# Compliant Framework for Federal and DoD Workloads in AWS GovCloud (US)

## Implementation Guide

# Compliant Framework for Federal and DoD Workloads in AWS GovCloud (US): Implementation Guide

# Table of Contents

# Deploy a secure, scalable, multi-account environment in AWS GovCloud (US) based on AWS best practices

Publication date: *December 2020*

The Compliant Framework for Federal and DoD Workloads in AWS GovCloud (US) solution enables you to quickly deploy a secure, scalable, multi-account environment in AWS GovCloud (US) based on AWS best practices. This solution is architected to follow the Defense Information Systems Agency (DISA) Cloud Computing Security Requirements Guide (CC SRG) for hosting Impact Level (IL) 4 and 5 workloads in the cloud. Using this solution, you can quickly deploy an architecture baseline that accommodates U.S. federal and Department of Defense (DoD) requirements to rapidly achieve Authority to Operate (ATO).

In addition to U.S. federal and DoD customers, this solution is also architected to support defense industrial base customers to achieve Cybersecurity Maturity Model Certification (CMMC) readiness. For more information about CMMC, refer to the Compliance (p. 16) section of this guide.

This guide provides instructions to aid in the preparation and deployment of the Compliant Framework for Federal and DoD Workloads in AWS GovCloud (US) solution. Due to the large number of design choices, setting up a multi-account environment can take a significant amount of time and require a deep understanding of AWS services. This solution helps you by automating and accelerating the setup of an initial cloud environment, suitable for hosting these secure workloads.

This solution also provides the following:

- complimentary functionality, including tenant account creation and management
- identity and access management
- data security and governance
- core networking
- centralized logging

> **Important**
> This solution will not, by itself, make you DoD CC SRG or CMMC compliant. It provides the foundational infrastructure from which additional complementary solutions can be integrated. The information contained in this solution implementation guide is not exhaustive. You must review, evaluate, assess, and approve the solution in compliance with your organization's particular security features, tools, and configurations. It is the sole responsibility of you and your organization to determine which regulatory requirements are applicable and to ensure that you comply with all requirements. Most of the requirements under the DoD CC SRG or CMMC are administrative and not technical (that is, people- and process-oriented). Although this solution discusses both the technical and administrative requirements, this solution does not help you comply with the non-technical administrative requirements.

This implementation guide discusses architectural considerations and configuration steps for deploying Compliant Framework for Federal and DoD Workloads in AWS GovCloud (US) in the Amazon Web

Services (AWS) Cloud. It includes links to an AWS CloudFormation template that launches and configures the AWS services required to deploy this solution using AWS best practices for security and availability.

The guide is intended for government civilians, contractors, and military personnel who deploy or manage IT applications, workloads, and capabilities.

# Cost

You are responsible for the cost of the AWS services used while running this reference deployment. As of the date of this guide's publication, the cost for running this solution with default settings in the AWS GovCloud (US-West) Region is approximately **$1,300 per month**. Prices are subject to change. For full details, refer to the pricing webpage for each AWS service you will be using in this solution.

## Cost per month

This solution uses the following resources that are billed on a monthly basis.

| AWS service | Quantity | Monthly cost |
|---|---|---|
| Amazon CloudWatch | Standard logs (200 GB), vended logs (200 GB), log storage (1 month retention), logs delivered to Amazon S3 (100 GB) | $306.14 |
| Amazon Elastic Compute Cloud (Amazon EC2) | Operating system (Windows Server), quantity (4), pricing strategy (on-demand instances), storage for each Amazon EC2 instance (general purpose SSD (gp2)), storage amount (30 GB), instance type (t3.medium) | $207.74 |
| Amazon EC2 | Operating system (Linux), quantity (4), pricing strategy (on-demand instances), storage for each Amazon EC2 instance (general purpose SSD (gp2)), storage amount (100 GB), instance type (t3.medium) | $180.90 |
| Amazon Simple Storage Service (Amazon S3) | Amazon S3 standard storage (150 GB per month) | $16.65 |
| Amazon S3 | DT Inbound: Not selected (0 TB per month)<br><br>DT Outbound: Internet (250 GB per month) | $38.45 |
| Amazon Virtual Private Cloud (Amazon VPC) | Number of Transit Gateway attachments (3) | $254.28 |
| Amazon VPC | Number of Site-to-Site VPN connections (2) | $94.90 |
| AWS CloudTrail | Management events units (millions), write management trails (2), read management trails (1), data events units | $40.00 |

| AWS service | Quantity | Monthly cost |
|---|---|---|
| | (millions), S3 trails (1), Lambda trails (1), Insights events units (millions), trails with Insights events (1), write management events (2 per month) | |
| AWS Config | Number of configuration items recorded (5000)<br><br>Number of AWS Config rule evaluations (5000) | $24.00 |
| AWS Directory Service | Number of directories (1) | $137.97 |
| **Total** | | **$1,301.03** |

Additionally, refer to a sample AWS Pricing Calculator analysis.

# Architecture overview

Deploying this solution builds the following environment in the AWS Cloud.

