



Title: Senior Enterprise System Lead Position ID: 2026-0012	Type Position: Full Time Level: PL4
Primary Location: Colorado Springs, CO / ON-SITE	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. This role is centered on engineering new capabilities. The ideal candidate brings a strong technical foundation and applies it to design, build, and lead the development of complex systems that meet evolving mission needs. You will take loosely defined problems and translate them into engineered solutions, guiding both the architecture and the team responsible for implementation. 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) Translate mission needs and high-level requirements into system architectures, infrastructure designs, and implementation roadmaps; (2) Lead technical teams in the design, build, and sustainment of lab and enterprise systems, ensuring alignment with mission and security requirements; (3) Decide and communicate engineering tradeoffs across security, performance, scalability, and cost constraints; (4) Serve as the technical authority for system design decisions, integration strategies, and infrastructure evolution; (5) Architect network segmentation across security domains, separating CUI, development, and classified enclaves per DoD requirements; (6) Responsible for full lifecycle of lab software and hardware: procurement coordination, installation, configuration, inventory, and decommissioning; (7) Deploy and maintain virtualization and container orchestration platforms for multi-tenant, multi-classification workloads; (8) Integrate cross domain solution (CDS) hardware and software into the development and integration testbed, coordinating with software developers and engineers on emulation and validation; (9) Implement identity management, access control, and authentication services; enable secure remote access for distributed team members; (10) Establish change management processes for infrastructure modifications; and (11) 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 ability to design and build systems from concept to operational use, not just maintain existing environments
- Strong systems engineering mindset with the ability to decompose complex problems, define architectures, and drive implementation
- Experience leading technical teams or acting as a technical lead on complex system builds
- Demonstrated experience with virtualization platforms in classified or air-gapped environments.
- Experience managing hardware-in-the-loop or integration testbed environments for defense programs.
- 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.
- Familiarity with container orchestration and identity/access management in secure on-prem environments.
- Certifications such as CISSP, Security+, or vendor-specific infrastructure certs.
- Experience with space, satellite, or missile defense systems; CI/CD in air-gapped environments.