

Amazon Web Services Partner Package – State and Local Government and Education

April 2019

"This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document and is subject to change. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. 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. For current prices for AWS services, please refer to the AWS website at www.aws.amazon.com."



Table of Contents

| 1.0 | AWS Overview | . 1 |
|---|---|----------------------|
| 1.1 1.2 | AWS and State and Local Government What you can do with AWS | .1 .1 |
| 2.0 3.0 | Benefits of Cloud Computing Shared Responsibility Model | .2 .4 |
| 3.1 3.2 3.3 | Shared Controls for Security and Compliance Data Privacy and Ownership Customer Control of Data Residency | .5 .5 .6 |
| 4.0 | Services Overview | . 6 |
| 4.1 4.2 4.3 4.4 | Compute Services Storage Services Database Services Analytics Services | .7 .7 .7 .7 |
| 4.5 4.6 4.7 4.8 | Networking and Content Delivery Services Migration and Transfer Services Management and Governance Services Security Identity and Compliance Services | .7 .8 .8 |
| 4.9 4.1(4.1 ² 4.12 | Developer Tools | .8 .8 .9 .9 |
| 5.0 | AWS Cloud Infrastructure | . 9 |
| 5.1 5.2 5.3 5.4 | Data Center Physical Location Data Center Audits Data Center Virtual Tours Data Center Security | 10 10 11 11 |
| 6.0 | Automatically Scaling your Resources | 12 |
| 6.1 6.2 6.3 | AWS Auto Scaling Elastic Load Balancing Amazon CloudWatch | 12 13 13 |
| 7.0 | Architecting for High Availability and Reliability | 15 |
| 7.1 7.2 7.3 | AWS Responsibility: Data Center Availability and Reliability Customer Responsibility: Designing for Availability and Reliability Resources and Reference Architecture | 15 15 16 |
| 8.0 | Security | 18 |
| 8.1 | Granting and Managing Account Access | 18 |
| 8 8 8 | .1.1 IAM Users .1.2 IAM Groups .1.3 IAM Roles | 18 19 19 |
| | | |

| 8.1. 8.1. 8.1. | .4 Identity Federation | 19 19 19 |
|----------------------|---|----------------|
| 8.2 8.3 | Tools for Logical Separation | 20 20 |
| 8.3. 8.3. | .1 Protecting Data at Rest | 20 21 |
| 8.4 8.5 8.6 | Automating your Security and Compliance Penetration Testing Security for New AWS Software | 21 21 21 |
| 9.0 C | Compliance | 22 |
| 9.1 | Certifications/Attestations | 23 |
| 9.1. 9.1. 9.1. | Federal Risk and Authorization Management Program (FedRAMP) Federal Information Processing Standard (FIPS) International Organization for Standardization (ISO) 9001:2015 | 23 24 24 |
| 9.1. | .4 ISO/IEC 27001:2013 | 25 |
| 9.1. | .5 ISO/IEC 27017:2015 | 26 |
| 9.1. 9.1. | .7 Pavment Card Industry Data Security Standard (PCI DSS) | 20 27 |
| 9.1. | .8 SOC Reports | 27 |
| 9.2 | Laws/Regulations/Privacy | 29 |
| 9.2. 9.2. Info | .1 Family Educational Rights and Privacy Act (FERPA) | 29 th 30 |
| 9.2. | .3 Internal Revenue Service Publication 1075 (IRS Pub 1075) | 31 |
| 9.2. | .4 Voluntary Product Accessibility Template (VPAT)/Section 508 | 31 |
| 9.3 | Alignments/Frameworks | 32 |
| 9.3. | .1 Criminal Justice Information Services (CJIS) | 32 |
| 9.3. | .2 Cloud Security Alliance (CSA) | 34 |
| 9.3. Q 3 | .3 Federal Information Security Management Act (FISMA) | 34 35 |
| 9.3. | .5 Uptime Institute Tiers | 36 |
| 10.0 N | /anaging your AWS Resources | 37 |
| 10.1 | AWS Management Console | 37 |
| 10.2 | Command Line Interface | 38 |
| 10.3 | AWS Developer Tools | 38 |
| 10.4 | Management Tools | 38 |
| 11.0 B | Back-up and Disaster Recovery | 39 |
| 11.1 | Disaster Recovery on AWS | 39 |
| 12.0 S | Security Questionnaires | 41 |



| 41 |
|----|
| 42 |
| 44 |
| 44 |
| 44 |
| 44 |
| 44 |
| 44 |
| 44 |
| 44 |
| 45 |
| 45 |
| 45 |
| 45 |
| 45 |
| 45 |
| 45 |
| 45 |
| 46 |
| 46 |
| 46 |
| 46 |
| 46 |
| 46 |
| 46 |
| 47 |
| 47 |
| 47 |
| 47 |
| 47 |
| |



Tables and Figures

| Table 1– Benefits of the Cloud | 2 |
|---|---|
| Table 2 – Summary of AWS Assurance Programs | |
| Table 3 – AWS SOC Reports | |

| Figure 1 - Number of Total Features by Cloud Provider | 2 |
|--|-------|
| Figure 2 - Significant service and feature releases - AWS has launched more than | 4,300 |
| new features and/or services since 2006 | 3 |
| Figure 3 – AWS Shared Responsibility Model | 4 |
| Figure 4 – Map of North American AWS Regions and Availability Zones | 9 |
| Figure 5 – Regions and Availability Zones | 10 |
| Figure 6 – Auto Scaling with Elastic Load Balancing and Amazon CloudWatch alar | ms 14 |
| Figure 7 – Fault Tolerant AWS Reference Architecture | 17 |
| Figure 8 – Spectrum of DR Options. | 39 |
| Figure 9 – Gartner 2018 Magic Quadrant for Cloud IaaS, Worldwide | 42 |
| Figure 10 – Gartner 2018 Magic Quadrant for Public Cloud Storage Services, | |
| Worldwide | 43 |



How to Use this Document

This document contains information on the most frequently requested proposal topics from our AWS Partner Network (APN) Partners. Please reach out to your proposal manager if you need additional information to meet specific RFx requirements.

The content in this document is intended as informational material regarding AWS Services that may be used to inform your responses to particular requests for proposal/quotation/tender, etc. (RFx) from your public sector customers. While AWS encourages you to rely on the Partner Package content to formulate your response, you may not attach the Partner Package to your response or copy and paste Partner Package content into your response without prior consent from AWS. Graphics or images may be copied and pasted into your response, as long as clear and appropriate attribution is given to AWS or the third party source of such images, and such images are copied in their entirety and without modification.

AWS is not a party to any contract resulting from a proposal/tender. As it relates to your RFx response, AWS is a supplier—not a subcontractor—and we are not submitting a joint response or co-drafting a project scope. Your response must be on your letterhead and in your voice. AWS cannot write your response—or any part of your response—on your behalf.

AWS Partner Package - SLED



Guidance on Service Name Usage

On first use, all service names must be written out completely. After that, you may abbreviate the service name in conformance with the service names noted in parentheses below. Note that these are our most commonly referenced services. For questions regarding usage of a service name that does not appear here, please contact your AWS proposal manager. The following service names must always include "Amazon" based on trademark rights:

Amazon Pinpoint

Amazon QuickSight

Amazon Machine Learning (Amazon ML)

- Amazon Cognito
- Amazon Glacier
- AWS Config
- Amazon Inspector
- Amazon Kinesis

Amazon Redshift Amazon Chime

.

.

- AWS CodeStar
- Amazon GameLift
- Amazon Polly
- Amazon Rekognition

| Amazon API Gateway (API Gateway) | AWS Device Farm (Device Farm) | AWS Key Management Service (AWS KMS) | |
|--|---|--|--|
| AWS Application Discovery Service (Application Discovery Service) | Amazon DevPay (DevPay) | AWS Lambda (Lambda) | |
| Amazon AppStream 2.0 (AppStream 2.0) | AWS Direct Connect | AWS OpsWorks | |
| AWS Auto Scaling | AWS Directory Service | Amazon Relational Database Service (Amazon RDS) | |
| AWS Billing and Cost Management (Billing and Cost Management) | Amazon DynamoDB (DynamoDB) | Amazon Route 53 (Route 53) | |
| AWS CloudFormation | Amazon EC2 Container Registry (Amazon ECR) | AWS Security Token Service (AWS STS) | |
| Amazon CloudFront (CloudFront) | Amazon EC2 Container Service (Amazon ECS) | AWS Server Migration Service (AWS SMS) | |
| AWS CloudHSM | AWS Elastic Beanstalk (Elastic Beanstalk) | AWS Service Health Dashboard | |
| Amazon CloudSearch | Amazon Elastic Block Store (Amazon EBS) | AWS Shield | |
| AWS CloudTrail (CloudTrail) | Amazon Elastic Compute Cloud (Amazon EC2) | Amazon Simple Email Service (Amazon SES) | |
| Amazon CloudWatch (CloudWatch) | Amazon Elastic File System (Amazon EFS) | Amazon Simple Notification Service (Amazon SNS) | |
| Amazon CloudWatch Logs (CloudWatch Logs) | Elastic Load Balancing | Amazon Simple Queue Service (Amazon SQS) | |
| AWS CodeCommit | Amazon Elastic Transcoder (Elastic Transcoder) | Amazon Simple Storage Service (Amazon S3) | |
| AWS CodeDeploy | Amazon ElastiCache (ElastiCache) | Amazon Simple Workflow Service (Amazon SWF) | |
| AWS CodePipeline | Amazon Elasticsearch Service (Amazon ES) | AWS Snowball (Snowball) | |
| AWS Command Line Interface (AWS CLI) | Amazon EMR | AWS Storage Gateway | |
| AWS Config | Amazon Glacier | AWS Trusted Advisor (Trusted Advisor) | |
| AWS Data Pipeline | AWS Identity and Access Management (IAM) | Amazon Virtual Private Cloud (Amazon VPC) | |
| AWS Database Migration Service (AWS DMS) | AWS Import/Export | AWS WAF | |

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.



