Senior Associate | Senior Technical Advisor | Subject Matter Expert (SME) Senior Associate | Senior Technical Advisor | Subject Matter Expert (SME) Senior Associate | Senior Technical Advisor | Subject Matter Expert (SME) - 1 Inc Gaithersburg, MD Versatile, creative information security executive with over thirteen (13) years' of experience in secure technology implementations of networking equipment, systems architecture, systems configuration, and systems administration. Effective information security executive able to build excellent relationships with: team members, upper management, and customers. Extensive experience in the National Institute of Standards and Technology (NIST) Risk Management Framework, providing expertise to multiple government agencies in ensuring security without compromising confidentiality, integrity and availability (C-I-A). Authorized to work in the US for any employer Work Experience Senior Associate | Senior Technical Advisor | Subject Matter Expert (SME) 1 Inc - Germantown, MD April 2019 to Present 20874 Responsibilities: Senior Technical advisor for the agencies cloud computing models/environments. Ensuring Cloud Service Providers (CSPs) are complying with agencies security policies and procedures. System Owner for the agencies CSAM application. Ensuring all FISMA system control requirements are implemented and maintained. Ensuring that weaknesses are identified and addressed through the process of Plan of Action and Milestones (POA&M's), Waivers and/or Exceptions. Ensuring that the Security Plan (SP) is appropriately developed and maintained. Ensuring that the Contingency Plan (CP) is appropriately developed, tested, and maintained. Ensuring that all security requirements are being or will be met to obtain/maintain a valid Authorization to Operate (ATO) status. Created the agencies Common Control Provider (CCPs) Program. Identified and designated (Common, Hybrid, System Specific) NIST 800-53 rev4 security controls based on assessment objective and service(s) provided by the agencies CCP(s). Identified and designated (Customer, Shared, Inherited, N/A) NIST 800-53 rev4 security controls based on assessment objective for the three (3) Cloud Computing Model(s): Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Advised agency executive(s) on cybersecurity best practices/standards to ensure the agency is in compliance with Federal statue(s)/mandate(s). Senior Information System Security Officer (ISSO) AmVet Technologies, LLC

- Germantown, MD December 2018 to April 2019 20874 Responsibilities: Senior ISSO for the agencies cloud computing models/environments. Assist in the development, deployment, and implementation of security measure(s) within the various cloud computing environments. Ensure security authorization boundary is described and documented. Ensure that all FISMA system control requirements are implemented and maintained. Ensuring that weaknesses are identified and addressed through the process of Plan of Action and Milestones (POA&M's), Waivers and/or Exceptions. Ensuring that the Security Plan (SP) is appropriately developed and maintained. Ensuring that the Contingency Plan (CP) is appropriately developed, tested, and maintained. Ensuring that security requirements for the Major Application (M.A) or General Support System (G.S.S) are being or will be met to obtain/maintain a valid Authorization to Operate (ATO) status. Ensuring that requests for Security Assessment and Authorization (SA&A) of computer systems are completed in accordance with federal statue(s) and mandate(s). Ensuring compliance with all legal requirements concerning the use of commercial proprietary software. Maintaining an up-to-date inventory of hardware and software that encompasses the M.A or G.S.S accreditation boundary. Ensuring that risk assessment(s) report(s) are completed to determine cost-effective and essential safeguards against identified threat source(s). Attending security awareness and related training programs and distributing security awareness information to the user community as appropriate. Reporting IT security incidents (i.e. computer viruses) in accordance with established agency policies and procedures. Reporting security incidents not involving IT resources, to the appropriate office and/or department. Providing input to appropriate IT security personnel for preparation of reports to higher authorities concerning sensitive and/or national security information systems. Subject Matter Expert (SME) II/Information System Security Officer (ISSO) eGlobalTech Inc - Arlington, VA January 2018 to December 2018 22203 Responsibilities: SME/ISSO ensuring that all FISMA system control requirements are implemented and maintained. Ensuring that weaknesses are identified and addressed through the process of Plan of Action and Milestones (POA&M's), Waivers and/or Exceptions. Ensuring that the Security Plan (SP) is appropriately developed and maintained. Ensuring that the Contingency Plan (CP) is appropriately developed, tested, and

