyst Anchorage Consulting LLC - Bowie, MD February 2013 to February 2014 Conducted kick-off meetings to collect system information and categorize system based on NIST SP 800-60. Conducted Security Control Assessments to assess the adequacy of management, operational, privacy and technical security controls implemented. Developed System Security Plans to provide overview of Federal Information System requirements and described the controls in place to meet those requirements. Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, Security Test and Evaluations (ST&Es), Risk Assessments (RA), Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, Plan of Action and Milestones (POA&Ms). Developed Risk Assessment Reports by identifying the threats and vulnerabilities and evaluating the likelihood that vulnerabilities can be exploited by assessing the impact level. IT Help Desk Atlanta Affordable Limousine - Roswell, GA January 2012 to August 2012 Performed remote troubleshooting through diagnostics techniques and pertinent question. Logged events, issues, and their resolutions. Installed, configured, and maintained PC hardware and operating systems. Diagnosed and resolved the root cause of hardware and software issues. Configured and reset the network access accounts when required.

Maintained daily performance of computer system. Education Bachelor of Science in Mechanical Engineering Lagos State University 2003 to 2009 compliance NIST Skills SECURITY, SHARE POINT, NESSUS, MS OFFICE, EXCEL Additional Information TECHNICAL SKILLS Software/

Hardware/Platform: Security Control Testing, System Monitoring, MS Office Suite (Power Point, Word, Share Point, Excel, Access), Nessus, Zap.

Name: Megan Mccormick

Email: jameslopez@example.org

Phone: 001-959-612-8681x4959