Stephenson Stellar Corporation

Title: Senior Enterprise System Lead **Position ID:** 2026-0012	**Type Position:** Full Time **Level:** PL4
Primary Location: To be determined	**Travel Required:** 10% CONUS and HI
Alternate Location: N/A	**Contact:** Technical: taxberg@stephensonstellar.org (Tom Axberg) Human Resource: bmoyer@stephensonstellar.org (Barb Moyer)

Company Background: Stephenson Stellar Corporation (Stellar) 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.

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

Additional information at: www.stephensonstellar.org

Job Description: In this position you will serve as a Senior Enterprise System Lead for the Mission Performance & Security Systems Directorate. The candidate will build and oversee the integration laboratory and enterprise infrastructure that will prove out the next generation of complex solutions for space defense. This is a ground-floor opportunity to stand up a classified development and integration lab from scratch - designing the network architecture, deploying virtualization platforms, integrating hardware-in-the-loop testbeds, and creating the environment where cross-domain solutions are validated before they go operational. The candidate will be the primary technical authority for all lab and enterprise infrastructure decisions and will work alongside software developers, MLS engineers, cloud architects, and government stakeholders to ensure that every physical and virtual environment meets the security, performance, and compliance standards required for classified defense programs. This role is for a candidate who can rack servers, segmenting networks across classification boundaries, writing code, and briefing infrastructure architecture to government partners. Key responsibilities include: (1) Design, build, and operate the development and integration lab from the ground up - virtualization platforms, network infrastructure, and hardware-in-the-loop test environments; (2) Architect network segmentation across security domains, separating CUI, development, and classified enclaves per DoD requirements; (3) Responsible for full lifecycle of lab software and hardware: procurement coordination, installation, configuration, inventory, and decommissioning; (4) Deploy and maintain virtualization and container orchestration platforms for multi-tenant, multi-classification workloads; (5) Integrate cross domain solution (CDS) hardware and software into the development and integration testbed, coordinating with software developers and engineers on emulation and validation; (6) Implement identity management, access control, and authentication services; enable secure remote access for distributed team members; (7) Establish change management processes for infrastructure modifications; and (8) Produce and maintain lab documentation - integration guides, network diagrams, SOPs, and handoff materials.

Requirements

Clearance: Active U.S. Secret clearance required; TS/SCI preferred.

Citizenship: Candidate must be a United States citizen.

Education:
- BS in Software Engineering, Systems Engineering, Computer Engineering, IT, Cybersecurity or a related technical field.
- An advanced degree is preferred.

Experience:
- 10+ years designing, building, and operating lab or enterprise infrastructure for DoD programs.

Required Skills:
- Demonstrated experience with virtualization platforms in classified or air-gapped environments.
- Hands-on network architecture and segmentation for multi-classification environments (VLAN design, firewall config, inter-domain routing).
- Experience managing hardware-in-the-loop or integration testbed environments for defense programs.
- Familiarity with container orchestration and identity/access management in secure on-prem environments.
- Strong understanding of DoD cybersecurity standards and the authorization process for classified systems.
- Proven change management and configuration management process development.
- Strong documentation skills - architecture diagrams, integration guides, SOPs.

Desired Skills:
- Experience with FPGA-based or embedded systems integration in lab environments.
- Experience with MBSE and SysML v2 modeling tools.
- Familiarity with DoD compliance frameworks (RMF, NIST 800-171, CMMC).
- Experience supporting CDS integration or testing.
- Certifications such as CISSP, Security+, or vendor-specific infrastructure certs.
- Experience with space, satellite, or missile defense systems; CI/CD in air-gapped environments.