ANTHROP\C

Best Practice Guide:
Claude Code for Public Sector



January 2026

Contents

Overview **2**
Background: FISMA and Federal Information Security Requirements **2**
NIST Risk Management Framework (RMF) 2
Purpose of This Guide 3
Recommended Deployment Architecture **3**
Local Installation Approach 4
Configuration Recommendations **4**
Option 1: AWS Bedrock in GovCloud 4
Option 2: Google Cloud Vertex AI 5
NIST 800-53 Best Practices **5**
Access Control (AC Family) 6
Audit and Accountability (AU Family) 6
Configuration Management (CM Family) 7
Identification and Authentication (IA Family) 8
System and Communications Protection (SC Family) 8
System and Information Integrity (SI Family) 9
Shared Responsibility Model **9**
Operational Governance Best Practices **11**
Access Control 11
Data Handling 11
Monitoring & Logging 11
Incident Response 11
Continuous Monitoring 11
Summary **12**
Additional Resources **13**

Overview

This best practices guide provides recommendations for federal agencies deploying Claude Code in environments subject to FISMA requirements. It outlines security considerations, configuration principles, and alignment with NIST 800-53 controls for the on-premise deployment of the Claude Code CLI tool.

Background: FISMA and Federal Information Security Requirements

The Federal Information Security Modernization Act (FISMA) requires federal agencies to establish and enforce information security policies that protect agency information, IT systems, operations, and assets. Under FISMA, agencies must provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of:

- Information collected or maintained by or on behalf of an agency
- Information systems used or operated by an agency, contractor, or other organization on behalf of an agency

NIST Risk Management Framework (RMF)

Agencies use the **NIST Risk Management Framework (RMF)** to develop and implement a risk-based approach to managing information security risk. The RMF helps organizations:

1. **Prepare** for risk management through essential activities critical to designing and implementing a risk management program
2. **Categorize** systems and information based on an impact analysis
3. **Select** a set of NIST SP 800-53 controls to protect the system based on risk assessments
4. **Implement** the controls and document how they are deployed
5. **Assess** the control implementation to determine if controls are in place, operating as intended, and producing desired results
6. **Authorize** the system to operate by a senior-level official who understands the controls in place and any residual risk
7. **Monitor** control implementation and changes to system risks continuously

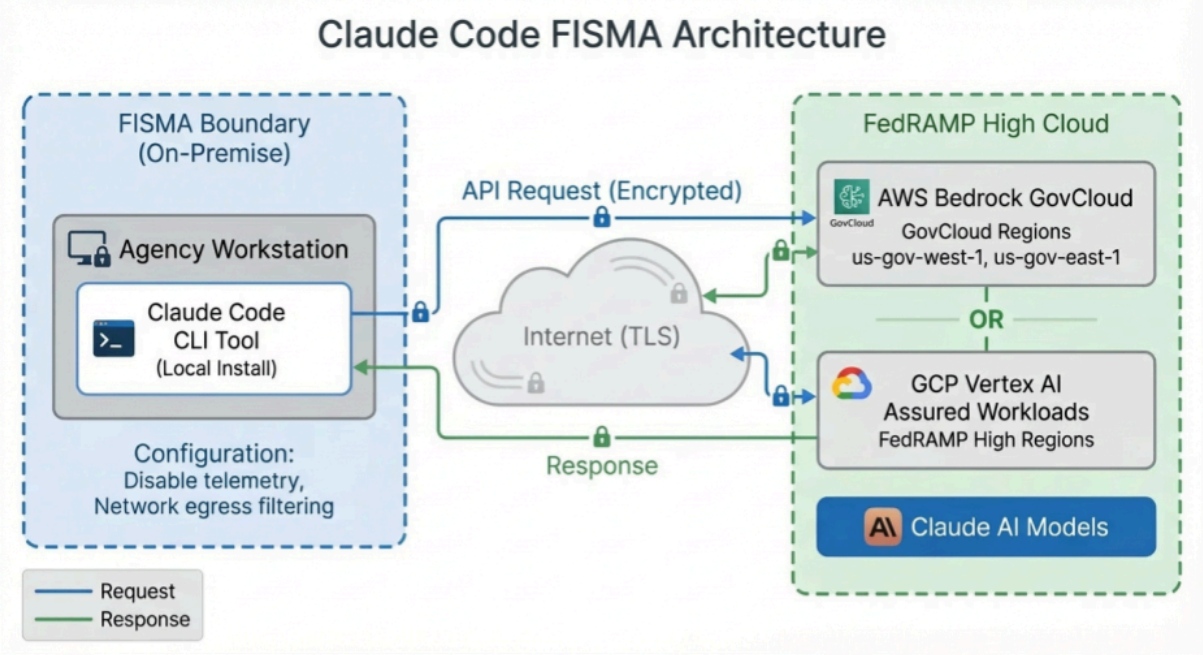
Purpose of This Guide

While agencies are responsible for following FISMA and leveraging the NIST RMF process, service providers can help agencies by sharing best practices for utilizing their services in alignment with NIST 800-53 security controls. **This document outlines best practices for using Claude Code in environments subject to FISMA requirements.**

Recommended Deployment Architecture

Claude Code consists of a locally installed CLI tool that routes AI processing requests to cloud-based services. For FISMA compliance, agencies should:

1. Deploy the Claude Code CLI tool on agency-managed workstations (on-premise)
2. Configure the tool to route all AI processing through FedRAMP High authorized cloud infrastructure
3. Implement appropriate NIST 800-53 controls for the local installation and configuration



Local Installation Approach

The Claude Code CLI should be installed on agency workstations within your FISMA boundary.

