IT SECURITY ANALYST IT SECURITY ANALYST IT SECURITY ANALYST - VINDS INC Glenn Dale, MD Information Security Professional with over 6 years of experience in identifying, assessing and providing recommendations for mitigating organizational risk using NIST Special Publication 800-30, 800-37. Extremely skillful in preparing Authorization Package - SSP, SAR and POAM. Good Communication skills, analytical ability, strong judgement and the ability to work effectively with clients & IT Management & Staff. Functional areas of expertise include: Assessment and Authorization (A&A) Certification and Accreditation (C&A) IT Security Compliance Risk Assessment Vulnerability Assessment Systems Development Life Cycle Requirement Traceability Matrix (RTM) Project Management and Support Work Experience IT SECURITY ANALYST VINDS INC - Laurel, MD July 2013 to Present Provided security expertise and guidance in support of security assessments Supported A&A (C&A) activities according to the A&A project plan Reviewed authorization documentation for completeness and accuracy for compliance Facilitated Security Control Assessment (SCA) and Continuous Monitoring Activities Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4 Ensured cyber security policies are adhered to and that required controls are implemented Validated information system security plans to ensure NIST control requirements are met Developed resultant SCA documentation, including but not limited to the Security Assessment Report (SAR) Authored recommendations associated with findings on how to improve the customer's security posture in accordance with NIST controls Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies Updated and reviewed A&A Packages to include Core Docs, Policy & Procedures, Operations and Maintenance Artifacts, SSP, SAR, FIPS 200, FIPS 199, POA&M, CPT, PTA, PIA, and more Collected Operation and Maintenance artifacts on an ongoing basis so that Security Control Assessment (SCA) is seamless Uploaded supporting docs in the System's Artifact Libraries, Google Docs, and CSAM Updated, reviewed, and aligned SSP to the requirements in NIST 800-53, rev4; so that assessments can be done against the actual requirements and not ambiguous statements Managed vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single or multiple assets across

the enterprise network Reviewed SAR post assessment; created and completed POAM's milestones to remediate findings and vulnerabilities Independently reviewed complex security analysis of existing systems for compliance with security requirements Monitored security controls post authorization to ensure continuous compliance with the security requirements ADMIN COORDINATOR VMT HEALTH AGENCY - Washington, DC August 2011 to June 2013 Ensure proper system categorization using NIST 800-60 and FIPS 199; implement appropriate security controls for information system based on NIST 800-53 rev 4 and FIPS 200. Conduct security assessment interviews to determine the Security posture of the System and to Perform kick Off Meetings Apply appropriate information security control for Federal Information system based on NIST 800-37 Rev 1. Facilitate Security Control Assessment (SCA) and monitor activities. Develop a Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. Reviewing, maintaining, and ensuring all assessment and authorization (A&A) documentation is included in the system security package. Perform information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements. Work with system owners to develop, test, and train on contingency plans and incident response plans. Tests, assess, and document security control effectiveness. Collect evidence, interview personnel, and examine records to evaluate effectiveness of controls. Review and update remediation on plan of action and milestones (POA&Ms), in organization's CSAM Work with system administrators to resolve POA&Ms, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M. PRODUCTION IT SECURITY ANALYST BUCHANAN & MITCHELL November 2010 to August 2011 CPA, MD Developed, and evaluated information security governance policies, standards, and procedures Conducted security assessments through vulnerability testing and risk analysis Performed both internal and external security audits Analyzed security breaches to identify the root cause Verified the

security of third-party vendors and collaborated with them to meet security requirements EXECUTIVE ASSISTANT CATHOLIC CHARITIES - Washington, DC August 2007 to September 2010 Performed administrative and clerical duties Managed client database Created and oversee database for all on/off site staff and contractors Oversee database to track and monitor timely payments of services to contractors Monthly and timely generated client stipends to increasing client satisfaction Collaborated with care managers, and coordinated monthly trainings for clients Oversee the care and maintenance of organization's offsite and client residential facilities Scheduled repairs, maintenance, and all appropriate services, as required Education MSc. in Cyber security Policy and Management University of Maryland University College 2020 B.S. in HEALTH MANAGEMENT AND GERONTOLOGY University of Maryland University College 2016 BIOLOGY AND PSYCHOLOGY Southwest Minnesota State University 2002 to 2006 Skills Excel (10+ years), interviewing (8 years), Microsoft project (Less than 1 year), Microsoft sharepoint (7 years), Microsoft windows (10+ years), Ms project (Less than 1 year), Oracle (Less than 1 year), Powerpoint (10+ years), presentation skills (10+ years), Security (8 years), security policies (6 years), Sharepoint (5 years), Splunk (Less than 1 year), system security (7 years), Word (10+ years), Customer Service (10+ years), Typing (10+ years), Organizational Skills Certifications/Licenses Security+ Additional Information TECHNICAL SKILLS Microsoft Windows, Excel, Word, PowerPoint, MS Project, Oracle virtual box, CSAM, secure file solution, SharePoint, Splunk SKILLS - Ability to establish and maintain effective working relationships with clients and co-workers - Skills in interviewing users to help analyze and resolve issues - Strong organizational, analytical and planning skills - Ability to read and interpret system security policies, rules and regulations - Ability to communicate security and risk-related concepts to both non-technical and technical audiences - Strong communication (verbal & written) and presentation skills

Name: Angela Ryan

Email: stevensedwin@example.org

Phone: 570-729-3384x9757