

Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - System High Corporation
Bowie, MD Skilled Information Security Analyst with expertise in risk management unauthorized
access viruses and a wide range of vulnerabilities and threats. Well-versed in direct and remote
analysis with strong critical thinking communication and people skills. Able to thrive in fast-paced
and challenging environments where accuracy and efficiency matter. Core Qualifications

Assessment and Authorization (A&A) Certification and Accreditation (C&A) IT Security
Compliance Vulnerability Assessment Vulnerability Scanning Information gathering

Information Assurance Risk Assessment Systems Development Life Cycle Project
Management and Support Analysis and reporting Technical and Specialized Skills Nessus

Vulnerability Scanner, RiskVision, AWS, Oracle Database, Microsoft SQL, LINUX/UNIX OS, Mac,
Microsoft Windows, Excel, Word, PowerPoint, Access, MS Project, MS Visio, and VMware, Oracle
virtual box, CSAM, Microsoft SQL Server Management Studio, NextGen, eMass Work Experience

Cyber Security Analyst System High Corporation - Chantilly, VA February 2018 to December 2018

Identify security risks through the analysis of known information Assess the Cyber Security risk of
IT systems documenting them in formal risk assessments and supporting artifacts associated with
the A&A process Use of RiskVision to view SSP, assist in generating PO&AM, Generated SARs

and SAPs. Organize, develop, and present security briefings, written summaries, and written
reports incorporating narrative, tabular, and/or graphic elements on A&A activities Implement IT
security solutions and assure successful implementation Apply knowledge of security principles,

policy, and regulations to daily tasking Developed IT security policy guides for the VA and model
templates. Used Risk Vision(GRC) for responding and receiving questions Provide IT security

analysis support to cross-functional project teams to ensure that VA security policies, processes,
and controls are adhered to, planned for, implemented throughout the project lifecycle, and provide
strategic cyber security support for OIS Support projects from initiation and throughout the

development lifecycle to provide hands-on security subject matter expertise and support to include
assisting in knowledge transfer, VA Agency specific security policy and controls coaching, and
drafting of security documentation. 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 Research policies, procedures, standards, and guidance, and applies needed changes under specific conditions for the protection of information and information system Experienced with Cyber Security document management and familiar with security and privacy rules associated with Risk Management Framework and NIST 800-53rev4 Experienced in security analysis and information assurance IT Security Analyst Medstar - Washington, DC May 2014 to February 2018 Supported client Security policies and activities for networks, systems and applications including Vulnerability Management, Incident Reporting, Mitigation, and Continuous Monitoring Supported the development of security policy guides for the organization. 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 Knowledge and hands-on experience with cloud-based solutions like AWS Experience with Security operations centers 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 Direct experience with formatting, customizing, and providing feedback for documentation relating to Information Assurance & IT Security Vulnerability Provided security expertise and guidance in support of security assessments. Supported A&A (C&A) activities according to the A&A project plan Review, analyze and evaluate business system and user needs, specifically in Authorization and Accreditation (A&A) 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 Validated information system security plans to ensure NIST control requirements are met 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 Assisted team members with proper artifact collection and detail to client's examples of artifacts that will satisfy assessment requirements 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 Collected Operation and Maintenance artifacts on an ongoing basis so that Security Control Assessment (SCA) is seamless 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 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 Johns Hopkins - Columbia, MD March 2013 to May 2014 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 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 Solve unique and complex problems with broad impact on the business Provide time estimates at various levels of confidence for tasks from initiation through development Identify dependencies across programs, milestones, systems, and solutions Coordinate effort across business, technical, and program teams

Services Manager Visual Eyes - Mitchellville, MD June 2012 to March 2013 Supervised staffs Conducted periodic program evaluations for departmental policies, procedures, quality

standards, and safety standards Coordinated staff meetings to discuss operational performance
Coordinated training sessions for new users Developed, presented and implemented new financial
strategies through marketing Conducted deposits and insurance inquiries Assisted clients in
selecting frames based on prescription from optometrist Project Manager Medstar - Olney, MD
March 2011 to June 2012 Utilized EMRs such as: IDX Scheduling, Cerner and Centricity
Monitored projects and reports to project managements about progress Directed staff, recruited,
and trained new employees Performed training, interviews and staff development Coordinated
monthly meetings to discuss operational activities with staff members Used Microsoft Excel to
keep track of financial transactions within the medical practice Monitored billing and coding of
procedures Responsible for processing payroll, accounts payable and accounts receivables
Responsible for obtaining prior authorization and pre-service reviews from insurance companies
Clinic Services Coordinator Medstar National Rehabilitation Network - Chevy Chase, MD July 2010
to March 2011 Conducted periodic program evaluations for departmental policies, procedures,
quality standards, and safety standards Responsible for controlling, reviewing, and improving
billing procedures Reviewed electronic medical records Managed the achievement of
established goals and objectives and adheres to department policies, procedure, quality standards,
and safety standards Coordinated policy information and assisted in implementations Education
Master of Science in Cyber Security Technology University of Maryland - College Park, MD 2018 to
Present Master of Science in Health Care Administration University of Maryland - College Park, MD
2014 to 2016 Bachelor of Arts in Psychology University of Maryland Baltimore County - Baltimore,
MD 2007 to 2010 Skills SECURITY (6 years), SECURITY POLICIES (5 years), SYSTEM
SECURITY (4 years), CLIENTS (Less than 1 year), INTERVIEWING (Less than 1 year)
Certifications/Licenses CISSP CAP AWS Certified Developer-Associate November 2018 to
November 2021 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 Strong communication (verbal &
written) and presentation 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 ability to multi-task

Name: Anthony Miles

Email: jamesjones@example.com

Phone: 407.869.8815x7493