Stephenson Stellar
Corporation

Title: Senior Cloud Engineer **Position ID:** 2026-0010	**Type Position:** Full Time **Level:** PL4
Primary Location: To be determined	**Travel Required:** 10% CONUS and HI
Alternate Location: Home office anywhere in USA	**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 Cloud Engineer for the Mission Performance & Security Systems Directorate. We are seeking a Senior Cloud Engineer who has built and operated defense cloud environments at the highest impact levels. This role is about more than cloud architecture - it is about building the secure, compliant, resilient infrastructure that classified defense missions depend on every day. The candidate will make cloud architecture decisions across AWS GovCloud and commercial regions, design network isolation for air-gapped and hybrid environments, manage cross-domain data flow between classification levels, and maintain the compliance posture that keeps workloads authorized to operate. Defense cloud is a different discipline from commercial cloud - network isolation, cross-domain enforcement, and authorization to operate are not considerations here, they are the defining constraints. This is a high-impact role where infrastructure decisions directly enable the secure operation of national security missions in space. Key responsibilities include: (1) Design, deploy, and maintain AWS cloud infrastructure at DoD Impact Levels IL2 through IL5; (2) Architect cloud networking for air-gapped, classified, and hybrid environments - VPC design, cross-account routing, and secure on-prem connectivity; (3) Implement and maintain security controls aligned with DoD compliance frameworks, ensuring continuous authorization and audit readiness; (4) Design and operate cross-domain data flow mechanisms between cloud partitions at different classification levels; (5) Manage IAM architecture - RBAC, credential management, and identity federation across multi-account, multi-region environments; (6) Implement infrastructure-as-code for repeatable, auditable deployments in classified environments; (7) Configure monitoring, logging, and alerting infrastructure for security operations and compliance; (8) Collaborate with MLS engineers on cross-domain solution integration and security label enforcement; (9) Manage cloud cost governance - rightsizing, reserved capacity, tagging enforcement, service control policies, and budget alarms; and (10) Produce and maintain architecture documentation - network diagrams, control mappings, and authorization artifacts for government review.

Requirements

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

Citizenship: Candidate must be a United States citizen.

Education:

- BS in Computer Science, Cloud Computing, Cybersecurity, IT or a related technical field.
- An advanced degree is preferred.

Experience:

- 10+ years designing and operating cloud infrastructure for DoD or national security programs.

Required Skills:

- Deep AWS experience including GovCloud, multi-account architectures, and classified workloads at IL4/IL5.
- Hands-on cloud networking in air-gapped, classified, or hybrid (on-prem + cloud) environments.
- Working knowledge of RMF, FedRAMP, CMMC, NIST SP 800-171, and NIST SP 800-53.
- Experience with IaC, IAM architecture (cross-account roles, identity federation, least-privilege), and compliance-driven monitoring/logging.
- Strong documentation skills for government review - authorization artifacts, control mappings, architecture decision records.

Desired Skills:

- AWS certifications (Solutions Architect Professional, Security Specialty) or CISSP, CCSP, Security+.
- Experience with container orchestration, CI/CD pipelines, and DevSecOps in classified environments.
- Familiarity with cross-domain solutions and secure data transfer between cloud partitions.
- Experience with MBSE and SysML v2 modeling tools.
- Experience supporting space, satellite, or missile defense programs.
- Experience with Amazon Dedicated Cloud (ADC) air-gapped regions.
- FinOps experience - cloud spend optimization and financial governance in DoD environments.
- Experience with Azure or other DIB cloud providers; AWS Landing Zone Accelerator (LZA) for multi-account governance.