Security Control Assessor Security Control Assessor Security Control Assessor - Kforce Fredericksburg, VA Information Assurance Analyst knowledgeable in Risk Management Framework (RMF), Systems Development Life Cycle (SDLC), security life cycle, and vulnerabilities management using FISMA, and applicable NIST standards. Organized, Solutions-focused, deadline-focused, team oriented, work well independently, or in team providing all facets of computer supports with in-depth knowledge and understanding of numerous software packages and operating systems. A proven project and team lead with aptitude for good customer service, leadership, excellent communication (both oral and written), and presentation skills. Specialized in providing IT security expertise and guidance in support of security assessments and continues monitoring for government (FISMA & NIST) and commercial clients TECHNICAL AND SPECIALIZED SKILLS Excel, Word, PowerPoint, Microsoft Windows, CSAM and SharePoint. Functional Area Of Expertise Assessment and Authorization (A&A) IT Security Compliance Vulnerability Assessment Information Assurance Systems Risk Assessment Technical Writing Policy Writing Work Experience Security Control Assessor Kforce - Washington, DC May 2018 to Present Provided security expertise and guidance in support of security assessments. Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4.

Conducted security control assessments to assess the adequacy of management, operational, privacy, and technical security controls implemented. Security Assessment Reports (SAR) were developed detailing the results of the assessment along with Plan of Action and Milestones (POA&M). Uploaded supporting documents in the System's Artifact Libraries, SharePoint and CSAM Ensured Systems' Plan of Action & Milestone (POA&Ms) are closed or updated in a timely manner using a tracking tool CSAM Participated in weekly IT Security Team meetings to provide guidance and support for the development of enterprise security architecture. Prepared Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. Performed vulnerability assessment, making sure risks are assessed and proper actions taken to mitigate them. Conduct IT controls risk assessments including reviewing organizational policies, standards and procedures

and providing advice on their adequacy, accuracy and compliance with industry standards. Developed resultant SCA documentation, including but not limited to the Security Assessment Report (SAR). Assisted team members with proper artifact collection and detail to clients' examples of artifacts that will satisfy assessment requirements. Reviewed system-specific Standard Operating Procedures, Rules of Behavior, Contingency Plan, Incidence Response Plan, Configuration Management Plan, Service Level Agreement, and Memorandum of Understanding to aid security assessment and authorization efforts. Information Assurance Analyst Department Of Labor - Washington, DC June 2014 to May 2018 Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, FIPS 200, SSP, Core Docs, Policy and Procedures, Security Test and Evaluations (ST&Es), Risk Assessments (RAs), Security Assessment Reports (SAR), Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Plan of Action and Milestones (POAMs). Conducted kick off meetings to collect systems information (information type, boundary, inventory, etc.) and categorize systems based on NIST SP 800-60. Conducted security control assessments to assess the adequacy of management, operational privacy, and technical security controls implemented. Security Assessment Reports (SAR) were developed detailing the results of the assessment along with Plan of Action and Milestones (POA&M). Uploaded supporting docs in the System's Artifact Libraries, Google Docs, and CSAM Ensured Systems' Plan of Action & Milestone (POA&Ms) are closed or update in a timely manner using a tracking tool CSAM Developed system security plans to provide an overview of federal information system security requirements and described the controls in place or to meet those 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. Performed vulnerability assessment, making sure risks are assessed and proper, actions taken to mitigate them. Conduct IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. Developed risk assessment reports. These reports identified threats and vulnerabilities. In addition, it also evaluates the likelihood that vulnerabilities

can be exploited, assess the impact associated with these threats and vulnerabilities, and identified the overall risk level. IT Security Analyst Department of Interior - Washington, DC January 2012 to June 2014 Hold kick-off and weekly meetings with system owners prior to assessment engagements and weekly activities relating to CSAM Collected, reviewed and analyzed audit logs for anomalies Created reports detailing identified vulnerabilities and the steps to remediate them. Tested and document comprehensive security assessment results that include a full description of the weakness and deficiencies discovered during assessment information System Security controls per the NIST 800-53A Revision 4 guidelines. Assisted in identifying and communicating application control deficiencies and the associated risks. Assisted with the development and maintenance of plan of action and milestones (POA&Ms) to document security vulnerabilities and mitigation strategies. Monitored controls post-authorization to ensure continuous compliance with security requirements. Provided expertise and assistance in the development of continuous monitoring programs and plans. IT Security Specialist Co-operative Group - Harrisonburg, VA February 2010 to January 2012 Supported client's information security governance, risk and compliance activities to align with the NIST Risk Management Framework (RMF) Developed security C&A artifacts, to include but not limited to, sensitivity assessments, SSPs, POA&Ms, and ATO package according to SP 800 - 37 Generated, reviews and updates System Security Plans (SSP) against NIST 800-18 and NIST 800-53 requirements. Conducted risk assessments regularly; ensures measures raised in assessments are implemented in accordance with risk profile, and root-causes of risks were fully addressed following NIST 800-30 and NIST 800-37 Risk Analysis/risk mitigation, assessed the security risk of vendor partners Participated in the FIPS 199 process in which security categorization takes place, and selecting the technical, operational and managerial controls using NIST SP 800 -60 guidelines Analyzed and advise on the risk and remediation of security issues based on reports from vulnerability assessment scanners, patch management tools, and emerging threat information Education Bachelor of Business Administration in Marketing University of Ghana

Name: Tara Mayer

Email: bbauer@example.com

Phone: 552-768-0472x74233