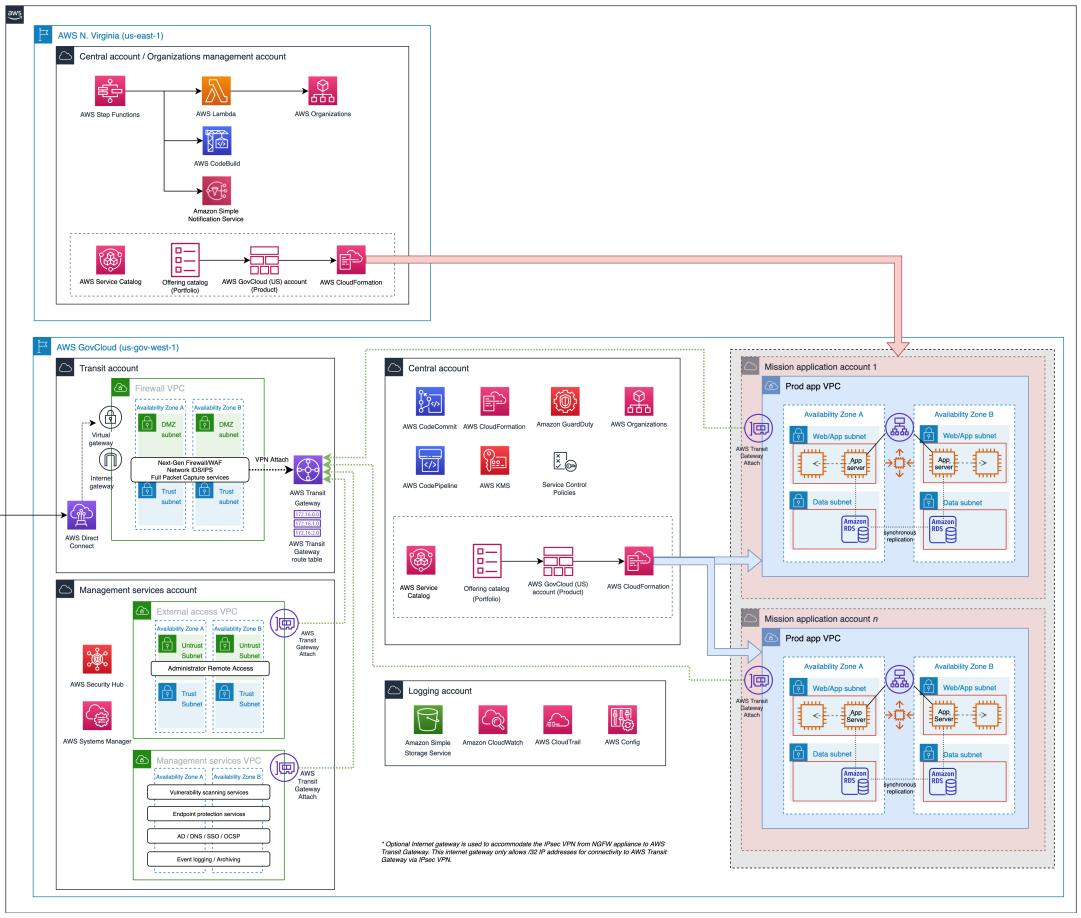


**Figure 1: Compliant Framework for Federal and DoD Workloads in AWS GovCloud (US) architecture on AWS**

The AWS CloudFormation template deploys an AWS Step Functions that runs a series of tasks that deploy the solution. These tasks are implemented as AWS Lambda functions (used to initialize AWS Organizations and create AWS GovCloud (US) accounts) and an AWS CodeBuild project that is used to orchestrate the deployment of the solution into the newly-created AWS accounts. Additionally, an Amazon Simple Notification Service (Amazon SNS) topic is created to track the deployment status of this solution.

> **Note**
> AWS CloudFormation resources are created from AWS Cloud Development Kit (AWS CDK) components.

## AWS Step Functions (Commercial Central account)

The AWS Step Functions runs the following steps:

1. An Amazon SNS subscription is created using the email address that was provided during template launch. You must accept the subscription notification email that is sent to the supplied notification email.
2. An Amazon Lambda function verifies that the AWS access key and secret access key for AWS GovCloud (US) is valid from the values stored in AWS Systems Manager Parameter Store. The AWS CodeBuild project uses the API keys to run subsequent deployment steps. Refer to Prerequisites (p. 18) for additional instructions.
3. AWS Organizations is enabled in both the Commercial and AWS GovCloud (US) partitions. The Commercial Central account is designated as the AWS Organizations Management account for each partition. Refer to AWS Organizations (p. 13) for more information.
4. The Logging, Management services, and Transit accounts are created using the CreateGovCloudAccount API and are added to the appropriate organizational unit (OU) within AWS Organizations.
5. An AWS CodeBuild project runs to deploy the AWS GovCloud (US) resources.
6. An email is sent to the registered Amazon SNS subscription to notify you of the deployment results.

# AWS CodeBuild (Commercial Central account)

After the AWS CodeBuild project launches from the Commercial Central account using the AWS GovCloud (US) CLI API keys stored within AWS Systems Manager Parameter Store, the following steps run in the AWS GovCloud (US) accounts:

1. The following AWS CodeCommit repositories are created and populated into the Central account:
   - `compliant-framework-central-pipeline`
   - `compliant-framework-central-core`
   - `compliant-framework-transit-core`
   - `compliant-framework-management-services-core`
   - `compliant-framework-security-baseline`

   Refer to Solution components (p. 9) for more details about the purpose of each CodeCommit repository.
2. Environment parameters for each of the accounts are initialized and configured into AWS Systems Manager Parameter Store.

   **Note**
   This solution uses AWS Systems Manager Parameter Store to store all input parameters that define the solution, and store all the output values for generated resources. You can extend the Compliant Framework for Federal and DoD Workloads in AWS GovCloud (US) by using these values as inputs when deploying your own solutions or other products. Refer to AWS Systems Manager Parameter Store in the *AWS Systems Manager User Guide* for ways you can reference Systems Manager parameters in your scripts, commands, automation, documents, and configuration workflows.
3. The CDK is initialized by bootstrapping the Central account and deploying the cross-account support stacks into the Logging, Transit, and Management services accounts.
4. CDK deploys the following two AWS CodePipeline pipelines:
   - `compliant-framework-core-pipeline`
   - `compliant-framework-environment-pipeline`
5. The pipelines are configured to utilize the CodeCommit repositories as input triggers to deploy this solution into the AWS GovCloud (US) accounts.

# AWS CodePipeline - Core pipeline (AWS GovCloud (US) Central account)

The `compliant-framework-core-pipeline` pipeline is invoked whenever changes are made to the `core-pipeline` GitHub branch of the `compliant-framework-central-core` CodeCommit repository.

