

Information Security Analyst Information Security Analyst Information Security Analyst - DATAWIZ Corporation Greenbelt, MD Authorized to work in the US for any employer Work Experience Information Security Analyst DATAWIZ Corporation - McLean, VA March 2017 to Present Assist in developing information system documentation in accordance with NIST's' SP 800-18. ? Conducts security controls assessment of government agencies' systems. ? Cooperate with system administrators and IT engineers to mitigate and document weaknesses discovered during systems' vulnerability scans. ? Supporting the ISO in assembling the Authorization package. ? Maintaining the POAM and assisting in the remediation of identified vulnerabilities. Information Security Analyst IAG Technologies - Silver Spring, MD January 2013 to February 2017 Have a very good understanding of SDLC and RMF process. ? Experience with Nessus to scan servers, AppDetective to scan databases, and Webinspect to scan URL's. ? Experience supporting the ISO to assemble the Authorization package. ? Experience developing information system documentation (NIST'S SP 800-18) and other security artifacts. ? Proficiency in understanding the NIST/FISMA compliance requirements, using FIPS 200 and 199 ? Successfully assessed the management, technical and operational security controls. ? Working experience with all the steps of the NIST's RMF, from Categorization of IS through Authorization, to Continuous Monitoring (NIST 800 - 37). ? Experience assessing the A&A artifacts and determining the security posture of system. ? Interface with IT operators and network engineers to mitigate system vulnerabilities discovered in network devices. ? Perform a security impact analysis for every suggested change to the system's configuration. ? Monitor remediation of system vulnerabilities discovered by scanning tools. ? Assist in maintaining plan of actions and milestones (POA&Ms) and the remediation of identified weaknesses and vulnerabilities. ? Maintaining and updating system security documentation as required, in accordance with agency policies and NIST. ? Maintaining an inventory of hardware and software for the system. ? Knowledge of the following security regulations and/or frameworks: NIST 800-53 rev4, 800-37 rev1, 800-53 A rev4, FISMA, 800-18, etc. ? Ensure that the accounts of users are managed in accordance to agency's policies and procedures, and validating common control inheritance of applications. ? Ensuring that security assessment and authorization (SA& A) of

agency information systems are completed in accordance with the published procedures and providing appropriate level of support for SA& A activities. ? Supporting continuous monitoring testing, and the management of the POAM. ? Analyzed vulnerability and baseline scan results on department network. ? Ensuring risk analyses are completed to determine cost-effective and essential safeguards. ? Developing SA & A documentation and assisting with 3PAO assessment where necessary. ? Performing continuous monitoring activities in accordance with agency and NIST continuous monitoring requirements. ? Prepared and submitted SAP to CISO for approval. ? Ensured that security requirements for the agency's information system are met or will be met by a designated dateline. ? Collaborating with the ISO, project team, and the agency information assurance (IA) division to ensure that system security requirements are identified, documented, constructed and validated during the project's life cycle.

IT Technical Support Specialist Marathon Services - Lanham, MD April 2010 to June 2013

Evaluated system potential by testing compatibility of new programs with existing programs. ? Evaluated expansions or enhancements by studying work load and capacity of computer system. ? Improved existing programs by reviewing objectives and specifications; evaluating proposed changes; recommending changes; making modifications. ? Placed software into production by loading software into computer; entering necessary commands. ? Placed hardware into production by establishing connections; entering necessary commands. ? Maximized use of hardware and software by training users; interpreting instructions; answering questions. ? Maintained system capability by testing computer components. ? Maintained historical records by documenting hardware and software changes and revisions. ? Maintained client confidence and protects operations by keeping information confidential. ? Contributed to team effort by accomplishing related tasks as needed.

Education Bachelor's Skills INFORMATION SECURITY (5 years), SECURITY (5 years), FEDERAL INFORMATION SECURITY MANAGEMENT ACT (4 years), FISMA (5 years), NIST (4 years) Certifications/Licenses Certified Authorization Professional 2017 to 2020 (ISC)2 Certification number: ID#580007

Additional Information SKILLS SUMMARY A highly motivated and proficient Information Security Analyst, with ample knowledge in the role of security assessment and authorization from initiation to

continuous monitoring. Skilled in the development of System Security Plans, S.A.P, S.A.R and POA&M, management and vulnerability scanning, in accordance with FISMA, OMB and applicable NIST standards. Has strong writing and verbal communication skills, capable to deliver effective security solutions.

Name: Lisa Hawkins

Email: brandy49@example.com

Phone: +1-481-772-4256x813