IT Security Analyst IT Security Analyst IT Security Analyst - Ladatech Inc Mitchellville, MD IT Controls - Frameworks - IT Security Standards: (SAR) Security Assessment Reports, Certification and Accreditation, Vulnerability Scans, Project Management, Risk Assessment, Change Management, Configuration Management, Security Maintenance, Contingency Planning; Policies and Procedures, Implementation, Incident Response, Media Protection, Physical Security, Computer Operations, Environmental Security, Personnel Security, PCI DSS compliance, ISO, Sans-20 Critical Security Controls standards, NIST 800-53, DIACAP, FISMA, NIST RMF frameworks. Software /Hardware /Platform: Mainframes RACF; UNIX; Sun Solaris; and Linux, SQL Server, VMware, Windows, SAP, LAN/WAN, Wireless Network, Remedy, Office suite: PowerPoint, Word, SharePoint, Excel, Access, Nessus, Webinspect. Work Experience IT Security Analyst Ladatech Inc August 2011 to Present Perform compliance reviews, tracking, and continuous monitoring of C&A packages.   Advise and assist with the Lifecycle Certification and Accreditation (C&A) process and developing System Security Plan (SSP).   Maintain a document repository where C&A project documentation is stored.   Work closely with developers to identify the appropriate certification/approval processes and authorities.   Record/register actions concerning project approvals to operate in the C&A database.   Read and analyze SSPs and develop understanding of systems and applications into security test plans.   Ensure POA&M actions are completed and tested in timely fashion to meet client deadlines.   Develop risk assessment reports.
   Participate in the FIPS 199 process using SP 800-60   Assemble and submit C&A packages to Principal Accreditation Authority/Designated Accreditation Authority.   Assist with analyzing, developing, implementing, integrating, and maintaining secure Agency IT solutions.   Document and finalize Security Assessment Report (SAR).   Develop and conduct security tests and evaluations based on NIST 800-53/53A.   Ensure Contingency Plan Test is performed annually.   Auditing compliance of security plans based on the National Institute of Standards and Technology (NIST) Security Publications.   Review E-Authentication risk assessment, privacy threshold analysis (PTA), Privacy Impact Assessment (PIA), perform vulnerability scanning and develop IT Security policies and procedures   Meridian LLC, Washington DC Helpdesk IT   Provided customer service to

resolve computer issues.   Maintained records of daily business transactions, problems and remedial actions   Used Web based ticketing System to transmit client request to senior technical team.   Installed wireless networks for small businesses and client   Antivirus installation. Scanning PCs using antivirus software Symantec, MacAfee and Web root   Ensured that client's computers have access to servers and other Network resources   Updated and documented Helpdesk tickets with Remedy ticket system.   Performed computer systems repairs and services.   Performed Operating System upgrades   Configuration and troubleshooting of mobile devices   Familiarity with network systems such as servers, switches, firewalls and routers.   Troubleshoot desktop applications issues while maintaining excellent customer service. Education High School Diploma in Certified Information System Security Professional St Patrick's High School 1997 BS in Sociology University of Ibadan Additional Information Computer Skills: Microsoft Office Suite, Microsoft Visio, SharePoint, PeopleSoft, Mainframes RACF; UNIX; Sun Solaris; and Linux, SQL Server, VMware, Windows, SAP, LAN/WAN, Wireless Network, Remedy, ESRI, Nessus, WebInspect, Fluke Network Analyzer.

Name: Sarah Wallace

Email: tsanchez@example.org

Phone: (427)217-9836