Information Security Analyst Information Security Analyst Information Security Analyst - TM3 Solutions, INC Gaithersburg, MD A solutions-focused and passionate Security Analyst with over 4 years experience in the Information system arena. Experienced in, Risk Management Framework (RMF), Systems Development Life Cycle (SDLC), with in-depth understanding of FISMA, NIST, and FIPS Work Experience Information Security Analyst TM3 Solutions, INC December 2018 to Present Knowledgeable on Authority to Operate requirements, system security plans (SSP), security assessment reports (SAR), plan of action and milestones (POA&M) and related documentation. ? Perform Yearly Assessments on multiple systems utilizing CSAM tool, HUD Information Technology Security Policy Handbook and System Security Plan. ? Identify and analyze business violations of security policy and standards, perform research by reviewing NIST 800-53 Rev 4 Privacy Controls. ? Initiate POA&Ms with identified weaknesses and suspense dates for each information system, based on findings and recommendations based on Security Assessment Report, System Security Plan & HUD Policy. ? Reviewed FISCAM and A-123 financial audits and prepared high-level overview of what a system owner needs to do to plan and prepare for an audit on one of these policies by a third party ? Assist in developing policies, procedures, or processes that add to the overall effectiveness of the information security program IT Security Analyst I Astra Zeneca August 2017 to November 2018 Intern)   ? Experienced with National Institute of Standards and Technology (NIST) security controls, the governance, risk management, and compliance (GRC) security documentation tool, the risk management framework (RMF), and security compliance processes ? Assisted in Implementing IT security process using Risk Management Framework NIST 800-37, Certification & Accreditation, and Assessment & Authorization document from categorization of information system to monitoring security control ? Familiarity with more than one framework (NIST 800-series, HIPAA, FISMA, FedRAMP other common security control frameworks. ? Ability to assess the organizational impact of identified security risks and recommend solutions or mitigating controls Information Security Analyst Department of Health & Mental Hygiene - Baltimore, MD October 2014 to August 2017 Intern) ? Responsible for monitoring compliance with information security policies by coaching others within the organization on acceptable uses of information technology and how to protect organization systems ? Prepared and reviewed Authorization to Operate (ATO) packages for Medicaid Long Term Services and Support System (LTSS) ? Perform Vulnerability Assessment. Make sure that risks are assessed, evaluated and a proper action have been taken to limit their impact on the Information and Information Systems ? Apprise and analyze System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M) ? Experienced with Federal Information Security Management Act (FISMA) and Federal Information System Controls Audit Manual (FISCAM) criteria Education Project Management Certification University of Maryland University College - College Park, MD April 2020 Master of Science in Health Informatics in Health Informatics Grand Canyon University - Phoenix, AZ May 2017 Bachelor of Science in Health Administration in Technical Tools / Skills Eastern Michigan University - Ypsilanti, MI December 2014 Skills Security, Vulnerability assessment

Name: Diane Stevens

Email: proach@example.org

Phone: 524.907.3647x48000