Stephenson Stellar Corporation

Title: Senior Systems Administrator **Position ID:** 2026-0013	**Type Position:** Full Time **Annual Salary:** TBD **Level:** PL3 or 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 Systems Administrator for the Mission Performance & Security Systems Directorate. We are seeking a highly experienced and hands-on candidate to support a defense systems software, hardware, and network integration laboratory. This role is critical to enabling engineers and developers to design, build, integrate, and test complex mission systems in both standalone and cloud-based environments. The ideal candidate brings deep technical expertise across systems administration, networking, and infrastructure, combined with strong organizational and operational discipline required for classified environments. This position requires a proactive problem solver who thrives in dynamic lab settings and can manage multiple systems, configurations, and priorities simultaneously. Additional responsibilities include: (1) Design, deploy, configure, and maintain secure lab environments supporting software, hardware, and network integration efforts; (2) Administer and sustain standalone (air-gapped) and cloud-connected systems across multiple classification levels; (3) Install, configure, and troubleshoot servers, workstations, storage systems, and networking equipment; (4) Support integration of complex systems including embedded hardware, simulation environments, and test platforms; (5) Manage system baselines, configurations, and documentation in accordance with security and compliance requirements; (6) Implement and enforce cybersecurity controls in compliance with DoD policies (e.g., STIGs, RMF, CMMC); (7) Maintain accreditation artifacts and support system Authority to Operate (ATO) processes; (8) Provide hands-on support for system builds, upgrades, patching, and troubleshooting in lab and test environments; (9) Develop and maintain automation scripts and tools to streamline system provisioning and maintenance; (10) Coordinate with engineers, developers, and program teams to ensure infrastructure meets evolving project needs; (10) Monitor system performance, reliability, and security posture; proactively resolve issues; (11) Maintain inventory and lifecycle management of lab assets and infrastructure; and (12) Support incident response, audit readiness, and compliance inspections.

Requirements

Clearance: Active DoD Security Clearance (Secret/TopSecret, with eligibility for SCI as required).
Citizenship: Candidate must be a United States citizen.
Education:

- BS in Information Technology, Computer Science, Engineering or related technical field.

Experience:

- 8+ years of experience in systems administration in complex, mission-critical environments.

Required Skills:

- Demonstrated experience working in classified environments with strong understanding of security protocols and operational constraints.
- Strong hands-on experience with:
  - Linux and Windows system administration
  - Virtualization platforms (e.g., VMware, Hyper-V)
  - Networking fundamentals (routing, switching, firewalls, VLANs)
  - Storage systems and backup solutions
- Experience managing both standalone/air-gapped systems and cloud environments (e.g., AWS GovCloud, Azure Government).
- Proficiency with scripting and automation (e.g., PowerShell, Bash, Python).
- Experience implementing and maintaining security controls (STIGs, SCAP, patching, hardening).
- Strong organizational skills with the ability to manage multiple systems, configurations, and priorities.
- Excellent troubleshooting and problem-solving abilities.
- Strong communication skills and ability to work closely with multidisciplinary engineering teams.
- Linux certifications

Desired Skills:

- Experience with FPGA-based or embedded systems integration in lab environments.
- Experience supporting defense or aerospace integration labs or test environments.
- Familiarity with DevSecOps practices and CI/CD pipeline infrastructure.
- Experience with containerization technologies (e.g., Docker, Kubernetes).
- Knowledge of configuration management tools (e.g., Ansible, Puppet, Chef).
- Experience with cross-domain solutions and multi-level security (MLS) environments.
- Relevant certifications such as:
  - Security+ (required for DoD 8570 compliance if applicable)
  - CISSP, CASP+, or equivalent
  - VMware or Microsoft