When invoked, the pipeline runs the following tasks in the AWS GovCloud (US) accounts:

1. The Logging account is initialized.
   - Amazon Simple Storage Service (Amazon S3) buckets are created and used to consolidate all member account logs (for example, logs and data generated by AWS Config, AWS CloudTrail, Amazon Virtual Private Cloud (Amazon VPC) Flow Logs). The S3 buckets are shared with the organization and configured with AWS Key Management Service (AWS KMS) custom master keys (CMKs).
   - CloudTrail, AWS Config, AWS Security Hub, and Amazon GuardDuty are enabled.
2. The Central account is initialized.
   - CloudTrail is enabled.
   - AWS Config is enabled and the Central account is configured to aggregate AWS Config information from all solution accounts.
   - Security Hub is enabled and the Central account is configured to aggregate Security Hub findings from all solution accounts.
   - GuardDuty is enabled.

# AWS CodePipeline - Environment pipeline (AWS GovCloud (US) Central account)

The `compliant-framework-environment-pipeline` pipeline is invoked whenever changes are made to the `environment-pipeline` GitHub branch of the following AWS CodeCommit repositories:

- `compliant-framework-transit-core`
- `compliant-framework-management-services-core`
- `compliant-framework-security-baseline`

When invoked, the pipeline runs the following tasks in the AWS GovCloud (US) accounts:

1. The Organizations OUs are configured for the environment, and the Transit and Management services accounts are moved into the environment OU.
2. Amazon S3 buckets are created and used to consolidate all environment account logs (for example, logs and data generated by AWS Config, CloudTrail, and Amazon VPC Flow Logs).

   **Note**
   These S3 buckets can also be configured to store operating system (OS) and application logs. They are intended to help you meet compliance requirements specific to log aggregation.
3. The S3 buckets are shared with the Organizations OU and configured with AWS KMS CMKs. Replication is also enabled to forward all objects to the consolidated logs S3 bucket in the Logging account.
4. The Transit account is initialized and networking resources are created. These resources include the Firewall VPC, AWS Transit Gateway and related AWS Transit Gateway route tables, and AWS Transit Gateway VPN attachments that can be used when configuring a Next Generation Firewall appliance.

5. The Management services account is initialized. The management services, directory, and external access VPCs are created and attached to the AWS Transit Gateway created in the Transit account.
6. The CloudTrail, AWS Config, Security Hub, and GuardDuty services are enabled using an AWS CloudFormation StackSets that is configured to apply to the Organizations OU.

The solution's infrastructure is suitable for migrating, building, and deploying applications and capabilities in the AWS Cloud. This includes web-based application servers, database servers, or workloads running on Amazon Elastic Compute Cloud (Amazon EC2). These workloads are hosted in mission application accounts, which are logically separated enclaves that allow for data and access segregation between different mission owners.

The infrastructure also includes key shared services, including boundary protection (for example, Next Generation Firewalls (NGFW) and gateways such as AWS VPN endpoints and AWS Direct Connect gateways) and workload management (for example, endpoint protection, vulnerability scanning and management, centralized identity management, and directory services).

For more details about each of the accounts, refer to Solution components (p. 9).

# Solution components

## Commercial accounts

### Central account

The commercial Central account launches the Compliant Framework for Federal and DoD Workloads in AWS GovCloud (US) solution through AWS CloudFormation and AWS Step Functions. This account is configured to be the AWS Organizations management account. An automated account provisioning capability is available within this account (implemented using AWS Service Catalog) and is used to provision new accounts in the organization.

> **Note**
> AWS GovCloud (US) accounts are associated with standard AWS accounts for billing, service, and support purposes. Customers must have an existing standard account before signing up for an AWS GovCloud (US) account. We recommend creating a new AWS account that will only be used for AWS GovCloud (US) signup and billing. A dedicated AWS account for the new AWS GovCloud (US) account enables you to transfer the AWS GovCloud (US) account to another party in the future and fully close the AWS GovCloud (US) accounts without affecting your other AWS workloads. For more information about the relationship between AWS standard accounts and AWS GovCloud (US) accounts, refer to the AWS Blog. For more information about Billing and Cost Management, refer to What is AWS Billing and Cost Management?

### Logging account / Management services account / Transit account

The commercial Logging, Management services, and Transit accounts are created and invited into the commercial AWS Organizations organizational unit (OU) when the solution is deployed.

These accounts are only used for billing and support purposes and not otherwise utilized in this solution.

## AWS GovCloud (US) accounts

This solution requires access to an AWS GovCloud (US) account. Refer to Signing Up for AWS GovCloud (US) for more information.

### Central account

The Central account is the location of the AWS CodeCommit code repository for all Infrastructure as Code (IaC) artifacts that are utilized in this solution. An automated CI/CD pipeline (implemented using AWS CodePipeline) is used to deploy the solution from source repositories hosted in CodeCommit.

The Central account is the AWS Organizations root account in AWS GovCloud (US), and it is the parent container for all AWS GovCloud (US) accounts in the architecture. As the Organizations root, the Central account is enabled to aggregate compliance findings from GuardDuty, AWS Config, and AWS Security Hub, from all child accounts. The Central account contains the AWS Service Catalog portfolio for all of the other accounts, including the mission application accounts. This enables a centralized strategy for IT

governance, allowing mission application owners to deploy approved products and services into tenant workload accounts.

# Logging account

The Logging account provides a centralized, immutable location for various types of log data generated across the environment. Log data is collected primarily within Amazon Simple Storage Service (Amazon S3) buckets. This includes AWS CloudTrail, AWS Config, Amazon CloudWatch, Amazon Virtual Private Cloud (Amazon VPC) Flow Logs, operating system and application logs, and any other logs that require consolidation, aggregation, and retention. File integrity is enabled for all log files, creating SHA-256 hashes for every delivered log file. By placing all of the logs into a single account, you can utilize the principle of least privilege, and delegate discrete permissions to for accessing data within this account, separate from the other AWS accounts. This helps ensure log integrity and fidelity.

# Transit account

The Transit account provides a Transit VPC model which produces ingress and egress points for all traffic within the environment. In the DISA SCCA construct, this account corresponds to the DISA SCCA Virtual Data center Security Stack (VDSS) component.