maintained. Ensuring that security requirements for the Major Application (M.A) or General Support System (G.S.S) are being or will be met to obtain/maintain a valid Authorization to Operate (ATO) status. Ensuring that requests for Security Assessment and Authorization (SA&A) of computer systems are completed in accordance with federal statue(s) and mandate(s). Ensuring compliance with all legal requirements concerning the use of commercial proprietary software. Maintaining an up-to-date inventory of hardware and software that encompasses the M.A or G.S.S accreditation boundary. Ensuring that risk assessment(s) report(s) are completed to determine cost-effective and essential safeguards against identified threat source(s). Attending security awareness and related training programs and distributing security awareness information to the user community as appropriate. Reporting IT security incidents (i.e. computer viruses) in accordance with established agency policies and procedures. Reporting security incidents not involving IT resources, to the appropriate office and/or department. Providing input to appropriate IT security personnel for preparation of reports to higher authorities concerning sensitive and/or national security information systems. IT Specialist Woodlawn, MD August 2012 to January 2018 21207 Responsibilities: Information Technology (IT) Specialist/Lead Security Analyst/Technical Advisor/ Subject Matter Expert (SME), directing technical and security evaluation(s) on various agency programmatic application(s) and service(s). IT Specialist/Lead Security Analyst performing Security Assessment and Authorization (SA&A) activities performing Security Control Assessment(s) (SCA) on the NIST Special Publication (SP) 800-53 rev.4 security control(s). Interviewing stakeholder(s) to determine implementation status of the NIST SP rev.4 security controls, examining the Security Authorization Package (SAP) documentation (i.e. SP, Audit Plan, Configuration Management Plan (CMP), CP, etc.), and testing NIST 800-53rev4 security control(s) utilizing Tenable Nessus, DBProtect, McAfee Endpoint Protection, Splunk, and ArcSight. Documenting SCA result(s) and SA&A artifacts in the Cyber Security Assessment and Management (CSAM) application. Technical Advisor for the re-engineered integrity review process (R-CIRP) system. Delegating task(s) to various developer(s), contractor(s), and analyst(s) to ensure completion of project milestone(s). Serving as the configuration manager, risk executive, ensuring architecture and implementation are aligned with

agency standard(s). Ensuring all security controls comply with NIST 800-53rev4 guideline(s). Certifying manager for case(s) submitted within the R-CIRP system to detect and deter internal/external fraudulent behavior. Subject Matter Expert (SME) for the agency Audit Trail System (ATS) identifying security violation(s), examining user behavior, and analyzing threat vectors to determine auditable event(s). ISSO/ISSM for the ATS ensuring adequate implementation of moderate baseline NIST 800-53rev4 security control(s). Authoring and publishing the agency Information Security Policy (ISP) chapter on "Internal Security Controls". CyberSecurity Analyst Veris Group Inc - Woodlawn, MD October 2010 to 2012 21207 Responsibilities: Lead Security Control Assessor, performing SA&A in-depth analysis of the SSP, CMP, CP and other SAP documentation related to M.A and GSS's. Ensuring all necessary requirements for infrastructure and operations are adequately documented and addressed. Analyzing vulnerability scans using automated tools (Tenable Nessus) and creating POA&Ms along with the appropriate mitigating controls. Providing in-depth analysis of client's information system security program and making adequate recommendations based on analysis. Providing technical expertise to enhance the agency/organization overall security posture. CyberSecurity Analyst SAIC Secure Infrastructure Division, Cyber Security Solutions Operation - Columbia, MD June 2008 to October 2010 21046 Responsibilities: Technical Lead/Team Lead providing SA&A and continuous diagnostics mitigation (CDM) support of various line offices within the client's organization. Managed a test team of five (5) (up to ten (10)) individuals and was responsible for ensuring deliverables were submitted on time, testing procedures were conducted according to policy, and all stakeholders were aware of the current security posture of their system. Performing review and verification of clients systems utilizing NIST SP 800-53 rev4, and Risk Management Framework (RMF) (NIST SP 800-37 rev1) and assisted in the update of SAP package development. Provided in-depth analysis of vulnerabilities identified from the SA&A and vulnerability scan(s). Furthermore, presented findings from the SA&A effort to various system owner(s), executive(s), and CIO(s), acknowledging action(s) needed in order to enhance the security posture of a particular system. Updating publishing, and providing recommendation(s) regarding agency wide Common Controls. Assisting in the

development and distribution of internal automated SA&A testing tools that provided a more efficient and effective reporting mechanisms of the agency security flaw(s). Information Assurance (IA) Engineer SRA International - Washington, DC June 2006 to June 2008 20548 Responsibilities: IA Engineer responsible for providing and maintaining workstation and network security, agency wide. Utilizing a variety of security software, tool(s), and appliance(s) reporting security flaw(s), potential threat(s), and harmful user(s) activities. Participating in the deployment and configuration of new network analysis tools, Intrusion Detection Sensor(s), and hard-drive encryption software. Responsible for providing presentation(s) to the executive committee on any/all security finding(s). Maintaining all security server(s) related to workstation and network security. This included, updating each server, ensuring the server was collecting adequate information, and implementing hardening guidelines set-forth by the agency. Providing end-user support to those having difficulties with the various security software employed on their system. Education BSc. in Information System- Security Johns Hopkins University 2006 Aa. in Business Administration Carroll Community College 2003 Skills SECURITY, IDS, NESSUS, NMAP, SIEM

Name: Michael Williams

Email: stephanievalentine@example.net

Phone: 001-749-689-5485x431