

Junior IT Security Analyst Junior IT Security Analyst Security+, Security Control Assessor, Technical Writer Germantown, MD ,NIST SP 800 series and PCI-DSS Subject Matter Expert(SME). Information Assurance leader in Information Security and Risk Management with focus on FISMA documentation, System security evaluation, validation, vulnerability monitoring, risk assessments and audit engagements. Alexandria is an accomplished analyst with over five years of experience in assessing information security risks and coordinating remediation efforts across Health programs. In addition to technical expertise, she has developed strong communication skills in developing strategic partnerships with technical and non-technical stakeholders to meet security requirements.

Work Experience Junior IT Security Analyst Department of Aging - New York, NY July 2016 to Present Conduct Kickoff meetings with System Owners to prepare and advise security control assessments to assess the adequacy of management, operational, and technical security controls implemented. Develop Security Assessment Report (SAR) detailing the results of assessment along with plan of action and milestones (POA&M). Assist in the development of an Information Security Continuous Monitoring Strategy to help agency's in maintaining an ongoing awareness of information security (ensure continued effectiveness of all security controls), vulnerabilities, and threats to support organizational risk management decisions. Review SSP documents from System Owners Assist System Owners with writing compliance descriptions for controls these systems when firewalled from assessors. Ensure that system's security controls, policies and procedures are examined, and validated. Collaborate with System Owners and ISSOs in preparing Assessment and Authorization packages for new systems receiving their ATO or pre-existing systems. IT Security Analyst Deloitte Consulting LLC June 2012 to July 2016 Planned and worked with assessment and compliance teams to conduct assessments and ensure compliance for the agency's Insurance centers, Data centers for low, moderate and high impact systems, and validated their HIPAA compliance based on Policy and Procedures of the Organization. Assessed security controls selection for systems in accordance with the requirements in NIST 800-53A. Conducted FISMA-based security risk assessments for various government contracting organizations and application systems. Planned and worked closely with POA&M teams to remediate Vulnerabilities of

various Insurance center and Data centers. Delivered an assessment of the severity of weakness or deficiencies discovered in information. Led teams to work onsite with each facility's technical team and leadership to ensure recommendations are maximized. Created, revised, and reviewed System Security Plans (SSP), Security Assessment Plans (SAP), Plan of Action & Milestones (POA&M), Security Assessment Reports (SAR) for low, moderate and high systems. Developed POA&M (Plan of Action & Milestones) documents to take corrective actions resulting from ST&E (System Test & Evaluation). Experienced in the Healthcare environment and assessed primarily Federal Health systems. Areas of Expertise and Technologies FIPS 199, NIST SP 800-60, NIST SP 800-53rev4, Security Assessment Reporting (SAR), Plan of Action & Milestones (POA&M), ATO, Windows OS, MS Office Suite, ST&E, Nessus, Wireshark, Packet Analysis, Vulnerability Scanning, Monitoring alerts/SIEM. Education BS in Bachelor of Science Business Administration minor Information Technology Southern Columbia University - Orange Beach, AL Skills security, Microsoft Office Certifications/Licenses Security+ June 2018 to Present

Name: Gabriel Patrick

Email: cassidy50@example.net

Phone: 366-260-2364x285