The Transit account provides multiple options to extend an on-premises network. Terminating at a Next Generation Firewall (NGFW) appliance (deployed within the Firewall VPC), one or more AWS Direct Connect virtual interfaces can be utilized to provide a secure, private, low-latency connection from an existing on-premises data center. You can also create an IPsec VPN link between an on-premises network and an NGFW appliance within the Transit VPC. The VPN connection can also serve as a redundant communications path to back up the AWS Direct Connect link.

AWS Transit Gateway provides a centralized network hub that is used to interconnect the VPCs and NGFW appliances within this solution. Using Transit Gateway route tables, Border Gateway Protocol (BGP) dynamic routing, and the functionality provided by the NGFW appliance, you can control, monitor, and inspect all network traffic within the environment. Utilizing BGP dynamic routing reduces the need to manually manage route tables.

# Management services account

The Management services account hosts all of the core services that are needed in operating and managing the environment. In the DISA SCCA construct, this account corresponds to the Virtual Data center Management Stack (VDMS) component.

By default, the workloads in this account are accessible by all the mission application workloads, and provide shared services including endpoint protection (for example, antivirus scanning), vulnerability management and scanning, centralized logging services (for example, syslog), centralized patch management services (for example, yum repositories or Microsoft Endpoint Configuration servers), and centralized identity management or directory services (such as AWS Managed Microsoft AD and Microsoft Active Directory Federation Services (ADFS)).

# Mission application account

The mission application account provides a location for the deployment of end user-facing applications and services. Web application servers, databases, and other compute or data workloads are deployed in this account. By distributing these workloads within separate accounts, developers and administrators can have privileged access to their workloads without introducing risk to other mission applications, and without introducing risk to the Management services, Logging, or Transit accounts. This is implemented through the use of AWS OrganizationsService Control Policies (SCP), AWS Identity and Access Management (IAM) roles and policies, and centralized identity federation.

A mission application account is connected to the environment using AWS Transit Gateway attachments. Routes defined by the Transit Gateway only allow specific network traffic into and out of the mission application account. This allows the mission application workloads to access Management Services as required, and allows external clients and users access to only the specific endpoints in the mission application account as needed.

By segregating workloads into separate mission application accounts, you can implement granular security and cost controls, providing important guardrails that are required to maintain compliance. AWS services billing can be tracked and managed at the account level.

You can deploy additional mission application accounts using AWS Service Catalog functionality within the commercial Central account. You can create a mission application VPC using the product that is deployed in AWS Service Catalog within the AWS GovCloud (US) Central account.

# Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This Shared Responsibility Model helps reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. For more information about security on AWS, visit AWS Cloud Security.

## IAM users and roles

The AWS Identity and Access Management (IAM) users and roles created in this solution are designed as a starting point to provide full administrative access into the environment. Do not use these IAM users and roles in an operational or production environment. We recommend you develop and deploy IAM roles as applicable for your mission needs.

## Security groups

The security groups created in this solution are designed to control and isolate network traffic between the applications deployed into the mission application accounts, and also with external users and clients. We recommend that you review the security groups and further restrict access as needed once the deployment is up and running.

## AWS Key Management Service(AWS KMS) Customer Master Keys (CMK)

This solution creates Customer Master Keys (CMKs) in the deployed AWS accounts. Some keys are pre-configured to encrypt resources such as Amazon Simple Storage Service (Amazon S3) buckets and AWS CloudTrail trails. The keys are also intended to be used for other data-at-rest encryption needs, such as the encryption of Amazon Elastic Block Store (Amazon EBS) volumes. You are responsible for rotation of these CMKs. For more information, review the AWS Key Management Service documentation.

# Design considerations

## Planning

To ensure a successful deployment of this solution, you must make several key design decisions prior to deployment.

### AWS accounts and email addresses

Initial deployment creates several AWS accounts. To create these accounts, you must provide unique email addresses in the AWS CloudFormation template. The following table provides a way to track the email addresses used, as well as their corresponding AWS account IDs.

> **Note**
> If you would like to use existing AWS accounts, you must enter the email addresses representing those accounts into the AWS CloudFormation template parameters during deployment. If these accounts are part of an existing AWS Organizations organizational unit (OU) that has been defined in the Central account, you must move all member accounts to the root Organization OU and verify that any resources you have added to the accounts have been removed. Refer to Uninstall the solution (p. 25) for more information on reverting your accounts to an uninstalled state.

| Account role | Email address | AWS account ID |
|---|---|---|
| Central | TBD | TBD |
| Logging | TBD | TBD |
| Management services | TBD | TBD |
| Transit | TBD | TBD |

### AWS Organizations

This solution creates a customizable AWS Organizations organization as defined in Figure 2. We recommend that you create any future mission application accounts underneath the Environment Tenants OU.

