

Cyber Security Specialists, 1 year + Huntersville, NC., Hartsville, SC

Rate: DOE .

Scope of Work:

The Cyber Security Specialists duties include but are not limited to:
CDA assessment activities:

- Performing or overseeing stages of the cyber security assessment process.
- Documenting key observations, analyses, and findings during the assessment process of critical digital assets (CDAs).
- Confirming information acquired during tabletop reviews and walk-downs.
- Participate in the development and integration of a security development lifecycle to include secure development, testing, and configuration of plant digital applications and technologies. Evaluation CDAs against the NEI 08-09 controls

Cyber Security program development:

- Providing technical expertise in the areas of security risk management, security architectures and implementations, and utilizing effective security risk assessment practices.
- Develop the cyber security program including guidance documents and procedures.
- Develop the cyber security training and awareness program.

Cyber Security Program maintenance:

- Provide cyber and information security consultation to internal business units and support organizations through establishment and maintenance of the nuclear cyber security program.
- Demonstrate technical skills in security risk assessment, requirements development, secure design analysis, architecture assessment and development, and security testing of applications and systems.
- Perform security requirements analysis, engineering design reviews, security testing oversight, and risk remediation planning.
- Perform routine security functions for risk detection, prevention, and response.
- Securing, reviewing and comprehending various system, application and security control configurations (eg. firewalls, VPNs, VOIP, AD, SCADA)

Required Qualifications:

- 2+ years experience performing cyber security assessments under NIST and/or NEI 08-09 requirements.
- IT or engineering technical background in the areas of Network design, Server design and administration, or IT Security.
- Understanding and experience with computer architecture and hardware including but not limited to computers, computer networks, digital process components.
- Understanding and experience with various operating systems and software including but not limited to Microsoft Windows products, QNX, Unix, Linux.
- Understanding and experience with multiple vulnerability tracking methodologies and tools.

- Past nuclear experience and able to pass background and badging requirements
- Ability to communicate effectively both written and verbal
- Strong analytical skills
- SANS or CISSP certification

Desired Qualifications:

- BS degree in Engineering, Computer Science or related technical field with 3 to 5 years experience in cyber security
- Digital System and/or component engineering experience
- Familiarity with 10CFR73.54 and NEI 08-09
- Experience with CDA identification and/or assessments