Senior Cyber Risk Consultant Senior Cyber Risk Consultant Senior Cyber Risk Consultant - Deloitte & Touch LLC Hyattsville, MD Work Experience Senior Cyber Risk Consultant Deloitte & Touch LLC May 2017 to Present Conduct Cybersecurity organizational Gap Analysis Benchmark Assessment using Deloitte maturity model methodology ? Create Cybersecurity Stakeholder Operating Model for both TIGTA and GAO audits stakeholders ? Create Evidence Plan to assist cybersecurity audit stakeholders in evidence submission ? Create Audit training guide for cyber security stakeholder audit management team ? Conducted ongoing support for the cyber security stakeholders Computer Security Deficiency Action Plan (CSDAP) ? Analyze and update 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) ? Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60 ? Conduct interviews with selected personnel, document and evaluate business processes, and execute audit test programs to determine the adequacy and effectiveness of internal controls and compliance with regulations ? Project Lead in a team of 4, direct and train junior team members on auditing techniques and software ? Assist System Owners and ISSO in preparing C&A package for companies' IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4 ? Conduct cloud system assessments, primarily with AWS (Amazon Web Services) by utilizing FedRAMP and NIST guidelines ? Evaluate the effectiveness of internal control systems and identify areas of improvement, best practices, and lessons learned ? Conduct Self-Annual Assessment based on NIST SP 800-53A ? Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). ? Review and analyze Nessus Vulnerability and Compliance scans, WebInspect scans, IBM Guardian, Burp Suite and DbProtect scans for possible remediation. ? Assess systems of varying scope and complexity and comprised of various technologies. ? Create 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 ? Provide weekly status reports on ongoing tasks and deliverables

IT Security Analyst Genesis Mid Atlantic, Inc June 2015 to May 2017 Conducted Certification and Accreditation (C&A) on major applications following the Risk Management Framework (RMF) from Categorization through Continuous Monitoring using the various NIST Special Publications in order to meet the necessary Federal Information Security Management Act (FISMA). ? Developed System Security Plan (SSP), Security Assessment Report (SAR) and POA&Ms that are presented to the Designated Approving Authority (DAA) in order to obtain the authority to operate (ATO). ? Conducted security assessments on major applications, updated POA&Ms with findings and monitored for remediation deadlines. ? Work on System Interconnection Agreements ? Provide weekly status reports on ongoing tasks and deliverables IT Security Analyst Columbia Technology Partners February 2012 to June 2015 Developed, reviewed and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices. ? Performed vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple asset across the enterprise network. ? Updated IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. ? Performed risk assessments, reviewed and updated, Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Management Plans (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation. (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). ? Monitored controls post authorization to ensure constant compliance with the security requirements Education MBA in Business Administration University of Maryland University College - College Park, MD May 2018 BS in Political Science in Political Science Bowie State University - Bowie, MD May 2014 Certifications/Licenses Certified Information Systems Auditor (CISA) January 2019 to Present CompTIA Security+ May 2019 to May 2022

Name: Samantha Jones

Email: cynthia84@example.org

Phone: 369.570.7711x3794