**White Paper: DevSecOps and CI/CD Pipeline Architecture**

Secure, Automated Software Delivery at Scale (VA Context)

White Paper: DevSecOps and CI/CD Pipeline Architecture – Secure, Automated Software Delivery at Scale (VA Context)

## Executive Summary

Modern software delivery within the Department of Veterans Affairs (VA) demands secure, scalable pipelines that integrate governance and automation. DevSecOps aligns Agile practices with cybersecurity frameworks like VA TRM, FedRAMP, and NIST 800-53. This paper expands on pipeline tools, infrastructure as code (IaC), and Authority to Operate (ATO) automation using secure-by-design principles for platforms such as VA.gov and My Education Benefits.

1. DevSecOps Toolchains

## 1.1 Jenkins

- Overview: Jenkins is an open-source CI/CD orchestration server.

- Key Features:

- Uses Groovy-based Jenkinsfiles for defining pipelines as code.

- Supports plugins for Git, Docker, Kubernetes, SonarQube, and more.

- Enables dynamic agents, notifications, and parallel builds.

- VA Use Case:

- Jenkins is used to manage full DevSecOps workflows, integrating tools like SonarQube (SAST), OWASP ZAP (DAST), and Cosign (artifact signing).

## 1.2 GitHub Actions

- Overview: Native automation framework for GitHub repos.

- Key Features:

- Triggers on pull requests (PRs), branches, tags, etc.

- Matrix builds, job dependencies, and custom runners.

- Native integration with Dependabot and GitHub Packages.

- VA Use Case:

- Pre-merge CI security scanning.

- Inline IaC validation.

- Maintains audit trail for each Git event.

## 1.3 GitLab CI/CD

- Overview: Integrated platform for GitOps-style automation.

- Key Features:

- Built-in container registry, static scanning, and Git workflows.

- Auto DevOps pipelines with stages from test to monitor.

- VA Use Case:

- Enables full traceability from issue to deployment.

- Often used with Kubernetes (EKS/GKE) for GitOps deployments.

2. Infrastructure as Code (IaC)

## 2.1 Terraform

- Overview: Cloud-agnostic IaC tool from HashiCorp.

- VA Practices:

- Modular design for reusable templates.

- OPA/Sentinel policies enforce compliance pre-deployment.

- Secrets stored in Vault or AWS Secrets Manager.

- Use Case: Provisioning EC2, IAM, VPC, and other AWS GovCloud resources.

## 2.2 AWS CloudFormation

- Overview: AWS-native template system using YAML/JSON.

- Features:

- Supports rollback protection and change sets.

- Integrates with AWS Config and GuardDuty for compliance.

- VA Use Case:

- Deployed within CI pipelines for infrastructure creation.

- Templates linted with CFN Guard for FedRAMP alignment.

3. ATO Integration and Continuous Compliance

## 3.1 Pipeline-Embedded Controls

- Compliance Actions:

- Run OpenSCAP and InSpec for STIG checks.

- Validate templates and build artifacts for encryption, RBAC.

- Use Cosign to sign images with KMS-encrypted keys.

- Outputs:

- SSP (System Security Plan) drafts auto-generated.

- CIS (Control Implementation Summary) updated during each release.

- Logs retained in S3 or CloudWatch.

## 3.2 DoD Reference Architecture (Platform One)

- Components:

- Iron Bank: Pre-approved hardened images.

- Platform One: Secure DevSecOps environment.

- Pipeline Phases:

1. Plan & Code: Define stories, IaC, APIs.

2. Build & Test: Run scans, unit tests, dependency analysis.

3. Release: Sign and tag.

4. Deploy: Infrastructure provisioning + deploy image.

5. Operate: Telemetry and logging (Splunk, CloudTrail).

- VA Use:

- Adopted by VEO and Lighthouse teams.

- Aids Zero Trust enforcement with signed components.

4. Secure CI/CD Pipeline Example

## Use Case: Deploy VA.gov microservice to AWS GovCloud.

- Pipeline Steps:

1. Code push triggers GitHub Actions.

2. Jenkins runs unit/integration tests.

3. Trivy + Anchore scan container from Iron Bank.

4. Terraform deploys infrastructure with policies.

5. InSpec validates against STIG.

6. Logs stream to Splunk.

## Security Controls:

- IAM boundaries validated by OPA.

- Signed with Cosign, encrypted with KMS.

- Audit logs archived in S3 with expiration rules.

## 5. Tools and Resources

| Function | Tools |

|----------------------|----------------------------------------|

| CI/CD | Jenkins, GitHub Actions, GitLab |

| Security Scanning | SonarQube, Trivy, Anchore, OWASP ZAP |

| Infrastructure as Code | Terraform, AWS CloudFormation |

| Compliance Validation| OpenSCAP, InSpec, CFN Guard |

| Artifact Security | Sigstore, Cosign, SOPS |

| DoD Tooling | Iron Bank, Platform One |

| Documentation | DoD DSOP, NIST 800-53, Terraform Docs |

## Conclusion

DevSecOps frameworks enable VA teams to integrate security from the start, automating evidence generation for ATO and reducing operational risks. These architectures enhance resilience, shorten delivery cycles, and maintain regulatory alignment across agile portfolios.

## Next Steps:

- Establish DevSecOps governance under VA Handbook 6500.

- Standardize container and IaC templates.

- Automate SSP/CIS generation and STIG scoring.

- Expand Zero Trust and GitOps adoption across portfolios.