Senior IT Security Analyst Senior IT Security Analyst Senior IT Security Analyst - Aspect Security, Inc Fort Washington, MD Work Experience Senior IT Security Analyst Aspect Security, Inc - Columbia, MD May 2017 to Present   Analyze and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M)   Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60   Conduct interviews with selected personnel, document and evaluate business processes, and execute audit test programs to determine the adequacy and effectiveness of internal controls and compliance with regulations   Project Lead in a team of 7, direct and train junior team members on auditing techniques and software   Assist System Owners and ISSO in preparing C&A package for companies' IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4   Conduct cloud system assessments, primarily with AWS (Amazon Web Services) by utilizing FedRAMP and NIST guidelines   Assist the SOC team in documenting and reporting vulnerabilities by utilizing tools such as Splunk and SNORT.   Evaluate the effectiveness of internal control systems and identify areas of improvement, best practices, and lessons learned   Conduct Self-Annual Assessment based on NIST SP 800-53A   Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs).

   Review and analyze Nessus Vulnerability and Compliance scans, WebInspect scans, IBM Guardian, Burp Suite and DbProtect scans for possible remediation.   Assess systems of varying scope and complexity and comprised of various technologies.   Create standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages   Provide weekly status reports on ongoing tasks and deliverables IT security specialist Compass Cybersecurity - Baltimore, MD May 2015 to Present   Supports the Security Assessment and Authorization process of the clients' systems as a Security Analyst   Conducted scan analysis Reviewed technical security controls and provide implementation responses to meet requirements Reviewing and confirming configurations and policies utilized prior to Nessus scans being

conducted.   Meet with client to discuss findings and process of remediation   Experience in cloud system assessments, primarily with AWS (Amazon Web Services) by utilizing FedRAMP and NIST guidelines   Experience in executing Step 4 (Security Assessment) of the NIST Risk Management Framework (RMF).   Experience in developing and disseminating Security Assessment Plans.   Experience in interpreting and evaluating implementations of NIST 800-53 rev 4 security controls.   Documenting findings within Requirements Traceability Matrixes (RTMs) and Security Assessment Reports (SARs).   Experience reviewing and interpreting Nessus Vulnerability and Compliance scans, WebInspect scans, IBM Guardian, Burpsuite and DbProtect scans   Ability to execute Security Assessments and develop and deliver supporting documentation within aggressive timelines.   Assessing systems of varying scope and complexity and comprised of various technologies. IT Security Analyst Redowl, Inc - Baltimore, MD June 2015 to May 2017   Conducted Certification and Accreditation (C&A) on major applications following the Risk Management Framework (RMF) from Categorization through Continuous Monitoring using the various NIST Special Publications in order to meet the necessary Federal Information Security Management Act (FISMA).   Developed System Security Plan (SSP), Security Assessment Report (SAR) and POA&Ms that are presented to the Designated Approving Authority (DAA) in order to obtain the authority to operate (ATO).   Conducted security assessments on major applications, updated POA&Ms with findings and monitored for remediation deadlines.   Work on System Interconnection Agreements   Provide weekly status reports on ongoing tasks and deliverables Junior IT Security Analyst Saint corporation - Bethesda, MD February 2012 to June 2015   Developed, reviewed and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices.   Performed vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple asset across the enterprise network.   Updated IT security policies, procedures, standards, and guidelines per the respective department and federal requirements.   Performed risk assessments, reviewed and updated, Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Management Plans (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other

tasks and specific security documentation. (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls).   Monitored controls post authorization to ensure constant compliance with the security requirements. Diplomatic Security Officer/ Intern Inter-Con Security Systems - Arlington, VA January 2009 to February 2012   Worked in a SOC environment and assisted with report writing and monitored network   Worked with network security (network administrator policies and procedures, firewalls, etc.   Policy writing and understanding of NIST publication   Interned as an IT security analyst as well as worked with different SIEM tools at the Department of State where I provide a safe and secure environment for the conduct of U.S. Foreign Policy   Ensure the safety of, and protect the Secretary of State and high-ranking foreign dignitaries and officials that visit the United States   Investigate Passports, visa fraud, and conduct personnel security investigations   As a member of DS, I ensure that America can conduct diplomacy safely and securely   As a member of DS, I help protect U.S. Embassies, secure critical information systems and fight war on terror Apply security policy, procedures, and practices in conjunction with federal statutes and authorities to physical and technical security of overseas projects in high-threat environments   Applied in-depth knowledge of security policies   Received training on how to implement systems to counter dynamic and fluctuate threat levels in areas such as terrorism, civil disorder, violence, and espionage.   Coordinate with DS officers to ensure timely coverage of posts   Recommends improvements to current physical and technical security systems   Maintains inventory of security equipment Education Bachelor's Degree in Criminal Justice Greensboro College - Greensboro, NC May 2010 Skills NESSUS (6 years), LINUX, MYSQL, PROBLEM SOLVING, TRAINING (3 years) Additional Information PROFESSIONAL SKILLS   Proficient in Microsoft Suite   Experience in MYSQL   Complex Problem Solving   Research & Analysis   Interpersonal & Teamwork Lifesaver Certified   Leadership & Training   Nessus   WebInspect   Kali Linux

Name: Angela Lawrence

Email: sandra54@example.com

Phone: (604)961-0929x8007