IT Security Analyst IT Security Analyst IT Security Analyst Laurel, MD Information system and IT security analyst with 7 years experience in Information Systems Development Security Life Cycle and the use of NIST Risk Management Framework (RMF) as a methodology to manage the security of information systems. Adept and proficient in Security assessment and Authorization including threat analysis, Nessus vulnerability scanning, Security Assessment Reports creation and reviews, PO&AMs, SANS Framework, IT system Audits and FISMA. Work Experience IT Security Analyst COLA INC - Columbia, MD June 2016 to July 2019 Develop, review and update Information Security System policy documents, System Security Plan (SSP), and Security Assessment Plan (SAP), Security Requirement Traceability Matrix (SRTM), Security Assessment Report (SAR), Security Impact Assessment (SIA), Risk Assessment Report (RAR) and other Security Package artifacts Update Systems Security Plans, as changes are implemented in the system through established configuration management policies Audited networks and security systems to identify vulnerabilities Verified completeness of SSP Implementations statements using NIST SP 800-18 and NIST SP 800-53, access security controls using NIST 800-53A to determine the extent to which controls are implemented correctly, and operating as intended Performed a review of existing procedures and updated when appropriate to determine the internal control measures and ensure its strict implementation Reviewed user accounts and access on a monthly basis to ensure regulatory and corporate compliance Monitor systems security controls after authorization to ensure continuous compliance with the security requirements Conduct FISMA-based security risk assessments for various government contracting organizations SECURITY ANALYST BRIGHT SEAT HEALTH - Temple Hills, MD January 2015 to June 2016 Provided security support and evaluation to development teams in order to integrate information assurance/ security throughout the System Life Cycle Development of major and minor application releases Analyzed system risk to identify and implement appropriate security countermeasures Applied appropriate information security controls for Federal Information Systems based on NIST 800 Series, 800-37 REV.1, SP 800-53 REV.4, FIPS 199 and FIPS 200 Perform information security risk assessments and assist with the internal auditing of information security processes Tests, assess, and document security

control effectiveness Collect evidence, interview personnel, and examine records to evaluate effectiveness of controls Created reports detailing the identified vulnerabilities and the steps taken to remediate them Provided technical support in the areas of vulnerability assessment, risk assessment, and security implementation Installed and configured antivirus software on desktop and notebooks Updated virus protection systems based on computer virus reports Responded to user requests for system and applications issues Utilized Remote Desktop to solve user-oriented problems JOHNS HOPKINS UNIVERSITY May 2014 to January 2015 SECURITY ANAYLST Conducted system security assessments using security controls relating to cyber security and training (NIST 800 series, FISMA, and FIPS 199 and 200) Monitored network activities to identify and effectively respond to security threats and incidents using logs and various tools Supported in certification and accreditation (C&A), conducting cyber assessments, and incident response (using hardware and software): setup and customized interfaces for analysis Analyzed user's requirements, concept of operations documents, and high-level system architectures to develop system requirements specifications Guided system development and implementation planning through assessment or preparation of system engineering management plans and system integration and test plans IT AUDITOR AUXANO LOGISTICS LLC March 2012 to May 2014 Prepared audit scope, reported findings, and presented recommendations for improving data integrity and operations Performed routine audits to determine compliance with laws, rules and regulations Reviewed systems and application strengths and weaknesses as well as and recommended appropriate compensatory controls to mitigate against any potential risk Determined and detailed gaps in process, procedure and system controls Coordinated with various department to create remediation plans for deficiencies found during audit Advised on the requirements, liabilities, and penalties of compliance and noncompliance, and recommend improved accounting or management operation systems controls Education Graduate Certificate in Information Assurance in Information Assurance University of Maryland - Adelphi, MD 2017 Master of Science University of Maryland - Adelphi, MD 2016 Skills Security, Information security, Nessus, Configuration management, Risk assessment

Name: John Adkins

Email: thomasconrad@example.net

Phone: 001-809-773-8946x215