

Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Top Group Technologies  
Washington, DC Work Experience Cyber Security Analyst Top Group Tech - St. Louis, MO June  
2016 to Present Update and analyze 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) ? Support System Owners and ISSO in preparing Certification and  
Accreditation 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 ? Designate systems and categorize its C.I.A using FIPS 199 and NIST SP  
800-60 ? Perform Self-Annual Assessment (NIST SP 800-53A) ? Perform Vulnerability  
Assessment. Make sure that risks are assessed, evaluated and a proper action have been taken to  
limit their impact on the Information and Information Systems ? 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 ? Performing I.T controls risk assessments that included reviewing organizational  
policies, standards and procedures and provided advice on their adequacy, accuracy and  
compliance with the Payment Card Industry Data Security Standard (PCI DSS) Associate Network  
Analyst Intec Logic Global - Worcester, MA December 2015 to June 2016 Configuration and support  
of network using Cisco routers, switches. LAN, WAN, DNS, TCP/IP, WLAN, NAT, OSPF, EIGRP,  
Port Channels ? R&S Network Services (HSRP, GLBP, VRRP, NTP, DHCP, DNS, NAT, Syslog,  
SNMP) ? Troubleshooting the network and cabling when needed ? Provided telephone, email  
support and field support to internal customers and colleagues providing an excellent level of  
service. ? Ensured that the Web Help Desk system is updated in a timely manner so that the status  
of logged calls can be monitored and problem reporting can be done effectively. This includes  
recording time taken to complete calls. ? Ensured that all daily tasks are carried out according to  
the agreed IT Security Analyst Matrix Solutions - Houston, TX October 2013 to December 2015  
Documented and managed Risks in accordance with SP 800-30 and SP 800-37 using nine steps to  
evaluate the threats, vulnerabilities and security controls surrounding the Information System as well

as the likelihood of an exploit and the impact it will have to systems operations. ? Responsible for monitoring compliance with information security policies by coaching others within the organization on acceptable uses of information technology and how to protect organization systems ? Prepared and reviewed Authorization to Operate (ATO) packages (i.e. SSP, RA, CMP, ISCP, DRP, IRP and PIA) for over 1200 systems and facilities ? Collected and evaluated assessment artifacts in order to determine compliance with the NIST SP 800-53 rev 4 control requirements ? Participated in the FIPS 199 process in which security categorization takes place, and selecting the technical, operational and managerial controls using NIST SP 800-60 guidelines. ? Developed POA&M (Plan of Action & Milestones) document to take corrective actions resulting from ST&E (System Test & Evaluation) Education B.Sc. in Insurance in Insurance Lagos State Polytechnic - Lagos, NG May 2000 Skills SECURITY (4 years), LIFE CYCLE, SYSTEMS DEVELOPMENT, RISK ASSESSMENT (2 years), VULNERABILITY ASSESSMENT (2 years), Cyber Security, Information Security, Nist Additional Information Area of Expertise ? Assessment and Authorization (A&A) ? IT Security Compliance ? Vulnerability Assessment ? Network Vulnerability Scanning ? Systems Risk Assessment ? Systems Development Life Cycle

Name: Amber Jones

Email: maloneerik@example.org

Phone: 915-932-3562