

|  |  |
| --- | --- |
| **Date:** | **January 26, 2024** |
| **Position Title:** | **Cyber Security Analyst** |
| **Department:** | **Strategic Programs**  |
| **Salary:** | **D.O.E.** |

**Primary Function:**

This position is responsible for designing, developing, documenting, testing, and implementing the cyber security controls necessary to obtain/maintain DoD accreditation on a broad variety of government furnished and commercial off the shelf systems.

**Essential Responsibilities:**

1. Coordinate, develop, and finalize test results required to achieve/maintain and Authority to Operate (ATO) on a broad variety of government furnished and commercial off the shelf systems utilizing the Enterprise Mission Assurance Support Service (eMASS) website for both classified and unclassified information systems.
2. Develop, maintain, and update Plan of Actions and Milestones (POAMs)
3. Manage and perform vulnerability assessments using Tenable ACAS/Nessus
4. Generate Cybersecurity Vulnerability and Compliance reports as necessary.
5. Perform Continuous Monitoring activities (STEP 6 of the RMF process)
6. Support Assessment and Validation activities (i.e., Annual Security Review (ASR), Assessment and Authorization (A&A), etc.)
7. Ability to work as a member of a team and coordinate tasks of team members to ensure the goals of the project are met in a timely manner.
8. Must be able to communicate effectively in the English language.
9. Ability to work with little or no supervision.
10. Perform other duties as assigned.

**Work Conditions:**

The employee should be capable of lifting up to 50 pounds, involving activities like bending, stooping, crawling, and stretching, as necessary for handling materials, equipment, and shelving. The majority of the work will take place in an office setting. The employee may need to travel to various work site locations, where dressing appropriately for client and customer interactions is expected. Some travel is essential to meet the position's requirements.

There may be instances where the employee is required to work in a Secret or Top-Secret space, where the use of personal electronic devices, such as cell phones and smartwatches, are not permitted. This restriction applies up to 50% of the time at Long Wave and up to 10% of the time at Tinker AFB.

**Job Requirements:**

*Minimum Requirements:*

* High School Diploma or Equivalent
* Must hold and maintain DoD approved Cybersecurity workforce certifications as listed in DoD 8570.01 for IAT level II. Security+ is preferred.
* Two (2) years recent experience working with DoD Cyber Security requirements.
* Experience with DoD and Navy IT policies and standards and knowledge of computer equipment evaluation techniques to perform systems analysis and performance analysis assignments.
* Proficient in Microsoft Office to include Word, Excel, and Outlook.
* Proficient in Windows Server Administration, group policy, and registry.
* Proficient in Windows 10/11 Administration.
* US Citizenship.
* Current Secret Clearance (will be validated upon hiring)

*Recommended Requirements:*

* Bachelor’s degree computer science, information technology or related and/or equivalent experience accepted.
* Four (4) years recent experience working with DoD Cyber Security requirements.
* eMASS proficiency.
* Current/Ability to obtain Top Secret Clearance
* SCAP Compliance Checker proficiency
* ACAS Assured Compliance Assessment Solution proficiency
* Proficient in writing Plan of Actions and Milestones
* Familiar with RMF Step 6 requirements and capable of performing said requirements with little to no supervision
* Experience in planning, developing, and configuring information systems based on customer requirements

**To Apply:** https://secure6.saashr.com/ta/6179114.careers?ApplyToJob=537312668

**EOE AA M/F/Vet/Disability**