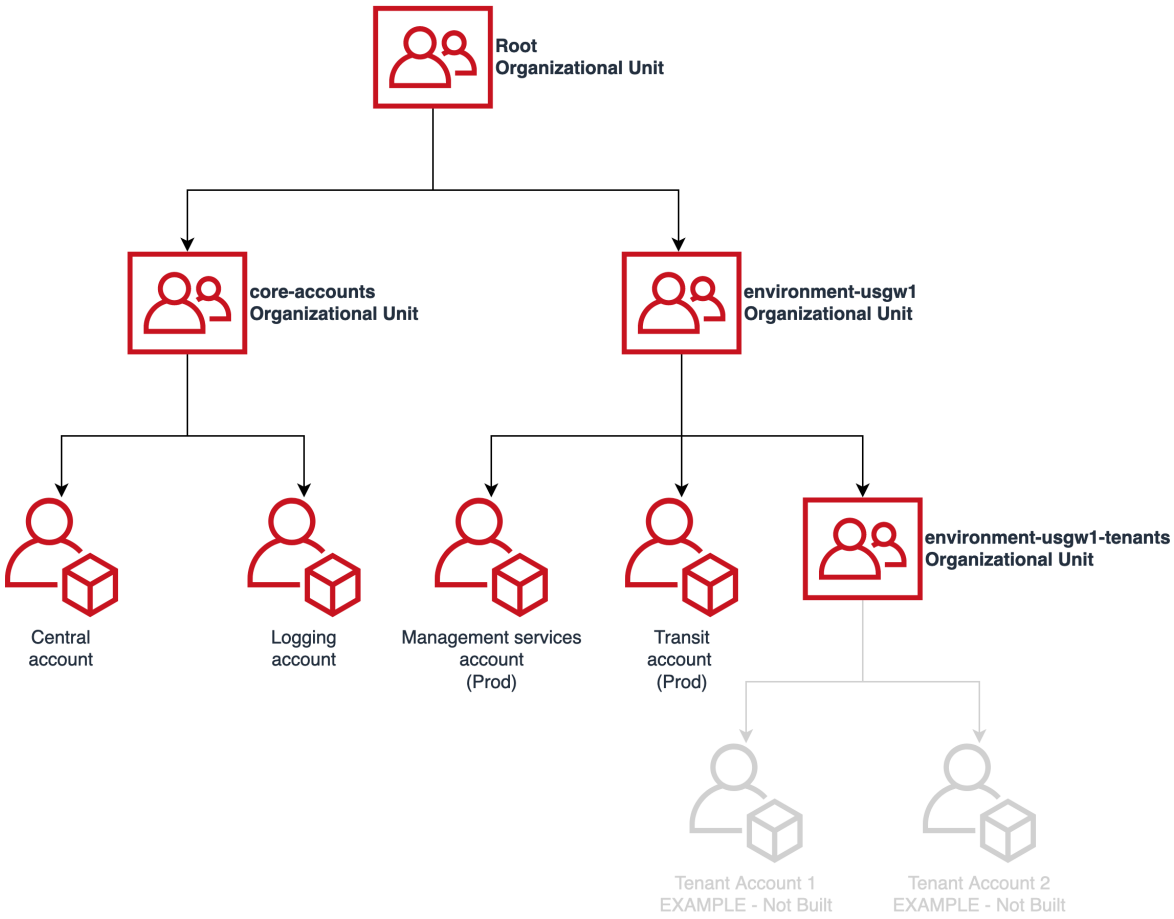


**Figure 2: AWS Organizations structure**

## Account limit increases

The initial limit for number of accounts in an Organizations is four, which is sufficient to deploy this solution. However, to support the creation of new mission application accounts, request a Quota Limit Increase from the account that the solution is being launched in. For more information, refer to Quotas for AWS Organizations. Request quota increases through the AWS Organizations console.

# Data classification

This solution can be deployed across many AWS Regions, but selection of a deployment Region is dependent upon the workloads to be hosted. It also requires a thorough understanding of the classification of the data that is to be stored and processed within the environment.

U.S. Department of Defense data classified at Impact Level 2 can be hosted in an AWS Region that has been accredited to host data at that classification level. At the time of publication, these Regions include:

- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

- AWS GovCloud (US-West)
- AWS GovCloud (US-East)

If the data is classified at Impact Level 4 or Impact Level 5, you must deploy the solution into a Region that is accredited to host data at that level. At the time of publication, these Regions are:

- AWS GovCloud (US-West)
- AWS GovCloud (US-East)

For more details, review the following information:

- Department of Defense Cloud Computing Security Requirements Guide
- AWS Services in Scope by Compliance Program
- AWS Infrastructure

# Management services and transit services

This solution provides a network topology and infrastructure to support many of the compliance requirements mandated by U.S. Federal agencies and the DoD. However, there are cases where additional shared services and transit services are needed to meet workload-specific compliance requirements.

The following table outlines some common functions and AWS services that help you meet additional security and compliance requirements. In addition to the listed alternatives, you can find additional open-source solutions.

| Function | AWS service | Alternatives |
|---|---|---|
| Next Generation Firewall (NGFW)<br><br>Web Application Firewall (WAF) | AWS WAF | AWS Partner Network<br><br>AWS Marketplace |
| Endpoint protection<br><br>Vulnerability management and scanning | Amazon Inspector | AWS Partner Network<br><br>AWS Marketplace |
| Identity management and federation | AWS Identity and Access Management (IAM)<br><br>AWS Directory Service<br><br>AWS Single Sign-On | AWS Partner Network<br><br>AWS Marketplace |
| Centralized logging, log analysis, and auditing | Amazon CloudWatch<br><br>Amazon Elasticsearch Service | AWS Partner Network<br><br>AWS Marketplace |

# Compliance

This solution is designed to meet the compliance requirements for several popular frameworks.

## Defense Information Systems Agency (DISA) Cloud Computing Security Requirements Guide (CC SRG) and Secure Cloud Computing Architecture (SCCA)

The CC SRG is developed and maintained by DISA, and it outlines requirements that must be met by mission owners running DoD workloads in commercial cloud environments, such as AWS GovCloud (US). The architecture in this solution is designed to meet the controls as defined in the DISA CC SRG, together with AWS native security controls. Key components of SCCA include:

- VDSS – Virtual Data Center Security Services
- VDMS – Virtual Data Center Management Services
- TCCM – Trusted Cloud Credential Manager
- CAP – Cloud Access Point

This solution builds infrastructure to support VDSS and VDMS functionality, and can accommodate a CAP connection within the Transit account.

For more information, review the following resources:

- Department of Defense Cloud Computing Security Requirements Guide
- AWS Services in Scope by Compliance Program
- Department of Defense Cloud Computing Security Requirements Guide (PDF)

## Cybersecurity Maturity Model Certification (CMMC)

The Cybersecurity Maturity Model Certification (CMMC) is developed and maintained by the United States Department of Defense Office of the Under Secretary of Defense for Acquisition & Sustainment. It contains sets of controls and required data reports to verify and validate adherence to the defined controls. At the time of this guide's publishing, the architecture in this solution was designed to meet these controls.

