PSL FedRAMP Secure Configuration Guide

TransAccess GovCloud Records (GCR) System

Version 2.0 - FedRAMP Rev5 Compliant
March 5, 2026

Document Control

Document Title	PSL FedRAMP Secure Configuration Guide
Version	2.0
Last Updated	March 5, 2026
Classification	FedRAMP Moderate
Effective Date	March 1, 2026
Next Review	September 1, 2026, by Senior Management Review (SMR) with approval from the President, PSL

Executive Summary

This Secure Configuration Guide (SCG) provides comprehensive, actionable guidance for Federal agencies and authorized personnel on securely configuring, operating, and maintaining the TransAccess GovCloud Records (GCR) system in compliance with FedRAMP requirements. This document addresses all mandatory and recommended requirements from the FedRAMP Secure Configuration Guide effective March 1, 2026, including detailed procedures for secure connections, administrative account management, privileged access controls, and security monitoring.

1. Purpose and Scope

1.1 Purpose

The purpose of this Secure Configuration Guide is to provide Federal agencies with clear, detailed instructions for securely configuring the GCR system to meet their security requirements. This guide explains the security implications of configuration choices and provides step-by-step procedures for implementing secure configurations across all system components.

1.2 Scope

This guide applies to all GCR system components, including infrastructure, platform services, and application components deployed in AWS GovCloud (US). It covers development, staging, and production environments and applies to all authorized users, administrators, and contractors involved in system configuration, operation, and maintenance.

1.3 Applicability

This guide is mandatory for all Federal agencies deploying the GCR system and recommended for all authorized users. Compliance with this guide is required for FedRAMP authorization and continuous monitoring.

2. System Overview

2.1 System Description

Cloud Service Offering (CSO)	TransAccess GovCloud Records (GCR)
Cloud Service Provider (CSP)	Peniel Solutions, LLC (PSL)
FedRAMP ID	FR2500967834
Impact Level	FedRAMP Moderate (NIST SP 800-53 Moderate)
Cloud Environment	AWS GovCloud (US)
Authorization Status	FedRAMP Authorized
Continuous Monitoring	Annual Assessment + Quarterly Reviews
System Baseline	NIST SP 800-53 Moderate Baseline

2.2 Key System Components

The GCR system consists of the following key components: AWS infrastructure (VPC, security groups, IAM), application platform, database layer (RDS MariaDB with encryption), API server (AWS API server with authentication), and monitoring/logging (CloudWatch, VPC Flow Logs, application logs).

3. Administrative Account Security

3.1 Top-Level Administrative Accounts

Top-level administrative accounts are the highest-privilege accounts in the GCR system and control enterprise access to all system components. These accounts must be protected with the strongest security controls available.

3.1.1 Account Types and Naming Conventions

Account Type	Naming Convention	Purpose
AWS Root Account	Not used for daily operations	Emergency access only; protected in secure vault
AWS Master Account Admin	First char of first name + Last	Master account administration

	name.	
GCR Application Admin	H# or C# as defined by the customer	Application-level administration
Security Admin	First char of first name + Last name.	Security configuration and monitoring

3.1.2 Account Creation and Initial Setup

Follow these steps to create and secure top-level administrative accounts:

1. Generate a strong, random password (minimum 14 characters, including uppercase, lowercase, numbers, special characters)
2. Store password in AWS Secrets Manager with encryption at rest
3. Enable multi-factor authentication (MFA) using hardware security key (FIPS 140-2 Level 2 minimum)
4. Configure account lockout after 3 failed login attempts (30-minute lockout duration)
5. Set password expiration to 90 days for administrative accounts
6. Enable CloudTrail logging for all administrative actions
7. Configure VPC Flow Logs to capture all network traffic
8. Enable AWS Config to track configuration changes
9. Set up SNS notifications for any administrative account activity
10. Document account creation in change management system

3.1.3 Password Policy Requirements

Requirement	Value
Minimum Length	14 characters
Uppercase Letters	Required (minimum 1)
Lowercase Letters	Required (minimum 1)
Numbers	Required (minimum 1)
Special Characters	Required (minimum 1) - !@#$%^&*()
Password Expiration	90 days
Password History	Cannot reuse last 24 passwords

3.1.4 Multi-Factor Authentication (MFA) Configuration

All top-level administrative accounts MUST use multi-factor authentication. Hardware security keys are required (FIPS 140-2 Level 2 minimum). Backup MFA devices must be stored in secure location separate from primary device.

11. Obtain FIPS 140-2 Level 2 hardware security key (e.g., YubiKey 5 Series)
12. Register primary hardware key with AWS IAM
13. Register backup hardware key with AWS IAM
14. Store backup key in secure location (safe, vault, or secure storage facility)
15. Document MFA device serial numbers and storage location
16. Test MFA authentication with both primary and backup devices
17. Configure account to require MFA for all operations
18. Set up notifications when MFA device is added or removed

3.1.5 Session Management

Setting	Configuration
Session Timeout (Idle)	15 minutes
Maximum Session Duration	4 hours
Concurrent Sessions	Maximum 3 per account
Session Logging	All sessions logged to CloudTrail

4. Secure Connection Configuration

4.1 Overview

The GCR system requires all administrative and user connections to use encrypted, authenticated secure connections. This section provides detailed procedures for configuring and validating secure connections.

