System Enhancement and compliance manager System Enhancement and compliance manager System Enhancement and compliance manager - Galaxy Medical Services, LLC Lanham, MD I have 5 years of experience as a Cyber Security Analyst developing and updating system security plan (SSP), security assessment plan (SAP), security assessment report (SAR), plan of action and milestone (POAM). Strong understanding of NIST risk management framework (RMF). I have experience assessing security controls based on NIST SP 800-53A guidelines. Other security controls based on NIST SP 800 that I have involvement with are including: NIST SP 800-37, FIPS 199, NIST SP 800-60, FIPS 200, NIST SP 800-53 within the Security Assessment and Authorization process. Software Technologies: The following are software technologies that I have utilized and analyzed. HIPPA, SharePoint, privacy impact assessment, cyber security asset management (CSAM), Nessus. Work Experience System Enhancement and compliance manager Galaxy Medical Services, LLC May 2019 to Present Modification of systems, applications, hardware and application functionality Check systems and review compliance with HIPAA Manage material enhancements for data base and operational functionality, to further ensure compliance of company objectives Measure performance scalability Maryland organizational Campaign Administrative Compliance Communications specialist Maryland Organizational Campaign August 2018 to December 2018 *Contract Established communication tools for elections and related all digital channels. Maintain policies and procedures for compliance analysis. Consume maintenance of security controls and technological assessments through CSAM and Nessus tools. Lead assessments and onsite consulting Consulted on NIST 800 SP 53 Rev 5. Compliance Analyst / IT Consultant U-site Technologies June 2016 to January 2018 I performed vulnerability assessments through Nessus scanner to make sure that risks are assessed and evaluated; I viewed reports of programs and performed scans across the network. Worked closely with compliance departments to screen existing clients and analyze the risk of new clients. I created an adherence to ensure that projects met compliance of policy and security controls in accordance to NIST 53 rev 5 and FIPS 200 Compose detailed assessment results with applying the POA&M, plan of action and milestones. I analyzed and updated 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). I wrote policy procedures interpreting RMF NIST and applicable stages to the system description. Lead department meetings to create a level of transparency to address issues regarding compliance violations and recommend courses of action to resolve the issues. IT Security Analyst ARTHUR GROUP August 2015 to December 2016 I regularly assessed and evaluated proper action to have been taken to limit the impact on the Information and Information Systems. Created standard templates for required security assessment and authorization documents using risk assessment (RA), system security plan (SSP), contingency plan (CP) and security plan (SP). I wrote policy procedures elaborating security controls and explain control failures and success. Developed security baseline controls implemented security controls for different projects and security analyst finding from assessment reports. Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages. Evaluated remediation suggestions and provide consultative support with the implementation of remediation steps, standards and best practices where needed.

Conduct pre and post assessment review write-up for FISMA systems and provide recommendations to system personnel and ITSO. Utilizing NIST SP 800-53 Revision 4 and NIST SP 800-53A revision 4 and conducting security control assessments. Compliance Analyst ACCENTIA December 2013 to January 2015 Performed IT risk assessment and documented the system security keys controls Designed and conducted walkthroughs, formulated test plans tested results and developed remediation plans for each area of the testing in RMF where needed. Wrote audit reports for distribution to management and senior management documenting the results of the audit. Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53 rev4, FIPS 199, FIPS 200 and OMB 130 Appendix III Outlined and assessed threats from assessment through identifying the boundaries in the policy procedure. Conducted systems and network vulnerability scans in order to identify and remediate potential risks. Conducted Security Assessment using NIST 800-53A and write policy procedures with

Developed and Conducted Contingency Plan and Test Developed and updated system security plan (SSP), plan of action and milestone (POA&M) Prepared and submitted security and assessment plan (SAP) to CISO for approval Ensured that established internal control procedures were in compliance by examining reports, records, documentation and operating practices. Attended and recommended security controls for Fed-RAMP Compliance. Education Bachelors of Art in Public Policy St. Mary's College of Maryland May 2014

Name: Jennifer Hill

Email: clarkejamie@example.com

Phone: +1-975-940-6175