IT Security Analyst IT Security Analyst IT Security Analyst - CyberVision Technologies, LLC Hagerstown, MD Authorized to work in the US for any employer Work Experience IT Security Analyst CyberVision Technologies, LLC - Bronx, NY April 2016 to Present IT Security Analyst Analyse 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) * Assist System Owners and ISSO in preparing certification and Accreditation package for IT systems, to ensure management, operational and technical security controls are adhered to. * Utilizing NIST SP 800-53 Revision 4 and NIST SP 800-53A Revision 4 and conducting security control assessments * Perform Vulnerability Assessment. Make sure that risks are assessed, evaluated and proper actions have been taken to limit their impact on the Information and Information Systems * Created 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 Compliance Testing Analyst Grant Thornton (Chicago) - Chicago, IL March 2015 to March 2016 Compliance Testing Analyst, * Perform IT risk assessment and document the system security key controls * Design and Conduct walkthroughs, formulate test plans, test results and develop remediation plans for each area of the testing * Wrote audit reports for distribution to management and senior management documenting the results of the audit * Develop a Business Continuity Plan and relationship with outsourced vendors Perform Information Technology Risk analysis and assessments * Analyze and define Security Requirements for a variety of IT issues. * Develop, analyze and implement security specifications in line with NIST, FISMA. * Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53 rev3, FIPS 199, FIPS 200 and OMB 130 Appendix III IT Compliance Analyst State of Maine May 2013 to February 2015 * Developed, reviewed and updated Information Security System Policies, System Security Plans and Security baseline in accordance with NIST, FISMA, and OMB App. * Established schedules and deadlines for assessment activities. * Prepared and submitted Security Assessment Plan (SAP) to CISO for approval. * Conducted Security Assessment using NIST 800-53A * Developed and

conducted Contingency Plan and Test * Developed and updated system security plan (SSP), plan of action and milestone (POA&M). * Continuous monitoring and assessment for compliance. * Created reports detailing the identified vulnerabilities and the step taken to remediate them. Education Bachelor's in Sociology and Social Work University of Science and Technology August 2008 to February 2011 St. Joseph's College of Education (University of Cape Coast) 2002 to 2005 Skills Cobit, Disaster recovery, Hipaa, Ids, Information security, Ips, Iso, Iso 27001, Itil, Nist, Saas, Fisma, Health insurance portability and accountability act, Incident response, Network security, Sap, Systems management, Database, Cyber security Certifications/Licenses CompTIA Security+ Present Additional Information Summary of Skills and Accomplishments Experienced in governance, risk, and compliance management. Experienced in Risk Management Frameworks (RMF) processes and compliance using NIST publications and standards, FedRAMP and Cloud services - SaaS, PaaS, and IaaS. Experienced in UTM, IDS/IPS tools of different kinds to ensure effective system security compliance. Compliance/Policy and Procedure scripting and cross-referencing using ERM/COSO/COBIT procedures as well as ISO 27001:2013 standards. Experienced in the implementation of ISO 27001 controls to achieve ISO 27001:2013 certification. Also takes responsibility in the writing and documentation of guide wire policies and procedures with audit evidence for compliance in preparation of certification audit. Responsible for the implementation of Information Security Management System (ISMS). Experienced in system classification and categorization using the RMF processes to ensure system CIA. This ensures compliant security control selections and implementation for continuous system protection. Skilled in FIPS 199 based information security Risk Management Frameworks (RMFs) relating to regulatory and incident response and remediation actions. Some of these RMFs have been in the Federal Information Systems Management Act (FISMA), and the Health Information Technology for Economic and Clinical Health Act/Health Insurance Portability and Accountability Act (HITECH/HIPAA) sectors. Specialized in FISMA and the CIA of information and NIST SP 800-53 based information systems compliance standards with external auditing all my years of experience.

Specialized in areas of Information Technology (IT) such as Network Security, Cyber security,

Information Assurance (IA), Security Assessment & Authorization (SA&A), Risk Management, System Monitoring, Regulatory Compliance, Physical and Environmental Security, Incident Response, and Disaster Recovery. Skilled in analytical and organizational skills as well as familiarity with a wide variety of applications, database, operating systems and network devices. Efficient, responsible and accountable, with demonstrated knowledge in information security artefacts. Strong verbal and written communication skills. Fast learner and highly adaptive with ability to multi-task whilst working with little or no supervision. Great report writing skills for risk assessment recommendation documents such as SSP, RAR, SAP, ST&E, PTA, PIA, and POA&M. Using IBM Qradar to analyse logs relating to Vulnerabilities, network devices, operating systems, applications etc. Standards and Frameworks Security Assessment & Authorization (SA&A), OMB Circular A-130 Appendix III, FIPS 199, NIST 800-53, NIST 800-60 rev I Vol II, NSA Guide COSO/COBIT, SAS-70/SSAE 16, ITIL, ISO 27001, Privacy Act of 1974, Gramm-Leach-Bliley Act (GLB), HITECH/HIPAA, DoD 8500.2, DITSCAP, DoD 8510.bb, DIACAP, FISMA, FISCAM, Security Content Automation Protocol (SCAP), the FedRAMP framework and Cloud services like SaaS, PaaS, and IaaS.

Name: Susan Brooks

Email: halldrew@example.net

Phone: 001-429-585-0193x16291