1.0 AWS Overview

Amazon has a long history of using a decentralized IT infrastructure. After over a decade of building and running the highly scalable e-commerce website Amazon.com, the company realized that it had developed a core competency in operating massive scale technology infrastructure and data centers. Amazon then embarked on a much broader mission of serving a new customer segment—developers and businesses— with web services customers can use to build sophisticated, scalable applications. Today, Amazon Web Services, Inc. (AWS) is the fastest-growing multi-billion enterprise IT vendor in the world. AWS has been operating since 2006 and currently supports an almost limitless variety of workloads for millions of customers worldwide.

1.1 AWS and State and Local Government

The AWS Cloud is uniquely positioned to provide scalable, cost-efficient solutions to the State and Local public sector, whether through open data initiatives, public safety modernization, education reform, citizen service improvements, or infrastructure programs. AWS cloud services can be employed to meet mandates, reduce costs, drive efficiencies, and increase innovation. Over 4,000 government agencies, over 9,000 academic institutions, and over 27,000 nonprofit organizations around the world are already using AWS to address a diverse set of use cases.

1.2 What you can do with AWS

With AWS, you can programmatically provision, monitor, and automate all the components of your cloud environment. AWS offers more than 165 fully featured services, including compute, storage, networking, database, analytics, application services, deployment, management, developer, mobile, internet of things (IoT), artificial intelligence (AI), security, hybrid, and enterprise applications, all of which are listed at <u>AWS Cloud Products</u>.

AWS offerings are provided with a range of <u>supporting components</u> like management tools, networking services, and application augmentation services. These supporting components have multiple interfaces to AWS application programming interface (API)based services, including software development kits (SDKs), integrated development environment (IDE) toolkits, and command line tools. AWS tools and features enable you to maintain consistent controls without restricting development velocity.

AWS provides four kinds of <u>management tools</u>: provisioning, operations management, monitoring and logging, and managed services for configuration management. These management tools work together and are integrated with every part of the AWS Cloud, allowing you to easily control all parts of your cloud infrastructure.



2.0 Benefits of Cloud Computing

Table 1 highlights the benefits of cloud computing, many of which are unique to the AWS Cloud.

| Cloud | Benefit to Customers | | |
|--|---|--|--|
| Trade Capital Expense for VariableThe fundamental cloud model, cust heavily in data ce (capital expense) consume (variable) | The fundamental difference between cloud computing and traditional IT is that in a cloud model, customers are not buying physical assets. Instead of having to invest heavily in data centers and servers before you know how you're going to use them (capital expense), you can use cloud computing and only pay for the resources you consume (variable expense). | | |
| Access to Greater Service Breadth and Depth Cloud computing allows you to acco- industry-shaping technology quickl and at an affordal cost, no matter withe scale. AWS has develop the broadest collection of servi available from any cloud provider (Figure 1). We have been continually expanding our services to suppor virtually any cloud workload, and we now have more the 165 services that from compute, stor networking, datated analytics, applica more. Refer to the third-party assess | ess storage security, Identity & Compliance Networking & Content Delivery Mobile Services Management Tools Internet of Things Developer Tools Developer Tools Database Compute Business Productivity Artificial Intelligence Analytics An | | |
| Scalability When you make a either end up sitti With cloud compu as you need and Combining softwa programming met resources (and co | When you make a capacity decision prior to deploying an application, you often either end up sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little as you need and scale up and down as required with only a few minutes' notice. Combining software-defined infrastructure with AWS products featuring modern programming methods lets you design your computerized systems to rapidly scale resources (and costs) up or down based on the actual demands on the system. | | |
| Increase Speed and Agility In a cloud compute means you reduct developers from v for the organization | In a cloud computing environment, new IT resources are only a click away, which means you reduce the time it takes to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower. You also have continual access to the newest resources and services to keep your business on the leading edge. | | |
| significantly lower services to keep y | e the time it takes to make those resources available to your weeks to just minutes. This results in a dramatic increase in agility on, since the cost and time it takes to experiment and develop is . You also have continual access to the newest resources and your business on the leading edge. | | |

Table 1– Benefits of the Cloud

parallel fleets are not always used optimally: a lot of expensive hardware sits unused for long periods of time. In the AWS Cloud, you can provision testing fleets as you need them. Additionally, you can simulate user traffic on the AWS Cloud during load testing. You can also use these parallel fleets as a staging environment for a new production release, enabling quick switchover from current production to a new application version with little or no service outages.

| Pace of Innovation | Since our inception, AWS has been an innovator in defining cloud computing by working to get new products into the hands of customers quickly, then rapidly iterating and improving on those products based on customer feedback. Our continual innovation helps customers maintain state-of-the-art IT infrastructure without having to make recapitalization investments. | 722 722 82 2011 2013 2015 2017 Figure 2 – AWS has launched more than 4,300 new features and/or services since 2006 | | |
|--|--|---|--|--|
| Benefit from Massive Economies of Scale | By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from millions of customers is aggregated in the cloud, AWS can achieve high economies of scale, which translates into lower prices. AWS continues to lower the cost of cloud computing for our customers. We continually focus on reducing our data center hardware costs, improving our operational efficiencies, lowering our power consumption, and passing savings back to customers. We have a history of continually lowering prices and have reduced prices 69 times since AWS launched in 2006. | | | |
| Global Footprint | Cloud computing allows you to easily deploy applications in multiple geographic regions around the world with just a few clicks, providing higher availability, lower latency, and a better experience at minimal cost. AWS currently has 20 geographic Regions and 61 Availability Zones throughout the world (with 12 more Availability Zones and 4 more Regions announced). Information on each Region can be found at <u>AWS Global Infrastructure</u> . | | | |
| Security and Compliance | AWS customers obtain greater security in the cloud than is available in traditional data centers. The AWS Cloud infrastructure has been designed and managed in alignment with many regulations, standards, and industry best practices, and AWS manages over 1,800 security controls. AWS is under a constant state of audit to comply with multiple risk management and compliance regimes, all of which are described on the <u>AWS Compliance page</u> . AWS also offers a suite of services to help you manage security and compliance, from access control to encryption to threat detection. | | | |
| Auditability | The message-based interoperability of web services allows customer configuration and use of AWS products to be uniformly logged, monitored, and audited. <u>AWS</u> <u>CloudTrail</u> , for example, records API calls to supported AWS Cloud services within your account. | | | |
| Focus on Core Competencies | The ultimate benefit of the clouundifferentiated tasks and mo value to their organizations. | cloud is that customers can spend less time on more time focusing on the core competencies that add 5. | | |

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.



3.0 Shared Responsibility Model

Because our customers build systems on top of AWS Cloud infrastructure, security and compliance responsibilities are shared between AWS and the customer. This <u>shared</u> <u>responsibility model</u> can help relieve customers' 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 service operates. Customers—and in some cases, our AWS Partner Network (APN) Partners who work with those customers—control how they architect and secure their applications and data put on the AWS Cloud. AWS provides a wide array of security and compliance services, and customers should carefully consider the services used, integration of those services into their IT environment, and applicable laws and regulations. AWS's shared responsibility/security model is depicted in **Figure 3**.



Figure 3 – AWS Shared Responsibility Model

This differentiation of responsibility is commonly referred to as security *of* the cloud versus security *in* the cloud.

- **AWS Responsibility (Security of the Cloud)** AWS is responsible for protecting the infrastructure that runs all of the services offered on the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.
- Customer/APN Partner Responsibility (Security in the Cloud) Customers/APN Partners assume responsibility and management of the guest operating system (including updates and security patches); other associated application software; configuration of the AWS-provided security group firewalls; and other security, change management, and logging features.

AWS's shared responsibility model is further explained on the AWS Compliance webpage.



3.1 Shared Controls for Security and Compliance

Some controls apply to both the infrastructure layer (AWS responsibility) and customer layers (customer/APN Partner responsibility), but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure, and the customer/APN Partner must provide their own control implementation within their use of AWS Cloud services. Examples of these shared controls include the following:

- Patch Management AWS is responsible for patching and fixing flaws within the infrastructure, but customers/APN Partners are responsible for patching their guest operating systems and applications.
- Configuration Management AWS maintains the configuration of its infrastructure devices, but customers/APN Partners are responsible for configuring their own guest operating systems, databases, and applications.
- Awareness and Training AWS trains AWS employees, but customer/APN Partners must train their own employees.

