Senior Security Assessor Senior Security Assessor Senior Security Assessor - ManTech International Corporation New Market, MD Well versed at communicating with stakeholders to provide accurate reporting and information regarding ongoing projects and initiatives. Security Assessment and Authorization professional with strong problem solving and project management skills knowledgeable in Risk Management Framework (RMF), Systems Development Life Cycle (SDLC), Security Life Cycle and Vulnerability Management, using FISMA and applicable NIST standards. Thrive under pressure in fast-pace environments while directing multiple projects from concept to implementation. Core Qualifications Team leadership skills Vulnerability Scan Information Assurance Project Management and Support Security Control Assessment Excellent communication and diagnostic skills Security policies and procedures Risk Assessment Framework Systems Development Life Cycle Business Application User Support FedRAMP Work Experience Senior Security Assessor ManTech International Corporation - Washington, DC April 2016 to Present Responsible for conducting the Security Assessments and Authorization (SA&A) and evaluation of client's information system and software applications, as well as third party Vendors. Perform security assessment of network configurations and recommend corrective actions to mitigate identified vulnerabilities. Report findings and recommendations for corrective action to stakeholders. Perform vulnerability assessments utilizing appropriate security tools and methodologies. Provide weekly project status reports, including outstanding issues to all stakeholders. Conduct assessment and evaluation of security controls of client's third-party system and review of third-party FedRAMP packages to ensure compliance Create reports detailing identified vulnerabilities, recommend corrective measures and ensure the effectiveness of existing information security controls Conduct risk assessments on new projects or existing infrastructure to identify and reduce risk to client's infrastructure to which the system is connected Monitor information system security controls post-authorization to ensure continuous compliance with security requirements Prepare and submit Security Assessment Report (SAR) to all stakeholders Develop schedules and deadlines for projects and control assessment Information Security Analyst Datawiz Cor - Washington, DC July 2015 to March 2016 Developed, reviewed and updated Information Security System Policies, System Security Plans and Risk Assessment Report in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices. Responsible for assessing the management, operational, and technical security controls implemented on an information system via security assessment and authorization (SA&A) methods. Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53 rev 4, SP 800-53A, FIPS 199 and FIPS 200 Conducted systems and network vulnerability scans in order to identify and remediate potential risks.   Coordinated and managed team activities during annual assessment engagement   Coordinated weekly Change Management Board meeting   Established schedules and deadlines for assessment activities   Held kick-off meetings with system owners prior to assessment engagements   Prepared and submitted Security Assessment Plan (SAP) to ISO for approval   Developed and updated system security plan (SSP), plan of action and milestone (POA&M) in CSAM   Monitored controls post-authorization to ensure continuous compliance with security requirements   Managed vulnerabilities using Nessus vulnerability scanners to detect potential risks on a single and multiple asset across the enterprise network   Created reports detailing identified vulnerabilities and the steps to remediate them   Worked with various stakeholders to remediate vulnerability, resolve and close past findings (POAMs) IT Risk Analyst TekSystem - Columbia, MD March 2015 to July 2015   Developed and analyzed security policies, procedures and technical standards including corporate compliance, security training, and end-user awareness   Monitored Medical applications, software, and networks to ensure the integrity, availability, and confidentiality of information and ensured the integrity and availability of IT systems.   Ensured that personnel accessing systems complied with HIPAA (Health Insurance Portability and Accountability Act.   Ensured that systems security measures are taken to protect Personal Identifiable Information (PII)   Enhanced and optimized the existing log monitoring and analysis process to identify, scope, track, and report on potential security incidents, unauthorized configuration changes, and policy violations Network Security Analyst TekSystem - Catonsville, MD October 2012 to March 2015 Assisted clients in developing, reviewing and updating Information Security System Policies, System Security Plans (SSP), and Security baselines in accordance with NIST, FISMA, OMB App. III A-130, and industry best security practices. Conducted network vulnerability assessments, using Nessus vulnerability scans to identify system vulnerabilities and develop remediation plans and security procedures. Identified, responded to, and reported security violations and incidents as encountered. Reviewed and provided findings of Vulnerability scan and Audit log results to management. Investigated potential or actual security violations or incidents in an effort to identify issues and areas that require new security measures or policy changes. Maintained security and the overall data integrity within the company's network systems. Conducted annual employee IA awareness training. System Admin/Desktop Support ValueOptions - Linthicum, MD August 2009 to September 2012 Worked with management to update security manuals and address current concerns. Identified and classified hardware and software issues on systems running Microsoft Operating Systems. Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies. Key Responsibilities: Installed and maintained of Local Area Networks Implemented a company wide PC training and development program Set standards for PC hardware, software and peripherals Recommended and implemented complete desktop solutions Install PC/LAN hardware, software and peripherals Performed network scans in search of vulnerability Education Master of Science University of Maryland, University College - Adelphi, MD 2016 Bachelor of Science in Political Science University of Maryland, University College - Adelphi, MD 2013 Skills SECURITY (8 years), NESSUS (5 years) Certifications/Licenses Security+ April 2015 to April 2021 Additional Information Skills Retina Vulnerability Scanner, Nessus Vulnerability Scanner, Nmap vulnerability scanner, Acunetic web scanner, CIS-CAT, Microsoft Baseline Security Analyzer (MBSA), Excel, Word, PowerPoint, Access, Mac, Microsoft Windows.

Name: Anne Miller

Email: leebriana@example.net

Phone: (418)488-2122x032