IT Security Specialist IT Security Specialist IT Security Specialist - Computer World Services Corporation Fredericksburg, VA Results-driven Information Security Specialist with combined work experience in information Security and Information Technology, seeking a challenging position with a progressive company for continuous career development where my skills and experiences can be further fully utilized in achieving the goals and objectives of the organization. Work Experience IT Security Specialist Computer World Services Corporation December 2016 to Present Ensured Systems compliance to guidance, standards, and regulations such as NIST Special Publications, FIPS, FedRAMP, OMB A-130 Appendix III, DHS 4300A Sensitive System Policy Directives, and other internal and federal regulations and policies. Used the NIST Special Publication (SP) 800-37 Rev. 1 "Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems: A Security Life Cycle Approach" and NIST SP 800-53 Rev. 4 " Security and Privacy controls for Federal Information Systems and Organization" to assess Information System's security controls; measured the effectiveness of controls and identified control gaps. Created reports on compliance with internal policies, controls, and standards, then, provided recommendations for remediation of identified deficiencies. Prepared Security Authorization Packages to include System Security Plan, Contingency Plan and Contingency Plan Test, Configuration Plan, System Design Documentation, Security Assessment Plan, Security Assessment Report, Risk Assessment, and Plan of Action and Milestone (POA&M). Tracked and reported on Plans of Action and Milestones weekly (i.e., findings, continuous monitoring to closure of the deficiency). Managed Vulnerabilities and Compliance (using DISA STIG and CIS benchmark) Scanning using Nessus Professional. Analyzed automated and manual scan results (laptops/desktops, Databases and Web Application); and created Plan of Action and Milestone to remediate identified vulnerabilities. Performed Account/Access Management for personnel's access to Software, Data and Documentation. Management include assessing personnel's Suitability and position sensitivity level in accordance with OBIM policy and Information Memorandum. Developed and updated Standard Operating Procedures (SOPs) for Interconnection Security Agreement (ISA) process, Vulnerability Management (Scanning/Vulnerability count metrics/Remediation) process, Change Management

process, Account Management process. Developed and updated over sixteen ISAs with DHS, Other Government Agencies, and International stakeholders on behalf OBIM. Monitored security controls post authorization to ensure continuous compliance with security requirements. Participated in the Configuration Management process; activities include review of Change Request for potential security implication analysis. Review and analysis of Interface Control Agreement (ICA) document. SECURITY ANALYST Charles E Smith Life Communities June 2009 to December 2016 Performed backup and recovery, migrate database for upgrade and administrative purposes. Retrieve and restore archived data for testing. Troubleshoot database connection, permission, space management, and performance issues. Run trace and gather statistics on SQL statements causing issues. Conducted users training to ensure systems security and increase user awareness. Conducted weekly review of security logs and vulnerability scans on Operating Systems, Databases, Applications and developed Plan of Action and Milestone (POA&M). Ensured all information systems are operated, maintained, and disposed in accordance with internal security policies and procedures. Identified, respond to, and report security violations and incidents as encountered to ensure that senior management is kept apprised of all pertinent security systems issues. Assist with the development and updating of security policies and procedures. Performed compliance Map and Gap Analysis on systems Conducted Risk Assessment on all system changes. Install and maintain security infrastructure, including IDS, log management, and security assessment systems. Perform and create procedures for system security audits, and vulnerability assessments. Monitors security infrastructure for policy violations or security events, and participates in problem management activities. Performs monthly vulnerability scans, maintenance and expansion of related tools, identification of new issues, tracking of remediation efforts. IT SUPPORT ANALYST Target Corporation May 2008 to June 2009 Assembled, troubleshot and repaired computer systems (clone desktop system) as well as network components/devices (LAN/WAN). Monitored Remedy queue for new call tickets to resolve them. Monitored system performance, gathered data, and prepares management reports. Performed installation, configuration and maintenance of client computer software and hardware. This included

local and network printer maintenance, diagnosis and troubleshooting. Creates and maintains user login identification (User ID). Changed file system permissions as outlined in security reports and management of system processes. Configured centralized syslog services for auditing requirements. Provided day-to-day Management of the Help Desk and Network Administration personnel assigned to the Information Technology Department. Support all requirements needs by the engineering staff with respect to Repairs, Office Applications, E-mails, Internet (Support-Desk Administration). Education Master's Skills SECURITY, IDS, INFORMATION SECURITY, IPS, FIREWALLS, Cissp, Cyber Security, It Security, Siem, Nist

Name: Antonio Steele

Email: todddaniel@example.net

Phone: 001-875-787-6752