For example, services such as <u>Amazon Elastic Compute Cloud (Amazon EC2)</u>, <u>Amazon Virtual Private Cloud (Amazon VPC)</u>, and <u>Amazon Simple Storage Service (Amazon S3</u>) are categorized as infrastructure as a service (IaaS) and, as such, require the customer to perform all of the necessary security configuration and management tasks. If a customer deploys an Amazon EC2 instance, they are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

3.2 Data Privacy and Ownership

As a customer, you maintain ownership of your content, and you select which AWS Cloud services can process, store, and host your content. We do not access or use your content for any purpose without your consent. AWS gives you ownership and control over your content through simple, powerful tools that allow you to determine where your content will be stored, secure your content in transit and at rest, and manage your access to AWS Cloud services and resources for your users. We also implement responsible and sophisticated technical and physical controls that are designed to prevent unauthorized access to or disclosure of your content.

Four basic rules of ownership and control of customer content include the following:

 Access – As a customer, you manage access to your content and user access to AWS Cloud services and resources. We provide an advanced set of access, encryption, and logging features to help you do this effectively (such as <u>AWS</u> <u>CloudTrail</u>). We do not access or use your content for any purpose without your consent. Customer virtual instances are solely controlled by the customer who has full root access or administrative control over accounts, services, and applications. AWS personnel do not have the ability to log into customer instances. We never use your content or derive information from it for marketing or advertising.



- **Geographical Location of Data** You choose the AWS Region(s) in which your content is stored. We do not move or replicate your content outside of your chosen AWS Region(s) without your consent.
- Security You choose how your content is secured, including via tokenization, data decomposition, cyber detection, and encryption. We have developed a security assurance program that uses best practices for global privacy and data protection to help you operate securely within AWS, and to make the best use of our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments. We also offer you strong encryption for your content in transit and at rest, and we provide you with the option to manage your own encryption keys.
- Disclosure of Customer Content We do not disclose customer content unless we're required to do so to comply with the law, or with a valid and binding order of a governmental or regulatory body. Unless we are prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing customer content so they can seek protection from disclosure. Additional information can be found in our latest transparency report and our <u>Amazon Law Enforcement Guidelines</u>.

3.3 Customer Control of Data Residency

Some customers mandate <u>data residency</u>—the requirement that all customer content processed and stored in an IT system remain within specific geographical borders. Although data residency does not inherently mean stronger security, it is possible for customers to adhere to these regulations on AWS. Customers own their data and choose the Region(s) in which they store their data. AWS does not access customer data, and it does not move unless the customer decides to move it. It is therefore possible for a customer to benefit from our inherited physical and environmental controls while still keeping their data within the United States. Read more in our <u>Data Residency</u> policy perspectives whitepaper.

4.0 Services Overview

AWS has been continually expanding its services to support virtually any cloud workload. We now have more than 165 fully featured services.

Our <u>AWS Documentation</u> page provides user guides, developer guides, API references, and tutorials to help our customers and APN Partners get started on AWS and learn more about each of our services. You can also watch videos or read through AWS reference architectures and architecture whitepapers at <u>AWS Architecture Center</u>. Further, you can visit the AWS <u>This is My Architecture</u> web page for innovative cloud architectures from customers and APN Partners.



4.1 Compute Services

AWS offers a comprehensive portfolio of <u>compute services</u>, allowing you to develop, deploy, run, and scale your applications and workloads in the world's most powerful, secure, and innovative compute cloud. Our compute services range from virtual machines and servers—with <u>Amazon EC2</u> and <u>Amazon Lightsail</u>—to containers and serverless computing—with <u>Amazon Elastic Container Service (Amazon ECS)</u> and <u>AWS Lambda</u>.

4.2 Storage Services

AWS offers a complete range of <u>cloud storage services</u> to support both application and archival compliance requirements. Select from object, file, and block storage services like <u>Amazon S3</u>, <u>Amazon Elastic File System (Amazon EFS)</u>, and <u>Amazon Elastic Block</u> <u>Store (Amazon EBS)</u>—and archive, backup, and hybrid storage—like <u>Amazon S3</u> <u>Glacier</u>, <u>AWS Backup</u>, and <u>AWS Storage Gateway</u>.

4.3 Database Services

AWS offers fully managed <u>database services</u> such as relational databases for transactional applications (<u>Amazon Aurora</u> and <u>Amazon Relational Database Service</u> [<u>Amazon RDS</u>]), non-relational databases for internet-scale applications (<u>Amazon DynamoDB</u>), a data warehouse for analytics (<u>Amazon Redshift</u>), an in-memory data store for caching and real-time workloads (<u>Amazon ElastiCache</u>), a graph database for building applications with highly connected data (<u>Amazon Neptune</u>), a time series database for measuring changes over time (<u>Amazon Timestream</u>), and a ledger database to maintain a complete and verifiable record of transactions (<u>Amazon Quantum Ledger Database [Amazon QLDB</u>]).

4.4 Analytics Services

Each analytic service AWS provides is purpose-built for a wide range of analytics use cases such as interactive analysis (<u>Amazon Athena</u>), big data processing using Apache Spark and Hadoop (<u>Amazon EMR</u>), data warehousing (<u>Amazon Redshift</u>), real-time analytics (<u>Amazon Kinesis</u>), operational analytics (<u>Amazon Elasticsearch Service</u>), data catalog (<u>AWS Glue</u>), integrated data lake service (<u>AWS Lake Formation</u>), and dashboards and visualizations (<u>Amazon QuickSight</u>).

4.5 Networking and Content Delivery Services

AWS <u>networking and content delivery services</u> enable you to isolate your cloud infrastructure with <u>Amazon VPC</u>, scale your request handling capacity with <u>Elastic Load</u> <u>Balancing</u>, and connect your physical network to your private virtual network with <u>AWS</u> <u>Direct Connect</u>. We also offer a secure global content delivery network (CDN) with <u>Amazon CloudFront</u> and a scalable cloud Domain Name Service (DNS) with <u>Amazon Route 53</u>.



4.6 Migration and Transfer Services

Whether you're migrating a server, database, or raw data into the AWS Cloud, AWS offers a suite of tools to help you with your migration. <u>AWS Server Migration Service</u> (<u>AWS SMS</u>), for example, allows you to automate, schedule, and track incremental replications of live server volumes. <u>AWS Database Migration Service (DMS</u>) helps you migrate databases while the source database remains fully operational. The <u>AWS Snow Family</u> of devices helps you to physically transport up to exabytes of data into and out of the AWS Cloud. To help track your migration, <u>AWS Migration Hub</u> provides a single location to track the progress of application migrations across multiple AWS solutions. In addition, <u>AWS Application Discovery Service</u> helps you plan migration projects by gathering information about your on-premises data centers.

4.7 Management and Governance Services

AWS provides a set of <u>management tools</u> that allows you to programmatically provision, monitor, and automate all the components of your cloud environment. Using these tools, you can maintain consistent controls without restricting development velocity. AWS provides four kinds of management tools that work together and are integrated with the AWS platform. These tools include provisioning tools such as AWS <u>CloudFormation</u>, operations management tools such as <u>AWS Systems Manager</u>, monitoring and logging tools such as <u>Amazon CloudWatch</u>, and configuration management services such as <u>AWS OpsWorks</u>.

4.8 Security, Identity, and Compliance Services

AWS provides <u>security tools and services</u> that can help you every step of the way to ensure understanding of and transition to a secure cloud, from encryption with <u>Amazon</u> <u>Key Management Service (KMS)</u> to threat detection with <u>Amazon GuardDuty</u> to Distributed Denial of Service (DDoS) protection with <u>AWS Shield</u>. <u>AWS Identity and</u> <u>Access Management (IAM)</u> allows customers to have granular control over access to your services. Furthermore, <u>Amazon Macie</u> can help you discover, classify, and protect your most sensitive data.

4.9 Developer Tools

The <u>AWS Developer Tools</u> is a set of services designed to enable developers and IT operations professionals practicing <u>DevOps</u> to rapidly and safely deliver software. Together, these services help you securely store and version control your application's source code and automatically build, test, and deploy your application to AWS or your on-premises environment.

4.10 Machine Learning and IoT Services

AWS offers pre-trained AI services for computer vision, language, recommendations, and forecasting. <u>Amazon SageMaker</u> helps you to quickly build, train and deploy machine learning models at scale. Since AWS IoT integrates with AI services, you can make your devices smarter, even without internet connectivity. <u>AWS IoT</u> provides broad



and deep functionality so you can build IoT solutions for virtually any use case across a wide range of devices.

4.11 Mobile Services

AWS offers a suite of services for building and deploying mobile applications, including <u>AWS Amplify</u> for provisioning and managing backends for your mobile applications, <u>AWS Device Farm</u> for app testing, and <u>Amazon Pinpoint</u> for customer engagement.

