Senior Compliance Lead Senior Compliance Lead Senior Compliance Analyst/Lead - GAMA-1 Technologies Silver Spring, MD INSIGHTFUL | LEADERSHIP | INTEGRITY Diligent, result-driven and analytical IT security professional with 7 years of extensive experience in conducting cyber/ IT security assessment and compliance, system controls, system verification and validation testing techniques. Working experience in the application of FISMA guidelines including the NIST special publications 800-18, 800-30, 800-34, 800-37, 800-39, 800-53, 800-53A etc. Cognizant of various industry standards pertaining to Federal and Commercial industries, resourceful, detail-oriented, and client focused, with a continuing passion for growth. Work Experience Senior Compliance Lead GAMA-1 Technologies - Greenbelt, MD April 2019 to Present Client: National Oceanic and Atmospheric Administration (NOAA) Conduct ongoing pre-assessment reviews of authorization packages, provide reports to the system personnel and senior Federal management addressing noted deficiencies and areas for improvement. Complete reviews of all post-assessment documentation packages and provided write-ups to system personnel and the assessment team concerning noted deficiencies and suggested modifications. Collaborate with system personnel as part of a dry-run process to go over mitigation strategies for all findings. Initiate, coordinate and track the patching and remediation of security weaknesses via a Plan of Actions and Milestones (POA&M). Review all artifacts presented in support of POA&M closure requests, and work with the Information System Security Officer (ISSO) to modify remediation plans and evidential support as needed. Lead a weekly Security Assessment and Authorization (SA&A) staff meeting to discuss the plans, progress and challenges of attaining information system ATOs for the current fiscal year. Participate in ATO briefings to provide compliance support for information system stakeholders. Perform on-boarding and off-boarding duties related to compliance team personnel. Generate monthly reports (ISSO Notifications, POA&M reminders, Contingency Plan Tests, ISSO/SO Training requirements etc.), fulfill requests for data calls and other compliance metrics requests. Develop Security Control Assessment (SCA) scoping and Security Assessment Reports (SAR) as part of annual security assessments for applicable systems. Senior FISMA Analyst Triumph Enterprises, Inc - McLean, VA September 2017 to April 2019 Developed and updated the information systems

security documentation templates (e.g. System Security Plan (SSP), Contingency Plan, Contingency Plan Test, Business Impact Analysis, FIPS-199, Configuration Management Plan etc.) based on changing NIST and federal guidance. Assisted in coordinating remediation of Plan of Action and Milestones (POA&M) findings with various organizations within the enterprise. Trained and assisted System Owners, ISSOs and other Stakeholders in understanding documentation requirements. Responded to multiple customer inquiries regarding A&A utilizing a ticketing system; ensure timely and complete responses. Reviewed and processed waivers and exceptions for federal information systems that are not compliant with federal and organizational policies. Worked with the clients to develop capabilities briefings and presentations in support of the program.

Coordinated with ISSOs and System Owners across the organization to ensure timely compliance with federal and organizational policies, and procedures. Produced required reporting (data calls) for various management levels. Developed and updated various internal and external A&A related guidance documentation. IT Security Analyst Deloitte - Rosslyn, VA August 2015 to September 2017 Client: Department of Labor, National Institutes of Health (NIH) Reviewed Security Authorization Packages of federal information systems seeking an Authority To Operate (ATO) in order to be FISMA compliant. Developed and updated federal information systems' security documentation templates such as the System Security Plan (SSP), Contingency Plan, Contingency Plan Test, SAR etc. utilizing NIST Special Publications such as NIST SP 800-18 Rev. 1, NIST SP 800-34 Rev. 1 etc. Coordinated the remediation of Plan of Action and Milestones (POA&M) with identified weaknesses, timelines, milestones and point of contacts for each finding from the SAR. Coordinated with ISSOs across the organization to ensure timely compliance with federal and organizational policies, and procedures. Established and maintained information security procedures and guidelines pursuant to federal laws and regulations. Reviewed Security Assessment and Authorization packages of Cloud Service Providers (CSP) in the pipeline of the agency. IT Security Specialist ICF International - Rockville, MD September 2012 to July 2015 Client: Department of Education, Georgia Power Performed internal IT security audits based on ISO 27001 and ISO 27002 standards, and mapping to internal policies. Conducted security control

assessments for federal information systems utilizing NIST SP 800-53A. Coordinated and guided ISSOs to ensure timely compliance with Federal and organizational policies and procedures. Drafted and reviewed templates and standard operating procedures to ensure completeness and accuracy. Assisted System Owners, ISSOs and other Stakeholders in understanding documentation requirements. Education Master of Science in Cyber Security University of Maryland University College - Adelphi, MD January 2018 to Present Bachelor of Science in Information Systems University of Maryland - Baltimore, MD Skills Powerpoint, Microsoft Office, Typing, CSAM, Archer, Tenable Security Center Certifications/Licenses CompTIA Security+ CAP CISA

Name: Steven Reynolds

Email: allisonrodriguez@example.com

Phone: +1-705-675-4948x22058