IT Security Analyst IT Security Analyst IT Security Analyst - Alion Science Inc Baltimore, MD A Cyber Security professional knowledgeable in risk management framework (RMF), systems development life cycle (SDLC), security life cycle, and vulnerabilities management using FISMA, and applicable NIST standards. Organized, Solutions-focused, deadline-focused, team oriented, work well independently, or in team providing all facets of computer supports with in-depth knowledge and understanding of numerous software packages and operating systems. A proven ability with aptitude for good customer service, leadership, excellent communication skills. Specialized in providing IT security expertise and guidance in support of security assessments and continues monitoring for government (FISMA & NIST) and commercial clients Functional areas of expertise include: Assessment and Authorization (A&A) Certification and Accreditation (C&A) IT Security Compliance Vulnerability Assessment Network Vulnerability Scanning Information Assurance Systems Risk Assessment Systems Development Life Cycle Technical Writing Project Management and Support Authorized to work in the US for any employer Work Experience IT Security Analyst Alion Science Inc - Laurel, MD November 2017 to Present Responsibilities: Performed, developed, reviewed, and updated Information Security System Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA and OMB Provided security expertise and guidance in support of security assessments Prepared and reviewed A & A packages for information systems. Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53, FIPS 199, FIPS 200 and OMB A-130 Appendix III. Reviewed authorization documentation for completeness and accuracy for compliance. Facilitated Security Control Assessment (SCA) and Continuous Monitoring Activities Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4 Ensured cyber security policies are adhered to and that required controls are implemented Developed resultant SCA documentation, including but not limited to the Security Assessment Report (SAR) Authored recommendations associated with findings on how to improve the customer s security posture in accordance with NIST controls Ascertain all FISMA documents are updated within 6months of a new policy release Assisted team members with proper artifact collection and detail

to clients examples of artifacts that will satisfy assessment requirements Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies Updated and reviewed A&A Packages to include Core Docs, Policy & Procedures, Operations and Maintenance Artifacts, SSP, SAR, FIPS 200, FIPS 199, POA&M, CPTPR, BIA, PTA, PIA, and more Uploaded supporting docs in the System s Artifact Libraries, Google Docs, and CSAM Updated, reviewed, and aligned SSP to the requirements in NIST 800-53, rev4; so that assessments can be done against the actual requirements and not ambiguous statements Managed vulnerabilities with the aid of Nessus vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network Reviewed SAR post assessment; created and completed POAM s milestones to remediate findings and vulnerabilities Monitored security controls post authorization to ensure continuous compliance with the security requirements IT Security Analyst Lentech LLC - Silver Spring, MD December 2015 to September 2017 Responsibilities: Investigate use and configuration organizationally of multiple business process tools, and create gap analysis on current solution vs. ideal solution Communicate analysis, design, and specifications both functional and technical to all supporting organizations Collaborate and direct efforts within Quality Assurance to ensure desired results Develop innovative solutions to meet the needs of the business that can be reused across the enterprise creating the environment for consolidation of tools to robust, customizable solutions Supported client Security policies and activities for networks, systems and applications including Vulnerability Management, Incident Reporting, Mitigation, and Continuous Monitoring Supported all Assessment and Authorization (A&A) phases and processes Proven ability to support the full life-cycle of the Assessment and Authorization (A&A) process Developed, reviewed, and updated Information Security System Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices

Worked independently and on teams to implement HMS Software applications adhering to HMS defined best practices and customer design plan. Solve unique and complex problems with broad impact on the business Identify dependencies across programs, milestones, systems, and solutions Coordinate effort across business, technical, and program teams Software

Implementation Consultant Plantek Consultants - Annapolis, MD February 2015 to November 2015 Responsibilities: Managed numerous of clinical and financial applications and projects within the specifications of a project schedule Researched & resolved client open issues Provided support to end users on a variety of system application. Identified, researched, and resolved technical problems. Documented, tracked and monitored the problem to ensure a timely resolution Managing the planning, development, testing, implementation, maintenance, administration, performance, stability, disaster recovery, availability, support and documentation of various departmental and enterprise wide mainframe, midrange, web-based, and client-server based systems Identifying and providing tools and standards for gathering data for use in trend analysis and reporting Ensuring that an IT industry standard system development life cycle project management technique is used in all software application implementation, enhancements and development Managing Software Configuration Management to establish and maintain consistency of a system s or product s performance and its functional and physical attributes with its requirements, design and operational information throughout its life Managing and directing software support specialists, application specialists, programmer analysts and Database administrators Allocating resources to accomplish goals and objectives through assigned staff Selecting, training, mentoring and evaluating staff Effectively utilizing team member to their fullest potential, while motivating the team to work together in the most cohesive and efficient manner Reviewed work for completeness and technical accuracy Education Bachelor's in Cyber- security Management and Policy University of Maryland-University College - Largo, MD May 2021 Associate in Political Science Community College of Baltimore County - Essex, MD September 2010 to May 2013 Information systems and developed Security NIST Skills Security (3 years), security policies (3 years), System Security (3 years), It Security (4 years), Information Security (3 years), Cyber Security (4 years), SEC (3 years), Cybersecurity (3 years), NIST (3 years), Information Assurance, Comptia, FISMA (3 years), FedRAMP (1 year), Network Security (3 years) Certifications/Licenses Security+ Additional Information SKILLS - Ability to establish and maintain effective working relationships with clients and co-workers - Skills in interviewing users to help analyze and resolve

issues - Strong organizational, analytical and planning skills - Ability to read and interpret system security policies, rules and regulations - Ability to communicate security and risk-related concepts to both non-technical and technical audiences - Strong communication (verbal & written) and presentation skills

Name: Derek Miller

Email: smithronald@example.net

Phone: 485-609-1637