4.12 Other Services

In addition to the types of services listed above, AWS also offers <u>services</u> for application integration, desktop apps, blockchain, call center, media streaming, satellite, robotics, AR/VR, game development, and more.

5.0 AWS Cloud Infrastructure

Our AWS Cloud infrastructure allows customers to build solutions that are more highly available, fault tolerant, and scalable than would be possible with a single data center. This is because the AWS Cloud infrastructure is built around Regions and Availability Zones. A Region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities.

AWS currently has 6 regions and 21 Availability Zones in the United States. **Figure 4** depicts the current AWS Regions and Availability Zones in North America. Information on each region can be found at the <u>AWS Global Infrastructure</u> page. The AWS products and services that are available in each region are listed at the <u>Region Table</u> webpage.



US East (Northern Virginia) Availability Zones: 6 Launched 2006

US East (Ohio) Availability Zones: 3

Launched 2016

US West (Oregon) Availability Zones: 3 Launched 2011

US West (Northern California) Availability Zones: 3 (new customers can access 2) Launched 2009

GovCloud (US-West) Availability Zones: 3 Launched 2011

GovCloud (US-East) Availability Zones: **3** Launched 2018



Figure 5 illustrates the relationship between regions and Availability Zones.



Figure 5 – Regions and Availability Zones

5.1 Data Center Physical Location

AWS does not disclose the exact location of data centers and does not allow data center access to customers, as this exposes a wide range of customers to physical access of a third party. To meet this customer need, an independent and competent auditor validates the presence and operation of controls as part of our System and Organization Controls (SOC 1) Type 2 report. This broadly accepted third-party validation provides customers with the independent perspective of the effectiveness of controls in place. AWS customers that have signed a non-disclosure agreement (NDA) with AWS may request a copy of the SOC 1 Type 2 report.

5.2 Data Center Audits

Instead of allowing customers to perform physical audits, AWS has an independent third party perform audits of its data centers. These audits are conducted in accordance with the Federal Risk and Authorization Management Program (FedRAMP), American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements [SSAE] 16), and International Standards for Assurance Engagements (ISAE) 3402 professional standards.

The auditors produce a SOC 1 Type 2 report in connection with the audit. Independent reviews of data center physical security are also part of an International Organization for Standardization (ISO) 27001 audit, a Payment Card Industry (PCI) Data Security Standard (DSS) assessment, and an International Traffic in Arms Regulations (ITAR) audit.

Our rigorous attention to auditing provides peace of mind to our customers. Much as a customer trusts a bank based on reputation and regulation by the Federal Deposit Insurance Corporation (FDIC), our customers trust the independent third party audits described above. It is widely accepted that such accrediting organizations are competent and qualified to assure customer confidence and acceptance without a personal inspection and accreditation—or customers having to hire their own accreditor.



To help you fulfill your own audit and regulatory requirements, we detail our controls on our <u>website</u>.

5.3 Data Center Virtual Tours

You can take a <u>virtual tour</u> of our data centers. The following provides a list of each data center layer with a link to a virtual tour for each one.

- **Perimeter Layer** AWS data center physical security begins at the <u>Perimeter</u> <u>Layer</u>. This layer includes a number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.
- Infrastructure Layer The Infrastructure Layer is the data center building and the equipment and systems that keep it running. Components like back-up power equipment, the HVAC system, and fire suppression equipment are all part of the Infrastructure Layer. These devices and systems help protect servers and ultimately your data.
- Data Layer The <u>Data Layer</u> is the most critical point of protection because it is the only area that holds customer data. Protection begins by restricting access and maintaining a separation of privilege for each layer. In addition, we deploy threat detection devices, video surveillance, and system protocols, further safeguarding this layer.
- Environmental Layer The Environmental Layer is dedicated to environmental considerations from site selection and construction to operations and sustainability. AWS carefully chooses our data center locations to mitigate environmental risk such as flooding, extreme weather, and seismic activity.

5.4 Data Center Security

AWS's data centers are state of the art, using innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS Cloud. The following subsections address some of our customers' frequently asked questions about our data center security.

 Physical and Environmental Security – AWS data centers are housed in nondescript facilities for anonymity. Physical access is strictly controlled at both the perimeter and at building ingress points by professional security staff using video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or AWS. All physical access to data centers by AWS employees is logged and audited.



- Fire Detection and Suppression Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.
- Power The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations 24 hours a day and seven days a week. Uninterruptible power supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.
- **Climate and Temperature** Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.
- Physical Plant Management AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.
- Storage Device Decommissioning As part of AWS's storage decommissioning process, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process.

AWS will provide the SOC 1 Type 2 report to customers under NDA. The <u>AWS Security</u> <u>Center</u> provides up-to-date information on AWS audits by independent third-party auditors.

6.0 Automatically Scaling your Resources

To be confident that your infrastructure can handle a spike in traffic, you can use AWS Auto Scaling and Elastic Load Balancing to automatically scale your AWS cloud-based resources up to meet unexpected demand, and then scale those resources down as demand decreases. While AWS Auto Scaling adjusts capacity for multiple resources, Elastic Load Balancing distributes incoming application traffic across targets such as Amazon EC2 instances and containers.

6.1 AWS Auto Scaling

<u>AWS Auto Scaling</u> monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. The service provides a user interface that lets you build scaling plans for resources including <u>Amazon EC2</u> instances and Spot Fleets, <u>Amazon ECS</u> tasks, <u>Amazon DynamoDB</u> tables and indexes, and <u>Amazon Aurora</u> Replicas.



Auto Scaling maintains the number of instances that you specify by performing periodic health checks on the instances in the group. If an instance becomes unhealthy, the group terminates the unhealthy instance and launches another instance to replace it.

Auto Scaling policies can be used to automatically increase or decrease the number of running Amazon EC2 instances in a group of servers to meet changing conditions. When the scaling policy is in effect, the Auto Scaling group adjusts the desired capacity of the group and launches or terminates the instances as needed, either dynamically or on a schedule if there is a known and predictable ebb and flow of traffic.

6.2 Elastic Load Balancing

<u>Elastic Load Balancing</u> automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and AWS Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. When combined with Auto Scaling, the number of healthy nodes is automatically rebalanced with the other Availability Zones, and no manual intervention is required.

Elastic Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault tolerant:

- Application Load Balancer Best suited for load balancing of HTTP and HTTPS traffic
- **Network Load Balancer** Best suited for load balancing of Transmission Control Protocol (TCP) traffic where extreme performance is required
- Classic Load Balancer Best suited for applications that were built within the Amazon EC2-Classic network

6.3 Amazon CloudWatch

Customers can use <u>Amazon CloudWatch</u> to collect and track metrics, collect and monitor log files, and set alarms. Customers can architect their solutions so that Amazon CloudWatch's metrics and alarms can work together with Auto Scaling and Elastic Load Balancing to dynamically deploy new instances on-demand, as depicted in **Figure 6**. This type of automation takes some of the administrative burden off of the customer and allows the infrastructure to manage itself on-the-fly.



Figure 6 – Auto Scaling with Elastic Load Balancing and Amazon CloudWatch alarms

7.0 Architecting for High Availability and Reliability

Availability and reliability are shared responsibilities between AWS and the customer. AWS is responsible for ensuring that our services are continuously available and that we are prepared to handle a wide range of events that could affect our infrastructure. You are responsible for designing, deploying, and testing your applications on AWS to achieve the availability and resiliency you need, including for mission-critical applications that require almost no downtime. The following subsections further detail AWS and customer responsibilities for availability and reliability.

7.1 AWS Responsibility: Data Center Availability and Reliability

AWS builds to guard against outages and incidents, and we account for them in the design of our services—so when disruptions do occur, their impact on customers and the continuity of services is as minimal as possible.

To minimize disruptions, AWS employs compartmentalization. We have multiple constructs that provide different levels of independent, redundant components. For example, our Regions are isolated from each other, meaning that a disruption in one Region does not result in contagion in other Regions. Our Availability Zones are physically separated and isolated, and they are built with highly redundant networking to withstand local disruptions. AWS also leverages a concept known as cell-based architecture, by which resources and requests are partitioned into "cells" that are designed to be independent of each other. This design minimizes the chance that a disruption in one cell—for example, one subset of customers—would disrupt other cells.

Additionally, although the likelihood of large-scale incidents is very low, AWS is prepared to manage them should they occur. We maintain a series of incident response plans covering both common and uncommon events, and we update them regularly to incorporate lessons learned and prepare for emerging threats.

