



Title: Senior Systems Administrator Position ID: 2026-0013	Type Position: Full Time Level/Salary: PL3 (\$99,000 - \$192,000) or PL4 (\$138,600 - \$276,000)
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, Enterprise Systems Project Manager, and IT Manager. We are seeking a highly experienced and hands-on candidate to support research, development, and 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, on-premises, and cloud-based environments. The ideal candidate brings deep technical expertise across Linux-based systems administration 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) Plan, design, deploy, configure, and maintain secure lab environments supporting software, hardware, and network integration efforts; (2) Install, configure, and troubleshoot servers, workstations, and storage systems; (3) Support integration of complex systems including embedded hardware, simulation environments, and test platforms; (4) Create and manage system baselines, containers, virtualized environments, directory objects, configurations, and documentation in accordance with DoD RMF, ATO, and CMMC security and compliance requirements; (5) Provide hands-on support for system builds, upgrades, patching, and troubleshooting in lab and test environments; (6) Develop and maintain automation scripts and tools to streamline system provisioning and maintenance; (7) Monitor system performance, reliability, and security posture; proactively resolve issues; (8) Maintain inventory and lifecycle management of lab assets and infrastructure; and (9) Support incident response, audit readiness, and compliance inspections.

Requirements

Required Clearance: Ability to obtain a Secret DoD Security Clearance.

Preferred Clearance: Active DoD Security Clearance (Secret/Top Secret, 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.
- 3+ years of DoD/Federal work experience.

Required Skills:

- Demonstrated experience working in CUI, and classified environments with strong understanding of security protocols and operational constraints.
- Strong hands-on experience with: Linux-based system administration in a virtualized environment (e.g., VMware, ProxMox)
- Software maintenance using package management software and compilation from source when required.
- Integration with hardware and software systems covering various operating systems and interfaces.
- Networking fundamentals (routing, switching, firewalls, VLANs).
- Storage systems and backup solutions.
- Proficiency with scripting and automation (e.g., PowerShell, Bash, Python).
- Experience implementing and maintaining security controls (STIGs, SCAP, patching, hardening, CMMC requirements).
- Strong organizational skills with the ability to manage multiple systems, configurations, and priorities.
- Excellent troubleshooting and problem-solving abilities.
- Hunger to learn and develop cross-functional skills.
- Linux certifications (e.g., RHCSA, LFCS, or Linux +).
- DCWF Work Role 451 compliant.

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:
 - DCWF Work Role 651 compliant
 - CISSP, CASP+, or equivalent
 - LFCS and/or RHCSA