For detailed installation instructions, see the Claude Code setup documentation.

Configuration Recommendations

Claude Code should be configured to route AI processing exclusively through FedRAMP authorized cloud infrastructure. Agencies have two options:

Option 1: AWS Bedrock in GovCloud

Key Configuration Parameters:

```shell
# Enable Bedrock routing
export CLAUDE_CODE_USE_BEDROCK=1

# Specify GovCloud region
export AWS_REGION=us-gov-west-1  # or us-gov-east-1

# Configure AWS profile for GovCloud
export CLAUDE_CODE_AWS_PROFILE=your-govcloud-profile

# Disable non-essential traffic
export CLAUDE_CODE_DISABLE_NONESSENTIAL_TRAFFIC=1

# Disable error reporting, telemetry, and bug reporting
export CLAUDE_CODE_DISABLE_TELEMETRY=1
```

For detailed Bedrock configuration, see AWS Bedrock Configuration documentation.

Available Models: See AWS Bedrock model documentation for current Claude model availability in GovCloud regions.

Option 2: Google Cloud Vertex AI

Key Configuration Parameters:

```shell
# Enable Vertex AI routing
export CLAUDE_CODE_USE_VERTEX=1

# Specify GCP project with Assured Workloads
export ANTHROPIC_VERTEX_PROJECT_ID=your-fedramp-project-id

# Specify FedRAMP High authorized region
export CLOUD_ML_REGION=us-east5

# Disable non-essential traffic
export CLAUDE_CODE_DISABLE_NONESSENTIAL_TRAFFIC=1

# Disable error reporting, telemetry, and bug reporting
export CLAUDE_CODE_DISABLE_TELEMETRY=1
```

For detailed Vertex AI configuration, see Google Vertex AI Configuration documentation.

Available Models: See GCP Vertex AI documentation for current Claude model availability in FedRAMP High regions.

NIST 800-53 Best Practices

The following sections outline recommended approaches for addressing relevant NIST 800-53 controls for Claude Code deployment in FISMA environments.

Access Control (AC Family)

AC-2: Account Management

- Implement unique user accounts for Claude Code access
- Leverage existing agency identity management systems
- Document account creation, modification, and removal procedures

AC-3: Access Enforcement

- Configure IAM policies (AWS) or service accounts (GCP) with least privilege
- Restrict Claude Code usage to authorized personnel only
- Implement role-based access control aligned with job functions

AC-6: Least Privilege

Best practice is to grant only minimum required permissions:
AWS Bedrock minimum permissions:

- `bedrock:InvokeModel`
- `bedrock:InvokeModelWithResponseStream`
- `kms:Decrypt` (if using CMEK)

See AWS Bedrock IAM documentation for detailed policy examples.

Google Cloud Vertex AI minimum permissions:

- `roles/aiplatform.user` (or custom role with equivalent permissions)
- `aiplatform.endpoints.predict`
- `aiplatform.endpoints.computeTokens`

See Vertex AI IAM documentation for detailed configuration.

Audit and Accountability (AU Family)

AU-2: Audit Events

Best practices for audit logging:

- Enable logging for all Claude Code API calls through cloud provider audit mechanisms
- Log user authentication and session activities
- Capture data access and processing events

AU-3: Content of Audit Records

Ensure logs contain:

- User identity
- Timestamp
- Event type
- Success/failure status
- Resource accessed

AU-12: Audit Generation
AWS CloudTrail (for Bedrock): Enable CloudTrail logging for all Bedrock API calls. See AWS CloudTrail documentation.

GCP Cloud Audit Logs (for Vertex AI): Enable audit logging for Vertex AI API calls. See GCP audit logging documentation.

Configuration Management (CM Family)

CM-2: Baseline Configuration
Recommended practices:

- Document standard Claude Code configuration for agency deployment
- Maintain configuration baselines in version control
- Implement automated configuration verification

CM-7: Least Functionality
Best practices for minimal functionality:

- Disable non-essential features using `CLAUDE_CODE_DISABLE_NONESSENTIAL_TRAFFIC=1`
- Restrict Claude Code to only required cloud endpoints
- Remove or disable unused components

Example Persistent Configuration:

```shell
# Location: ~/.claude/settings.json
{
  "env": {
    "CLAUDE_CODE_USE_BEDROCK": "1",
    "AWS_REGION": "us-gov-west-1",
```

```
    "CLAUDE_CODE_AWS_PROFILE": "govcloud-profile",
    "CLAUDE_CODE_DISABLE_NONESSENTIAL_TRAFFIC": "1"
  }
}
```

For system-wide configuration options, see Claude Code configuration documentation.