7.2 Customer Responsibility: Designing for Availability and Reliability

While AWS goes to great lengths to provide availability and reliability *of* the cloud, our customers share responsibility for ensuring availability and reliability *within* the cloud. Some best practices we recommend for building highly resilient systems on the AWS Cloud include the following:

- Design for Failure It is best practice to architect across multiple AZs in the same Region to achieve extremely high Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and service availability. For mission-critical applications, it is best practice to architect across Regions to handle the rare case of an entire Region failing—perhaps as a result of a major physical attack.
- Automate Failover and Recovery You can use <u>AWS Auto Scaling</u> to monitor your applications and automatically adjust capacity to maintain the optimal level to satisfy demand without over- or under-provisioning. You can also use <u>AWS</u>



<u>Personal Health Dashboard</u>, which provides alerts and remediation guidance when AWS is experiencing events that may impact you. AWS Personal Health Dashboard can integrate with <u>Amazon CloudWatch</u> Events, enabling you to build custom rules and select targets such as AWS Lambda functions to define automated remediation actions.

• **Test your Recovery Procedures** – You can use a test environment to simulate different failures or to recreate scenarios that led to failures before. This exposes failure pathways that you can test and fix before a real failure scenario, reducing the risk of components that have not been tested before failing.

7.3 **Resources and Reference Architecture**

<u>Building Fault-Tolerant Applications on AWS</u> is a great introduction to achieving high availability in the cloud. In addition, the <u>AWS Well-Architected Framework</u> codifies the experiences of thousands of customers, helping customers assess and improve their cloud-based architectures and mitigate disruptions. Our <u>Reliability Pillar</u> whitepaper provides guidance to help you apply best practices to achieve reliability.

In addition, the <u>AWS Architecture Center</u> is designed to provide customers with the necessary guidance and application architecture best practices to build highly scalable and reliable applications in the AWS Cloud. These resources provide architectural guidance for design and implementation of systems that run on the AWS infrastructure.

Figure 7 provides a reference architecture for fault tolerance and high availability.





System Overview

Load balancing is an effective way to increase the availability of a system. Instances that fail can be replaced seamlessly behind the load balancer while other instances continue to operate. Elastic Load Balancing can be used to balance across instances in multiple availability zones of a region.

Availability zones (AZs) are distinct geographical locations that are engineered to be insulated from failures in other AZs. By placing Amazon EC2 instances in multiple AZs, an application can be protected from failure at a single location. It is important to run independent application stacks in more than one AZ, either in the same region or in another region, so that if one zone fails, the application in the other zone can continue to run. When you design such a system, you will need a good understanding of zone dependencies.

Elastic IP addresses are public IP addresses that can be programmatically mapped between instances within a region. They are associated with the AWS account and not with a specific instance or lifetime of an instance.

With a specific instance or intetime of an instance. Elastic IP addresses can be used to work around host or availability zone failures by quickly remapping the address to another running instance or a replacement instance that was just started. Reserved instances can help guarantee that

such capacity is available in another zone. Valuable data should never be stored only on instance storage without proper backups, replication, or the ability to re-create the data. Amazon Elastic Block Store (EBS) offers persistent off-instance storage volumes that are about an order of magnitude more durable than on-instance storage. EBS volumes are automatically replicated within a single availability zone. To increase durability further, point-intime snapshots can be created to store data on volumes in Amazon S3, which is then replicated to multiple AZs. While EBS volumes are tied to a specific AZ, snapshots are tied to the region. Using a snapshot, you can create new EBS volumes in any of the AZs of the same region. This is an effective way to deal with disk failures or other host-level issues, as well as with problems affecting an AZ. Snapshots are incremental, so it is advisable to hold on to recent snapshots.

Figure 7 – Fault Tolerant AWS Reference Architecture

8.0 Security

AWS manages over 1,800 security controls to provide a secure environment for our customers. The AWS virtual infrastructure is designed to provide optimum availability while ensuring customer security, privacy, and segregation. AWS's highly secure data centers use state-of-the-art electronic surveillance and multi-factor access control systems and maintain strict, least-privileged-based access authorizations. Our environmental systems are designed to minimize the impact of disruptions to operations, and our multiple Regions and Availability Zones allow customers to remain resilient in the face of most failure modes. AWS Regions are connected to multiple internet service providers (ISPs) as well as to a private global network backbone, which provides lower cost and more consistent cross-region network latency when compared with the public internet.

The following subsections provide further information on some of our most-inquiredabout aspects of security. You can find more detail about security and responsibilities in our <u>Overview of Security Processes</u> and <u>AWS Security Best Practices</u> whitepapers, and by visiting the <u>AWS Security webpage</u>.

8.1 Granting and Managing Account Access

Identity and access management are key parts of an information security program, ensuring that only authorized and authenticated users are able to access your resources, and only in a manner that you intend. Using <u>IAM</u>, you can create and manage AWS users and groups, assign them security credentials (e.g., access keys, passwords, and multi-factor authentication [MFA] devices), and use permissions to allow and deny their access to AWS resources. You can also request temporary security credentials for users who only require short-term access.

8.1.1 IAM Users

An IAM <u>user</u> is an entity that you create in AWS. The IAM user represents the person or service who uses the IAM user to interact with AWS. A user in AWS consists of a name, a password to sign into the <u>AWS Management Console</u>, and up to two access keys that can be used with the API or CLI.

When you create an IAM user, you grant it permissions either by making it a member of a group that has appropriate permission policies attached (recommended) or by directly attaching policies to the user. You can also clone the permissions of an existing IAM user, which automatically makes the new user a member of the same groups and attaches all the same policies.

A root user is a single sign-in identity that has complete access to all AWS Cloud services and resources in the account. It is a security best practice to *not* use your root account because of its complete access. Instead, create individual users and grant them each the minimum amount of privilege necessary, which is known as least



privilege. Note that all users have zero privileges by default. You can manage users' privilege by individual user or by groups.

8.1.2 IAM Groups

An IAM <u>group</u> is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users. For example, you could have a group called Admins and give that group the types of permissions that administrators typically need. Any user in that group automatically has the permissions that are assigned to the group. Note that a group is not truly an identity because it cannot be identified as a Principal in a <u>resource-based or trust policy</u>. It is only a way to attach policies to multiple users at one time.

8.1.3 IAM Roles

An IAM role is very similar to a user, in that it is an identity with permission policies that determine what the identity can and cannot do in AWS. However, a role does not have any credentials (password or access keys) associated with it. Instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. An IAM user can assume a role to temporarily take on different permissions for a specific task. A role can be assigned to a <u>federated user</u> who signs in by using an external identity provider instead of IAM. AWS uses details passed by the identity provider to determine which role is mapped to the federated user.

8.1.4 Identity Federation

With <u>federation</u>, you can use single sign-on (SSO) to access your AWS accounts using credentials from your corporate directory. Federation uses open standards such as <u>Security Assertion Markup Language 2.0</u> (SAML) to exchange identity and security information between an identity provider and an application.

8.1.5 Setting Granular Permissions

Access control policies are attached to users, groups, and roles to assign permissions to AWS resources. By default, IAM users, groups, and roles have no permissions; users with sufficient permissions must use a policy to grant the desired permissions.

Using policies, you can specify several layers of permission granularity. First, you can define specific AWS service actions you wish to allow or explicitly deny access to. Second, depending on the action, you can define specific AWS resources the actions can be performed on. Third, you can define conditions to specify when the policy is in effect (for example, if <u>MFA</u> is enabled or not).

8.1.6 Temporary Security Credentials

You can use the <u>AWS Security Token Service (AWS STS)</u> to create and provide trusted users with temporary security credentials that can control access to your AWS



resources. Temporary security credentials are short-term and are not stored with the user; rather, they are generated dynamically and provided to the user when requested.

8.2 Tools for Logical Separation

AWS Cloud services and features that provide logical separation are enough to meet most security requirements, despite legacy requirements for physical separation. Amazon VPC, for example, allows you to define and provision your own logically isolated section of the AWS Cloud. Amazon VPC provides a networking layer for Amazon EC2, a service that provides compute capacity within the AWS Cloud. Your VPC is logically separated from other virtual networks on the AWS Cloud, and it allows you to launch your resources into an IP address range that you determine.

Within your VPC, you can create subnets, each with an associated route table. You can configure these route tables to control network traffic. You can attach an internet gateway to your VPC, allowing your Amazon EC2 instances to communicate with the public internet. You can also create private subnets that only allow your Amazon EC2 instances to communicate with each other. Our <u>Amazon VPC User Guide</u> provides several example scenarios for building both public and private subnets.

In addition, AWS offers services like <u>VPC Peering</u>, <u>AWS Transit Gateway</u>, and <u>AWS</u> <u>PrivateLink</u>, which allow your VPCs to communicate with each other and with your other services on the AWS Cloud both securely and privately.

8.3 **Tools for Encryption**

By defining an encryption approach, you can provide protection for your content against unauthorized users and against unnecessary exposure to authorized users. The combination of <u>AWS Key Management Service (KMS)</u> and <u>AWS CloudHSM</u> are the centerpiece of a rigorous encryption solution.

AWS KMS helps you manage encryption keys and integrates with many AWS Cloud services. This service provides durable, secure, and redundant storage for your master keys. You can define your key aliases as well as key-level policies. The policies help you define key administrators as well as key users. For example, a secret management system can be the only system that has access to the master key that encrypts the secrets for storage.

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. It helps you meet corporate, contractual, and regulatory compliance requirements for data security by using Federal Information Processing Standard (FIPS) 140-2 Level 3 validated HSMs.

