Cyber Security Analyst (Team Lead) Cyber Security Analyst (Team Lead) Cyber Security Analyst (Team Lead) - Department of Veterans Affairs - CRISP Program Bowie, MD Information Security Professional with 7 years experience in information Technology compliance. Specialties in Assessment and Authorization (A&A), Plan of Action and Milestone (POA&M), Federal Information Security Management Act (FISMA), Information Assurance, Risk Management, National Institute of Standards & Technology (NIST), Federal Information Processing Standards (FIPS) and SP-800 Series Guidance, Information Security Continuous Monitoring (ISCM), and developing Security Policies and Procedures. Ability to successfully multitask, prioritize multiple requests, and complete difficult tasks within deadlines. Work Experience Cyber Security Analyst (Team Lead) Department of Veterans Affairs - CRISP Program May 2017 to Present Duties include: Providing Cyber Security Analyst services as part of CRISP Remediation Services Support (RSS) program to Department of Veterans Affairs to ensure information security controls are implemented correctly, working as intended and producing desired outcome throughout the systems life cycle. Training team members on Assessment and Authorization (A&A) processes, POA&M Management/Review and Continuous Monitoring Providing Team leadership, guidance and instruction to team members. Representing my team in the daily meeting with the VA Cybersecurity Risk Management Team for updates on the task at hand. Conducting interviews/meetings with the System Owners/Area Managers to determine the Security posture of the System/Facility and to assist in the completion of the Security Assessment Plan using NIST SP 800-53A test required to maintain/obtain Authorization to Operate (ATO). Assessing assigned systems to determine system security status/posture and ensures adherence to security policy, procedures and standards using NIST SP 800-53A and VA Handbook 6500 as a guide. Reviewing implementation statements and supporting evidence of security controls as to determine if the systems are currently meeting the requirements and provide findings/suggested mitigations to stakeholders. Performing reviews of RMF Security Controls on assigned systems/facilities ensuring compliance with FISMA, NIST and VA 6500 Handbook Developing, reviewing, and updating Information Security Standard Operating Procedures in accordance with FISMA, NIST and VA 6500 Handbook. Communicating and enforcing security

policies, procedures and safeguards for all systems based on NIST Performing security control assessment as part of Assessment and Authorization (A&A) and Continuous monitoring projects using NIST SP 800-53A and VA Handbook 650as a guide. Performing a review of security documents/evidence for implementation of the controls to confirm they are FISMA compliant Developing POA&Ms (Plan of Action and Milestone) for vulnerabilities uncovered during assessment and continuous monitoring. Developing and tracking for corrective actions/milestones on the Plan of Action and Milestones (POA&M) of all accepted risks upon completion of Security Control Assessment. Assisting client in getting ready for the OIG visit by assessing their security controls and ensuring that they are implemented correctly, working as intended and producing desired outcome. Reviewing and validating items/evidence uploaded into POA&M tracking tool in support of remediation of the findings. Remediating vulnerabilities of various Veterans Administration's entities/systems for low, moderate and high impact systems and ensuring all POA&M actions are completed in timely manner to meet client deadlines. Performing quarterly reviews for POA&Ms that passed Scheduled Completion Date. Participating in the Security Test and Evaluation (ST&E) Kick-off Meeting. Conducting SCA findings meeting with the System Owner, ISSO and other system personnel as required for remediation of the findings. IT Security Analyst Trinitech Consulting - Beltsville, MD December 2014 to May 2017 Duties include: Performed Security Categorization using FIPS 199 and NIST 800-60 vol 2 Using FIPS 200 as a guide for minimum security requirements for federal and information systems. Conducted meetings with the IT team to gather documentations and evidences (Kick-off meeting) about the control Developed and maintaining Plan of Action and Milestones (POA&MS) to remediate findings and get an ATO Conducted assessment of controls on Information Systems by interview, examine and test methods using NIST SP 800-53A as a guide. Created, updated and reviewed System Security Plans using NIST 800-18, Contingency Plans using NIST 800-34, Incident Reports using NIST 800-61 Conducted risk assessments regularly; ensured measures raised in assessments were implemented in accordance with risk profile, and root-causes of risks were fully addressed following NIST 800-30 and NIST 800-37 Supported clients in creating a memo for findings that has passed Scheduled

Completion Date. Supported clients in creating Risk Base Decision (RBD) for Plan of Action and Milestones (POA&M) Provided continuous monitoring support for systems in accordance to FISMA guidelines - NIST 800-137. Reviewed and updated Security Artifacts such as System Security Plan (SSP), Security Assessment report (SAR), Security Assessment Plan (SAP), Contingency Plan (CP), Privacy Impact Assessment (PIA), and Plan of Actions and Milestones (POA&M) Provided ongoing gap analysis of current policies, practices, and procedures as they relate to established guidelines outlined by NIST, OMB and FISMA. Supported client in creating Standard Operating Procedures (SOP) as guidance through Risk Management Framework. IT Security Analyst Document System Inc - Washington, DC June 2011 to December 2014 Duties include: Supported client on Systems Re-Authorization efforts and Security Authorization Processes, and best practices. Provided continuous monitoring support for systems using NIST 800-137 as a guide. Provided ongoing gap analysis of security controls, policies, practices, and procedures using guidelines outlined by NIST, OMB and FISMA. Documented and reviewed System Security Plan (SSP), Security Assessment Report (SAR), Plan of Action and Milestones (POA&M). Evaluated and selected policy-based solutions to support information security governance requirements for HIPPA, and Privacy Act of 1974. Reviewed and ensured Privacy Impact Assessment (PIA) document after a positive PTA is created. Reviewed and updated Security Assessment plan (SAP). Ensured security policies, procedures, and recommendations comply with NIST, FISMA, organizational guidelines, and technical best practices. Supported sites in remediation of the vulnerabilities in POA&M. Updated Plan of Action & Milestones (POA&M) and Risk Assessment based on findings assessed through monthly updates. Education Master of Engineering in Environmental Engineering in Environmental Engineering University of Port Harcourt March 2004 Bachelor of Engineering in Chemical Engineering in Chemical Engineering Enugu State University of Science and Technology November 1996 Skills Federal Information Security Management Act (7 years), FISMA (7 years), NIST (7 years), Security (7 years), system security (7 years), RMF, Plan of Action and Milestones, Assessment and Authorization, Cyber Security, Information Security, It Security Certifications/Licenses CompTIA Security+ September 2018 to September 2021 AWS

Developer Associate October 2018 to October 2020 Additional Information Technical Expertise Federal Information Security Management Act (FISMA) Risk Management Framework (RMF) Processes - NIST 800-37, FIPS 199, FIPS 200, NIST SP 800 60 vol 2, NIST SP 800-53A and NIST SP 800-53 rev 4. Audit Readiness Assessment of security controls using NIST SP 800-53A Development of Security Artifacts - Security Assessment Plan (SAP), Plan of Action &Milestone (POA&M), Risk Assessment, System Security Plans (SSP), Security Assessment Report, Contingency Plans, and Incident Response Plans. System Development Life Cycle (SDLC) Continuous Monitoring Governance Risk Compliance - Risk Vision Health Insurance Portability & Accountability Act (HIPAA) Microsoft Suite Strong verbal, written and interpersonal skills

Name: Brian Alvarado

Email: tammy40@example.org

Phone: 214-282-7255