IT Security Analyst IT Security Analyst IT Security Analyst - Delloite New Carrollton, MD Authorized to work in the US for any employer Work Experience IT Security Analyst Delloite - Washington, DC June 2016 to Present Provided input to management on 8 systems using appropriate FIPS 199 impact level designations; NIST 800 60 volume 2 as a guide to Categorize the Data types. ? Provide input to management on the appropriate FIPS 199 impact level designations: using NIST 800 60 volume 2 as guide to Categorize the information types based on the Confidentiality, Integrity and Availability (CIA) of the information that the system processes and or stores. ? Identify appropriate security controls baseline on Security Categorization of the Information Systems ? Conduct comprehensive assessments of the security controls employed within or inherited by an Information System to determine the overall effectiveness of the controls. ? Provide IA Support and Risk Management Framework and Continuous Monitoring processes. ? Develop and maintain artifacts supporting the Risk Profile SP, CP, CM, IR and POA&Ms. ? Review and Perform Security Impact Analysis (SIA) for all change requests in the environment ? Responsible for preparing all Assessment and Authorization (A&A) documentation, working very closely with the Information System Security Officer (ISSO), Information System Owner (SO) and the other members of the Information Assurance team. ? Create, update and revise System Security Plans, FISMA and FISCAM audits, Contingency Plans, Incident Reports and Plan of Action & Milestone ? Document results of security assessment in a Security Assessment Report ? Ensure security assessment are completed for each of the information systems that the Authority to Operate (ATO) has expired or about to expire. IT Security Analyst Cyber Coders - Ashburn, VA October 2014 to June 2016 Risk Management Framework (RMF) assessments and Continuous Monitoring: Perform RMF assessment on several different environments at the Dept. of Agriculture using both scanning tools and manual assessment. Assessments include initiating meetings with various System Owners and Information System Security Officers (ISSO), providing guidance of evidence needed for security controls, and documenting findings of assessment. ? POAM Remediation: Performed evaluation of policies, procedures, security scan results, and system settings to address controls that were deemed insufficient during Certification and Accreditation (C&A), RMF, and continuous monitoring.

? Expertise in National Institute of Standards and Technology Special Publication (NIST SP) documentation: Performed assessments, POAM remediation and document creation using NIST SP 800-53 Rev.2 and NIST SP 800-53 Rev.3. ? Developed solution to security weaknesses: Developed solutions to security weaknesses while working on POAM remediation and Corrective Action Plan (CAP) for the US Dept. of Agriculture. Assist ISSOs create solutions to weaknesses based on system functionality and pre-existing architecture. ? Performed on-site security testing using vulnerability scanning tools such as Nessus. Actively working to become a Certified Information Security System Professional (CISSP), June 2019. Education Master of Science in Cybersecurity in Cybersecurity University of Maryland August 2017 Bachelor of Science in Economics in Risk Assessment and Risk Management Nnamdi Azikiwe University June 2002 NIST

Name: Laura Brown

Email: robert76@example.com

Phone: +1-706-637-3259x2581