8.3.1 Protecting Data at Rest

Multiple AWS Cloud services provide built-in integration with AWS KMS to allow easy encryption of your data. <u>Amazon S3</u> allows you to encrypt content by selecting a KMS

key on object upload. <u>Amazon EBS</u> allows you to choose a KMS key to encrypt a block storage volume or Amazon Machine Image (AMI) copy operation. <u>Amazon RDS</u> allows you to choose an encryption key for encrypting DB instance storage at rest (including backup snapshots).

You also have the option of implementing your own encryption-at-rest approach. For example, you can encrypt content before storing in an AWS Cloud service. Amazon S3 provides you the facility to upload an already encrypted object. It also provides the ability for you to upload an object along with an encryption key that's used in-memory to encrypt an object. To retrieve the object, you must supply the same key.

8.3.2 Protecting Data in Transit

When protecting your data in transit, selecting secure protocols that implement the latest in cryptography standards such as Transport Layer Security (TLS) is a common best practice. AWS Cloud services provide HTTPS endpoints using TLS for communication, thus providing encryption in transit when communicating with the AWS APIs. You have full control over your computing resources to implement encryption in transit across your services. Additionally, the <u>AWS Certificate Manager (ACM)</u> service provides you the ability to manage and deploy public and private certificates for your workloads. You can also leverage virtual private network (VPN) connectivity into your VPC or across your VPCs to facilitate encryption of traffic.

8.4 Automating your Security and Compliance

AWS offers a variety of security tools that you can use to secure the applications you build on the AWS Cloud, from AWS CloudTrail and AWS CloudWatch for logging and monitoring, to Amazon GuardDuty for threat detection, to AWS Shield for DDoS protection. Our <u>Cloud Security</u>, <u>Identity</u>, <u>and Compliance with AWS</u> page provides a more complete listing and details on the myriad services we offer. Customers can use these tools—and the tools of our APN Partners—to automate security.

8.5 **Penetration Testing**

AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their Amazon EC2 instances, Amazon RDS databases, and various other applications. (Refer to <u>Vulnerability and Penetration</u> <u>Testing</u> for terms of service regarding penetration testing.) Penetration tests should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans.

8.6 Security for New AWS Software

AWS Cloud services in production are managed in a manner that preserves their confidentiality, integrity, and availability. AWS has implemented secure software development procedures that are followed to ensure appropriate security controls are



incorporated into the application design. As part of the application design process, new applications must participate in an AWS Security review, including registering the application, initiating the application risk classification, participating in the architecture review and threat modeling, performing code review, and performing a penetration test.

9.0 Compliance

A properly-secured environment results in a compliant environment. AWS has many compliance-enabling features that you can use for your regulated workloads in the AWS Cloud. By using AWS, you get the benefit of the many security controls that we operate, thus reducing the number of security controls that you need to maintain. Your own compliance and certification programs are strengthened, while at the same time lowering your cost to maintain and run your specific security assurance requirements.

Compliance is a shared responsibility between you and AWS. We demonstrate our compliance posture to help you verify compliance with industry and government requirements. We engage with external certifying bodies and independent auditors to provide you with detailed information regarding the policies, processes, and controls we establish and operate. You can use this information to perform your control evaluation and verification procedures as required under the applicable compliance standard. You can also incorporate the information that we provide about our risk and compliance program into your own compliance framework. We use thousands of security controls to monitor that we maintain compliance with global standards and best practices.

We categorize the AWS Assurance Programs into three categories:

- Certifications/Attestations
- Laws/Regulations/Privacy
- Alignments/Frameworks

Table 2 provides an overview of these categories, and the following subsections provide additional detail on the programs that our APN Partners most frequently ask about for the US state, local, and education market.

| Certifications/Attestations | Laws/Regulations/Privacy | Alignments/Frameworks |
|-----------------------------|--------------------------|--------------------------|
| FedRAMP | FERPA | CJIS |
| FIPS | HIPAA/HITECH | CSA |
| ISO 9001 | IRS 1075 | FISMA |
| ISO 27001 | VPAT/Section 508 | NIST |
| ISO 27018 | | Uptime Institute Tiering |
| PCIDSS | | |
| SOC Reports | | |

Table 2 – Summary of AWS Assurance Programs

9.1 Certifications/Attestations

Certifications and attestations are performed by a third-party independent auditor. Our certifications, audit reports, and attestations of compliance are based on the results of the auditor's work. Below are the most frequently requested certifications in the US state, local, and education market. The full list of certifications and attestations can be found at https://www.amazon.com/compliance/.

9.1.1 Federal Risk and Authorization Management Program (FedRAMP)

<u>FedRAMP</u> is a US government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud products and services. The governing bodies of FedRAMP include the Office of Management and Budget (OMB), US General Services Administration (GSA), US Department of Homeland Security (DHS), US Department of Defense (DoD), National Institutes of Standards & Technology (NIST), and the Federal Chief Information Officers (CIO) Council.

Cloud services providers (CSPs) like AWS who want to offer their products and services to the US government must demonstrate FedRAMP compliance. FedRAMP uses the NIST Special Publication 800 series and requires CSPs to receive an independent security assessment conducted by a third-party assessment organization (3PAO) to ensure that authorizations are compliant with the Federal Information Security Management Act (FISMA).

There are two paths for CSPs to be FedRAMP compliant:

- Joint Authorization Board (JAB) Authorization To receive FedRAMP JAB Provisional Authority to Operate (P-ATO), a CSP is reviewed by the FedRAMP Program Management Office (PMO), is assessed by a FedRAMP-accredited 3PAO, and receives a P-ATO from the JAB. The JAB is made up of the CIOs from DoD, DHS, and GSA.
- Agency Authorization To receive FedRAMP Agency Authority to Operate (ATO), a CSP is reviewed by a customer Agency CIO or Delegated Authorizing Official(s) to achieve a FedRAMP-compliant ATO that is verified by the FedRAMP PMO.

AWS and FedRAMP

AWS offers the following FedRAMP compliant systems that have been granted authorizations:

• **AWS GovCloud (US)**, which has been granted a JAB P-ATO and multiple ATOs for high impact level. The services in scope of the AWS GovCloud (US) JAB P-

April 2019



ATO boundary at high baseline security categorization can be found within the <u>AWS Services in Scope by Compliance Program</u>.

 AWS US East/West, which has been granted a JAB P-ATO and multiple ATOs for moderate impact level. The services in scope of the AWS US East-West JAB P-ATO boundary at moderate baseline security categorization can be found within the <u>AWS Services in Scope by Compliance Program</u>.

FedRAMP for APN Partners

APN Partners and prospective customers can request access to the AWS APN Partner FedRAMP Security Package using <u>AWS Artifact</u>. Note that some AWS Artifact documentation is available under NDA, and use of the content is subject to the terms of that NDA.

9.1.2 Federal Information Processing Standard (FIPS)

The <u>FIPS Publication 140-2</u> is a US government standard that specifies the security requirements for cryptographic modules that protect sensitive information.

AWS and FIPS

AWS works with customers to provide the information they need to manage compliance when using the AWS US East/West or AWS GovCloud (US) Regions. For more information about the standard, see <u>Cryptographic Module Validation Program</u> on the NIST Computer Security Resource Center website.

FIPS for APN Partners

The Amazon VPC VPN endpoints in the AWS GovCloud (US) Regions operate using FIPS 140-2 validated cryptographic modules. If you require use of FIPS 140-2 validated cryptographic modules when accessing AWS US East/West or AWS GovCloud (US) through use of the CLI or programmatically by using the APIs, the list of available FIPS endpoints by AWS Region can be found on our <u>FIPS Publication 140-2</u> page.

9.1.3 International Organization for Standardization (ISO) 9001:2015

<u>ISO 9001:2015</u> outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining, and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner in which AWS products and services consistently satisfy ISO 9001:2015 quality requirements.

AWS and ISO 9001:2015

April 2019



AWS has undergone a systematic, independent examination of our quality system to determine whether the activities and activity outputs comply with ISO 9001:2015 requirements. A certifying agent found our quality management system to comply with the requirements of ISO 9001:2015 for the activities described in the scope of registration. You can download AWS's ISO 9001:2015 certification from our website.

ISO 9001:2015 for APN Partners

The certification covers the quality management system over a specified scope of AWS Cloud services and Regions of operations. If you are pursuing ISO 9001:2015 certification while operating all or part of your IT systems on the AWS Cloud, you are not automatically certified by association. However, using an ISO 9001:2015 certified provider like AWS can make your certification process easier.

9.1.4 ISO/IEC 27001:2013

<u>ISO/IEC 27001:2013</u> is a security management standard that specifies security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System (ISMS) which defines how AWS perpetually manages security in a holistic, comprehensive manner. This widely-recognized international security standard specifies that AWS do the following:

- Systematically evaluate our information security risks, taking into account the impact of threats and vulnerabilities.
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address customer and architecture security risks.
- Have an overarching management process to ensure that the information security controls meet our needs on an ongoing basis.

