

Information Security Assessor Information Security Assessor Information Security Assessor - Eaton Cooperation, MD Gwynn Oak, MD Authorized to work in the US for any employer Work Experience Information Security Assessor Eaton Cooperation, MD December 2016 to Present Conduct kick off meetings using the approved IT security framework, FIPS 199/NIST 800-60 to categorize information and information system. Conduct IT Controls risk assessment to identify system threats, vulnerabilities and risk, and generate reports Develop and Conduct Security Assessment and Authorization (SA&A) according to NIST SP 800-53A. Develop a security baseline controls and test plan that is used to assess implemented security controls Develop System Security Plan (SSP) to provide an overview of the system security requirements and describe the controls in place

Develop Security Assessment Report (SAR) detailing the results of the assessment along with Plan of Action & Milestones (POAM) Create standard templates for required security assessment and authorization documents; Risk Assessment (RA), System Security Plan (SSP), Contingency Plan (CP) and Security Plan (SP) Conduct periodic IT Risk Assessment and Reviewed IA controls for any deficiencies and report to the ISSO for appropriate mitigation actions. Assist in the development of an information security continuous monitoring strategy. Conduct Business Impact Analysis (BIA) to identify mission critical functions and high-risk areas where audit efforts will be focused. Information Security Analyst SLAMM Technologies, VA November 2014 to December 2016

Developed POA&M (Plan of Action & Milestones) to remediate actions resulting from security control assessments, monitored and tracked remediation progress Developed Security Assessment Plans (SAPs) and perform assessment per NIST SP 800-53A. Documented NIST 800-53 security control compliance findings within Requirements Traceability Matrixes (RTMs) and Security Assessment Reports (SARs). Assisted System Owners and ISSO in preparing Security Assessment and Authorization packages for IT systems, ensuring that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4. Prepared and review ATO packages (i.e. SSP, RA, ISCP, PTA, PIA, SAP, SAR, etc.) for continuous operation. Ensured confidentiality, data integrity and availability of systems, networks and data were maintained Completed a Risk Assessment Report

of the failed controls to determine their risk levels for the POAM. IT Auditor True IA LLC April 2013 to November 2014 Conducted Assessment on IT Security Controls to identify system threats, vulnerabilities and risk, and generated reports. Developed Security Assessment Plan (SAP) and Conducted Security Assessment according to NIST SP 800-53A. Facilitated kick-off meetings as well as briefing meetings with system stakeholders throughout the IT Security Control Assessment process. Developed Security Control Assessment report containing passed and failed controls with source and comments for each control. Reviewed penetration test reports for control deficiencies: internal external penetration testing, network and application (including web application) penetration testing, social engineering Assisted in the development of an information security continuous monitoring strategy. Scoped and delivered security-testing engagements on time according to stakeholder requirements. Developed Security Assessment Report (SAR) detailing assessment findings along with recommendations. Education Bachelors in Business Administration in Business Administration Kwame Nkrumah University of Science and Technology Skills Access Control (Less than 1 year), risk assessment (4 years), SAR (6 years), Security (6 years), System Security (2 years)

Name: Lisa Briggs

Email: duranangela@example.org

Phone: 3736712178