

Security Analyst Security Analyst Security Analyst - TEKSystems Columbus, GA Authorized to work in the US for any employer Work Experience Security Analyst TEKSystems August 2015 to Present

- * Scheduled kick off meeting with Stakeholders to help identify assessment scope, system boundary, information types (information process, store or transmitted by the information system), and eventually categorize information system accordingly.
- * Ensured that system's security controls, policies and procedures are examined, and validated.
- * Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures, interview appropriate personnel, and provide recommendations on adequacy, accuracy and compliance with regulatory standards using NIST SP 800-53A.
- * Help guide System Owners and ISSOs through the Security Assessment and Authorization (SA&A) process ensuring that management; operational and technical controls for securing either sensitive Security Systems and IT Systems are in place and are followed according to federal guidelines (NIST 800-53).
- * Other responsibilities included assurance of vulnerability mitigation, training on C&A tools, supporting System Test and Evaluation (ST&E) efforts and other support to the IT Security Office.

Information Security Analyst The Arthur Group June 2014 to August 2015

- * Participated in weekly meeting to discuss the status of the assessment process.
- * Designated systems and categorized its C.I.A using FIPS 199 and NIST SP 800-60.
- * Developed test plans, testing procedures and evidence needed to validate the controls using NIST SP 800-53A.
- * Responsible for the development, implementation, assessment, and monitoring of common controls.
- * Conducted a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by the information systems to determine the overall effectiveness of the controls and the extent to which the controls were implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements.
- * Documented assessment findings in a security assessment report and produced a plan of action and milestones for all controls having weaknesses or deficiencies.
- * Reviewed system and audit logs and liaised with Database Administrators to remediate findings.
- * Monitored Office of Management and Budget and FISMA security requirements.
- * Reviewed existing documents, policies and procedures, and previous assessments

reports. * Established schedules and deadlines for assessment activities. * Monitored controls post-authorization to ensure continuous compliance with security requirement. IT Security Specialist Cyberion Solutions August 2010 to June 2014 * Responsible for ensuring that appropriate operational security posture is maintained for the U.S Department of Education information systems. * Verified and validated security categories for various information systems. * Coordinated with the information system owners in the continuous monitoring of DOE information systems and its environment of operation to include developing and updating the security plans, managing and controlling changes to the systems, and assessing the security impact of those changes. * Ensured that awareness and training materials are reviewed periodically and updated when necessary. * Provided guidance on security authorizations. * Performed Vulnerability Assessments to ensure that risks are assessed, evaluated and proper actions have been taken to limit their impact on the Information and Information Systems. * Provided security consulting and advisory services to business units and project teams. * Developed and maintained relationships with internal and external customers to formulate information security governance solutions. * Researched and maintained knowledge base regarding information security issues, solutions and potential implications. IT Support/ Help Desk University of Maryland University College January 2010 to August 2010 * Monitored and maintained technology to ensure maximum access. * Responsible for receiving, resolving, escalating and monitoring user issues/requests. * Provided immediate assistance and problem resolution, as needed for service inquiries concerning utilization and information regarding all client computer system applications, telephone, personal computers and mobile devices. * Maintained log and/or list of required repairs and maintenance. * Provided network accounts and passwords as required. * Monitored security of all technology. * Advised staff of security breach and/or change in password or security status, and performed training in regards to security. Education Bachelor of Arts in Anthropology Miami University - Oxford, OH August 2007 to May 2011 Additional Information * Develops FISMA compliant security policies and procedures * Perform Certification and Accreditation in compliance with company/ organization standards * In-depth knowledge of NIST, and related Special Publications * Perform

comprehensive assessments and reviews management, operational and technical security controls for audited applications and information systems. * Strong analytical skills, quantitative skills, and excellent verbal/written communication skills * Ability to multi-task, prioritizes daily duties, and meet strict deadlines * Highly adept to learning new technologies * Effective in communicating and working with diverse groups

Areas of Expertise * FIPS 199/ FIPS 200 * NIST Special Publications (NIST SP) * COSO/COBIT * Sarbanes-Oxley Act * SAS-70 * Security Categorization (SC) * Continuous Monitoring (CM) * Security Assessment Reporting(SAR) * Plan of Action & Milestones (POAM) * Certification & Accreditation (C&A)

Skills and Certifications * Proficient in Microsoft Office Suite (Ms Word, Ms Excel, Ms PowerPoint, Outlook and Share Point) * Nessus Security Scan * SY0-401: CompTIA Security+ Certification: Expected November, 2016 * CISA Certification expected December 2016

Name: Ronald Thompson

Email: bryanttyler@example.org

Phone: 971.591.7303x9382