4.2 TLS/SSL Configuration Requirements

All connections to GCR administrative interfaces and APIs must use Transport Layer Security (TLS) 1.2 or higher. TLS 1.3 is recommended for new deployments.

Requirement	Specification
Minimum TLS Version	TLS 1.2 (TLS 1.3 recommended)
Deprecated Versions	SSL 3.0, TLS 1.0, TLS 1.1 - MUST NOT be used
Certificate Type	X.509 v3 with 2048-bit RSA or 256-bit ECDSA
Certificate Authority	AWS Certificate Manager (ACM) or DigiCert
Certificate Validation	Full chain validation required; hostname verification mandatory
HSTS Header	Strict-Transport-Security: max-age=31536000; includeSubDomains

4.3 Cipher Suite Configuration

Only strong cipher suites meeting NIST and FedRAMP requirements are permitted. Weak cipher suites must be disabled.

4.3.1 Approved Cipher Suites

The following cipher suites are approved for use with TLS 1.2 and TLS 1.3:

TLS 1.3 Cipher Suites (Recommended):
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

TLS 1.2 Cipher Suites (Minimum):
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

4.3.2 Disabled Cipher Suites

The following cipher suites MUST be disabled:

- All NULL cipher suites
- All EXPORT cipher suites
- All DES and 3DES cipher suites
- All RC4 cipher suites
- All MD5-based cipher suites
- All PSK cipher suites
- All Anonymous Diffie-Hellman (ADH) cipher suites
- All cipher suites with key exchange less than 2048 bits

4.4 Certificate Management

4.4.1 Certificate Provisioning

19. Request certificate from AWS Certificate Manager (ACM) or approved CA
20. Specify fully qualified domain name (FQDN) for the GCR system
21. Include Subject Alternative Names (SANs) for all applicable domains
22. Validate domain ownership through DNS CNAME or email verification
23. Import certificate into AWS Certificate Manager
24. Configure certificate for use with AWS API Gateway, CloudFront, and ELB
25. Enable automatic certificate renewal (ACM handles this automatically)
26. Document certificate details in configuration management system

4.4.2 Certificate Validation Procedures

Implement the following certificate validation procedures for all connections:

27. Verify certificate is valid (not expired, not revoked)
28. Verify certificate hostname matches the requested domain
29. Verify certificate chain is complete and trusted
30. Verify certificate is signed by trusted Certificate Authority
31. Verify certificate key size meets minimum requirements (2048-bit RSA or 256-bit ECDSA)
32. Verify certificate does not have weak signature algorithm (SHA-1 prohibited)
33. Implement certificate pinning for high-security connections
34. Log all certificate validation failures and investigate

4.4.3 Certificate Renewal and Rotation

Certificates must be renewed before expiration. AWS Certificate Manager automatically renews certificates 60 days before expiration. Manual renewal procedures should follow these steps:

35. Request new certificate 60 days before current certificate expires
36. Validate domain ownership for new certificate

37. Import new certificate into AWS Certificate Manager
38. Update all services to use new certificate
39. Verify all connections are using new certificate
40. Revoke old certificate after 30-day grace period
41. Document certificate rotation in change management system
42. Update certificate inventory and tracking spreadsheet

4.5 Secure Connection Establishment

4.5.1 Administrative Access via AWS Management Console

43. Navigate to https://console.aws.amazon.com (verify URL is correct)
44. Verify browser displays secure connection indicator (padlock icon)
45. Verify certificate details match expected GCR system certificate
46. Enter AWS account ID or alias
47. Enter IAM username for administrative account
48. Enter password for administrative account
49. Enter MFA code from hardware security key
50. Verify successful authentication and secure session established
51. Monitor session timeout indicator (displays remaining session time)
52. Log out when administrative tasks are complete

4.5.2 Administrative Access via AWS CLI

Configure AWS CLI with secure connection settings:

```
[profile gcr-admin]
region = us-gov-west-1
output = json
ca_bundle = /path/to/ca-bundle.crt
signature_version = s3v4
s3 =
  max_concurrent_requests = 20
  max_queue_size = 10000
  max_bandwidth = 100MB/s
  max_in_flight_requests = 1000
  use_accelerate_endpoint = false
```

4.5.3 API Access via HTTPS

53. Obtain API credentials (access key ID and secret access key) from AWS IAM
54. Store credentials securely in AWS Secrets Manager or environment variables
55. Configure API client to use TLS 1.2 or higher
56. Configure API client to validate server certificate
57. Configure API client to use approved cipher suites
58. Set API request timeout to 30 seconds
59. Implement exponential backoff for failed requests

