Systems Security Analyst (contractor) Systems Security Analyst (contractor) IAT Level III certified (CISA, CAP, Sec +) Arlington, VA To contribute to the mission of the organization by performing analysis and advisory assignments related to the effectiveness of programs and/or the efficiency of the management of operations Work Experience Systems Security Analyst (contractor) Pernix Consulting - Arlington, VA November 2017 to Present Works as a member of a cyber team, and division, that conducts cybersecurity and risk assessments. Proactively mitigates system vulnerabilities and recommends compensating controls. Conducts independent scans of application, network and database and utilizes Managed Security Services Vulnerability Assessment Teams. Contribute to a team of security professionals providing DoS clients with assurance that complex IT systems and networks meet security controls and standards. Provide subject matter expertise support for development of cyber security policy. Plan and execute system security assessments to meet client requirements, analyze results, develop reports to be used to determine system vulnerabilities and risk posture, and provide recommendations for remediation to achieve desired security and risk posture. Mentor and develop assigned validation team members to meet client requirements. Prepare the risk management framework (RMF) security authorization packages needed to achieve system or network authorization. Monitor and respond to security data calls on behalf of the client organization, as needed. Analyze and advise on the risk and remediation of security issues based on reports from vulnerability assessment scanners, patch management tools, and emerging threat information Initiate, coordinate and track the patching and remediation of security weaknesses as they are discovered, via a "Plan of Actions and Milestones" (POAM) Cybersecurity Auditor Department of Defense - Alexandria, VA September 2016 to November 2017 Works as a member of a cyber audit team, and division, that conducts cybersecurity and information system related audits. Performs computer security assessments and evaluations of conventional (1) hardware and software applications/platforms; (2) telecommunications infrastructure; (3) operational practices; (4) utilization of information system resources; and (5) system development and acquisition. Conducts risk assessments to identify possible security violations by analyzing computer assets and establishing security requirements

based on possible countermeasures to achieve an optimum level of security. Executes and analyzes computer security plans and assists with access control techniques for trusted routers, gateways, or firewalls. Communicate the value of IT security throughout all levels of the organization's stakeholders. Reviews existing audit laws and ensures compliance and adherence with laws and regulations. Participates in audits or reviews of DoD IT systems, operational methods, management controls, assessment risks, and other IT related activities. Contributes to audit reports (findings, recommendations, and conclusions) by independently completing assigned sections of the required information and ensuring the technical accuracy of the findings and compliance with established reporting standards. Conduct systems security evaluations, audits, and reviews; participate in network and systems design to ensure implementation of appropriate systems security policies. IT Lead for Liquidations J.Crew - Lynchburg, VA September 2011 to September 2012 Managed a team that ran largescale liquidation operations for the company s wholesale operations. Set-up routers and networking equipment to support point of sale operations. Successfully implemented access controls to company information technology to ensure longevity of programs. Successfully implemented the use of IT programs to solve complex financial equations that would eventually allow our business unit to achieve management goals. Utilized macros in MS Excel to effectively manage financial and sales performance data. Used an automated financial system to facilitate the assessment, evaluate and review of reports, system output, and operational problems. Developed and maintained budgets/cash flow statements and developed pro forma statements based on future projects. These statements were presented to upper management to display the effectiveness of my performance. Established internal controls to create an effective checks and balances system to ensure customer data and money were managed properly . Education B.S. in Accounting Liberty University Lynchburg - Lynchburg, VA MBA in International Business Liberty University Lynchburg - Lynchburg, VA Skills SECURITY (2 years), CRYPTOGRAPHY (Less than 1 year), CSS (Less than 1 year), DISASTER RECOVERY (Less than 1 year), ENCRYPTION (Less than 1 year), System Analyst, Cyber Security, Information Security, Siem, Network Security, Nist, Comptia, Cybersecurity, Linux, It Security

Certifications/Licenses Security+ Certified Authorization Professional Additional Information Technical Skills Knowledge and experience with network and boundary security, cryptography and encryption, wireless network security, email security, incident response and disaster recovery, host based firewall/IDS configuration, and common attack vectors Ability to work with several operating systems: Windows, Mac OS, Linux (Kali, and Ubuntu) Experienced with eMass, Xacta, Nessus, Splunk Programming languages: Some experience Python, HTML/CSS, and Visual Basic. Experience with Information Assurance concepts and processes within the Federal government Strong understanding of and experience with Federal security regulations, standards, and processes including the NIST 800 series, FIPS, FEDRAMP and National Security publications.

Name: Wendy James

Email: craig50@example.net

Phone: (892)933-9160x4824