Sr IT Security Engineer Sr IT Security Engineer Sr IT Security Engineer - US Department of Labor Stafford, VA I am a Cyber Security professional with over 9 years' experience in Information Assurance and Cyber Security. I have experience working in audit engagements, security control assessment and authorization packages, and third party risk assessments. Experienced in assessing controls to ensure confidentiality, integrity, and availability of information system resources. I have experience in the various frameworks and guidelines such as the NIST Risk Management Framework (NIST-RMF), HIPAA, HITRUST, HITECH, SOX, SOC, COBIT, PCI-DSS, ISO 27K, and knowledge in Project Management. Work Experience Sr IT Security Engineer US Department of Labor - Washington, DC July 2017 to Present Performed Independent Verification and Validation (IV&V) assessments of local and FEDRAMP systems located on various SaaS, IaaS and PaaS platforms of Cloud Service Providers (CSPs) to determine compliance with NIST 800-53A rev 4 requirements. ? Conducted meetings including kick-offs and close-out meetings with various stakeholders. ? Managed project timelines for assessment activities. ? Developed various deliverables including Security Control Assessment Plan (SCAP), Prepared by Client (PBC) List, Rules of Engagement (ROE), Work Breakdown Structure (WBS), Security Assessment Report (SAR), Vulnerability Assessment Report (VAR) and other deliverables. ? Reviewed System Security Plans (SSP), Risk Assessment Reports (RAR), and Privacy Impact Assessments (PIA), policy and procedure documentation, Security Control Assessment Plans (SCAP), Plan of Actions and Milestones (POA&M) and Remediation Plans. ? Reviewed control tailoring to effectively safeguard sensitive data and validated those controls against NIST 800-53 rev 4, 800-37, 800-60, and FIPS 199/200 requirements. ? Interviewed subject matter experts (SMEs) to validate details of system documentation. ? Conducted reviews of various security scan reports (Nessus and WebInspect tools) and documented findings in the vulnerability assessment report for client review. ? Supported the development of Security Certification and Accreditation packages (SC & A) in order to secure an Authority to Operate (ATO) approval. Sr IT Security Engineer Blue Cross Blue Shield of Louisiana - Baton Rouge, LA August 2016 to December 2016 Supported the risk management program using relevant COBIT 5 Risk Scenarios, mapping associated managed risks in the SOC 2 Trust Services

Principle - Common Criteria development effort to ensure controls are linked with the associated people, process and tools details. ? Conducted walk-through assessments of each program boundary (e.g. asset management) to ensure SANS Top 20 controls are addressed. Conducted triple tier risk reviews by employing document reviews, interviews/questionnaires to capture key in-scope applications, technologies supporting critical business process and consolidating risk scores for each department as a whole. ? Coordinated and undertook risk assessments of third party vendors, internal business units, projects and processes. ? Supported compliance efforts such as controls cataloging, controls mapping (i.e. NIST 800-53, CSF, PCI, SOC 2, etc.), upkeep of controls library, performing Access Control Reviews (ACR's), following Remediation Plans aimed at addressing gaps in preparation for external audits. ? Hands on operational experience engaging with all technical staff in order to communicate and ingest supporting details and artifacts. ? Performed interviews with stakeholders and articulated control deficiencies and remediation techniques both internally and with client senior management. ? Maintained a working partnership between System Owners/Teams and the ISSO Analyst teams in order to maintain/update/track policy documentation submittal, and approve statuses, review working memos and templates. ? Participated in Vulnerability Assessment; ensured that risks were assessed, evaluated and proper actions taken to limit their impact on the Information Systems. ? Reviewed existing documents, policies and procedures, and previous assessments reports. IT Security Compliance Analyst Kaiser Permanente - Rockville, MD July 2011 to August 2016 Reviewed and disseminated HIPAA Security documentation implemented to safeguard the integrity, confidentiality, and availability of electronic PHI. ? Supported the annual HIPAA Security risk assessments and reviewed remediation plans for identified risks and vulnerabilities in consultation with the IT Security team and the Office of Compliance. ? Assisted the Privacy Officials' office in investigating, mitigating, and resolving suspected HIPAA security incidents. ? Partnered with key stakeholders in the business to identify, assess, aggregate and document risks and controls, including risks associated with new or modified products, services, distribution channels, regulations and third-party vendors and operations. ? Supported security assessments and ongoing monitoring activities of identified vulnerabilities. ?

Tested security controls across multiple business processes and/or locations, ensuring implementation techniques met the intent of organizational compliance framework and security requirements. ? Updated policies and procedures describing security requirements, guidance, and standards for organizational information systems and architecture ? Monitored the regulatory requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) law for updates. ? Collaborated cross-functionality with technology and business stakeholders to drive, track, and resolve all aspects of compliance readiness. ? Interfaced with external auditors to facilitate compliance audits. ? Coordinated delivery of audit milestones, ensuring audit timelines stayed on target by escalating and identifying roadblocks. ? Facilitated and tracked remediation, corrective action plans. ? Participated in continuous improvement initiatives. ? Assisted in the development of metrics and dashboards Education Certificate in Project Management University of California, Haas School of Business - Berkeley, CA April 2015 Bachelor of Arts University of Ghana Business School May 2001 Skills SECURITY, SHAREPOINT, WEB SERVICES, HIPAA, NESSUS, NIST, PCI, SPLUNK, FIREWALLS, NETWORKING, RISK ANALYSIS, MS PROJECT, TCP, MYSQL, ORACLE, LIFE CYCLE, SDLC, CSAM Certifications/Licenses Certificate Program in Project Management April 2015 to Present Certified Six Sigma Green Belt (CSSGB) November 2015 to Present Certified Six Sigma Black Belt (CSSBB) November 2015 to Present EC-Council Certified Ethical Hacker (CEH) November 2016 to November 2019 EC-Council Certified Network Defense Architect (CNDA) November 2016 to November 2019 CompTIA Security+ August 2017 to August 2020

Name: Thomas Turner

Email: iwilson@example.com

Phone: +1-553-936-4709