IT Security Specialist IT Security Specialist IT Security Specialist - 9 Solutions, Inc MD Expert level understanding of Risk Management Framework (RMF). Highly proficient with producing detailed documentation on processes from a controls perspective. Team Player with excellent communication skills Experience implementing efficient project management processes across a large number of projects and groups. Expert level understanding of compliance frameworks including NIST 800-53 Rev 4 Experience in managing and tracking outstanding remediation issues and working towards timely resolution (POA&M). Possess in-depth knowledge of operations through various roles of increasing responsibilities Work Experience IT Security Specialist 9 Solutions, Inc November 2016 to Present Develop, review and update Information Security System Policies, System Security Plans (SSP), and Security baselines in accordance with NIST, FISMA, OMB, NIST SP 800-18 and industry best security practices. Develop and update System Security Plan (SSP), Privacy Impact Analysis (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 Developed policy and procedural controls relating to Management, Operational and Technical Controls for the Organization. Conduct Security Control Assessment on General Support Systems (GSS), Major Applications and Systems to ensure that such Information Systems are operating within strong security posture. Update IT security policies, procedures, standards, and guidelines according to department and federal requirements. Reviewed and updated some of the system categorization using FIPS 199. Carried continuous monitoring after authorization (ATO) to ensure continuous compliance with the security requirements. Put together Authorization Packages (SSP, POA&M and SAR) for Information systems to the Authorization Officer. Develop Security Assessment Plan (SAP) to initiate Security Assessment for low, moderate and high control information systems. Security Specialist Top Group Technologies - MD September 2015 to November 2016 Provide security guidance and support to Information System Security Officers (ISSO) and other security POCS on the FISMA and NIST process. Interviews System Administrators to assist in generating custom reports and/or artifacts in support of the A&A process. Facilitate the development and maintenance of the Plan of Action and Milestones via

CSAM (Cyber Security Assessment & Management), and supported remediation activities. Manages security documentation deliverables and lead the Assessment & Authorization (A&A) team alongside the government ISSO to provide Security Packages (FIPS 199, System Description, System Environment & Component Inventory, Related Laws, Regulations, and Policies, Rules of Behavior, Privacy Threshold Analysis, Continuous Monitoring Plan, Interconnection Agreements, Business Impact Analysis, Contingency Plan, Contingency Plan Test Plan & Results, Risk Assessment Report, Designation Letters, Security Authorization Letter, FIPS 200, Incident Response Plan, Configuration Management Plan). Develops, coordinates, test and train on Contingency Plans (CP). Reviewed and verify policies and procedures are developed in line with all applicable federal and LOC security standards and regulations. Assists in conducting document reviews of NIST policy documents, and updating procedures resulting from the new guidance (Gap Analysis). Provide training to team mates and individual users on new or modified processes and procedures by demonstrating ability to learn and apply new knowledge quickly and to explain complex technical issues in a non-technical, easy to understand manner. Facilitate engagement with internal and external auditors to support their respective audits. Managed, tracked, reported on, and escalated outstanding remediation items to ensure timely completion (POA&M). Security Analyst Vtronix Tech - Washington, DC June 2013 to September 2015 Performed Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), E-Authentication with business owners and selected stakeholders. Conducted meetings with the IT Compliance team to gather documentation and evidence about their control environment. Counseled to ensure auditing, testing, preventive and reactive measures were being adequately implemented for systems with an active Authorization to Operate (ATO). Developed, maintained, and communicated a consolidated risk management activities and deliverables calendar. Performed comprehensive Security Control Assessments (SCA) and wrote reviews of management, operational and technical security controls for audited applications and information systems. Worked with business process owners to ensure timely identification and remediation of jointly owned risk related issues and action plans. Reviewed, updated and developed required security documentation including but not limited to

System Security Plans (SSPs), Contingency Plans (CP), Plan of Action and Milestones (POA&Ms), Security Assessment Reports (SAR). Education B.A. in French IMO State University September 2007 Lagos State Skills Nist, Fisma, Documentation, Technical documentation, Training, Account management, Problem solving, Written and verbal, Telecommunication, Microsoft office, Cyber Security, Comptia, Information Security, It Security, Cissp Certifications/Licenses CASP

Name: Jerry Burton

Email: ortizmarcus@example.com

Phone: 326.416.6706x0447