For more information, review the following resources:

- Office of the Under Secretary of Defense for Acquisition & Sustainment
- CMMC Model

# AWS CloudFormation template

To automate deployment, this solution uses AWS CloudFormation. It includes the following AWS CloudFormation template, which you can download before deployment:


**compliant-framework-for-federal-and-dod-workloads-in-aws-govcloud-us.template:** Use this template to launch the solution and all associated components. The default configuration deploys Amazon CloudWatch, Amazon GuardDuty, Amazon Inspector, Amazon Simple Notification Service (Amazon SNS), Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC), AWS CloudTrail, AWS CodeBuild, AWS CodeCommit, AWS CodePipeline, AWS Config, AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS), AWS Lambda, AWS Organizations, AWS Security Hub, AWS Service Catalog, AWS Step Functions, AWS Systems Manager, AWS Transit Gateway, and AWS Virtual Private Network (AWS VPN). You can customize the template to meet your specific needs. Refer to the README.md file in the GitHub repository for guidance to customize the template.

# Automated deployment

Before you launch the automated deployment, review the architecture, configuration, network security, and other considerations in this guide. Follow the step-by-step instructions in this section to configure and deploy this solution.

**Time to deploy:** Approximately 90 minutes

## Prerequisites

To launch this solution, you need the following:

1. The account used to launch the solution must be enabled to access AWS GovCloud (US).
2. You must be authorized to create accounts in the AWS GovCloud (US) Region. For more information on the AWS GovCloud (US) Region, refer to the *AWS GovCloud (US) User Guide*.
3. An IAM user and AWS CLI keys created in the AWS GovCloud (US) Central Account. For instructions, refer to Creating an IAM user in your AWS account in the *AWS Identity and Access Management User Guide* and Create a Systems Manager parameter (console) in the *AWS Systems Manager User Guide*.

   The corresponding AWS CLI keys and AWS GovCloud (US) Central Account information must be stored as the following SSM parameters in the commercial Central account:

   - `/compliant/framework/central/aws-us-gov/id` [String]
   - `/compliant/framework/central/aws-us-gov/access-key-id` [String]
   - `/compliant/framework/central/aws-us-gov/secret-access-key` [SecureString]
4. Trusted Access for AWS Organizations has been enabled for AWS CloudFormation StackSets within the AWS GovCloud (US) account. Refer to AWS CloudFormation StackSets and AWS Organizations for instructions.

## Step 1. Launch the stack

This automated AWS CloudFormation template deploys the Compliant Framework for Federal and DoD Workloads in AWS GovCloud (US) solution in the AWS Cloud. Ensure that you have reviewed and gathered all the necessary information for the parameters before launching the stack.

**Note**
You are responsible for the cost of the AWS services used while running this solution. Refer to the Cost (p. 3) section for more details. For full details, refer to the pricing webpage for each AWS service you will be using in this solution. Refer to Additional resources (p. 24) for links to the webpages for all services used in this solution.

1. Sign in to the AWS Management Console in the Commercial Central account in US East (N. Virginia) and select the button to launch the `compliant-framework-for-federal-and-dod-workloads-in-aws-govcloud-us` AWS CloudFormation template.

   Launch Solution

   Alternatively, you can also download the template as a starting point for your own implementation. Refer to the README.md file in the GitHub repository for guidance to customize the template.

**Important**
The template must be launched from the default US East (N. Virginia) Region. Do not select any other Region.

2. On the **Create stack** page, verify that the correct template URL shows in the **Amazon S3 URL** text box and choose **Next**.
3. On the **Specify stack details** page, assign a name to your solution stack.
4. Under **Parameters**, review the parameters for the template, and modify them as necessary. In many cases, the default values are suitable; however, some of the parameters do not have default values and require your input. This solution uses the following default values.

| Parameter | Default | Description |
|---|---|---|
| **Deployment Notifications Email** | *<Requires input>* | Specify an email address to receive notifications about this deployment. |
| **Core Notifications Email** | *<Requires input>* | Specify an email address to receive notifications about Core accounts. |
| **Environment Notifications Email** | *<Requires input>* | Specify an email address to receive notifications about Environment accounts. |
| **Logging Account Email** | *<Requires input>* | Specify an email address to use for the Logging account. This email address must not already be associated with another AWS account. You must use a valid email address to complete account creation. You can't access the root user of the account or remove an account that was created with an invalid email address. |
| **Transit Account Email** | *<Requires input>* | Specify an email address to use for the Transit account. This email address must not already be associated with another AWS account. You must use a valid email address to complete account creation. You can't access the root user of the account or remove an account that was created with an invalid email address. |
| **Management Services Account Email** | *<Requires input>* | Specify an email address to use for the Management services account. This email address must not already be associated with another AWS account. You must use a valid email address to complete account creation. You can't access the root user |

| Parameter | Default | Description |
|---|---|---|
| | | of the account or remove an account that was created with an invalid email address. |
| **AWS GovCloud (US)?** | `true` | Specify true to deploy the Compliant Framework into AWS GovCloud (US). If selecting GovCloud, verify that the current account is a GovCloud (US) / ITAR enabled primary payer account and AWS CLI access keys have been inputted into SSM Parameter Store, per prerequisites. |
| **Deployment Region** | `us-gov-west-1` | Specify the Region to deploy the solution into. This solution will install by default into `us-gov-west-1`. Please contact AWS Professional Services for more information about how to enable this solution to also deploy into `us-gov-east-1` . |
| **Transit Gateway Configuration** | | |
| **Amazon Side Autonomous System Number (ASN)** | `65224` | The Autonomous System Number (ASN) for the AWS side of a Border Gateway Protocol (BGP) session. The range is `64512` to `65534` for 16-bit ASNs. The range is `4200000000` to `4294967294` for 32-bit ASNs. If you have a multi-Region deployment, we recommend that you use a unique ASN for each of your transit gateways. |
| **Firewall A (ASN)** | `65200` | The range is `64512` to `65534` for 16-bit ASNs. The range is `4200000000` to `4294967294` for 32-bit ASNs. If you have a multi-Region deployment, we recommend that you use a unique ASN for each of your transit gateways. |
| **Firewall B (ASN)** | `65210` | The range is `64512` to `65534` for 16-bit ASNs. The range is `4200000000` to `4294967294` for 32-bit ASNs. If you have a multi-Region deployment, we recommend that you use a unique ASN for each of your transit gateways. |

