IT Security Analyst/ Assessor IT Security Analyst/ Assessor IT Security Analyst/ Assessor

Germantown, MD   Over 5 years of Information Technology (IT) Security Analyst experience supporting Federal Agencies.   Bachelor's Degree in Human Resources/Healthcare Management Experienced in the cyber security disciplines of Continuous Monitoring, Incident Response, and Security Engineering.   Strong working knowledge of a full range of IT security principles, concepts, practices, products, services, and methods for evaluating information system risk and vulnerabilities.

   Prevent, detect, analyze, and respond to security incidents, has operated and analyzed continuous monitoring tools (e.g., Nessus, CSAM, eMASS)   Ability to adapt quickly to changing environments.   Proficient Microsoft Excel, Outlook and Word.   Excellent analytical and problem-solving skills as well as interpersonal skills to interact with customers, team members and upper management   Strong organizational skills.   Strong attention to details.   Ability to work with little to no supervision.   Ability to interact with diverse groups.   Ability to handle multiple tasks Authorized to work in the US for any employer Work Experience IT Security Analyst/ Assessor FDA - Bethesda, MD January 2014 to Present Conduct Certification and Accreditation (C&A) on major applications following the Risk Management Framework (RMF) from Categorization through Continuous Monitoring using the various NIST Special Publications in order to meet Federal Information Security Management Act (FISMA) requirements.   Develop SSPs, SARs, and POA&Ms which were presented to the Designated Approving Authorities (DAAs) to obtain the Authority to Operate (ATO).   Experienced with Splunk   Provide weekly status reports on ongoing tasks and deliverables.   Perform risk assessments to identify the risk level associated with findings.   Review artifacts regarding POA&Ms created by ISSO before closing.   Assist in updates of IT security policies, procedures, standards, and guidelines according to department and federal requirements. Help with updating IT security policies, procedures, standards, and guidelines per the respective department and federal requirements.   Perform cloud and non-cloud system assessments. Support cyber security analysis by conducting Vulnerability Management, Security Engineering, Certification and Accreditation, and Computer Network Defense.   Monitor controls post authorization to ensure constant compliance with the security requirements.   Conduct annual

assessments based on NIST SP 800-53A.   Document findings within RTMs and SARs.   Review and analyzed Nessus Vulnerability and Compliance scan results for remediation.   Monitor security tools and correlated reporting and other appropriate information sources to identify incidents, issues, threats, and vulnerabilities.   Provide daily anomaly and alert reporting from all reviewed tools and sensors.   Provide risk analysis for vulnerabilities and incidents indicating any special issues the vulnerability or incident may present to organizational systems and resources.   Provide Security and Privacy expertise to assist with research and response to security and privacy incidents. Education Bachelor's in HR and healthcare management University of Maryland-University College - College Park, MD September 2014 to May 2017 Skills Microsoft office (10+ years), Windows 7/8/8.1/10 (7 years), Windows Server 2012 R2 (5 years), Linux /Red Hat (5 years), FIPS 199, FIPS 200 (5 years), NIST 800-53 Rev4, NIST 800-30, NIST 800-37, NIST 800-39, (5 years), SSP, ST&E, SAR, POA&M, ATO (5 years), HIPPA (10+ years), Sharepoint (5 years), Nessus Vulnerability Scanning Tool (5 years), Splunk (5 years), Risk Management Framework (5 years), CSAM (5 years), access, security, testing, training, Active Directory, HTML Certifications/Licenses CompTIA Security and CISSP certification in progress

Name: Jennifer Larson

Email: hmejia@example.org

Phone: 991.445.8985