Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - TrustTech Inc Maryland Seeking a cyber security position where attention to detail and dedication to customer satisfaction is paramount. FIVE YEARS INFOSEC SKILLS SUMMARY: Cyber Security analyst with over 5 years of working experience and 6 years of IT exposure. Knowledge of IT security architecture (Firewalls, Intrusion Detection Systems, Virtual Private Networking, and Virus Protection Technologies Working knowledge of NIST 800-53r4, 18, 115, 137, 30, 34, 200, 53Ar4, 60 vol 1&2, NIST 37 RMF, FIPS 199 and FISMA guidelines to comply with Federal and private agencies. Experienced in the development of security plans (SP), Contingency Plans, Disaster Recovery Plans, Incident Response Plans/Training, and Configuration Management. Plans, System Security Checklists, Privacy Impact Assessments, POA&M, Authority to Operate (ATO) letters, FISMA Reports, Standard Operating Procedures (SOP) in accordance with Federal, Agency and Organizational policy, to include FISMA, NIST, OMB, FIPS instructions. Possess in-depth ability performing information Security Risk Assessments and Analysis, Risk Mitigation in large-scale networked application environments. Working knowledge of Network Infrastructures, Data Warehouses, Web Applications, Oracle Databases, Application Servers, Windows and Unix/Linux systems. Excellent analytical and problem solving skills as well as inter-personal skills in interacting with team members, clients and top management as well Ability to work under difficult terrain and meet deadlines in required time frames Good communication and writing skills Certifications & Technical Skills Software: MS Office (Word, Excel, Outlook, Access, PowerPoint) Networking: LANs, WANs, VPNs, Routers, Firewalls, TCP/IP DS/IPS: ISS, Snort by Source fire Vulnerability & Penetration Testing Tools: Nessus Tenable Solutions Vulnerability Assessment and Password Cracking: Cain and Abel Working knowledge of SIEM tools ;Splunk, Archsight, Languard, and Kali Linux Work Experience Cyber Security Analyst TrustTech Inc - Fort Washington, MD September 2011 to Present Duties included: Supporting Senior Security Specialists with analyzing and evaluating significant cyber security problems and supporting with plan of action and milestones (POA&Ms) and corrective actions. Assisting with task on developing and updating Privacy documents in compliance with NIST 800 53 r4 such as PTA, PIA and SORN Creating memos for

POAMs that past Schedule Completion Date (SCD) Supporting client but creating SOPs for systems security controls Developing and/or reviewing Information System Security documentation. Reviewing and evaluating ATO packets for compliance such as RA, CPT, CMP, PIA, SAR, SAP, ATO, PTA, IR, MOU, ISA and POA&Ms, SSP and DRP Identifying vulnerabilities applicable to systems and applications to determine their severity and urgency. Working with system owners to determine whether and/or when corrective action will be taken, and perform necessary actions to verify corrective actions. Assisting with technical writing as applied to the development of draft Certification and Accreditation (C&A/A&A) package elements. Identifying vulnerabilities applicable to systems and applications, determine their severity and urgency, work with system owners to determine whether and/or when corrective action will be taken, and perform necessary actions to verify corrective actions. Conducting the ST&E Kick-off Meeting and populate the Requirements Traceability Matrix (RTM) according to NIST SP 800-53A r4. Experience with NIST standards on cyber security and incident handling (800-63, 800-61) Reviewing and evaluating POAMs for compliance with FISMA as part of continuous monitoring and preparation for OIG Audit Reviewing and updating SSP for compliance with FISMA and supporting client with implementation details as part of ongoing POAM remediation process. IT Security Analyst IT Security Officer (ITSO) Vital Solutions INC - Greenbelt, MD July 2010 to September 2011 Greenbelt, MD. July 2010 to September 2011 Department Interior Duties included: Performed data gathering techniques (e.g. questionnaires, interviews and document reviews) in preparation for assembling C&A/A&A packages. Updated Plan of Action & Milestones (POA&M) and Risk Assessment based on findings assessed through monthly updates. Utilizes the Cyber Security Assessments and Management (CSAM) to record, manage, and assess common threats and vulnerabilities. Tracks and manages POA&M in CSAM. Monitored and analyze Intrusion Detection Systems (IDS) to identify security issues for remediation. Performed vulnerability scanning on web applications and databases to identify security threats and vulnerabilities. Ensured security policies, procedures, and recommendations to comply with NIST, FISMA, organizational guidelines, and technical best practices. Assisted in the development and maintenance of system security plans and contingency plans for all systems under their responsibility  Maintained cooperative relationship with business partners or other interconnected systems  Notify the responsible IT Security Officer (ITSO) of any suspected incidents in a timely manner, and assist in the investigation of incidents, as necessary  Provided ongoing gap analysis of current policies, practices, and procedures as they relate to established guidelines outlined by NIST, OMB and FISMA  Prepared and delivers documentation, reports and proposals to senior level personnel. Education certification in Enviromental Science University of Buea September 2006 Associate Cyber Security Montgomery College

Name: Michael Jones

Email: gwoodard@example.org

Phone: (636)409-4636