# ============================================================  
# Author: TGibson  
# File: Chapter\_1\_Executive\_Summary.docx  
# Repo: AWS EKS CI/CD (Commercial + GovCloud) via CloudFormation  
# Version: 1.0  
# Date: 2025-08-27  
# ============================================================

AWS EKS CI/CD (Commercial + GovCloud) via CloudFormation  
Comprehensive Architecture & Compliance Document

# Table of Contents

* Acronyms & Definitions
* Chapter 1 — Executive Summary
* Chapter 2 — SaaS Principles
* Chapter 3 — Infrastructure Layer
* Chapter 4 — CI/CD Pipeline Layer
* Chapter 5 — Security & Compliance
* Chapter 6 — Supply Chain Security
* Chapter 7 — Tenant Lifecycle
* Chapter 8 — Public vs Private Partition (Commercial vs GovCloud)
* Chapter 9 — Approval & Governance
* Chapter 10 — Observability & Operations
* Chapter 11 — Criteria Compliance Matrix
* Chapter 12 — Conclusion
* Appendix A — AWS Services by Function
* Appendix B — Environment Checklist

# Acronyms & Definitions

ALB – Application Load Balancer

AMP – Amazon Managed Prometheus

AMG – Amazon Managed Grafana

ATO – Authority to Operate

AWS – Amazon Web Services

CAC – Common Access Card

CJIS – Criminal Justice Information Services (FBI) security policy

CI/CD – Continuous Integration / Continuous Delivery

CM-8 – NIST 800-53 Control: Information System Component Inventory

CodeBuild – AWS managed build service for CI/CD

CodeCommit – AWS managed Git-based source control service

CodePipeline – AWS managed CI/CD orchestration service

CUR – Cost and Usage Report (AWS Billing)

Dev/Stg/Prod – Development / Staging / Production environments

DoD SRG – Department of Defense Security Requirements Guide

EBS – Elastic Block Store

ECR – Elastic Container Registry

EFS – Elastic File System

EKS – Elastic Kubernetes Service

ELK – Elasticsearch, Logstash, Kibana stack

EO 14028 – U.S. Executive Order on Improving the Nation’s Cybersecurity (Supply Chain)

FedRAMP – Federal Risk and Authorization Management Program

FIPS – Federal Information Processing Standard (e.g., 140-2 for crypto)

HPA – Horizontal Pod Autoscaler

IAM – Identity and Access Management

IRSA – IAM Roles for Service Accounts (Kubernetes → IAM integration)

ITAR – International Traffic in Arms Regulations

KMS – Key Management Service (AWS cryptographic key management)

Kyverno – Kubernetes-native policy engine

NIST 800-37 (RMF) – Risk Management Framework

NIST 800-53 – Security and Privacy Controls for Information Systems

NLB – Network Load Balancer

OIDC – OpenID Connect (federated identity standard)

OTel – OpenTelemetry (observability framework)

PIV – Personal Identity Verification (government smart card)

RBAC – Role-Based Access Control

RMF – Risk Management Framework (NIST 800-37)

S3 – Simple Storage Service

SBOM – Software Bill of Materials

SCP – Service Control Policy

Seccomp – Secure Computing Mode (Linux kernel feature for sandboxing)

SNS – Simple Notification Service

STS – Security Token Service

Syft – SBOM generation tool

Tenant Stamp – A fully isolated environment (VPC, EKS, pipeline) provisioned per customer

Trivy – Vulnerability scanning tool

VPC – Virtual Private Cloud

Zero Trust – Security framework requiring continuous verification

# Chapter 1 — Executive Summary

This section will fully describe the SaaS architecture, its AWS-native foundation, compliance posture, multi-tenancy, GovCloud integration, and FIPS 140-2 enforcement...