SECURITY ANALYST SECURITY ANALYST SECURITY ANALYST - ACCENTURE FEDERAL SERVICES Glen Burnie, MD Over 3 years in Information Systems Development Security Life Cycle and the NIST's Risk Management Framework (RMF) as a methodology to manage the security of information systems, using applicable NIST guidelines and standards. Work Experience SECURITY ANALYST ACCENTURE FEDERAL SERVICES January 2016 to Present   Develops, reviews and updates Information Security System policy documents, System Security Plan (SSP), and Security Assessment Plan (SAP), Security Requirement Traceability Matrix (SRTM), Security Assessment Report (SAR), Security Impact Assessment (SIA), Risk Assessment Report (RAR) and other Security Package artifacts.   Updates Systems Security Plans, as changes are implemented in the system through established configuration management policies. Verified completeness of SSP Implementations statements using NIST SP 800-18 and NIST SP 800-53   Assesses security controls using NIST 800-53A to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome in addition to meeting the security requirements for the system.   Conducts assessment of security controls to assess the adequacy of Management, Operational, and Technical Controls implemented in accordance with NIST guidelines.   Monitors systems security controls after authorization to ensure continuous compliance with the security requirements. SECURITY ANALYST MORGAN STATE UNIVERSITY October 2014 to May 2015   Generated security documentation such as security assessment reports, system security plans, contingency plans; and disaster recovery plans.   Provided security support and evaluation to development teams in order to integrate information assurance/ security throughout the System Life Cycle Development of major and minor application releases.   Applied appropriate information security controls for Federal Information Systems based on NIST 800 Series, 800-37 REV.1, SP 800-53 REV.4, FIPS 199 and FIPS 200.   Created reports detailing the identified vulnerabilities and the steps taken to remediate them.   Provided technical support in the areas of vulnerability assessment, risk assessment, and security implementation.   Ensured that appropriate steps are taken to implement information security requirements throughout the life cycle, i.e., from the requirements definition phase through retirement or disposal.   Installed and configured antivirus

software on desktop and notebooks. Resolved problems on computers running Windows XP, Windows Vista and Windows 7 Operating Systems. Deployed myriads of engineering and scientific analysis applications as needed. Rebuilt computers with new operating systems. Managed company IT asset inventory. Responded to user requests for system and applications issues. Utilized Remote Desktop to solve user-oriented problems. SECURITY ANAYLST May 2014 to August 2014 Conducted system security assessments using security controls relating to cyber security and training (NIST 800 series, FISMA, and FIPS 199 and 200).   Monitored network activities to identify and effectively respond to security threats and incidents using logs and various tools.   Supported in certification and accreditation (C&A), conducting cyber assessments, and incident response (using hardware and software): setup and customized interfaces for analysis   Analyzed user's requirements, concept of operations documents, and high-level system architectures to develop system requirements specifications.   Guided system development and implementation planning through assessment or preparation of system engineering management plans and system integration and test plans. BUSINESS INSURANCE IT ANALYST TRAVELERS INC June 2013 to August 2013   Performed diagnostics and troubleshooting of application issues documented and tacked all support requests in ServiceNow, an enterprise asset management system dedicated to ticketing and managing help-desk requests, tickets/resolutions.   Provided prompt recovery and problem escalation for the exceptions, extrapolating and integrating information within defined boundaries, using multiple system management and problem management tools.   Monitored production systems, scheduling tools, jobs, processes. Service requests including proper management, creation, execution, documentation, and closure of tasks, changes, and requests. Created documentation (SOP) for bringing down processes for deployments without impacting other streams. Education Master of Engineering in Electrical & Computer Engineering Morgan State University - Baltimore, MD May 2015 Bachelor of Science in Electrical & Computer Engineering Morgan State University - Baltimore, MD December 2013 Skills security, HTML, access Additional Information CORE COMPETENCIES   Risk Management Framework (RMF) ? NIST SP 800-37 ? NIST SP 800-39   Security Control Assessment ? NIST SP 800-53 Rev. 4 ? NIST SP 800-53A

Rev. 4   Configuration Management   ? NIST SP 800-128   Continuous Monitoring and Risk Assessment ? NIST SP 800-137 ? NIST SP 800-30   Proficient in Oracle 11g, SQL Fundamentals, Unix/Linux systems, and Microsoft Office Suite

Name: Tina Thompson

Email: megan03@example.com

Phone: +1-359-924-8523x830