Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Department of Labor Cheverly, MD Work Experience Cyber Security Analyst Department of Labor - Washington, DC September 2016 to Present Coordinate in-depth interviews and examine documentation/artifacts in accordance with NIST SP 800-53A rev 4. Perform the Federal Information Security Management Act (FISMA) audit reviews using NIST 800-37. Working knowledge of Categorizing Information Systems (using FIPS 199 as a guide), NIST Risk Management Framework, FIPS and FISMA Act. Review and update some of the system categorization using FIPS 199, Initial Risk Assessment, E-authentication, PTA, PIA, SAR, SSP, SAP& POA&M. Participate in ST&E Kick-off Meeting and populate the Requirements Traceability Matrix (RTM) per NIST SP 800-53A. Conduct a Privacy Threshold Analysis (PTA), and Privacy Impact Analysis (PIA) by working closely with the ISSOs and the System Owner. Develop and maintain Plan of Action and Milestones (POA&MS) of all accepted risks upon completion of the system (C&A). Coordinate, participate and attend weekly ISSO forums for security advice and updates. Provide continuous monitoring support for control systems in accordance with FISMA guidelines and conduct FISMA-based security risk assessments. IT Security Specialist | Hilltop Consultant US Department of Transportation Washington, DC June 2014 to August 2016 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. Education BS in Cyber Security University of Buea Skills Cyber Security

Name: Jessica Holloway

Email: rachel93@example.net

Phone: 538-656-7095x93389