SECURITY ANALYST SECURITY ANALYST SECURITY ANALYST - Security Controls Work Experience SECURITY ANALYST Security Controls January 2018 to Present WASHINGTONTECH SOLUTION Conducted assessment on Management, operational and technical Security Controls. Determined security categorization using Confidential 800-60 vol. 2 as information guide. Selected security controls using Confidential 800-53 Rev 4 as guidance base on system security categorization Prepared Security Assessment Reports (SAR) in which all the weaknesses are reported. Created (RTM) Risk Traceable Matrixes in which Pass/fail assessment results were documented. Worked with Confidential and the Security assessment team to Access Security Controls selected. Review Privacy Impact Assessment (PIA) documents after Confidential positive Confidential were created and ensure PII findings are recorded in the System of Record Notice (SORN). Provided audit briefings to agency and Information Systems Security Officer (Confidential), ensuring that all findings are documented in the POA&M within their Trusted Agent Confidential (TAF) tool. Applied Risk Assessment to system security and likelihood of risk occurrence using Confidential 800-30 to determine. Managed Security Control Assessment schedules for the client's systems to ensure system remain compliant with Confidential and Continuous Monitoring requirements. Prepared and updated the confidential requirements in the Confidential & Confidential package ready for system authorizing officer to make confidential risk-base- determination base on the risk level reported. Performed Confidential Government-wide program that provides Confidential standardized approach for security assessment, authorization, and continuous monitoring for cloud products/ computing services on multi-agency systems in accordance to Confidential security control baselines. Conducted Security Assessments to determine if controls were implemented correctly, operating as intended and meeting desired objectives/results. Examined policies and procedures, interviewed personnel on tested controls and conducted screenshot testing of system configuration of technical controls. Managed vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on Confidential single or multiple assets across the enterprise network. Determined sources of threat and weaknesses to the system. Practice Manager Security Controls January 2018 to Present Doctor's

community hospital, MD. Ensure office is opened and closed daily, as per established schedules. Ensure office is opened and closed daily, as per established schedules Interview, hire and train new staff in accordance with HR guidelines Manage daily staffing to ensure optimal operation of the practice Regularly review productivity and make staffing adjustments as needed Monitor and approve time cards and track licensure requirements for staff Conduct regular staff meetings and annual performance evaluations for the administrative team Review accounts receivable reports monthly Monitor and approve time cards and track licensure requirements for staff Conduct regular staff meetings and annual performance evaluations for the administrative team Review accounts receivable reports monthly IT Security Analyst /Compliance Matrix Solutions - Houston, TX October 2016 to December 2017 Documented and managed Risks in accordance with SP 800-30 and SP 800-37 using nine steps to evaluate the threats, vulnerabilities and security controls surrounding the Information System as well as the likelihood of an exploit and the impact it will have to systems operations. Responsible for monitoring compliance with information security policies by coaching others within the organization on acceptable uses of information technology and how to protect organization systems Prepared and reviewed Authorization to Operate (ATO) packages (i.e. SSP, RA, CMP, ISCP, DRP, IRP and PIA) for over 1200 systems and facilities Collected and evaluated assessment artifacts in order to determine compliance with the NIST SP 800-53 rev 4 control requirements Participated in the FIPS 199 process in which security categorization takes place, and selecting the technical, operational and managerial controls using NIST SP 800-60 guidelines. Developed POA&M (Plan of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation) Utilized Microsoft Baseline Security Analyzer (MBSA) and command line tools to perform. scans of host computers and perform a comprehensive security analysis of enterprise network environment Performed vulnerability assessments and preventions on the development side by leveraging the tools like Nmap and Nessus. Responsible for web application vulnerabilities (OWASP TOP 10) to review application source code to find its security vulnerabilities and recommend remediation. Conducted system data backup and recovery on servers as needed. Utilized parameterized

