Information Systems Security Assessor Information Systems Security Assessor Information Systems Security Assessor - Metters Inc. VA Lanham, MD A skilled and highly organized Security Professional with high ability to adjust quickly to new technologies, environments, procedures and get the job done in a gamut of situations including interfacing with business, and stake holders in a challenging environment. Authorized to work in the US for any employer Work Experience Information Systems Security Assessor Metters Inc. VA January 2015 to Present Work as part of a team to perform System Certifications, Annual Assessments, and Continuous Monitoring Assessments. Experienced in performing system risk management following the NIST risk management framework Conduct security assessment on assigned systems to ensure FISMA compliance following NIST SP 800 publications especially NIST 800-53 and Federal Information Processing Standards (FIPS). Evaluate security controls on information system platforms that include Windows, Linux, UNIX, Databases, and Networks Evaluating and creating System Security Plans (SSP), Contingency Disaster Recovery Plans (CDRP), Risk Assessment Reports (RAR), Security Assessment Reports (SAR) and Executive Summaries. Support higher level employees in research, examinations, investigations, audits, and inspections of security controls for compliance to NIST SP 800 series. Review work of peers to ensure timeliness and quality of work. Support the work of other employees. Coordinate with project lead to plan time, prioritize tasks and use assigned resources. IT Security Assessment Compliance Analyst Lolubyte Inc MD 2014 to December 2014 Serves as an assessor for the program and making sure that Security Control Assessments and other advanced-level Continuous Monitoring Activities are implemented in the environment. Provide professional and security based assistance to the incident response team to ensure that security controls are adhered to as stipulated in security policies and procedures. Validate respective system security plans to ensure that security control requirements are effectively configured in the environment. Coordinate with system engineers to monitor, investigate, log and report systems activities resulting from unauthorized access and possible modification of sensitive data. Collaborate with business and stake holders to develop security control authorization documentations needed to authorize system operations. Collaborate with SOC engineers to scan

the environment for possible vulnerabilities using tools like Nessus and others Experience researching and giving recommendations associated with findings on how to improve the customer's security posture by NIST controls. Monitors and assesses selected security controls in the environment on continuous bases to make sure that changes are authorized and documented. Work with stake holders to develop system contingency plan and ensures that the plan is tested, authorized and maintained. Monitors the introduction and use of commercial or third party software in the environment to make sure that they are inspected and approved for use. Strong written and verbal communication skills including the ability to explain technical matters to a non-technical audience. Flexibility to adjust quickly to multiple demands, shifting priorities to meet business needs and standards. Junior Security Assessment Analyst Acethia MD January 2012 to January 2013 Collaborates with business and engineers to provide advice/technical assistance to security related incidents and system audit related requirements. Work with engineers to analyzes assigned portions of existing IT applications, both hardware, and software, to determine current and future potential for enhancements. Promote awareness of security issues and participate in network/system designs to ensure implementation of sound security principles and application of information security/information assurance policies and practices. Ensures that FISMA requirements are adhered to and collaborates with engineers to generate reports for leadership when needed. Collaborates with SOC engineers to make sure that Nessus scans are run on schedule and results examined to make sure that vulnerabilities are quickly addressed for the security of the system. Identifies problem areas along with a variety of possible solutions and alternatives and submits change recommendations and requests. Assesses and identifies training needs that address activities where gaps in competency exist in either current or new technology. Ensures that all employees are duly trained and cleared to access and use IT infrastructure and equally retrain or recertify when the time comes. Education Master's in Information Systems Security Management Strayer University Military Service Branch: Army Service Country: United States Rank: E4 July 2015 to Present

Name: Kyle Miller

Email: jessicaphillips@example.com

Phone: 001-997-780-3278x99897