AWS and ISO/IEC 27001:2013

AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, and 27018:2014. These certifications are performed by independent third-party auditors. <u>AWS's ISO/IEC 27001:2013 certification</u> can be downloaded from our website.

ISO/IEC 27001:2013 for APN Partners

The ISO/IEC 27001:2013 certification for AWS covers the AWS security management process over a specified scope of services and data centers. If you are pursuing ISO/IEC certifications while operating part or all of your IT on the AWS Cloud, you are not automatically certified by association. However, using an ISO/IEC 27001:2013 certified provider like AWS can make your certification process easier.

9.1.5 ISO/IEC 27017:2015

<u>ISO/IEC 27017:2015</u> provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO/IEC 27002 and ISO/IEC 27001 standards. This code of practice provides additional information security controls implementation guidance specific to CSPs like AWS.

AWS and ISO/IEC 27017:2015

AWS's attestation to the ISO/IEC 27017:2015 guidance not only demonstrates our ongoing commitment to align with globally-recognized best practices, but also verifies that AWS has a system of highly precise controls in place that are specific to cloud services. <u>AWS's ISO/IEC 27017:2015 certification</u> can be downloaded from our website.

ISO/IEC 27017:2015 for APN Partners

AWS's ISO/IEC 27017:2015 certification covers the security management process and cloud provider specific controls. If you are pursuing ISO/IEC certifications while operating part or all of your IT environment on the AWS Cloud, you are not automatically certified by association. However, using an ISO/IEC 27017:2015 certified provider like AWS can make your certification process easier. The AWS ISO/IEC 27017:2015 assessment provides evidence that our security controls are aligned with the 27017:2015 guidance specific to CSPs.

9.1.6 ISO/IEC 27018:2014

ISO/IEC 27018:2014 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO/IEC information security standard 27002 and provides implementation guidance on ISO/IEC 27002 controls applicable to public cloud personally identifiable information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO/IEC 27002 control set.

AWS and ISO/IEC 27018:2014

AWS maintains the high bar of data protection and privacy controls outlined in ISO/IEC 27018:2014 for all customer content, regardless of whether or not any particular data is PII. <u>AWS's ISO/IEC 27018:2014 certification</u> can be downloaded from our website.

ISO/IEC 27018:2014 for APN Partners

Alignment demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. AWS's alignment with and independent third-party assessment of this internationally recognized code of practice demonstrates AWS's commitment to the privacy and protection of customers' content.



9.1.7 Payment Card Industry Data Security Standard (PCI DSS)

<u>PCI DSS Level 1</u> is a proprietary information security standard administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

PCI DSS applies to all entities that store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD), including merchants, processors, acquirers, issuers, and service providers. PCI DSS is mandated by the card brands and administered by the PCI Security Standards Council.

AWS and PCI DSS

AWS is certified as a PCI DSS 3.2 Level 1 Service Provider, the highest level of assessment available. The compliance assessment was conducted by Coalfire Systems Inc., an independent Qualified Security Assessor (QSA). The PCI DSS Attestation of Compliance (AOC) and Responsibility Summary is available to AWS customers by using <u>AWS Artifact</u>. Note that some AWS Artifact documentation is available under NDA and use of the content is subject to the terms of that NDA.

PCI DSS for APN Partners

As a customer who uses AWS products and services to store, process, or transmit cardholder data, you can rely on AWS technology infrastructure as you manage your own PCI DSS compliance certification.

AWS does not directly store, transmit, or process any customer CHD. However, you may create your own cardholder data environment (CDE) that can store, transmit, or process cardholder data using AWS products.

Customers must manage their own PCI DSS compliance certification, and additional testing will be required to verify that your environment satisfies all PCS DSS requirements. However, for the portion of the PCI CDE that is deployed in AWS, your QSA can rely on AWS AOC without further testing.

9.1.8 SOC Reports

AWS <u>SOC Reports</u> are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help you and your auditors understand the AWS controls established to support operations and compliance. **Table 3** describes the four AWS SOC Reports.

Table 3 – AWS SOC Reports

| Report | What is the report? | What's the Primary Report Purpose? | Who is the Primary Report |
|---|---|--|---|
| | | | Audience? |
| SOC 1 | A description of the AWS control environment and external audit of AWS defined controls and objectives. | To provide information to customers about AWS's control environment that may be relevant to their internal controls over financial reporting. To provide information to customers and their auditors for their assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR). | Customer management and their auditors. AWS's SOC 1 report is available through <u>AWS Artifact</u> . Note that some AWS Artifact documentation is available under NDA and use of the content is subject to the terms of that NDA. |
| SOC 2: Security, Availability and Confidentiality | A description of the AWS controls environment and external audit of AWS controls that meet the AICPA Trust Services Security, Availability, and Confidentiality Principles and Criteria. | To provide customers and users with a business need with an independent assessment of AWS's control environment relevant to system security, availability, and confidentiality. | Users with business need. AWS's SOC 2 report is available through <u>AWS Artifact</u> . Note that some AWS Artifact documentation is available under NDA and use of the content is subject to the terms of that NDA. |
| AWS SOC 2 Privacy Type I Report | A description of the AWS controls environment and external audit of AWS controls that meet the AICPA Trust Services Privacy Principles and Criteria. | To provide customers with an independent assessment of AWS's systems and the suitability of the design of AWS's privacy controls. The SOC 2 Privacy Trust Principle, developed by the AICPA, establishes criteria for evaluating controls related to how personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives. | Users with business need to understand the AWS controls relevant to privacy. AWS's SOC 2 report is available through <u>AWS Artifact</u> . Note that some AWS Artifact documentation is available under NDA and use of the content is subject to the terms of that NDA. |
| SOC 3: Security, Availability and Confidentiality | A public facing report demonstrating AWS has met the AICPA Trust Services Security, Availability, and Confidentiality Principles and Criteria. | To provide customers and users with a business need with an independent assessment of AWS's control environment relevant to system security, availability, and confidentiality without disclosing AWS internal information. | Publicly available on our website. |

9.2 Laws/Regulations/Privacy

AWS customers remain responsible for complying with applicable compliance laws and regulations. In some cases, AWS offers functionality (such as security features), enablers, and legal agreements (such as the AWS Data Processing Agreement and Business Associate Addendum) to support customer compliance. No formal certification is available to (or distributable by) a CSP like AWS within these law and regulatory domains. The following subsections provide details on the laws, regulations, and privacy considerations that APN Partners ask about most in regards to the US state, local, and education market.

9.2.1 Family Educational Rights and Privacy Act (FERPA)

The <u>FERPA</u> of 1974 was enacted to support and promote the protection of privacy and reasonable governance of student education records. FERPA provides parents of students and eligible students with the following:

- The right to inspect and review their education records
- Governance over disclosure of their education records
- A mechanism to amend incorrect education records

FERPA requires states to use reasonable methods to ensure the security of their IT solutions. This may be achieved by hosting education records on cloud computing solutions. The law, in general, requires covered institutions and agencies to reasonably safeguard student education records from improper use or disclosure. Securing student record information, including students' PII, is essential for educational institutions and vendors that provide services which fall under the purview of FERPA.

AWS and FERPA

AWS implements physical and logical controls for internal services and provides robust offerings externally for customers to leverage in order to comply with FERPA. These controls are discussed in detail in our <u>FERPA Compliance on AWS whitepaper</u>.

FERPA for APN Partners

Because FERPA was authored in 1974, it lacks clear guidance on modern technology use, which means that educational institutions are often left to create their own solutions. As part of this solution, customers are encouraged to take steps such as creating device compliance policies, threat protection plans, and data loss prevention plans that suit their organization to protect sensitive information. In addition, customers are encouraged to use encryption and access controls. Access controls also provide auditing and logging capabilities to customers in order to validate privacy and data protection policies that customers have in place. AWS offers a comprehensive set of features and services to make encryption of PII easy to manage and simpler to audit,



including AWS KMS. Customers with FERPA compliance requirements have a great deal of flexibility in how they meet encryption requirements for PII.

9.2.2 Health Insurance Portability and Accountability Act of 1996 (HIPAA)/ Health Information Technology for Economic and Clinical Health (HITECH)

<u>HIPAA</u> legislation is designed to make it easier for US workers to retain health insurance coverage when they change or lose their jobs. This legislation also seeks to encourage electronic health records to improve the efficiency and quality of the US healthcare system through improved information sharing. Along with increasing the use of electronic medical records, HIPAA includes provisions to protect the security and privacy of protected health information (PHI).

<u>HITECH</u> expanded the HIPAA rules in 2009. HIPAA and HITECH together establish a set of federal standards that are intended to protect the security and privacy of PHI.

AWS and HIPAA

There is no HIPAA certification for a CSP such as AWS. In order to meet the HIPAA requirements applicable to our operating model, AWS aligns our HIPAA risk management program with FedRAMP and NIST 800-53, which are higher security standards that map to the HIPAA Security Rule. NIST supports this alignment and has issued <u>SP 800-66: An Introductory Resource Guide for Implementing the HIPAA</u> <u>Security Rule</u>, which documents how NIST 800-53 aligns to the HIPAA Security Rule.

