SECUREDIT SOLUTIONS

Position: **Patching Lead**

Education: B.S. in a Computer Information Systems or Business or a related field

Job Description:
The contractor shall have deep analytical thinking based on research results to assess software patches, registry updates and configuration changes to be applied to varied infrastructure. Provides assessment including cybersecurity, system, and business impact. The ideal candidate will have a good understanding of the cybersecurity implications of when applying patches. Experience supporting servers in a complex enterprise environment. Expertise in deploying patches to systems using WSUS, SCCM, and Azure Automation tools. Candidate should have experience supporting and troubleshooting Windows and Linux Servers.

Responsibilities:

- Serves as a POC for customer relations, acting as a SME in department-level working groups.
- Ensuring adequate program controls are applied to each task area, including scheduling, esource allocation, direction, cost quality control, report preparation, establishing and maintaining records, and resolution of customer complaints.
- Resolving quality, timeliness, and accuracy issues.
- Ensure CDRL quality prior to submission to the Government
- Adjudicating any contractor personnel performance issues with the TPOC and COR.
- Performing project management and business process development functions.

Qualifications:

- 5+ years of experience in Project Management in IT/Computer Network Operations field
- AZ-900
- Demonstrable history of leading successful patching deployments of enterprise class solutions
- skilled at producing technical documents and engineering diagrams, strong written and verbal skills, team focused
- Proficiency in scripting of packaged installation of patches, software, and configuration changes, including power shell automation to improve patch management processes
- History of optimizing pre- and post- patching process to ensure proper implementation without any outages
- Analyze and foresee the side effects of the patch and be able to quantify the risks business impact, and opportunities (for better cybersecurity) when the patch is applied
- Ability to work with product vendors to come up with suitable patch recommendations without compromising systems
- Demonstrated experience in researching, evaluating, developing, designing and implementing patch remediation designs and standards following industry best practices