Cyber Sercurity Analyst Cyber Sercurity Analyst Cyber Sercurity Analyst Greenbelt, MD Work Experience Cyber Sercurity Analyst Department of Labor - Washington, DC August 2014 to March 2019 Created, updated and revised System Security Plans, Contingency Plans, Incident Response Plans/Reports, and Plan of Action & Milestone Developed and completed Security Assessments Kick-off Meetings Briefings and populated the Security Requirements Traceability Matrix (SRTM) and Document Request Lists (DRLs) per NIST SP 800-53r4 Reviewed Privacy Impact Assessment (PIA) and PTA and ensured System of Record Notice (SORN) were published. Assembled Security Assessment Packages to include Security Assessment Reports (SARs), Risk Assessment Reports (RARs), Security Controls Assessments (SCA) Reports and POA&Ms Briefed Authorizing Official on information systems risks and vulnerabilities in support of the Security Assessment and Authorization process. Participated security controls assessment efforts to determine effectiveness (i.e., controls implemented correctly, operating as intended, and meeting security requirements). Evaluated vulnerabilities and risks based on Tenable, Nessus and HP Inspect scans reports Executed Security Impact Analysis/Risk Assessments/Subsystem Addendums in support of new on-premise and Cloud based applications/application systems. Participated in Configuration Management (CM) activities and weekly Change Control Board (CCB) Meetings in support of changes to the authorized baselines for information systems. Monitored security controls post authorization to ensure continuous compliance with the security requirements. Reviewed and updated some of the system categorization using FIPS 199, Initial Risk Assessment, E-authentication, PTA, PIA, SAR, SSP, SAP& POA&M. IT Security Specialist | Robert Half Technology US Department of Transportation - Washington, DC June 2012 to August 2014 Provided input to management on appropriate FIPS 199 impact level designations and selecting appropriate security controls. Oversee the preparation of Assessment and Authorization (A&A) packages for submission to the Authorizing Official (AO) for an Authorization to Operate (ATO). Performed evaluation of policies, procedures, and analyzed security scan results, to address controls that were deemed insufficient during Assessment and Authorization (A&A). Authentication with business owners and Performed Security Categorization (FIPS 199), Privacy Threshold

Analysis (PTA), E-d selected stakeholders. Monitored controls post authorization to ensure continuous compliance in accordance with FISMA guidelines. Generated, reviewed and updated System Security Plans (SSP) against NIST 800-18 and NIST 800 53 requirements. Documented and reviewed System Security Plan (SSP), Security Assessment Report (SAR), Security Plan of Action and Milestones (POA&M), Authorization letter/memorandum (ATO). Developed and conducted ST&E (Security Test and Evaluation) according to NIST SP 800-53A and perform on-site security testing using vulnerability scanning tools such as Nessus. Documented and finalized Security Assessment Report (SAR) and communicate a consolidated risk management activities and deliverables calendar. Applied appropriate information security control for Federal Information System based on NIST SP 800-53, FIPS 199, FIPS 200 and OMB A-130 Appendix III Created, updated and revise System Security Plans, FISMA and FISCAM audits, Contingency Plans, Incident Reports and Plan of Action & Milestone Education Bs in Computer Science University of Buea

Name: Brandon Coleman

Email: kayla73@example.net

Phone: +1-971-332-7116x6725