queries in back-end web servers to minimize future SQL attacks. SECURITY CONTROL ASSESSOR (Cyber Security Programs Analysis) SKYTECH INC - Westminster, MD January 2014 to February 2015 2115 Operate Risk Management Framework using Confidential 800 - 37 as confidential guide and FIPS 199 as Confidential guide to categorize information systems. Classify information Systems using the RMF processes to ensure system Confidentiality, Integrity and Availability. Select security controls using Confidential 800-53 Rev 4 as guidance base on system security categorization. Document selected security controls in the SSP that was earlier created using Confidential 800-18. Determine likelihood of risk occurrence using Confidential 800-30 as Confidential guide Most of my current projects are focused on RMF phase 4 (Assessing security controls) Effectively engage in the assessment processing & preparing for assessment, conducting assessment, communicate assessment results, and maintain the assessment. Coordinate, participate and attend weekly Confidential forums for security advice and updates. Use the implementation section of the (SSP) System Security Plan in addressing how each control is implemented (frequency of performing the controls, control types and status). Create SAP (to document assessment schedules, control families to be assessed, control tools and personnel, client's approval for assessment, assessment approach and scope, ROE if vulnerability scanning is involve). Determine assessment method (examining policies and procedures, interviewing personnel and testing technical controls), using Confidential 800-53A as Confidential guide. Create (R TM) and Risk Traceable Matrix in which to document assessment result (pass/fail) Prepare Security Assessment Reports (SAR) in which all the weaknesses are reported. Create Plans of Actions and Milestones to tracing corrective action and resolving weaknesses and findings. Conduct Confidential Privacy Threshold Analysis (Confidential) and Privacy Impact Analysis (PIA) where necessary by working closely with the Confidential and the System Owner. Review Confidential & Confidential package items Set- up and participate in the Assessment Kick-up meetings per Confidential SP 800-53A. Prepare Confidential package documents (SSP, SAR, POAM reports, and Confidential & Confidential package) to enable the Authorizing officer to make Confidential risk-base decision to sign the Authorization to Operate (Confidential) Determine

threat sources and applying security controls to reduce risk impact. Conduct risk management by identifying, assessing, responding and monitoring risk respectively. Use POA&M tracking tools like CSAM (Cyber Security Assessment and Management), Excel spread sheet to make sure the POA&M is not in delay status. Ensure that controls are implemented correctly, functioning as intended and producing the right results Authorization to Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. Assisted in conducted risk assessment on organizations various assets within the system boundaries and documented the vulnerabilities. Conducting assessment meeting kickoff and security Control meeting with ISSO and System Owner. Skills Access control (5 years), Active directory (Less than 1 year), Architecture (Less than 1 year), Cyber security (5 years), Dos (Less than 1 year), educating (5 years), Excel (5 years), Federal information security management act (Less than 1 year), Fisma (Less than 1 year), Governance (Less than 1 year), information security (5 years), Nessus (2 years), Nist (5 years), Nmap (1 year), operations. (1 year), Risk management (5 years), Security (3 years), security policies (5 years), Sql (1 year), Trading (1 year) Additional Information PROFESSIONAL/TECHNICAL SKILLS SUMMAY Experienced SECURITYANALYST/ SECURITY ASSESSOR with accomplishments in developing and implementing information security and assurance program in Private and Government Sectors. Excellent skills in utilizing Risk Management Framework (FISMA/NIST/FedRAMP/ISO 27000) to achieve compliance with federal, cloud and organizational information standards. Adept at training and educating internal users on relevant cyber security procedures and preventative measures. Specialize in network monitoring security software installation and working to prevent cyber-attacks especially in business and corporate settings. CORE COMPETENCIES Experience in C&A/A&A processes for Non-classified and Classified information systems. Good knowledge in security engineering guidance in C&A (A&A) Project Management, Excellent hands on experience with POA&Ms tracking manually using excel spreadsheet or Google Dos and also automated using CSAM, knowledge in Nessus, Active Directory, Splunk Experience using and analyzing technical assessment tools such as Nessus, McAfee Vulnerability Manager (MVM), HP Web Inspect, Appetitive, Wireshark, Nmap, Splunk Experience in multiple cyber security domains (Access

Control, Governance/Risk Management, Architecture & Design, and Operations). Working knowledge of cloud security tools such as tenant monitoring, Security Information and Event Management (SIEM - SPLUNK) and virtual network overlays, FedRAMP. Good understanding of the Federal Information Security Management Act (FISMA) requirements and National Institute of Technology and Standards (NIST) guidelines and special publications - NIST 800-53 Rev1 and rev4 and NIST SP 800-37 rev 1, 800-18, 800-53A, 800-30, 800-137, FIPS199, FIPS 200 and ISO 27001 -27002 In-depth knowledge of information assurance levels and risk impact thresholds in meeting applicable security policies, standards and requirements to ensure that accrediting authorities have the information necessary to make an objective authorization determination based on an acceptable level of risk. Practical skills in performance, development, implementation, and experienced in analyzing information requirements and delivering cost effective solution and diverse background. SKILLS/TOOLS Microsoft Office (Word, PowerPoint, Excel, Outlook, One Note, SharePoint), Google docs, MS Visio, Retina, Tenable Nessus, Active Directory, Splunk, IBM Q-Radar SIEM, Oracle DBA (Toad, SQL Developer, Data Guard, Golden Gate, Data Pump, RMAN), Service Now & Remedy and Shell Scripting, POAM, Nessus, Splunk, Snort, CVSS, Nmap, Wireshark, Snort.

Name: Jacqueline Trevino

Email: marshalllinda@example.net

Phone: (645)314-3943