Stephenson Stellar Corporation

Title: Senior Cybersecurity Engineer **Position ID:** 2024-0001	**Type Position:** Full Time **Annual Salary Range:** $150,000 - $220,000 **Level:** PL4
Primary Location: Chantilly, VA	**Travel Required:** 20% CONUS and HI
Alternate Location: At-home work optional	**Contact:** Ms. Jamie O'Quinn or Ms. Barbara Moyer joquinn@stephensonstellar.org bmoyer@stephensonstellar.org

Company Background: The Stephenson Stellar Corporation (SSC) is a nonprofit research and development organization focused on assuring our nation remains a global leader in the Space Domain. Our mission is to foster technological innovation and provide secure space-based solutions.

SSC is an equal opportunity employer, and all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, age, disability status, protected veteran status, or any other characteristic protected by law.

More information at: www.stephensonstellar.org

Job Description: In this position, you will serve as a Senior Cybersecurity Engineer for multiple programs, with a primary focus on supporting the Space Development Agency (SDA) and providing leadership among teammates and customers. Must have proven knowledge and experience in the cyberspace industry and preferably experience with and knowledge of space-based architecture and the sub-systems of a spacecraft; be able to work effectively on small teams; and be experienced with hands-on scripting, cyber security controls testing, penetration testing, and vulnerability assessments. The ideal candidate will have outstanding problem-solving skills and expertise in ground, space, and communications systems. Under the direction of a Lead Engineer, the candidate will be responsible for supporting multiple research and development programs. The Senior Cybersecurity Engineer will initially focus on supporting our SDA customer with test and evaluation of newly developed and deployed space systems, and performing research in the areas of Defense-in-Depth space architecture, Zero Trust architectures, and multi-level security.

Requirements:

Education:

Required: BS in Computer Science, Computer/Software Engineering, Information Technology, Cybersecurity studies or related

Desired: MS in Computer Science, Computer/Software Engineering, Information Technology, Cybersecurity studies or related

Clearance: Required: TS/SCI

Citizenship: Candidate must be a United States citizen

Required Experience:

- 7 years of experience in the cybersecurity field with focus on cyber evaluations (All layers of the architecture), vulnerability assessments or penetration testing
- 3-5 years of experience programming, performing computer or software analytics, or supporting software testing with knowledge in DevSecOps, Supply Chain Risk Management, and Software Bill of Materials
- 7+ years of experience working with DoD or intelligence community information systems to include cloud environments
- 3-5 years of experience working with space-based systems

Desired Experience:

- 10 years of experience cybersecurity testing and security architecting
- Familiarity with space-based systems and experience performing cyber assessments or evaluations for space based architectures and spacecraft
- Experience performing cyber testing in cloud environments

Required Skills:

- Hands on experience performing cyber test and evaluations and working knowledge of NIST 800-53
- Creative problem-solving skills and ability to lead a team delivering cyber solutions in space or cyberspace domains
- Experience crafting test plans and delivering state of the art reports for executive leadership
- Excellent communicator and ability to work effectively with a team delivering space based cyber engineering solutions

Desired Skills:

- Hands-on programming, scripting or software testing experience (…virtual environments, etc.)
- Networking experience. (firewalls, routers and switch configuration)
- Experience with common programming languages and security suites and tools such as Python, Kali Linux or Caldera and knowledge of agile methodology
- Certifications: Security+ or higher certification that meets DoD 8140/8570 requirements
- Familiarity with cloud native and containerization technologies