60. Log all API requests and responses for audit trail
61. Monitor API usage for anomalies or abuse

4.6 Secure Connection Monitoring and Validation

4.6.1 Connection Monitoring

62. Enable VPC Flow Logs to capture all network traffic
63. Enable AWS CloudTrail to log all API calls and administrative actions
64. Enable AWS Config to track configuration changes
65. Enable AWS GuardDuty for threat detection
66. Configure CloudWatch alarms for suspicious connection patterns
67. Review connection logs daily for anomalies
68. Implement automated alerting for failed authentication attempts
69. Implement automated alerting for certificate validation failures

4.6.2 Connection Validation Checklist

Use the following checklist to validate secure connections:

□ Verify TLS version is 1.2 or higher
□ Verify cipher suite is in approved list
□ Verify certificate is valid and not expired
□ Verify certificate hostname matches requested domain
□ Verify certificate chain is complete and trusted
□ Verify certificate key size meets minimum requirements
□ Verify MFA is enabled and functioning
□ Verify session timeout is configured correctly
□ Verify logging is enabled and functioning
□ Verify no weak cipher suites are enabled
□ Verify no deprecated TLS versions are enabled
□ Verify certificate pinning is implemented (if applicable)

5. Privileged Account Management

5.1 Privileged Account Types

Account Type	Naming Convention	Purpose
IAM Power User	First char of first name + Last name.	Elevated permissions for developers
Database Admin	First char of first name + Last name.	Database administration
Network Admin	First char of first name + Last name.	Network configuration
Application Support	First char of first name + Last name.	Application troubleshooting

5.2 Least Privilege Implementation

All privileged accounts must follow the principle of least privilege. Users should have only the minimum permissions necessary to perform their job functions.

6. Secure Defaults

6.1 Default Security Settings

The GCR system is provisioned with secure defaults for all security-related settings. These defaults are designed to provide strong security posture while maintaining usability for authorized users.

Setting	Default Value	Rationale
TLS Version	TLS 1.3	Latest secure version
Cipher Suite	TLS_AES_256_GCM_SHA384	Strongest approved cipher
MFA Required	Enabled	Prevents unauthorized access
Session Timeout	15 minutes	Limits exposure of inactive sessions
Password Expiration	90 days	Reduces risk of compromised credentials
Encryption at Rest	AES-256	Protects data if storage is compromised
Encryption in Transit	TLS 1.3	Protects data during transmission
Logging	Enabled	Enables audit trail and threat detection
Monitoring	Enabled	Detects security incidents

7. Monitoring and Audit Logging

7.1 Logging Requirements

All administrative activities, authentication attempts, and security-relevant events must be logged and retained for a minimum of 90 days.

Log Type	Retention Period	Destination
CloudTrail Logs	1 year	S3 with encryption
VPC Flow Logs	90 days	CloudWatch Logs
Application Logs	90 days	CloudWatch Logs
Security Logs	1 year	Tomcat access logs
Audit Logs	3 years	Secure archive

8. Incident Response for Secure Connections

8.1 Certificate Compromise

70. Immediately revoke compromised certificate
71. Request new certificate from Certificate Authority
72. Update all systems to use new certificate
73. Notify all users of certificate change
74. Review access logs for unauthorized access
75. Implement additional monitoring for suspicious activity
76. Document incident in security incident log
77. Conduct post-incident review to prevent recurrence

8.2 TLS/SSL Configuration Changes

Any changes to TLS/SSL configuration must follow change management procedures and be documented. Unauthorized changes should be treated as security incidents.

9. Compliance Verification

9.1 Configuration Verification Checklist

Use the following checklist to verify compliance with this guide:

Administrative Accounts:
□ Top-level administrative accounts exist and are properly named
□ All administrative accounts have MFA enabled
□ Password policy is enforced (14 characters, complexity requirements)
□ Session timeout is configured (15 minutes idle)
□ Account lockout is configured (3 failed attempts, 30-minute lockout)
□ CloudTrail logging is enabled for all administrative actions

Secure Connections:
□ TLS 1.2 or higher is required for all connections
□ Weak cipher suites are disabled
□ Certificates are valid and not expired
□ Certificate validation is enforced
□ HSTS header is configured
□ VPC Flow Logs are enabled

Monitoring and Logging:
□ CloudTrail is enabled and logging to S3
□ VPC Flow Logs are enabled
□ CloudWatch alarms are configured

□ Logs are retained for minimum period
□ Log analysis is performed regularly

10. Support and Contact Information

Support Type	Contact Information
Technical Support	info@pslsolutions.com |
Security Issues	info@pslsolutions.com
Compliance Questions	info@pslsolutions.com

Appendix A: Configuration Examples

A.1 AWS CLI Configuration for Secure Connections

[profile gcr-admin]
region = us-gov-west-1
output = json
ca_bundle = /etc/ssl/certs/ca-bundle.crt
signature_version = s3v4
max_concurrent_requests = 20
max_queue_size = 10000