Information Security Analyst Information Security Analyst Gaithersburg, MD A certified and subject matter expert knowledgeable in FISMA compliance, risk management framework (RMF), security life cycle and risk assessment. A proven project and team lead with aptitude for good customer service, leadership and excellent communication (both oral and written) skills. Functional areas of expertise include: Security Risk Analyses Application Risk assessment Business Systems Analysis FedRamp Google cloud Business Analyst Systems Risk Assessment System Security Documentation Systems Development Life Cycle SOP Development TECHNICAL AND SPECIALIZED SKILLS Burp Suite, McAfee Vulnerability Manager (MVM), STIG SCAP Checker, Retina Vulnerability Scanner, Nessus Vulnerability Scanner, CIS-CAT Baseline Scanner, Microsoft Baseline Security Analyzer (MBSA), Microsoft Project, Visio, Excel, Word, PowerPoint, Access, Microsoft Windows desktops and servers Work Experience Information Security Analyst System Security Plans, and Security - Frederick, MD August 2015 to October 2017 Developed, reviewed and updated Information System Security Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices. Applied appropriate information security control for Federal Information System based on NIST 800-37 Rev. 1, SP 800-53 Rev. 4, FIPS 199, FIPS 200 and OMB A-130 Appendix III. Conduct systems and network vulnerability scans in order to identify and remediate potential risks. Provided weekly status reports updates to the client. Assigned tasks and track team's progress in order to ensure timely delivery. Provided guidance to team members in order to ensure compliance with task requirements. Reviewed team deliverables prior to delivering to the client. Developed and document Standard Operating Procedures of security related processes within the organization. Conducted annual security assessments of systems in continuous monitoring phase of the security life cycle. Provided back-up technical coverage to the team Security Engineer. Conducted minor application assessments; submitted report to ISSO for approval or denial based on findings. Conducted iPhone apps assessments; submit report to ISSO for approval or denial based on findings. Conducted independent verification and validation (IV&V) of third-party system's ATO packages. Documented system security assessment findings in the Security Assessment Reports

(SARs) and POA&Ms. IT Risk Analyst Hewlett Packard Enterprise Houston TX - Houston, TX July 2012 to July 2015 Developed, reviewed and updated Information System Security Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices. Applied appropriate information security control for Federal Information System based on NIST 800-37 Rev. 1, SP 800-53 Rev. 4, FIPS 199, FIPS 200 and OMB A-130 Appendix III. Conduct systems and network vulnerability scans in order to identify and remediate potential risks. Coordinated and managed team activities during assessment engagements Established schedules and deadlines for assessment activities Held kick-off meetings with ISSM, System Owner and other system stakeholders prior to assessment engagements Prepared and submitted Security Assessment Plan (SAP) to ISSM or System Owner for approval Developed and updated security plan, plan of action and milestone (POA&M) Monitored controls post authorization to ensure continuous compliance with the security requirements Managed vulnerabilities with the aid of Retina, Nessus and MBSA vulnerability scanners to detect potential risks on a single or multiple assets across the enterprise network Created reports detailing the identified vulnerabilities and the steps taken to remediate them. It risk analyst Computer Technical Analyst Hewlett Packard - Houston, TX August 2011 to July 2012 Coordinated and led the design, implementation and evaluation of all phases of highly complex information security solutions and programs for a particular contract or company. Designed audits of computer systems to ensure they are operating securely and that data is protected from both internal and external attack. Made recommendations for preventive measures as necessary. Assessed assigned system to determine system security status. Designs and recommends security policies and procedures to implement; ensures compliance to policies and procedures. Designs training materials for computer security education and awareness programs. Education MS in Information Technology University of Maryland University College MD 2015 Master's in Business Administration in Business Administration University of Maryland University College MD 2014 Bachelor of Science in Biology in COMTIA State University of New York - Plattsburgh, NY 2009

Name: Mary Walter

Email: erin09@example.net

Phone: 001-912-764-8057x879