

INFORMATION TECHNOLOGY SECURITY ANALYST INFORMATION TECHNOLOGY SECURITY ANALYST INFORMATION TECHNOLOGY SECURITY ANALYST - Baltimore Gas and Electric Baltimore, MD Work Experience INFORMATION TECHNOLOGY SECURITY ANALYST Baltimore Gas and Electric - Baltimore, MD January 2016 to Present support client in creating risk based decision as part of plan of action and milestone, POA&M, remediation. support customers in writing implementation statement as part of system security plan development. Creating, reviewing and updating SOP for assigned systems. Supporting client and creating findings as part of POA&M remediation efforts. Creating and updating Plan Of Action and Milestones, POA&M, to track and correct audit findings. Experience with conducting Risk Assessment (RA) and completing Risk Management Framework (RMF) process to obtain Authorization to Operate, ATO, using NIST SP 800-37R1. Conducted a kick off meeting in order to categorize systems according to NIST SP 800-60 and FIPS 199 into Low, Moderate or High system, assist conduct security control assessment kick-off meetings and populate the Requirement traceability Matrix, RTM, in accordance to NIST SP 800-54. Documenting, reviewing and updating some security artifacts for Authorization to Operate, ATO, artifacts such as: System Security Plan (SSP), in accordance with NIST SP 800-18, security Assessment Report, (SAR), Plan of Action and Milestones (POA&M), memorandum of understanding, Privacy Impact Analysis. Privacy Threshold Analysis, Business Impact Analysis, Incident Response. Experience with vulnerability scanning and penetration testing in accordance with NIST 800-115, using tools like Nessus, WebInspect & Splunk. junior IT Security Analyst SecureInfo Corporation April 2014 to January 2016 Develop Security Assessment Report (SAR) detailing the results of the assessment along with Plan of Action and Milestones (POA&M) while creating the Security Authorization Package. Review the Plan of Action and Milestone (POA&M) with identified weaknesses, timelines, milestones and point of contacts for each based on findings and recommendations from the Security Assessment Report. Prepare recommendation reports that are made available to system owners to remediate identified vulnerabilities during the risk assessment process. Undertake External IT Audits based on ISO 27001 standards. Created e-authentication assessment reports to provide guidance on effective

authentication methods. Undertake security assessments of security and privacy controls using NIST 800-53A Rev4 publication guideline. Assisted in the development of an Information Security Continuous Monitoring Strategy to help in maintaining an ongoing awareness of information security (Ensure effectiveness of all security controls), vulnerabilities, and threats to support organizational risk management decisions. Led in the development of Privacy Threshold Analysis (PTA), and Privacy Impact Analysis (PIA) by working closely with the Information System Security Officers (ISSO), the System Owner, the Information Owners and the Privacy Act Office. Developed an E-Authentication report to provide technical guidance in the implementation of electronic authentication (e-authentication). Developed a system security plan to provide an overview of information system security requirements and describe the controls in place or planned to meet those requirements for FISMA compliance. Education Bachelor's in computer science in computer science University of Duala January 2014 to June 2014 Skills NIST (4 years), Risk Management (4 years), SECURITY (4 years), security plan (4 years), system security (4 years), Cyber Security, Information Security Assessments Technical Support Skills Familiar January 2019 Measures a candidate's ability to apply protocols to identify errors and solutions in order to maintain system function. Full results: [https://share.indeedassessments.com/share\\_assignment/ksjk9pinpbuggg0t](https://share.indeedassessments.com/share_assignment/ksjk9pinpbuggg0t) Indeed Assessments provides skills tests that are not indicative of a license or certification, or continued development in any professional field. Additional Information Skills Experienced doing penetration testing, vulnerability scanning. working with Risk Management Framework and NIST SP 800 series, and the Federal Information Processing Standard, FIPS, document. Perform specific quality control for packages validation of Risk Assessment development, update and reviewing of Authorisation to Operate, (ATO), package document like; system security plan, security assessment report, security control assessment, plan of action and milestone, privacy impact analysis, incidence response, disaster recovery plan, risk analysis, (RA).

Name: Audrey Walton

Email: bryantsylvia@example.com

Phone: 258.932.8266