

IT Security Specialist IT Security Specialist Security Control Assesor Temple Hills, MD Authorized to work in the US for any employer Work Experience IT Security Specialist Triumphant - Rockville, MD February 2018 to Present Position Responsibilities: Supports the Security Assessment and Authorization process of the clients' systems as a Security Analyst Works in 3PAO projects as well Utilizes FedRAMP requirements to assess cloud systems to ensure the proper security requirements are satisfied. Reviews technical security controls and provide implementation responses to meet requirements Document findings in the SAR Meet with client to discuss findings and process of remediation IT security specialist Hexis - Fulton, MD May 2016 to February 2018 Position Responsibilities: Assisted the SOC team in documenting and reporting vulnerabilities by utilizing tools such as Splunk and SNORT. 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. Work on multiple assessments simultaneously. IT Security Analyst XO Communications June 2014 to May 2016 Position Responsibilities: Conducted cloud system assessments Helped in updating IT security policies, procedures, standards and guidelines according to department and federal requirements Worked with client in safeguarding CUIs (Controlled Unclassified Information) by performing the necessary assessments which primarily deals with 14 control families. 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 Perform vulnerabilities scan and monitor continuously using NIST 800-137 as a guide with the aid of Nessus Education Communication Prince Georges Community College 2015 to 2016 Skills SHAREPOINT (4 years), NESSUS (3 years), NIST (5 years), SPLUNK (4 years), SAR (5 years), Information Security, It Security, Siem, Cyber Security Certifications/Licenses Certified Ethical Hacker (CEH) September 2018 to Present Security+ September 2018 to Present Additional Information 2. Specialized Skills FIPS 199, FIPS 200, NIST 800-53 Rev4, NIST 800-30, NIST 800-37, NIST 800-39, E-Authentication, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), Risk Assessment (RA), SSP, ISCP, ST&E, SAR, Plans of Action and Milestones (POA&M), Authorization to Operate (ATO) Letter, MS Office, Visio, SharePoint, Access, PeopleSoft, Nessus Vulnerability Scanning Tool, WebInspect, Splunk, DbProtect

Name: Justin Kirby

Email: tbennett@example.com

Phone: +1-587-767-1061