Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - MBI White Plains, MD Work Experience Cyber Security Analyst MBI - Washington, DC March 2017 to Present Performing categorization of information system using FIPS 199 as a guide or its equivalent NIST SP 800-60 Vol. 2. Review and update System Security Plan (SSP) based on findings from assessing controls using NIST SP 800-18 rev1, NIST SP 800-53a rev4 and NIST SP 800-53. Work with the Information System Security Officer (ISSO) to ensure compliance with information security requirements and obtain an Authorization to Operate for any system to which I have been appointed. Review Technical, Management, Operational and Privacy Security Controls and provide implementation responses as to how the systems meet security requirements. Develop and update Plan of Action and Milestones (POA&M) to remediate all controls that failed Security Testing and Evaluation (ST&E). Assist in developing Contingency plans/Disaster Recovery Plans and Incident Response plan for Information Systems using NIST SP 800 - 34 and NIST SP 800 - 61 rev2. Performed continuous monitoring after authorization (ATO) to ensure continuous compliance with the security requirements using NIST SP 800-137. Performed data gathering techniques (e.g. questionnaires, interviews and document reviews) in preparation for control implementation and assembling A&A packages. Supporting ISSO and CISO with analyzing and evaluating significant cyber security problems, and helping with Plan of Action and Milestones (POA&M) and corrective actions. Review vulnerability scan reports to identify vulnerabilities applicable to systems and applications, determine their severity and urgency, work with system owners to determine whether and/or when corrective action will be taken to remediate vulnerabilities. Providing assistance to "Meeting Management" duties; coordinating meetings to include the reservation of meeting spaces, preparation of reports, agenda items, presentations, minutes and action items. Ensuring that the AO, and CISO are adequately informed about operational system risk such that they can make knowledgeable risk-based decisions. Junior Security Assurance Engineer Saint Corp - Bethesda, MD October 2015 to March 2017 Support NIST Risk Management Framework (RMF) based Assessment and Authorization (A&A) activities. Assist in developing Security Assessment plan (SAP) according to NIST SP 800-53A. Determine security controls effectiveness (i.e., controls

implemented correctly, operating as intended, and meeting security requirements) using the three basic methods of assessment - Examine, Interview and Test (EIT). Assess existing security policies, processes, and templates against NIST guidance. Work alongside security team in testing the system using vulnerability scanning tools such as Nessus. Document findings in the Security Assessment Report (SAR). Conduct risk assessments regularly; ensure measures raised in assessments were implemented in accordance with risk profile, and root-causes of risk were fully addressed following NIST 800-30 and NIST 800-37. Work alongside the ISSO in developing Plans of Action and Milestones (POA&M), to address weaknesses identified during security assessment. Ensure customers are in compliance with security policies and procedures following NIST 800 53 and NIST 800-53A. Assisting in the development of security policies and procedures for the systems, along with ensuring compliance with those policies and procedures. IT Help Desk Support Keliz Services - Washington, DC February 2013 to September 2015 Assist in addressing user access issues. Provide technical assistance and support for incoming queries and issues related to computer systems. Provide employees with incident reference numbers, keep employees informed of resolution steps and problem-solving process. Follow-up with employees to confirm/verify resolution. Assist in setting up workstations. Performed Security Test and Evaluation assessment on customer computer using both scanning tools and manual assessment. Provided support for facility and identified their current security infrastructure and defined future implementation of security related to IT Systems. Education BS in Environmental Management and Biology University of Maryland April 2016 Skills Nessus, Splunk, Ms office, Excel, Outlook, Powerpoint, Word, Information Security, Nist, Cyber Security Certifications/Licenses Security+ A valid IT Specialist certification Additional Information Skills Tools: CSAM, Nessus, Splunk, Operating Systems: MS Office (Word, Excel, Outlook, PowerPoint, Access)

Name: Sharon Evans

Email: vfrey@example.org

Phone: 964.481.4503x3771