Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - TAKEDA PHARMACEUTICALS Chicago, IL Authorized to work in the US for any employer Work Experience Cyber Security Analyst TAKEDA PHARMACEUTICALS - Deerfield, IL September 2016 to Present Work face-to-face with multiple stakeholders:Planning and participating in a team effort to bring multiple complex projects to fruition in a highly motivated, fast paced environment. Develop SA&A process documents Review IA Security Plans Conduct security risk assessments Conduct in-depth technical reviews of new and existing IT systems in order to identify the appropriate mitigation strategies required to bring these systems into compliance with established policy and industry guidelines. Analyze business models, workflows, and organizational dimensions as they relate to the design, implementation and support of the information system. Provide ongoing gap analysis of current policies, practices, and procedures as they relate to established guidelines outlined by NIST, OMB, FISMA, etc. Knowledge of IT security architecture and design (firewalls, Intrusion Detection Systems, Virtual Private Networking, and virus protection technologies). Contribute to initiating FISMA metrics such as Annual Testing, POA&M Management, and Program Management. MERCHANT E-SOLUTION IT Security Analyst Atlanta, GA November 2014 to August 2016 Conducted Security Assessment and Authorization (SA&A) activities in accordance with NIST and departmental policies Developed and maintained security test plans and results Developed POA&M to address identified vulnerabilities and track POA&Ms for remediation Developed and documented security related processes/procedures Performed vulnerability scanning with Nessus Contributed to initiating FISMA metrics such as Annual Testing, POA&M Management, and Program Management. Evaluated threats and vulnerabilities of each system and ensure proper safeguards are in place to protect information systems Security Assessor MIDDLEGROUND TECHNOLOGIES - Westchester, IL May 2012 to November 2014 Assisted System Owners and ISSO in preparing Certification and Accreditation package for IT systems and ensuring that management, operational and technical security controls adhere to formal and well-established security requirement authorized by NIST SP 800-53 Contributed to initiating FISMA metrics such as Annual Testing, POA&M Management, and Program Management.

Assisted with review of policy, security alerts guidance, regulations and technical advances in IT Security Management. Performed ST&E according to NIST SP 800-53A and recommended solutions Performed vulnerability scanning with Nessus Reviewed artifacts and removed any PII (Personal Identifiable Information) for audit requests Updated and Review standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages Evaluated threats and vulnerabilities of each system and ensure proper safeguards are in place to protect information systems Documented and/or reviewed System Security Plan (SSP), finalized Security Assessment Report (SAR), Security Plan of Action and Milestones (POA&M) and Authorization letter Memorandum (ATO). .knowledged of the Information Systems Security Authorization process, performing Security Authorization activities using National Institute of Standards and Technology (NIST) Special Publication 800-Series guidelines and processes, as well as DoD Information Assurance Certification and Accreditation Process (DIACAP) DoD 8510.01, and FISMA policies and guidelines Communicated effectively through written and verbal means to co-workers, subordinates, clients, and leads Education Bachelors of Science in Mechanical Engineering in Mechanical Engineering KWARA STATE POLYTECHNIC Skills SECURITY, IDS, IPS, NESSUS, NIST

Name: Lisa Lewis

Email: johnny61@example.net

Phone: 001-937-613-6524x0443