Security Control Assessor/ Analyst Security Control Assessor/ Analyst Security Control Assessor/ Analyst - DelTaahTech Consulting LLC Cybersecurity/Soc Analyst professional with 7 years in IT/Security. Meticulously detailed and sound at communicating, through written and verbal means to co-workers, subordinates and senior leadership. Work Experience Security Control Assessor/ Analyst DelTaahTech Consulting LLC - Greenbelt, MD October 2017 to Present Develop and maintain System Security Plans (SSP) and additional A&A documentation Conduct system risk assessments and develop Plan of Actions and Milestones (POA&M) Assist with compliance reviews and conduct audits to ensure information systems (IS) maintain the authorization baseline Coordinate and implement security policies processes, procedures, and security control techniques Ensure that information security requirements, including necessary security controls, are effectively integrated into the enterprise architecture Assist with the initiation of protective and corrective measures when a security incident or vulnerability is identified; ensure IS security incidents are handled in accordance with established procedures Ensure that risk mitigation activities are taking place and appropriate documentation is provided from the project team(s), or customer Participate in a security governance program steering committee to provide centralized governance of security services, policies, processes and procedures Review new or modified infrastructure and application services to verify compliance, identify exceptions and work with requestor/architect to identify mitigations if necessary Ensure that risk mitigation activities are taking place and appropriate documentation is provided from the project team(s), or customer Review new or modified infrastructure and application services to verify compliance, identify exceptions and work with requestor/architect to identify mitigations if necessary Manage exceptions and potential mitigations for deviation in customer standards Communicate effectively through written and verbal means to co-workers, subordinates and senior leadership. Collaborate with the team of information security professionals to conduct Security Authorization packages (C&A) based on NIST standards for general support systems and major applications. Provide input to management on appropriate FIPS 199 impact level designations and identify appropriate security controls based on characterization of the general support system or major applications. Document findings in the

Security Assessment Report (SAR) and produce a Plan of Action & Milestones (POA&M) for all controls that have weaknesses and deficiencies. SOC Analyst ADP - Rockville, MD April 2014 to October 2017 Utilized advanced technical background and experience in information technology and incident response handling to scrutinize and provide corrective analysis to escalated cybersecurity events from Tier 2 analysts - distinguishing these events from benign activities and escalating confirmed incidents to the Incident Response Lead. Provided in-depth cybersecurity analysis, and trending/correlation of large data-sets such as logs, event data, and alerts from diverse network devices and applications within the enterprise to identify and troubleshoot specific cybersecurity incidents and make sound technical recommendations that enable expeditious remediation. Proactively searched through log, network, and system data to find and identify undetected threats. Identified, verified, and ingested indicators of compromise and attack (IOC's, IOA's) (e.g., malicious IPs/URLs, etc.) into network security tools/applications to protect the Government of the District of Columbia network. Coordinated with and provide expert technical support to enterprise-wide technicians and staff to resolve confirmed incidents. Reported common and repeat problems, observed via trend analysis, to SOC management and propose process and technical improvements to improve the effectiveness and efficiency of alert notification and incident handling. Formulated and coordinated technical best-practice SOPs and Runbooks for SOC Analysts. Provided analysis and trending of security log data from a large number of heterogeneous security devices. Investigated, documented, and reported on information security issues and emerging trends. Integrated and shared information with other analysts and other teams Participated in managing projects of networking related services such as Security, Mobility, Remote Access, Internet access. Database Administrator Hilton - Charlotte, NC June 2012 to 2014 Patched the Oracle E-Business Suite (EBS) and PeopleSoft application Designing and maintaining Oracle 10g, 11g and 12c relational databases. Implemented TDE and advance security to encrypt mask secure sensitive data with the use DB Vault Convert non - container database to pluggable in Container databases 12c Apply upgrade patches, maintenance and interim patches on production and non-production databases. Education Bachelor of Science

Computer Science University of Buea February 2018 Ph.D Cyber Defense Program Dakota State University Skills Security, Nessus, Nist, Pci, Snort Certifications/Licenses CISSP March 2019 CEH Additional Information SKILLS ? SDLC OWASP ? PCI ? NIST 800 Series ? Single Sign On (Okta) ? Security Control Assessment ? End Point Protection ? Vulnerability Assessment ? HIPPA ? E-Authentication ? Network Security Protocols ? Wireshark ? Mobile Device Management ? Nessus ? Assessment & Authorization ? Privacy Impact Analysis ? AWS ? POA&M ? Audit ? Linux ? FISMA Reporting ? Knowb4 ? Security Test & Evaluation ? Splunk ? Information Assurance ? Snort ? FIPS (199, 200) ? CSAM

Name: James Walsh

Email: martinezchad@example.org

Phone: 758.407.3457