IT Security Analyst IT Security Analyst IT Security Analyst Washington, DC * Risk Management Framework * NIST 800-53a rev4 * FIPS 199/200 * FedRAMP * Nessus * Splunk * Security Assessment Report (SAR) * Security Assessment Plan (SAP) * Microsoft office * Detail oriented Work Experience IT Security Analyst Skyline Technologies October 2016 to Present * 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, help review and update, Plans of Action and Milestones (POA&M), Security Control Assessments. * (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 * Conduct 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 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 Analyst Security Assessment and Authorization May 2014 to October 2016 * Supported the Security Assessment and Authorization process of the clients' systems as a Security Analyst * 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. * Helped with updating IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. * Performed risk assessments to identify the risk level associated with the findings * (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 * Reviewed artifacts regarding Plans of Action and Milestones (POA&M) created by ISSO before closing * Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). * Review and analyze Nessus Vulnerability and Compliance scans for possible remediation. * Assess systems of varying scope and complexity and comprised of various technologies. * Provide weekly status reports on ongoing tasks and deliverables Junior IT Security Analyst XO communications, L.L.C October 2012 to May 2014 * Assisted in conducting cloud system assessments * Helped in updating IT security policies, procedures, standards and guidelines according to department and federal requirements * Support Cyber Security analyst in conducting Vulnerability Management, Security Engineering, Certification and Accreditation, and Computer Network Defense. * Perform risk assessments, update and review System Security Plans (SSP) using NIST 800-18 (Guide for Developing Security Plans for federal information systems) Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration * Responsible for conducting analysis of security incidents. Perform investigations of unauthorized disclosure of PII. Responsible for reporting findings and provide status to senior leadership. Perform escalations to Regional Computer Emergency Response Team (RCERT) when required. * Perform vulnerabilities scan and monitor continuously using NIST 800-137 as a guide with the aid of Nessus Alarm monitor/ Entry level SOC analyst Washington Metropolitan Area Transit Authority September 2009 to October 2012 * Worked in a SOC environment, where I assisted in documenting and reporting vulnerabilities (Tier 1). * Assisted the SOC team in documenting and reporting vulnerabilities by utilizing tools such as Splunk and SNORT. * Monitor personnel or equipment locations and utilization to coordinate service and schedules. * Record facts to prepare reports that document incidents and activities. * Relay complaint and emergency-request information to appropriate agency dispatchers. * Question callers to determine their locations, and the nature of their problems to determine type of response needed.

* Receive incoming telephone or alarm system calls regarding emergency and non-emergency police and fire service, emergency ambulance service, information and after hours calls for departments within a city. * Determine response requirements and relative priorities of situations, and dispatch units in accordance with established procedures. Education High school or equivalent Skills Word, Security, Customer Service, Organizational Skills, Stocking, Microsoft Office (10+ years)

Name: Jacob Branch

Email: mcleanrobert@example.net

Phone: +1-681-465-4132x9769