Sr Security Specialist Sr Security Specialist Sr Security Specialist - Nautiquos Business Solutikns Inc Aurora, CO Seeking an Information Assurance and Compliance position in a growth oriented organization with focus on RMF, NIST, HIPPA, HI-TRUST, ISO 270001 and PCI-DSS Standards, system certification & accreditation, testing internal IT controls, system monitoring and vulnerability management. SKILLS: A&A artifact, System Categorization, Controls Selection and Implementation, Risk Assessment, Monitoring Compliance, Contingency Planning, Incident Response, Disaster Recovery Plan, POA&M Management, Vulnerability Management, FISMA, NIST SP 800-60, SP 800-53 Rev 3& Rev 4, SP 800-53A, SP 800-37, SP 800-137, SP 800-18, SP 800-34, FIPS 199 and FIPS 200. Work Experience Sr Security Specialist Nautiquos Business Solutikns Inc June 2017 to Present Creating and updating the following documents: Risk Assessment Report, E-Authentication, Security Assessment Plan, System Security Plan, Contingency Plan, Contingency Plan Test, Security Assessment Report, Plan of Action and Milestone (POA&M). Monitoring compliance with information security policies by coaching others within the organization on acceptable uses of information technology and how to protect organization systems. Working with engineers and developers to incorporate the best security safeguard and practice on both production and Test &Development Lab (TDL) systems. Assisted System Owner by coordinating the certification and accreditation process of the General Support Systems for field sites and telecommunications. Generated, reviewed and updated the Systems Security Plan (SSP) in accordance with NIST SP 800-53; as well as all security documentations required for the certification and accreditation, and took the system through full accreditation Assessed system security controls using 800-53A. Identified security risks, threats and vulnerabilities of networks/systems/applications. Reviewed and updated E-Authentication and Privacy Threshold Analysis (PTA). Developing POA&M (Plan of Action & Milestones) document to take corrective actions resulting from Security Assessment of systems controls. Preparing and presenting briefings to senior management officials on Information Assurance/Information Security principles to manage risks. Coordinating internal compliance review and monitor activities for Network Operations, including periodic reviews of departments within the Network Operations functional unit

and collaborate with Internal Audit. Reviewing system audit log events and identifying any suspicious activities. Security Analyst Douala IT - Baltimore, MD September 2013 to May 2017 Develop, review and update Information Security System Policies, System Security Plans (SSP), and Security baselines in accordance with NIST, FISMA and industry best security practices Categorize system and identify security objectives by applying appropriate information security control for Federal Information System based on NIST SP 800-60, SP 800-53, FIPS 199, FIPS 200, and OMB A-130 Appendix III. Prepare and review Authorization to Operate (ATO) packages (i.e. SSP, RA, CMP, ISCP, DRP, IRP and PIA) for systems and facilities using NIST publications. Assist POA&M teams to remediate vulnerabilities of various entities for low, moderate and high impact systems. Monitored controls post authorization to ensure continuous compliance with security requirements. Formulate security assessment reports and recommendations for mitigating vulnerabilities and exploits in the system. Perform the Assessment & Accreditation (A&A) on General Support Systems (GSS), Major Applications and Systems to ensure that such environments are operating within strong security posture. Perform Security Assessments to determine if controls are implemented correctly, operating as normal and meeting desired objectives. Create ATO package documents; SSP, RA, SAR, POAM reports, etc., based on the security assessments performed on systems. Perform the role of Security Control Assessor by reviewing the artifacts and implementations statements provided by the ISSO on a system to determine if the security controls are yielding the desired result. Update the controls changes from NIST-800 53 Rev3 to NIST-800 53 Rev4 and control assessment changes from NIST-800 53A to NIST 53A rev4. Performed ongoing security control Assessments Network System Administrator Ghana Atomic Energy Commission - Accra, GH March 2010 to August 2013 Ghana Diagnosed hardware and software problems, and replace defective components. Performed data backups and disaster recovery operations. Maintained and administer computer networks and related computing environments, including computer hardware, systems software, applications software, and all configurations. Planned, coordinated, and implemented network security measures in order to protect data, software, and hardware. Performed routine network startup and shutdown

procedures, and maintain control records. Designed, configured, and tested computer hardware, networking software and operating system software. Recommended changes to improve systems and network configurations, and determine hardware or software requirements related to such changes. Monitored network performance in order to determine whether adjustments need to be made, and to determine where changes will need to be made in the future. Analyzed equipment performance records in order to determine the need for repair or replacement. Maintained logs related to network functions, as well as maintenance and repair records. IT Support Airtel Ghana Limited - Accra, GH December 2003 to March 2010 Ghana Performed data backups and disaster recovery operations. Maintained and administered computer networks and related computing environments, including computer hardware, systems software, applications software, and all configurations. Planned, coordinated, and implemented network security measures in order to protect data & hardware. Operated master consoles in order to monitor the performance of computer systems and networks, and to coordinate computer network access and use. Performed routine network startup and shutdown procedures, and maintain control records. Conferred with network users about how to solve existing system problems. Monitored network performance in order to determine whether adjustments need to be made, and to determine where changes will need to be made in the future. Analyzed equipment performance records to determine the need for repair or replacement. Maintained logs related to network functions, as well as maintenance/repair records. Education Bachelor of Science in Information Technology in Information Technology University of Cape Coast May 2003

Name: Ryan Yates

Email: michael95@example.com

Phone: 894-344-9026x03745