IA Analyst IA Analyst IA Analyst - Apex Systems Laurel, MD Information Security professional experienced in Information Assurance, Information Security and Risk Management Framework (RMF) package development, NIST Special Publications (NIST SP 800-*), NIST guidance implementation, oversight and compliance. Assists in planning A&A packages, validating IA controls, ST&E, control analysis and risk assessment, risk mitigation analysis and tracking, contingency planning, meeting mandates, directives, reporting, and other security-related processes with respect to Federal regulations such as FISMA act 2002; OMB mandates; Federal Information Processing Standards (FIPS); to ensure that Information Systems and information they process are secure by ensuring the appropriate Controls are properly implemented, working as intended and yield expected results. CompTIA Security+, CASP, CEH, OCA, OCP, OCE, DVA, CSM. TOOLS: ? NIST SP NIST SP 800-18, 800-37, 800-53rev4, 53a rev4, 800-137, 800-30, 800-60, ? FIPS 199 ? VA 6500 ? Risk Management: CSAM, RiskVision (GRC Agiliance), eMASS ? Vulnerability Tools Nessus, Burp Suite, Retina, Web Inspect. ? Operating Systems Unix, Red Hat Linux, Solaris, Windows XP, Windows7, Microsoft Server 2003 ? Databases Oracle DB 9i, 10g, 11g , 11gR2 Microsoft SQL, MySQL ? Microsoft Tools Word, Project, Excel, and PowerPoint. ? Email Systems Microsoft Outlook, Lotus Notes. ? Servers DNS, DHCP, SSH. Work Experience IA Analyst Apex Systems - Austin, TX June 2018 to Present Continuous Monitoring of Information System ? Monthly vulnerability tracking reports from Nessus scan, DB scan, PenTest/WASA and Fortify scans ? Generate a draft PIA and PTA in coordination with the Program Manager and other members of the Project team. ? Review Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA). ? Generate a draft ISAMOU in coordination with the Project team and the contractors. ? Generate Security artifacts such as CMP, IRP, RA & SSP as part of ongoing Authorization process ? Create Initial,Quarterly & Closing response for findings and update the financials, and schedule completion date. ? Complete and update Information System Contingency Plan ISCP ? Perform ISCP Tabletop Exercise and complete the Tabletop After Action Report (AAR) ? Interacts with Project Team to educate and measure security policy compliance. ? Perform Disaster Recovery Plan (DRP) Test ? Develop Signatory Authority ? Update AOSB to keep track of the Information system

security posture in preparation for Authorization. ? Review Fortify scan reports and create findings to track remediation of vulnerabilities from the scan ? Review Nessus Vulnerability scan, Database scan, WASA/PenTest report and track remediation of open vulnerabilities. ? Performed Self Assessment of security controls to enusre that they are properly implemented, working as intended and producing the desired results and create findings for failed controls. ? Review System Documentation Assessment ? Meet with Project team to facilitate review and development of PTA, PIA, ISCP, IRP & ISA/MOU. ? Assistance in coordination and review of FISMA compliant ? Update Status of artifacts-assessment/Continuous monitoring checklist to keep track of the Information system security posture. ? Participated in annual Datacall exercise ? Basic Understanding of Information Security frameworks and best practices (RMF, OMB, FIPS, ISO & NIST). ? Understand encryption system requirements, standards, policies and procedures Information Security Analyst Gigasurge - Columbia, MD January 2015 to June 2018 Conduct security assessment and authorization (SA&A) and annual assessments of GSS, Major/Minor systems, and cloud systems. ? Work face-to-face with multiple stakeholders interviewing, planning, or participating in a team effort to bring multiple complex projects to fruition in a highly motivated, fast paced environment. ? Conduct in-depth technical reviews of new and existing IT systems in order to identify the appropriate mitigation strategies required to bring these systems into compliance with established policy and industry guidelines. ? Prepare and present authorization to operate (ATO) documents (SSP, SAR and POA&M) ? Provide ongoing gap analysis of current policies, practices, and procedures as they relate to established guidelines outlined by NIST, OMB, FISMA, etc. ? Develop and maintain a Standard Operating Procedures (SOP) to create or improve SA&A processes. ? Develop risk management guidelines associated with the SA&A process and recommend improvements to authorization processes. ? Create and manage POA&Ms and provide a quarterly POA&M status. ? Initiate and verify the completeness of authorization or re-authorization of all systems. ? Conduct vulnerability assessments on and review results to verify all systems (servers, workstations, laptops, printers, and network appliances (routers, switches, firewalls, intrusion detection systems, etc.) are in compliance with federal and organizational security requirements. ?

