Information Assurance Analyst Information Assurance Analyst Information Assurance Analyst - THE ARC Dumfries, VA Work Experience Information Assurance Analyst THE ARC July 2016 to Present

Assist proper system categorization using NIST 800-60 and FIPS 199; implement appropriate security controls for information system based on NIST 800-53 rev 4 and FIPS 200. Work with system owners to develop, test, and train on contingency plans and incident response plans. Work with the ISSO to perform continuous monitoring on information stems in accordance with NIST 800-137 to maintain ongoing ATO and also assist in the initial remediation action of failed security controls Reviewed vulnerability reports and submitted Plans of Action and Milestones (POA&Ms) for certification and accreditation packages Provided weekly metrics and reports on the effectiveness of the A&A process. Responsible for reviewing and finalizing Security Control Assessment Report (SAR) Developed and maintain, throughout the lifecycle of the system, network and application documentation and assisted with the production and maintenance of their supporting A&A documentation and artifacts Developed, reviewed, and assessed Security Assessment and Authorization (A&A) security documentation. Tests, assess, and document security control effectiveness. Collect evidence, interview personnel, and examine records to evaluate effectiveness of controls. Review and update remediation on plan of action and milestones (POA&Ms), in organization's cyber security and management (CSAM) system. Work with system administrators to resolve POA&Ms, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M. Conduct security assessment interviews to determine the security posture of the System and to Develop a security Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. Reviewing, maintaining, and ensuring all assessment and A&A) documentation is included in the system security package. Ensure vulnerabilities and risks are efficiently mitigated in accordance with the organization monitoring plan. Collaborate with ISSO colleagues on the planning and implementation of enhancements to the system's risk management processes. Information Security Analyst Manav

Consulting Inc May 2013 to August 2016 Participate in the system authorization process by working with the key stakeholders to create complete and accurate Risk Management Framework (RMF) packages. Led in the development of Privacy Threshold Analysis (PTA) and Privacy Impact Analysis (PIA)by using NIST privacy handbook, and also working closely with the Information System Officers (ISSO's) the System Owners (SO) and the information owners (IO). Conducts Security Test and Evaluation (ST&E) using NIST 800 53A. Rev 4 and develop supporting documentation to the result based on security control requirement. Support Security Assessment and Authorization (SA&A) activities, by preparing the complete ATO package for the authorization official to make accreditation decision. Review and Updates System Security Plans using the NIST 800-18 as a guide. Collect, review, and update, and maintain IT Supporting artifacts. Perform Security Assessment of the Federal systems and applications by NIST 800-54A Rev4 as guidance for current federal directives and policies. Ensure that system documents are created for POA&Ms and approved by ISD no less than 60 days prior to POA&M expiration. Provide reporting on POA&M remediation for all systems upon request by the Federal Government using the XACTA tool as repository for all POAM documents. Scheduled, tracked and managed quarterly POA&M review processes by coordinating meetings and tasking System Owners and support remediation of open items. Assisted in ensuring that vulnerabilities identified in the Plan of Action and Milestones (POA&M) database are addressed in a timely manner by working with system owners and managers Conducted IA vulnerability assessments as required for the Security Test & Evaluation for validation of secure configuration and as evidence to request ATO. IT Support AIRTEL GHANA LIMITED October 2012 to April 2013 Perform data backups and disaster recovery operations. Maintain and administer computer networks and related computing environments, including computer hardware, system software applications software and all configurations Plan, coordinate and implement network security measures in order to protect data & hardware. Operate master consoles in order to monitor the performance of computer systems and network. Perform routine network startup and shutdown procedures, and maintain control records. Monitor network performance in order to determine whether adjustments need to be made and to determine where

changes needs to be made in future. Analyze equipment performance records to determine the need for repair or replacement. Maintain logs related to network functions, as well as maintenance/repair records. Ensured the Contingency Plan Test was done annually. Education Bachelor of Science University of Professional Studies Certifications/Licenses A valid IT Specialist certification

Name: Christina Larson

Email: pricepatricia@example.com

Phone: 001-292-766-4372x573