IT Security Analyst IT Security Analyst IT Security Analyst Centreville, VA Detailed knowledge of information system security and contingency planning tools, technologies and best practices with an emphasis on FISMA/NIST and Federal Information Systems Control Audit Manual (FISCAM) compliance. Over four years of experience in system security auditing, monitoring, and evaluation, contingency planning, and risk assessments of GSS (General Support Systems) and MA (Major Applications). Authorized to work in the US for any employer Work Experience IT Security Analyst Qivliq LLC - Fairfax, VA September 2015 to January 2018 Conducted kick off meetings to categorize systems according to NIST requirements of Low, Moderate or High system using FIPS 199 and SP 800-60 Developed a security baseline controls and test plan that was used to assess implemented security controls Conducted Annual Security Assessments for client systems using NIST SP 800-53 and 53a 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) Developed a system security plan to provide an overview of federal information system security requirements and described the controls in place or planned based on requirements. Developed, coordinates, and maintains comprehensive business continuity and disaster recovery plans to ensure the ability for the office, firm, and technology platform to recover in the event of an unforeseen disruption. Performed risk analysis to identify points of vulnerability to assess the firm's resilience to withstand business disruption and recommends disaster avoidance and mitigation strategies. Developed, review and evaluate System Security Plans (SSP) and Information System Contingency Plans (ISCP) based on NIST Special Publications. Maintained Information Technology Disaster Recovery plan information in a technical continuity planning tool. Participated in the deploying security solutions in the cloud environment. Collaborate with Product Managers, Platform Leads, and Information Security teams, to design and implement cloud security solutions. Developed and reviewed Contingency Plan for cloud based systems. IT Compliance Assessor GAMA October 2014 to July 2015 Analyzed and updated ISCP, SSP, PIA, ST&E, POA&M, BIA, and ISCP Tests. Assisted System

Owners and ISSO in preparing C&A package for companies' IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4. Coordinated with stakeholders to gather contingency plan information and develop system (ISCP) and business (BCP)-focused contingency plans. Conducted Business Impact Analyses (BIA) to analyze mission-critical business functions, and identify and quantify the impact those functions if these are lost (e.g. operational, financial). Designated systems and developed system categorizations using FIPS 199 and NIST SP 800-60 Developed a Business Continuity Plan and managed relationships with vendors of outsourced functions. Conducted NIST Self-Annual Assessment based on NIST SP 800-53A. Performed Vulnerability Assessments and identified corrective actions to mitigate known vulnerabilities. Make sure that risks are assessed, evaluated and a proper action have been taken to limit their impact on the Information and Information Systems. Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages. Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance. Information Security Analyst Quadrant - Reston, VA July 2013 to June 2014 Conducted kick off meetings using the approved IT security framework, FIPS 199/NIST 800-60 to categorize information and information system. Conducted IT Controls risk assessment to identify system threats, vulnerabilities and risk, and generate reports. Developed and Conducted Security Test and Evaluation (ST&E) according to NIST SP 800-53A. Developed a security baseline controls and test plan that was used to assess implemented security controls. Developed System Security Plan (SSP) to provide an overview of the system security requirements and describe the controls in place. Developed Security Assessment Report (SAR) detailing the results of the assessment along with Plan of Action & Milestones (POAM). Created standard templates for required security assessment and authorization documents; Risk Assessment (RA), System Security Plan (SSP), Contingency Plan (CP) and Security Plan (SP). Involve in third party contract evaluation, Review

information security accreditation request. Conducted periodic IT Risk Assessment and Reviewed IA controls for any deficiencies and reported to the ISSO for appropriate mitigation actions. Assisted in the development of an information security continuous monitoring strategy. Conducted Business Impact Analysis (BIA) to identify mission critical functions and high-risk areas where audit efforts would be focused. Education M.B.A in Business Administration Anglia Ruskin University B.S. in Computer Science Kwame Nkrumah University of Science and Technology Skills Access Control (Less than 1 year), Authentication (Less than 1 year), Contingency Planning (Less than 1 year), Security (4 years), system security (3 years) Additional Information Develop Certification and Accreditation documentation in compliance with NIST and organizational standards. Develop, review and evaluate System Security Plans (SSP) and Information System Contingency Plans (ISCP) based on NIST Special Publications. Perform comprehensive assessments and write reviews of management, operational and technical security controls for audited applications and information systems. Develop and conduct Security Test and Evaluation (ST&E) according to NIST SP 800-53ACompile data to complete Residual Risk Report and to insert contents into the POA&M. Ability to multi-task, work independently and as part of a team. Strong analytical and quantitative skills. Effective interpersonal and verbal/written communication skills. Identify deficiencies in accordance with OMB Circular A-123, Appendix A. Software/Platform/Artifacts MS Office suite, Visio, SharePoint, FIPS 199, E-Authentication, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), Risk Assessment (RA), SSP, ISCP, ST&E, SAR, Plans of Action and Milestones (POA&M), Authorization to Operate (ATO) Letter. Key Skills System Security Contingency Planning Risk Management Authentication and Access Control System Monitoring & Regulatory Compliance

Name: Jeremy Mills

Email: estradasheri@example.com

Phone: 3353565831