Monitor and stay abreast of current applicable Federal and organization security laws, memorandums, mandates, guidance, and alerts. Information Security Analyst Cymatex Consults LLC - Laurel, MD September 2011 to January 2015 Coordinated and managed team activities during assessment engagements for Major Application Systems and General support systems (GSS). ? Created Security Assessment Plans (SAP) to initiate Information Security Assessment. ? Conducted assessments of security controls on Information Systems by interviewing, examining and testing methods using NIST SP 800-53a rev4 as a guide and documented control findings and status from Risk assessment and recommend solutions with detailed action plans in Security Testing and Evaluation (ST&E) worksheet. ? Reviewed and updated System Security Plan (SSP) based on findings from Assessing security controls using NIST SP 800-18 rev1, NIST SP 800-53a rev4 and NIST SP 800-53. ? Entered control findings and status from Risk Assessment in Security Testing and Evaluation (ST&E) and developed Plan of Actions and Milestones (POA&M) for security controls that should be put in place to remediate vulnerabilities. ? Generated Security Assessment Reports (SAR). ? Developed Contingency plans, Disaster Recovery Plans and Incident Response plans for Information Systems using NIST SP 800 - 34. ? Facilitated Kick off meetings and follow-up meeting with Management during projects. Information Security Analyst MTN - Lagos, NG January 2010 to June 2011 Developed plan of action and Milestone (POAM) through establishment of schedules and deadlines ? Conducted Vulnerability assessment of all network applications and operating system and recommend corrective actions. ? Applied appropriate information security controls for Federal Information System based on ISO 27001 ? Conducted vulnerability and baseline scan using various scanning tools. ? Extensive experience in system Development Life Cycle (SDLC) and Vulnerability Management. ? Consistently achieve optimal utilization of developing, delivering and management operations through process improvement planning and program coordination on complex IT projects. ? Performed Risk Assessment (RA), System Security Test Evaluation (ST&E) and track remediation activities via Plan of Actions Milestones (POAM). ? Held kick-off meetings with the Chief Information Security Officer (CISO), and system owners prior to assessment engagements. Oracle Database Administrator Iris Smart Technology FCT Abuja

January 2008 to December 2009 Troubleshoot and resolved log gap in Data Guard Configuration. ? Experience in applying CPU quarterly patches to different version of databases. ? Experience in Impdp and Expdp and sql loader ? Upgraded Oracle 10g database to 11g & from 11g Database 11.2.0.1 to 11.2.0.3 using patch set ? Knowledge of Oracle Automatic Storage Management ASM ? Ability to diagnose problems and resolve issues across various tiers (application, database, network and server) ? Evaluate new Database technologies and products and recommend to technical management team. ? Managed Undo Table spaces, Redo Logs, Control files and Archive logs. ? Implemented multiplexing control files and redo log files ? Administration of multiple instances of Oracle 10g and 11g databases supported on UNIX ? Managed Oracle real application clusters on unix servers, created services, installation in test and production environment with 2years of experience. ? Planned installation, configuration, management and troubleshooting of Oracle 10g and 11g databases on Linux and Windows OS ? Created databases, table spaces, tables, indexes and other database objects ? Installed and manage Oracle Enterprise Manager ? Installed and configured relevant network components to ensure database access as well as database consistency and integrity ? Troubleshoot and resolved various oracle connectivity issues. ? Documented database structure, changes, problems, issues for future references ? Administered database users' accounts. Created, modified and deactivated users' accounts; assigned and monitored users' access rights. ? Created Test and Development databases following OFA compliance rules. ? Provided database administration on production, testing and development database servers ? Managed Schema Objects. Monitored the user sessions and took appropriate action to kill the inactive sessions. Education MS in Information Technology Information Assurance University of Maryland University College April 2019 BSc in Civil Engineering Ladoke Akintola University of Technology 2007 Skills Information Assurance (9 years), RMF (9 years), Security Control Assessment (9 years), Security Assessment and Authorization SA&A (9 years), Security Artifacts and Documentation (9 years), Security Certifications/Licenses CompTIA Security+, CASP, CEH, OCA, OCP, OCE, DVA, CSM. Additional Information _INTERPERSONAL SKILLS ? Good Verbal and written communication skills. ? Effective problem solving skills with attention to details.

? Ability to work independently or on a team on multiple tasks. ? Strong collaboration skills and result oriented. ? Ability to communicate technical issues to non-technical people. ? Ability to think critically and creatively.

Name: Betty Miller

Email: thompsontonya@example.com

Phone: 227-508-0549x945