

Dallas Gallegos

☎ (919) 555-0148 ✉ dallas.gallegos@example.com 💼 linkedin.com/example/dallasgallegos 📍 Raleigh, NC 27606

SUMMARY

Cloud platform engineer with four years of experience building secure software development environments for defense research and engineering programs. Brings hands-on AWS delivery across **Amazon EKS**, Kubernetes, Helm, Terraform, Ansible, Jenkins, GitLab CI/CD, Python, CloudWatch, Prometheus, Grafana, and Splunk. Active **DoD Secret Clearance**, **Special Access Program** access, **U.S. citizenship**, and CompTIA Security+ support mission work requiring disciplined security controls. Builds repeatable cloud services from software, hardware, and security requirements, then improves reliability through automation, monitoring, controlled releases, and clear documentation. Raleigh-based and ready for daily on-site collaboration with multidisciplinary teams solving demanding problems across physical sciences, defense, civil, health, software, simulation, and testing programs.

EXPERIENCE

Staff Cloud Engineer – Cloud Platforms

May 2024 - Present

Northstar Mission Technologies

Raleigh, NC

Owns AWS platform patterns for secure development and test environments serving defense research application teams. Leads architecture decisions, automation standards, release controls, observability, incident learning, and cross-functional delivery with **hardware engineers**, software engineers, and **security specialists**. Provides dependable cloud foundations for controlled mission schedules and audit-ready operations.

- Owned **AWS** platform patterns across segregated development and test accounts, giving 11 defense research teams consistent services and clearer security boundaries.
- Standardized Amazon EKS clusters, **Helm** releases, IAM boundaries, and private networking through Terraform and Ansible, replacing manual setup with repeatable infrastructure.
- Rebuilt Jenkins and GitLab **CI/CD** workflows with **Python** validation, container scanning, artifact promotion, and approval gates, supporting controlled software releases.
- Partnered with hardware, software, and security engineers to resolve integration constraints, document architecture decisions, and keep cloud delivery aligned with mission schedules.
- Connected CloudWatch, Prometheus, Grafana, and Splunk dashboards for cluster health, deployment status, resource use, and security events, improving release-window visibility.
- Led troubleshooting and post-incident reviews for failed deployments, turning recurring findings into runbooks, automated checks, and prioritized backlog work.

Cloud Infrastructure Engineer

June 2022 - April 2024

Blue Mesa Analytics Group

Durham, NC

Delivered AWS infrastructure for simulation and systems-analysis applications across development and integration environments. Converted technical requirements into Terraform modules, Ansible playbooks, Kubernetes configurations, CI/CD workflows, validation utilities, and operating guidance. Supported reliable maintenance cycles through practical automation, monitoring, and traceable communication with program and security stakeholders.

- Delivered AWS infrastructure for **simulation** and systems-analysis applications by translating environment requirements into **Terraform** modules, Ansible playbooks, and documented deployment procedures.
- Maintained **Kubernetes** and Amazon EKS workloads through Helm chart updates, namespace controls, image configuration, and resource tuning across development and integration environments.
- Built Jenkins and GitLab pipelines for **Java**, **Go**, and Python services, adding tests, container builds, repository checks, and promotion steps for consistent releases.
- Wrote Python utilities that validated cloud configuration and collected deployment metadata, reducing repetitive checks during **software maintenance** activities.
- Implemented CloudWatch alerts plus Prometheus and Grafana dashboards for availability, node capacity, and pipeline failures, giving developers actionable feedback before demonstrations.
- Prepared architecture notes, operating guides, and technical briefings for program leads and security reviewers, preserving traceability from requirements through verification.

PROJECTS

Secure Research Cloud Factory 📅 2025

Built a reference delivery model for isolated AWS research environments using Terraform, Ansible, Amazon EKS, Helm, IAM, and private networking. Work centered on why secure access and repeatable delivery matter: researchers gain dependable tools without weakening mission boundaries. Automated checks and operating guides supported faster team adoption.

Mission Pipeline Reliability Initiative 📅 2024

Created a release workflow for Java, Go, and Python services with Jenkins, GitLab CI/CD, Python validation, container scanning, artifact promotion, and approval gates. Purpose stayed clear: give engineering teams confidence in every change. Monitoring through CloudWatch, Prometheus, Grafana, and Splunk helped teams act before failures affected demonstrations.

LEADERSHIP & AWARDS

- Recognized by program leadership for dependable AWS platform delivery across defense research teams.
- Received peer recognition for converting recurring deployment failures into practical runbooks and automated checks.
- Selected to brief security reviewers and program leads on cloud architecture, verification evidence, and release controls.

EDUCATION

Bachelor's Degree in Computer Science
North Carolina State University GPA: 3.7
Coursework: Cloud computing, Operating systems, Computer networks, Software engineering, Information security

2022
Raleigh, NC

CERTIFICATIONS

- CompTIA Security+  2023
- AWS Certified Cloud Practitioner  2023

TECHNICAL SKILLS

- **Cloud Platforms:** AWS, Azure, Amazon EKS
- **Container Platforms:** Kubernetes, Docker, OpenShift
- **Container Packaging:** Helm, Amazon ECS, OCI images
- **CI/CD Systems:** Jenkins, GitLab CI/CD, Argo
- **Infrastructure Automation:** Terraform, Ansible, SaltStack
- **Programming Languages:** Python, Go, Java
- **Monitoring Tools:** AWS CloudWatch, Prometheus, Grafana
- **Security Analytics:** Splunk, IAM, container scanning
- **Networking:** Private networking, VPC, security groups
- **Operating Systems:** Linux, shell scripting, system administration
- **Security Standards:** DoD 8570, IAT Level II, Security+
- **Delivery Methods:** Infrastructure as code, artifact promotion, approval gates

SKILLS

- | | | | |
|--------------|----------------|--------------|------------------------|
| • AWS | • Terraform | • Amazon EKS | • Grafana |
| • Azure | • Ansible | • Helm | • Splunk |
| • Python | • Jenkins | • CloudWatch | • DoD Secret Clearance |
| • Kubernetes | • GitLab CI/CD | • Prometheus | |

PROFESSIONAL AFFILIATIONS

- Member, Association for Computing Machinery, supporting continued learning in cloud engineering and software systems.
- Member, Cloud Native Computing Foundation community, following Kubernetes operations and container platform practices.

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST