IT Security Analyst IT Security Analyst IT Security Analyst - Martha Jefferson Hospital Charlottesville, VA Work Experience IT Security Analyst Martha Jefferson Hospital - Charlottesville, VA 2016 to Present Schedule, plan, and participate in internal auditing in accordance with HIPAA, NIST, and PCI standards Perform security assessments; design reviews; and provide guidance on new technologies for the customers. Develop POA&M (Plan of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation) Perform Assessment and Authorization (A&A) documentation in compliance with company standards Perform Security Categorization (FIPS 199 and NIST SP 800-60 vol 2), Privacy Threshold Analysis (PTA), e-Authentication with business owners and selected stakeholders Author or coordinate the development of other required system security plans: Configuration management (CM), Contingency Plan (CP), Continuity of Operations (COOP), Disaster Recovery Plan (DR) and Incident Response Plan (IRP). Conduct Systems Risk Assessment through Risk Analysis, assessed the various Assets within the systems boundaries and rigorously identifying all the possible vulnerabilities that exist within the system. Developed the audit plan and performed the General Computer Controls testing of Information Security, Business Continuity Planning, and Relationship with Outsourced Vendors. Performing Vulnerability scanning using Nessus Ensure all security-related incidents are documented and reported to the ISSM and Security Officer Perform systems security audit on a weekly basis to detect unauthorized activities and ensure systems maintain security compliance. Perform Security Control Assessment (SCA) according to NIST SP 800-53A Document and conform to processes related to security monitoring, patching and incident response Manage the organization's RMF continuous monitoring tool and complete specific control activities, Maintain security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Upgrade security systems by monitoring security environment; identifying security gaps; evaluating and implementing enhancements. Perform security engineering analysis, risk and vulnerability assessment, etc. Monitor and analyze security functional tests. Prepare A&A documentation such as SSP, SCOOPS, ST&E reports, etc. Information Security Analyst University of Virginia - Charlottesville, VA 2011 to

2016 Guided System Owners and ISSOs through the Certification and Accreditation (C&A) process, ensuring that management; operational and technical controls for securing either sensitive Security Systems or IT Systems are in place and are followed according to federal guidelines (NIST 800-53). Applied security risk assessment methodology to system development, including threat model development, vulnerability assessments and resulting security risk analysis Provided support and guidance through the phases of FISMA C&A, including monitoring of the C&A artifacts compliance, annual self-assessment (NIST SP 800-53A guidelines) and quarterly self-assessment completion using NIST SP 800-26 guidelines. Created or updated the System Security Plan and conducted an Annual Self-Assessment. Applied knowledge of C&A policies, guidelines, and regulations in the assessment of IT systems and the documentation and preparation of related documents Executed vulnerability assessment and vulnerability scanning tools such as Acas, Metasploit, on a challenging and complex systems-wide information assurance/ system security environment requiring analysis of user, operational, policy, regulatory, and resource demands Assesses and mitigates system security threats/risks throughout the program life cycle; determines/analyzes and decomposes security requirements at the level of detail that can be implemented and tested; reviews and monitors security designs in hardware, software, data, and procedures, Worked with C&A team members and senior representatives to establish and define programs, resources, schedules, and risks. Developed Test Plans, testing procedures and documented test results and exceptions. Conducted the IT Risk Assessment and documented the controls. IT Security Analyst Sunrise Assisted Living, Charlottesvilee, VA 2011 to 2013 Developed and implemented new IT Security Policies to meet HIPAA and NIST standards for ensuring optimum compliance Performed vendor documentation review and analysis Assessed current business practices and identify opportunities to promote effective third-party risk management Documented and reported risk to Vendor Assessment management team, business partners, and vendors Performed onsite assessments of vendor facilities Documented risks and made recommendations based on a vendor lack of controls Supported and responded to audit procedures and findings. Worked across the Global IT organization to ensure compliance activities are being performed as

required by PCI-DSS 3.1 Worked closely with team members, end users, and other departments to design, implement, support, and maintain application security and security policies that protects Speedway IT systems Reviewed existing policies to meet HIPAA security and privacy rules. Conducts risk assessment and formulates a road map for risk remediation Worked on risk remediation Analyzed Gap Analysis and prepares a roadmap for risk mitigation Analyzed the physical security environment and implemented policies to secure the overall security infrastructure Initiated and developed strong physical and technical security infrastructure from the scratch. Provided security training and awareness to the entire work force. Participated in the company's Technology Awareness forum Monitored the Network infrastructure for intrusion and vulnerabilities and applied update patches IT Help Desk Specialist FedEx - Charlottesville, VA 2010 to 2011 Provided support for application software installation and use. Acted as an advocate for the office in the resolution of any and all computer-related problems or issues. Assisted in the delivery, installation, and use of systems and services, (e.g., Washington to district office connectivity, Internet, remote access, etc.). Provided front line phone, Live Chat, and Remote Desktop support, may be required to resolve requests via on-site visit(s). Provide Hardware/Software Installation and Setup support. Troubleshoot and solve common network issues using physical and logical diagnostic tools. Troubleshoot and solve common Microsoft based platforms (Windows XP, Windows 7, Microsoft Office Suite, Etc.) and common hardware used throughout FOCH (Dell, Lenovo, and HP) Troubleshoot basic technical issues over the phone or by logging in remotely to their computers Provided second-tier support to end users for either PC, server, or mainframe applications or hardware. Information Security Analyst Vanguard Life Assurance Company 2007 to 2011 Responsible for assisting in pricing and product development Analyzed historical claims data Responsible for monitoring high risk accounts Assisted with internal and external reporting Assisted in ad hoc requests from internal and external customers Assisted with profit share calculations and reporting Assisted with reinsurance reports for ceding Conducted Periodic Underwriting and Policy Management Audit Education Master of Business Administration in Management Information Systems University of Mary Washington - Fredericksburg, VA May 2019

Master of Arts in Information Studies in Information Studies University of Ghana - Accra, GH May 2011 Bachelor of Arts in Social Science in Social Science University of Cape Coast May 2007 Skills Security, Hipaa, Iso, Nessus, Nist, Pci, Sox, Wireshark, Fisma, Incident response, Configuration management, Sps, Security policies, System security, Risk management, Cmp, Budget, Scanning, Sar Additional Information TECHNICAL COMPETENCY Working knowledge of Risk Management Framework (RMF) for Assessment & Authorization process to obtain an ATO using federal security policies, standards and guidelines including NIST 800 SPs such as 800-18, 800-30, 800-37 rev 1, 800-60, 800- 53/53A rev 4) and FIPS 199 & 200. Experience in developing and reviewing security Authorization and Assessment (A&A) artifacts including, but not limited to Contingency Plans (CP), Incident Response Plans (IRP), Configuration Management Plans (CMP), Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA). Knowledge of Federal and international regulatory bodies such as Office of Management Budget (OMB), FISMA Reports, FedRAMP, PCI DSS, SOX, HIPAA and ISO. Experience in performing on-site security testing using vulnerability scanning tools such as Nessus and Penetrating testing using tool such as Nessus and Wireshark * Experience in the development of ATO Package Documents such as System Security Plans (SSP), Security Assessment Reports (SAR) and Plan of Action and Milestones (POA&M). Proficient in explaining technical information, resolutions, documentations, and presentations to clients and non-technical personnel at all levels of the organization or enterprise. Team oriented with the ability to work independently and proactively while prioritizing competing priorities, often under time constraints.

Name: Stephen Weber

Email: kfoley@example.com

Phone: 2068648011