Identification and Authentication (IA Family)

IA-2: Identification and Authentication

Recommended approach:

- Leverage agency's existing multi-factor authentication (MFA) for cloud provider access
- Require MFA for all access to AWS GovCloud or GCP environments
- Implement PIV/CAC authentication where required

IA-5: Authenticator Management

Best practices:

- Use cloud provider IAM for authentication (no local API keys)
- Rotate credentials according to agency policy
- Protect authentication credentials using agency-approved methods

System and Communications Protection (SC Family)

SC-7: Boundary Protection

Recommended network controls:

- Configure network egress filtering to allow only authorized endpoints
- Implement firewall rules restricting Claude Code to required cloud endpoints

AWS GovCloud Bedrock authorized endpoints:

- `bedrock-runtime.us-gov-west-1.amazonaws.com`
- `bedrock-runtime.us-gov-east-1.amazonaws.com`

GCP authorized endpoints:

- Vertex AI endpoints in FedRAMP High authorized regions

SC-8: Transmission Confidentiality
Best practices:

- All communications between Claude Code CLI and cloud services use TLS encryption
- Verify TLS connections are properly configured

SC-12: Cryptographic Key Establishment and Management
Recommended approach:

- Implement customer-managed encryption keys (CMEK) for data at rest
- Maintain control of encryption keys within agency-managed KMS
- Document key rotation procedures

AWS Bedrock CMEK: Configure through AWS KMS. See AWS Bedrock security documentation for implementation guidance.

Google Cloud Vertex AI CMEK: Configure through Cloud KMS. See Vertex AI encryption documentation for implementation guidance.

System and Information Integrity (SI Family)

SI-4: Information System Monitoring
Recommended monitoring practices:

- Monitor Claude Code usage patterns for anomalies
- Integrate cloud provider logs with agency SIEM systems
- Establish baselines for normal usage patterns

SI-7: Software, Firmware, and Information Integrity
Best practices:

- Verify integrity of Claude Code installation package
- Implement change detection for Claude Code configuration files
- Document software version control procedures

Shared Responsibility Model

Understanding responsibility boundaries is critical for FISMA compliance:

Component	Responsible Party	Responsibilities
Cloud Infrastructure	AWS / GCP	• FedRAMP High authorization maintenance • Physical cloud data center security • Cloud infrastructure NIST 800-53 controls • Cloud platform availability and resilience
Model Security Posture	Anthropic	• Model safety and alignment • Protection against adversarial inputs • Model vulnerability management • Supply chain security for model weights
Claude Code CLI Tool	Federal Agency	• Local installation and configuration • Access control to the CLI tool • Proper routing to FedRAMP High services • Endpoint security on workstations • User authentication and authorization • NIST 800-53 control implementation
Data & Operations	Federal Agency	• Data classification and handling • System security plan documentation • Usage policies and governance • User training and awareness • Audit logging and monitoring • Risk assessment for AI use cases • Incident response procedures • Continuous monitoring

Operational Governance Best Practices

Access Control

- Implement role-based access control (RBAC)
- Maintain audit logs of all Claude Code users
- Require MFA for cloud service access
- Conduct regular access reviews (quarterly minimum recommended)

Data Handling

- Classify all data before processing with Claude Code
- Follow agency data classification policies
- Implement data loss prevention (DLP) controls where required
- Document data flows in system security plans

Monitoring & Logging

- Enable comprehensive audit logging through cloud provider mechanisms
- Integrate logs with agency Security Information and Event Management (SIEM) systems
- Establish alerting for anomalous usage patterns
- Maintain logs according to agency retention policies

Incident Response

- Define procedures for potential security incidents
- Establish escalation paths for security incidents
- Document incident response procedures in system security plans
- Consider conducting regular incident response exercises

Continuous Monitoring

- Perform regular security assessments of Claude Code deployment
- Monitor for configuration drift from approved baselines
- Update risk assessments as usage patterns change

- Review and update controls as needed

Summary

This best practices guide recommends that federal agencies deploy Claude Code in FISMA-compliant environments by:

1. **Installing the CLI locally** on agency-managed workstations within the FISMA boundary
2. **Configuring proper routing** to ensure all AI processing occurs through FedRAMP High authorized infrastructure (AWS GovCloud Bedrock or GCP Vertex AI)
3. **Implementing NIST 800-53 controls** appropriate for the system's security categorization
4. **Documenting the deployment** in system security plans and maintaining proper configuration baselines
5. **Establishing governance** through access controls, monitoring, and incident response procedures

Additional Resources

Technical Documentation

- Claude Code Documentation
- AWS Bedrock Configuration
- Google Vertex AI Configuration

FISMA and NIST Resources

- NIST Risk Management Framework
- NIST SP 800-53 Rev 5: Security and Privacy Controls
- FISMA Implementation Project

Cloud Provider Compliance

- AWS GovCloud Compliance
- GCP FedRAMP Compliance