IT SECURITY ANALYST IT SECURITY ANALYST IT SECURITY ANALYST - PARAGONE SOLUTIONS I am a dedicated and passionate individual, with 8 years experience in Information Technology and 5 years of working as an IT SECURITY ANALYST, Privacy and Data, Security Management and Operation. I have acquired excellent practical skills in performance, implementation, development and also experienced in analyzing information requirements and delivering cost effective solution and diverse background including solid knowledge, security planning management, C&A package, A&A process and POA&M. FIPS, FISMA Security Content, NIST Family of Security Control, System Security Plan, Incident Response and Contingency Planning. Work Experience IT SECURITY ANALYST PARAGONE SOLUTIONS May 2016 to Present Environment: WINDOWS 2003- 2008, DATABASE, LINUX Responsibilities: I have also developed plan of action and milestones (POA&Ms), security vulnerabilities and mitigation strategies; and also develop security A&A artifacts, to include but not limited to, sensitivity assessments, SSP, POA&Ms, and ATO and SAR. I worked with ISSO and Security team to Access Security Controls selected, and assess the finding and the result be reflex on the (RTM) or Test case and all weakness noted be reported in our SAR report. I perform Continuous Monitoring of Security Controls by using NIST 800-137 as a guide by testing a portion one-third of the Applicable Security controls Annually and performing periodic and Testing Controls I provided services as security control assessors (SCAs) and perform as an integral part of the Assessments and Authorizations process to include A&A, documentation, reporting and analysis requirements. Knowledge of FISMA tracking systems/tools to implement six steps NIST RMF aim at managing, monitoring and tracking ATO, POA&M, continuous assessment and ongoing authorization. Experience developing and updating System Security Plans (SSP), Contingency Plans, Disaster Recovery Plans, Incident Response Plans and Configuration Management I experience developing knowledge of NIST, 137, 30, 34, 53, NIST 37 RMF and FISMA guidelines to comply with Federal agencies. Assisted in the development of the A&A Process and security decisions are taken based on Continuous Monitoring of the system. Review and update of the System Security Plan (SSP) using NIST SP 800-18 guidelines. I have knowledge of the entire RMF process and its

compliance using NIST publications and standards, Performed daily ongoing (A&A) Assessment and Authorization projects in support of I am specialized in the entire FISMA Risk Management Framework (RMF), SA&A/C&A and system control assessment processes using FIPS NIST SP 800-60, NIST SP 800-53r4/53A, preparing and reporting SSP, SAP, ST&E, POA&M. Develop resultant SCA documentation, including but not limited to the security Assessment Report (SAR). Develop and conduct ST&E (Security Test and Evaluation) according to NIST SP 800-53A and perform on-site security testing and reviewing vulnerability scan results. Document and Review security plans (SP), contingency plans (CP), privacy impact assessments (PIA), and risk assessment (RA) documents per NIST 800 guidelines for various agencies. Facilitate Security Control Assessment, perform internal audits of the systems prior to external auditing and Continues Monitoring Activities. I provide services as security control assessors (SCAs) and perform as an integral part of the Assessments and Authorizations process to include A&A documentation, reporting and analysis requirements IT SECURITY ANALYST SKYTECH CONSULTING July 2012 to May 2016 Environment: AIX, HPX, Windows 2000/2003; Oracle 10g, Risk Management Framework (RMF) Using NIST 800-37 as a guide, assessments and Continuous Monitoring: Performed RMF assessment. AS a security assessor, i conduct assessment meetings with various System Owners and Information System Security Officers (ISSO), providing guidance of evidence needed for security controls, and documenting findings of assessment. Security Documentation: Perform updates to System Security Plans (SSP) Using NIST 800-18 as a guide to develop SSP NIST 800-53, Risk Assessments, Incident Response Plans and draft, review, update Plans of Action and Milestones (POA&M). I have Developed and updated security artifacts such as the System Security Plan(SP), Contingency Plan (CP), Configuration Management (CM), Disaster Recovery plan (DRP), Privacy Impact Assessments (PIA) and Risk Assessment(RA) documents per NIST 800 guideline I demonstrated the knowledge of NIST Risk Management Framework (RMF), NIST and FISMA, and as a Security Controls Assessment and review Authorization and Assessments (A&A) to validate security controls effectiveness. I also performed a review and update of the plan of action and milestones (POA&Ms), security vulnerabilities and mitigation strategies; and also develop

security A&A artifacts, to include but not limited to, sensitivity assessments, SSP, POA&Ms, and ATO and SAR. I have experience with FISMA compliance and NIST security standards like to develop Certification and Accreditation documentation (NIST special publication), working very closely with the Information System Security Manager (ISSM) and the other members of the Information Assurance team. I Perform Security Privacy Threshold Analysis (PTA), Privacy Impact Assessment, E-Authentication with business owners and selected stakeholders. Assist the System Owners and ISSOs through Certification and Accreditation (C&A) Process, ensuring that Operational, management and technical control securing sensitive Security Systems are in place and being followed according to the Federal Guideline (NIST SP 800-137 RMF). I worked with ISSO and Security team to Access Security Controls selected, and assess the finding and the result be reflex on the (RTM) or Test case and all weakness noted be reported in our SAR report. I perform Continuous Monitoring of Security Controls by using NIST 800-137 as a guide by testing a portion one-third of the Applicable Security controls Annually and performing periodic Vulnerability Scanning and Testing Controls I reviewed, developed and updated some of the system categorization using FIPS 199, Initial Risk Assessment, E-authentication, PTA, PIA, SAR, SSP, SAP and POA&M. I provided services as security control assessors (SCAs) and perform as an integral part of the Assessments and Authorizations process to include A&A vulnerability scanning, documentation, reporting and analysis requirements. Education Bachelors In Cyber Security UNIVERSITY OF BUEA September 2006 to December 2009 CCNA University Of Buea Skills Active Directory, security, testing, Microsoft Office

Name: Jonathan Espinoza II

Email: toddgonzalez@example.org

Phone: +1-450-442-9876x833