| Parameter | Default | Description |
|---|---|---|
| **Transit Account - Firewall VPC Configuration** | | |
| **Firewall VPC CIDR** | `10.0.0.0/21` | Classless Inter-Domain Routing (CIDR) block for the Transit Virtual Private Cloud (VPC). |
| **(Optional) Firewall VPC NIPR CIDR** | `0.0.0.0/0` | If specified, an additional CIDR range will be added to the VPC. The external subnet CIDR blocks should reflect the usage of this Non-classified Internet Protocol (IP) Router based range. |
| **VPC Instance Tenancy** | `default` | The allowed tenancy of instances launched into the VPC. |
| **External Subnet CIDR Block - Availability Zone A** | `10.0.0.0/24` | CIDR block for the specified subnet. |
| **External Subnet CIDR Block - Availability Zone B** | `10.0.1.0/24` | CIDR block for the specified subnet. |
| **Internal Subnet CIDR Block - Availability Zone A** | `10.0.3.0/24` | CIDR block for the specified subnet. |
| **Internal Subnet CIDR Block - Availability Zone B** | `10.0.4.0/24` | CIDR block for the specified subnet. |
| **Management Subnet CIDR Block - Availability Zone A** | `10.0.6.0/27` | CIDR block for the specified subnet. |
| **Management Subnet CIDR Block - Availability Zone B** | `10.0.6.32/27` | CIDR block for the specified subnet. |
| **Transit Gateway Attachment Subnet CIDR Block - Availability Zone A** | `10.0.7.208/28` | CIDR block for the specified subnet. |
| **Transit Gateway Attachment Subnet CIDR Block - Availability Zone B** | `10.0.7.224/28` | CIDR block for the specified subnet. |
| **Management Services Account - Management Services VPC Configuration** | | |
| **Management Services VPC CIDR** | `10.0.20.0/22` | CIDR block for the Management Services VPC. |
| **VPC Instance Tenancy** | `default` | The allowed tenancy of instances launched into the VPC. |
| **Application Subnet CIDR Block - Availability Zone A** | `10.0.20.0/24` | CIDR block for the specified subnet. |
| **Application Subnet CIDR Block - Availability Zone B** | `10.0.21.0/24` | CIDR block for the specified subnet. |

| Parameter | Default | Description |
|---|---|---|
| **Data Subnet CIDR Block - Availability Zone A** | `10.0.23.0/26` | CIDR block for the specified subnet. |
| **Data Subnet CIDR Block - Availability Zone B** | `10.0.23.64/26` | CIDR block for the specified subnet. |
| **Transit Gateway Attachment Subnet CIDR Block - Availability Zone A** | `10.0.23.208/28` | CIDR block for the specified subnet. |
| **Transit Gateway Attachment Subnet CIDR Block - Availability Zone B** | `10.0.23.224/28` | CIDR block for the specified subnet. |
| **Management Services Account - External Access VPC Configuration** | | |
| **External Access VPC CIDR** | `10.0.24.0/22` | CIDR block for the External Access VPC. |
| **VPC Instance Tenancy** | `default` | The allowed tenancy of instances launched into the VPC. |
| **Public Subnet CIDR Block - Availability Zone A** | `10.0.24.0/27` | CIDR block for the specified subnet. |
| **Public Subnet CIDR Block - Availability Zone B** | `10.0.24.32/27` | CIDR block for the specified subnet. |
| **Application Subnet CIDR Block - Availability Zone A** | `10.0.24.96/27` | CIDR block for the specified subnet. |
| **Application Subnet CIDR Block - Availability Zone B** | `10.0.24.128/27` | CIDR block for the specified subnet. |
| **Transit Gateway Attachment Subnet CIDR Block - Availability Zone A** | `10.0.24.208/28` | CIDR block for the specified subnet. |
| **Transit Gateway Attachment Subnet CIDR Block - Availability Zone B** | `10.0.24.224/28` | CIDR block for the specified subnet. |
| **Management Services Account - Directory VPC Configuration** | | |
| **Directory VPC CIDR** | `10.0.10.0/24` | CIDR block for the Directory VPC. |
| **VPC Instance Tenancy** | `default` | The allowed tenancy of instances launched into the VPC. |
| **Application Subnet CIDR Block - Availability Zone A** | `10.0.10.0/27` | CIDR block for the specified subnet. |
| **Application Subnet CIDR Block - Availability Zone B** | `10.0.10.32/27` | CIDR block for the specified subnet. |

| Parameter | Default | Description |
|---|---|---|
| **Data Subnet CIDR Block - Availability Zone A** | `10.0.10.96/27` | CIDR block for the specified subnet. |
| **Data Subnet CIDR Block - Availability Zone B** | `10.0.10.128/27` | CIDR block for the specified subnet. |
| **Transit Gateway Attachment Subnet CIDR Block - Availability Zone A** | `10.0.10.208/28` | CIDR block for the specified subnet. |
| **Transit Gateway Attachment Subnet CIDR Block - Availability Zone B** | `10.0.10.224/28` | CIDR block for the specified subnet. |

5. Choose **Next**.
6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Be sure to check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
8. Choose **Create stack** to deploy the stack.

   You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a **CREATE_COMPLETE** status in approximately 90 minutes.

**Important**
An Amazon SNS subscription is created using the email address that was provided during template launch. You must accept the subscription notification email that is sent to the supplied notification email. Otherwise, the AWS Step Functions (Commercial Central account) will fail.

