IT Security Analyst IT Security Analyst IT Security Analyst - Applica Inc Washington, DC Work Experience IT Security Analyst Applica Inc - Washington, DC October 2016 to Present Tailor Security controls to NIST SP 800-53rev4 for legacy systems or FedRAMP for Cloud Systems, with due cognizance of the mission-minded security controls matrix important to the System Owner's mission. Operate NIST 800-37 - the six-step FISMA Risk Management Framework; using NIST SP 800-series including but not limited to NIST SP 800-60 (or FIPS 199), NIST SP 800-53rev4 Appendix D & J (or FIPS 200), e-Authentication with NIST 800-63, NIST SP 800-18A, NIST SP 800-53A, NIST SP 800-30, NIST 800-34, NIST SP 800-137 etc. Provide support and guidance to System Owners through the various phases of System Certification and Accreditation FISMA-related deliverables including System Security Plans (SSP), Security Assessment Reports (SAR), Contingency Plans, Contingency Test Reports, Plan of Action & Milestone (POA&M) Reports, etc. PTA & PIA as necessary. Assess & secure Authorization to Operate (ATO) for new Cloud Case Management Platform (CMP) - a PaaS in Appian GovCloud, and re-assess integrated cloud application hosted on AWS IaaS. Conduct System Impact Analysis (SIA) and Business Impact Analysis (BIA) ahead of every deployment from Stage to Production, also thereafter for every release. IT Security Analyst/ Security Policy Analyst VMD Systems - Washington, DC April 2012 to October 2016 Provide support in the development and implementation of security policies and procedures. Develop, implement, and communicate IT security policy, standards, best practices, guidance and procedures. Develop IT security related policy briefings, presentations and white papers for distribution to the organization. Provide support and guidance to System Owners through the various phases of System Certification and Accreditation FISMA-related deliverables including System Security Plans (SSP), Security Assessment Reports (SAR), Contingency Plans, Contingency Test Reports, and Plan of Action & Milestone (POA&M) Reports. Draft, finalize, and submit Privacy Threshold Assessments (PTA), Privacy Impact Analyses (PIA), E-Authentication and FIPS199. Provide written responses, analyses and recommendations to audit reports Track the status of previous year's findings and new findings to ensure all items were accounted for and documented. Manage DOL, annual security awareness training requirements and track status of

over 1600 users through several different internal offices for compliance with the annual training requirement. Provide ongoing gap analysis of current policies, practices, and procedures as they relate to NIST, OMB, and FISMA guidance. Track and monitor Plan of Actions and Milestone (POA&M) tasks utilizing the Cyber Security Assessment and Management (CSAM) tool. Provide software security services IT Security Analyst MedTrends Inc - Washington, DC September 2010 to May 2012 Managed FISMA Security Compliance using NIST Standards for all of the 25 OSDI Major and Minor applications and working closely with senior federal staff resulting in consistent quality in security deliverables. Managed the full breadth of the System Security Lifecycle process including developing and updating FIPS 199 Security Categorization, Security Categorization Worksheets, Privacy Impact Assessments, E- Authentication Risk Assessments, Contingency Planning, Incident Response Planning, Risk Assessments, System Security Plans, Security Controls Testing/ Security Test and Evaluation, Vulnerability Scan Analysis, Plan of Action and Milestones per NIST and DOL Guidance. Used CSAM to perform security tests and evaluations and perform risk management. Reviewed DOL policies and procedures to ensure compliance with standards. Interviewed System Owners, ISSOs, and technical teams to complete risk analysis. Worked closely with the IT Security staff and ISSOs to remediate POAMs, provide mitigation recommendations, and track POAMs. Maintained quality control over all of the solution provider's C&A deliverables while ensuring that extremely tight internal deadlines were met. Provided expert guidance into security issues related to Personal Identify Verification (PIV) and the HSPD-12 implementation. Security Architect Unatek, Inc September 2009 to August 2010 Assisted the System owner with developing the Departmental Enterprise Architecture Management System (DEAMS) security policies, procedures, and processes. Provided System Owner with CSAM reports to track the continuous monitoring tasks for DEAMs. Inclusive of updating the FIPS199, SSP, Risk Assessment, PIA, and POAMs. Compiled the C&A package for review and approval by the authorizing official. Assisted the ST&E team will tailoring security controls based on NIST and DOL guidance. Assessed DEAMS by examining the system, performing hands-on technical tests and vulnerability scans. Reviewed DEAMs enterprise architecture diagrams, network/boundary diagrams, and researched enterprise architecture best

practices. Performed interviews with CIO Security staff, System Owner's, ISSO to complete the DEAMS FIPS199, PIA, SSP, and Risk Assessment using NIST. Reviewed DOL Computer Security Handbook for security policies, procedures, and processes Education Certification in Education Strayer University Skills Information Security, It Security, Cyber Security

Name: Karen Stewart

Email: mrogers@example.org

Phone: (295)412-9954