



Letter of Certification

December 10, 2018

Amazon Web Services
410 Terry Avenue North
Seattle, WA, 98109-5210

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an approved HITRUST CSF Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST CSF Assurance Program, the following services and infrastructure of the organization meet the HITRUST CSF v9.1 Certification Criteria:

Amazon Web Services (AWS) - AWS Management Environment services below:

- Amazon API Gateway
- Amazon CloudFront
- Amazon CloudWatch Logs
- Amazon Cognito
- Amazon Connect
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS) [both Fargate and EC2 launch types]
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Map Reduce (Amazon EMR)
- Amazon ElastiCache for Redis
- Amazon Inspector
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- Amazon Macie
- Amazon Polly
- Amazon QuickSight
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (Amazon RDS)
- Amazon S3 Glacier
- Amazon S3 Transfer Acceleration
- Amazon SageMaker [excluding Public Workforce and Vendor Workforce]
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- Amazon Simple Workflow Service (SWF)
- Amazon WorkDocs
- Amazon WorkSpaces
- AWS AppSync
- AWS Auto Scaling
- AWS Batch
- AWS CloudFormation
- AWS CloudHSM
- AWS CodeBuild
- AWS CodeCommit
- AWS Config
- AWS Database Migration Service (AWS DMS)
- AWS Direct Connect
- AWS Directory Service (excluding Simple AD and AD Connector)
- AWS Firewall Manager
- AWS Lambda
- AWS Lambda@Edge
- AWS Managed Services
- AWS OpsWorks Stacks
- AWS Secrets Manager
- AWS Service Catalog
- AWS Shield
- AWS Snowball
- AWS Snowball Edge
- AWS Snowmobile
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Web Application Firewall (AWS WAF)
- AWS X-Ray
- Elastic Load Balancing



The certification is valid for a period of two years assuming the following occurs:

- A monitoring program is in place to determine if the controls continue to operate effectively over time
- No data security breach reportable to a federal or state agency by law or regulation has occurred
- No significant changes in the business or security policies, practices, controls and processes have occurred that might impact its ability to meet the HITRUST CSF certification criteria
- Annual progress is being made on areas identified in the Corrective Action Plan(s) (CAPs); and
- Timely completion of the interim review as defined in the HITRUST CSF Assurance Program Requirements.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information security and privacy. With input from leading organizations within the industry, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST CSF Certified. For those HITRUST CSF control requirements that are not currently being met, the organization must have a CAP that outlines its plans for meeting such requirements.

HITRUST performs a quality assurance review consistent with the HITRUST CSF Assurance Program requirements to ensure that the scores are consistent with the testing performed by the approved HITRUST CSF Assessor organization.

A full copy of the HITRUST CSF Certification Report has also been issued to the organization listed above. This full report includes additional details on the scope of the assessment, a representation letter from management, testing results for those controls required for certification, details on CAPs required for HITRUST CSF Certification, and the completed questionnaire. If interested in obtaining a copy of the full report, you will need to contact the organization directly.

Additional information on the HITRUST CSF Certification Program can be found at the HITRUST website: www.hitrustalliance.net.

A stylized, handwritten signature of the word "HITRUST" in dark ink. The letters are connected and have a cursive, fluid appearance.

HITRUST