IT Security Analyst IT Security Analyst IT Security Analyst - USDA Upper Marlboro, MD Skilled Information Security Analyst with expertise in risk management framework (RMF), systems development life cycle (SDLC), risk management, and vulnerabilities management of 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. Functional areas of expertise include: Assessment and Authorization (A&A) IT Security Compliance Vulnerability Assessment Vulnerability Scanning Security Test and Evaluation (ST&E) Certification and Accreditation (C&A) Risk Assessment Systems Development Life Cycle Technical Writing Project Management and Support Work Experience IT Security Analyst USDA - Beltsville, MD December 2013 to Present - 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 - 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) - Perform internal audits of the systems prior to third party audits - 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 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 - Collected Operation and Maintenance artifacts on an ongoing basis so that Security Control Assessment (SCA) is seamless - 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 Capital One - Washington, DC August 2010 to November 2013 - 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 - 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 - 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 Project Manager (Intern) PG County Office of Community Relations - Upper

Marlboro, MD February 2009 to August 2009 - Assisted and supported division(s) in development of business projects, Business Communications, Analytics, and General Business - Prepare spreadsheets with data interpretation - Performed related duties in support of project efforts, such as design, monitoring, data extraction, research and reporting in areas of performance monitoring, outcomes and compliance with policies and rules. - Provided support with project meetings by scheduling project meetings, assisting with project documentation, documenting meeting minutes, and project action/task items. - Created and analyzed process workflows to increase efficiency with cross-functional divisions and departments; communicate project/program manager requirements; analyzing data trends, and creating reports. Education Bachelor of Science in Social Work Bowie State University - Bowie, MD May 2011 Information systems NIST Master of Science in Management Information Systems Bowie State University - Bowie, MD Additional Information Technical Skills Nessus Vulnerability Scanner, Mac, Microsoft Windows, Excel, Word, PowerPoint, Access, MS Project, MS Visio, and VMware, Oracle virtual box, CSAM, Accellion/WatchDox secure file solution. 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: Richard Tran

Email: ucannon@example.net

Phone: 889-844-9597x537