Information System Security Officer Information System Security Officer Information System Security Officer - Vignet Work Experience Information System Security Officer Vignet - Fairfax, VA October 2018 to Present Engage in all aspects of the Risk Management Framework (RMF) Assessment and Authorization process, including securing Authorization to Operate (ATO) and ongoing continuous monitoring efforts. Follow the Risk Management Framework to categorize, implement, and assess all security controls; then use client templates to create and manage ATO-related deliverables, some of which include: Business Impact Analysis (BIAs) / Privacy Threshold Analyses (PTAs) / Privacy Impact Assessments (PIAs) / System Security Plans (SSPs) / Security Assessment Reports (SARs) / Vulnerability Assessment Reports (VARs) / Plan of Action and Milestones (POA&Ms). Make recommendations to senior management on the results of risk analysis and work closely with other Information Technology groups to refine and enhance security controls. Monitor and maintain operational security posture to ensure information systems (IS) security policies, standards, and procedures are established and followed. Manage changes to system and assess the security impact of those changes. Prepare and review documentation to include SSPs, Risk Assessment Reports, A&A packages, and Security Controls Traceability Matrix (SCTM). Perform security control assessment using NIST 800-53 guidance and as per continuous monitoring requirements Preserve client specific Plan of Action and Milestones and supports remediation activities. Review and update SSP, System Security test and Evaluation (ST&E) Risk Assessment (RA), PIA, and POA&M Conduct system level audit reviews to track any unusual/inappropriate activity and report findings to the ISSM Develop, tests and train employees on Contingency and Incident Response planning. Proactively mitigates system vulnerabilities and recommends compensating controls. Facilitate the development and documentation of Vignet's FedRAMP System Security Plan and Program with our Advisory Services consulting team and third-party assessment organization (3PAO). Collaborate with the functional teams (e.g. IT, cloud services, support staff, etc.) and the 3PAO to provide clarity and prescribed solutions that are known to work in a FedRAMP environment. Experience with federal regulations such as HIPAA, SOX, GDPR, PCI DSS. Experience with GRC software such as XACTA in managing cyber risk and compliance. Senior IT Privacy & Compliance Analyst Department of Interior - Washington, DC May 2017 to October 2018 Contributed to the implementation of the privacy program and subsequent monitoring of Department of Interior's Systems that collects Personally Identifiable Information (PII). Provided support for the development and completion of Privacy Threshold Analysis (PTAs), PIAs, Third Party websites and applications (TPWAs) and SORNs in collaboration with stakeholders. Supported the development, maintenance and revision of policies and procedures for the general operation of the privacy program and related activities across DOI's OCIO's System. Periodically assisted with revisions to the privacy program in light of changes in laws or regulations; develops or revises policies or procedures to reflect industry standards, as directed. Responded to requests from data subjects requesting access and/or amendment rights to their data. Maintained knowledge of applicable international, federal, state and local regulatory agency guidelines and laws. Participated in periodic audits to demonstrate security control effectiveness. IT Risk & Compliance Analyst Department of Labor - Washington, DC September 2015 to May 2017 Utilized security documentation including National Institute of Standards and Technology (NIST) Special Publications 800-53, 800-34, Federal Information Processing Standard (FIPS) 199, and FIPS 200. Developed and maintained C&A documentations, including System Security Plans, Contingency Plans, Risk Assessment Reports and evaluated existing documents and their accuracy. Evaluated systems of records and implemented corrective actions to ensure privacy issues are addressed and business processes comply with legal requirements. Prepared Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. Provided review and progress reports of all POA&M. Coordinated with system administrators to provide fixes for vulnerabilities identified in systems. Analyzed organizational information security policy needs based on stakeholder interactions, develop and publish policy, standards, security handbook, and procedures for implementation ensuring alignment with NIST 800-53 Rev 4. Updated IT security policies, procedures, standards, and guidelines according to private and federal requirements. Created remediation strategies for weaknesses based on priorities. Reviewed and updated FIPS 199 (SP

800-60), Initial Risk Assessment (SP 800-37), E-Authentication, PTA, PIA, ST&E, POAM as part of the Security Assessment and Authorization (SA&A) IA Policy Analyst Federal Election Commission - Washington, DC June 2010 to August 2015 Identified vulnerabilities, recommended corrective measures and ensured the adequacy of existing information security controls. Coordinated with appropriate personnel to run vulnerability scans on a regular basis and ensured timely remediation actions. Collaborated with the system owner, business owner, and other key stakeholders to develop and implement business continuity capabilities including alternate user access methods, and manual processes to execute key system functions Performed IT risk assessment and documented the system security keys controls. Updated IT security policies, procedures, standards, and guidelines according to federal requirements. Developed and updated system security plan (SSP), Plan of Action and Milestone (POA&M) in CSAM Monitored POA&Ms and works with IT System POCs to resolve. Re-assessed controls upon POA&M resolution and provide status reports as necessary. Conducted IT controls risk assessments (NIST 800-53A) including reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with NIST standards. Prepared and reviewed documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages. Analyzed system risks and provided recommendations for risk acceptance or rejection. Scheduled and conducted security assessments of systems to determine compliance with applicable security controls and standards. Education Bachelor of Science in Biology Virginia Polytechnic Institute & State University - Blacksburg, VA May 2013

Name: Timothy Carson

Email: lwilkins@example.net

Phone: 376.873.0590