# Additional resources

**AWS services**

- Amazon CloudWatch
- Amazon GuardDuty
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon OpenSearch Service (Amazon ES)
- Amazon Inspector
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon S3 Glacier
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS CloudFormation
- AWS CloudTrail
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- AWS Config
- AWS Direct Connect
- AWS Directory Service
- AWS Identity and Access Management
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Organizations
- AWS Security Hub
- AWS Service Catalog
- AWS Single Sign-On
- AWS Step Functions
- AWS Systems Manager
- AWS Transit Gateway
- AWS Virtual Private Network (AWS VPN)
- AWS WAF

**AWS compliance**

- Department of Defense Cloud Computing Security Requirements Guide
- AWS Services in Scope by Compliance Program
- AWS Infrastructure
- Office of the Under Secretary of Defense for Acquisition & Sustainment
- CMMC Model

# Uninstall the solution

To uninstall this solution, first remove all third-party and custom dependencies and resources that have been deployed on top of the solution, such as Next Generation Firewalls (NGFWs).

Resources that have been deployed into accounts that have been created using the GovCloud Account Vending Machine Service Catalog product, such as hosted tenant workloads, must be manually deleted.

AWS accounts that have been created by this solution, such as the Logging, Transit, and Management services accounts, will not be deleted. Use the following instructions to Close an AWS Account.

> **Note**
> This solution can be redeployed to these same accounts if the same email addresses used to create the accounts are used as input parameters to the AWS CloudFormation template.

This solution includes Python scripts to allow you to uninstall the solution.

# Using AWS Command Line Interface

## Prerequisites

To utilize the Compliant Framework uninstallation scripts, you must have both the AWS Command Line Interface (AWS CLI) and Python version 3.8 or later installed. You must also have access to clone the solution's GitHub repository.

**AWS CLI**

The AWS CLI allows you to interact with AWS services from a terminal session. Ensure that you have the latest version of the AWS CLI installed on your system.

- Windows: MSI installer
- Linux, macOS or Unix: Bundled installer

For more details, refer to Installing, updating, and uninstalling the AWS CLI in the *AWS Command Line Interface User Guide*.

**Python**

To uninstall the solution you must have Python version 3.8 or later. For information about downloading and installing Python, refer to the Python website.

If you use Windows, ensure that Python is on your PATH.

To check that Python is on your path, type `python` in a command prompt.

If you already have Python installed, but it's not on your PATH, add it by editing the `PATH` environment variable: under **System Properties**, on the **Advanced** page, select **Environment Variables**.

If you are installing Python, select the **Add Python 3.x to PATH** checkbox on the first screen of the Python installer wizard to ensure that Python is on your PATH.

## Uninstallation

1. Use Git to clone a local copy of the Compliant Framework from GitHub.

```
$ git clone https://github.com/awslabs/compliant-framework-for-federal-and-dod-workloads-
in-aws-govcloud-us.git compliant-framework
```

2. Switch directories to the framework-nuke directory.

```
$ cd ./compliant-framework/deployment/framework-nuke
```

3. Uninstall this solution by reversing the steps used to deploy the solution. Start by removing the AWS CodePipeline pipelines that were deployed in the Central AWS GovCloud (US) account.
   a. Configure your AWS CLI environment to use the Central AWS GovCloud (US) Account.

```
$ aws configure
AWS Access Key ID [***]: <<GOVCLOUD ACCESS KEY ID >>
AWS Secret Access Key [***]: << GOVCLOUD SECRET ACCESS KEY >>
Default region name [us-east-1]: us-gov-west-1
Default output format [json]: << enter >>
```

   b. Run `framework_nuke_environment.py`. This script deletes all resources deployed by the AWS CodePipeline `compliant-framework-environment-pipeline` pipeline into the AWS GovCloud (US) accounts, including the CodePipeline itself.

```
$ python framework_nuke_environment.py --logging-id <logging_account_id> --transit-
west-id <transit_account_id> --management-west-id <management_services_account_id>
```

   Example:

```
$ python framework_nuke_environment.py --logging-id 111111111111 --transit-west-id
 222222222222 --management-west-id 333333333333
```

   c. Run `framework_nuke_core.py`. This script deletes all resources deployed by the CodePipeline `compliant-framework-core-pipeline` pipeline into the AWS GovCloud (US) accounts, including the CodePipeline itself.

```
$ python framework_nuke_core.py --logging-id <logging_account_id>
```

   Example:

```
$ python framework_nuke_core.py --logging-id 111111111111
```

4. After you delete the solution from your AWS GovCloud accounts, you can use the following steps to delete the AWS CloudFormation template from the Commercial Central account:
   a. Configure your AWS CLI environment to use the Central Commercial account.

```
$ aws configure
AWS Access Key ID [***]: << COMMERCIAL ACCESS KEY ID >>
AWS Secret Access Key [***]: << COMMERCIAL SECRET ACCESS KEY >>
Default region name [us-east-1]: us-east-1
Default output format [json]: << enter >>
```

   b. Delete the stack.

```
$ aws cloudformation delete-stack --stack-name compliant-framework
```

# Collection of operational metrics

This solution includes an option to send anonymous operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. When enabled, the following information is collected and sent to AWS:

- **Solution ID:** The AWS solution identifier
- **Unique ID (UUID):** Randomly generated, unique identifier for each deployment
- **Timestamp:** Data-collection timestamp

AWS owns the data gathered through this survey. Data collection is subject to the AWS Privacy Policy. To opt out of this feature, complete the following task:

Modify the AWS CloudFormation template mapping section from:

```
"Mappings": {
  "SolutionHelperAnonymousData14B64A81": {
    "SendAnonymousData": {
      "Data": "Yes"
  }
 }
},
```

to:

```
"Mappings": {
  "SolutionHelperAnonymousData14B64A81": {
    "SendAnonymousData": {
      "Data": "No"
  }
 }
},
```

# Source code

Visit our GitHub repository to download the templates and scripts for this solution, and to share your customizations with others. The `compliant-framework-for-federal-and-dod-workloads-in-aws-govcloud-us` AWS CloudFormation template is generated using the AWS Cloud Development Kit (AWS CDK). Refer to the README.md file for additional information.

# Contributors

The following individuals contributed to this document:

- Randy Domingo
- Todd Davenport
- Jim Collins

# Revisions

| Date | Change | |
|---|---|---|
| December 2020 | Initial release | |

# Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

# AWS glossary

For the latest AWS terminology, see the AWS glossary in the *AWS General Reference*.