Under the HIPAA regulations, AWS is considered a business associate. The BAA is an AWS contract that is required under HIPAA rules to ensure that AWS appropriately safeguards PHI. The BAA also serves to clarify and limit, as appropriate, the permissible uses and disclosures of PHI by AWS, based on the relationship between AWS and our customers, and the activities or services being performed by AWS.

AWS has a standard BAA we present to customers for signature. It takes into account the unique services AWS provides and accommodates the <u>AWS Shared Responsibility</u> <u>Model</u>. To review, accept, and manage the status of the BAA for your account, sign in to <u>AWS Artifact</u>. Note that some AWS Artifact documentation is available under NDA, and use of the content is subject to the terms of that NDA.

HIPAA for APN Partners

AWS enables covered entities and their business associates subject to HIPAA to use the secure AWS environment to process, maintain, and store protected health information.

April 2019

For detailed information about how you can use AWS for the processing and storage of health information, see the whitepaper <u>Architecting for HIPAA Security and Compliance</u> on Amazon Web Services.

The following resources are available for more information:

- HIPAA Compliance webpage
- <u>SlideShare presentation "Security and Privacy, Using AWS to Meet</u> <u>Requirements for HIPAA, CJIS, and FERPA"</u>

9.2.3 Internal Revenue Service Publication 1075 (IRS Pub 1075)

<u>IRS Pub 1075</u> provides guidance for US government agencies and their agents to protect Federal Tax Information (FTI).

While the IRS does not publish an official designation or certification for compliance with IRS Pub 1075, AWS supports organizations to protect FTI managed on the AWS Cloud by aligning our implementations of NIST 800-53 and FedRAMP security controls with the respective IRS Pub 1075 security requirements. AWS has worked closely with the IRS to ensure that the AWS GovCloud (US) and AWS US East/West Regions meet Pub 1075 requirements for storing and processing FTI. Refer to section 9.1.1 for information on AWS and FedRAMP security controls.

9.2.4 Voluntary Product Accessibility Template (VPAT)/Section 508

In 1998, the US Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an individual's ability to obtain and use information quickly and easily. <u>Section 508</u> was enacted to eliminate barriers in IT, make available new opportunities for people with disabilities, and encourage development of technologies that will help achieve these goals.

The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under <u>Section 508 (29 U.S.C. ' 794d)</u>, agencies must give disabled employees and members of the public access to information that is comparable to the access available to others. Because Section 508 is a federal and state requirement, any and all of AWS government customers will have Section 508 compliance needs.

AWS and VPAT/Section 508

AWS is committed to complying with all relevant government standards and compliance controls. This commitment is reflected in the importance we place on understanding, implementing, and maintaining ongoing compliance with these standards for all individuals who access and consume our services.

VPAT/Section 508 for APN Partners

AWS provides API-based cloud computing services with multiple interfaces to those services, including <u>SDKs</u>, <u>IDE Toolkits</u>, <u>and Command Line Tools</u> for developing and managing AWS resources. AWS provides two graphical user interfaces, the <u>AWS</u> <u>Management Console</u> and the <u>AWS ElasticWolf Client Console</u>. The AWS ElasticWolf Client Console has incorporated Section 508 requirements, and AWS has prepared a VPAT that outlines the AWS ElasticWolf Client Console's accessibility features. The VPAT is available to customers using <u>AWS Artifact</u>. Note that some AWS Artifact documentation is available under NDA and use of the content is subject to the terms of that NDA. APN Partners can use these tools to help build a solution compliant with Section 508.

9.3 Alignments/Frameworks

Compliance alignments and frameworks include published security or compliance requirements for a specific purpose, such as a specific industry or function. AWS provides functionality (such as security features) and enablers (including compliance playbooks, mapping documents, and whitepapers) for these types of programs.

Requirements under specific alignments and frameworks may not be subject to certification or attestation; however, some alignments and frameworks are covered by other compliance programs. The following subsections provide details on the alignments and frameworks that APN Partners ask about most frequently for the US state, local, and education market.

9.3.1 Criminal Justice Information Services (CJIS)

<u>Criminal Justice Information (CJI)</u> refers to the data necessary for law enforcement agencies to perform their mission and enforce the laws, such as biometric, identity history, person, organization, property, and case/incident history data. CJI also refers to data necessary for civil agencies to perform their mission, including data used to make hiring decisions.

The CJIS Security Policy reflects the shared responsibility between FBI CJIS, CJIS Systems Agency, and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The CJIS Security Policy provides a baseline of security requirements for current and planned services and establishes a minimum standard for new initiatives.

AWS and CJIS

AWS complies with the FBI's CJIS standard. AWS demonstrates compliance with applicable CJIS requirements as supported by our third-party assessed frameworks such as FedRAMP, which includes on-site data center audits by our FedRAMP-accredited 3PAO. We sign CJIS security agreements with our customers, including

allowing or performing any required employee background checks according to the CJIS Security Policy. AWS conducts criminal background checks, as permitted by law, as part of pre-employment screening practices for employees and commensurate with the employee's position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.

AWS Cloud services support customer <u>CJIS</u> requirements by addressing the CJIS Security Policy Areas. AWS infrastructure and services have been <u>reviewed by state</u> <u>and federal law enforcement agencies</u>, which confirm AWS's competence in supporting customer CJIS workloads.

CJIS for APN Partners

Using the AWS Cloud doesn't automatically mean that your environment is covered by our compliance with the FBI's CJIS standard. AWS only manages the implementation of security requirements within the AWS infrastructure. AWS doesn't manage the customer environment or data, which means you are responsible for implementing the applicable CJIS Security Policy requirements in your AWS environment. When using AWS, you must still:

- Review the CJIS Security Policy requirements to determine which are directly applicable to your environment.
- Implement solutions (as necessary) to address each of those requirements.
- Assess and audit the solution against the applicable control requirements.
- Submit your CJIS documentation using the AWS CJIS Workbook to your customer agency for review and formal CJIS authorization.

Finally, there are a few key points in supporting customer CJIS workloads:

- Encryption of data at rest is critical. AWS provides several resources to help you achieve this important solution, including solutions architect personnel available to assist you, and our <u>Encrypting Data at Rest</u> whitepaper.
- In the spirit of a shared responsibility model, AWS provides a <u>CJIS Security</u> <u>Policy Workbook</u> (in a system security plan template) that is aligned to the CJIS Policy Areas. This workbook helps customers to systematically document their implementation of CJIS requirements alongside the AWS approach to each requirement (along with guidance on submitting the document for review and authorization). Please request the most up-to-date workbook through your Account Manager.
- AWS provides multiple built-in security features in support of CJIS workloads, such as:
 - Secure access by using IAM with MFA



- Encrypted data storage with either AWS-provided options or customermaintained options
- Logging and monitoring with <u>Amazon S3 logging</u>, <u>AWS</u>
 <u>CloudTrail</u>, <u>Amazon CloudWatch</u>, and <u>AWS Trusted Advisor</u>
- Centralized, customer-controlled key management with <u>AWS</u> <u>CloudHSM</u> and <u>AWS KMS</u>

Customers can streamline compliance—from architecting a solution to preparing for an audit—with AWS's portfolio of compliance guides and programs, listed below:

- AWS CJIS Security Policy Requirements
- AWS CJIS Security Policy Template
- <u>AWS CJIS Workbook</u> (Excel file)
- CJIS Compliance on AWS whitepaper
- AWS Quick Starts for security and compliance
- AWS CJIS Workshop Series

9.3.2 Cloud Security Alliance (CSA)

<u>CSA</u> is a not-for-profit organization with a mission to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing."

AWS and CSA

AWS participates in the voluntary CSA Security, Trust & Assurance Registry (STAR) Self-Assessment to document our compliance with CSA-published best practices. We publish our completed <u>CSA Consensus Assessments Initiative Questionnaire (CAIQ)</u> on the AWS website.

CSA for APN Partners

The CSA CAIQ provides a set of questions that the CSA anticipates a cloud consumer and/or cloud auditor would ask of a CSP like AWS. It provides a series of security, control, and process questions that can then be used for a wide range of uses, including cloud provider security evaluation.

9.3.3 Federal Information Security Management Act (FISMA)

AWS enables US government agencies to achieve and sustain compliance with <u>FISMA</u>. The AWS infrastructure has been evaluated by independent assessors for a variety of government systems as part of their system owners' approval process. Numerous Federal Civilian and DoD organizations have successfully achieved security authorizations for systems hosted on AWS in accordance with the Risk Management Framework (RMF) process defined in NIST 800-37 and DoD Information Assurance Certification and Accreditation Process (DIACAP). AWS's secure infrastructure has



helped federal agencies expand cloud computing use cases and deploy sensitive government data and applications in the cloud while complying with the rigorous security requirements of federal standards.

9.3.4 National Institute of Standards and Technology (NIST) 800-53

<u>NIST</u> 800-53 security controls are generally applicable to US Federal Information Systems. Federal Information Systems typically must go through a formal assessment and authorization process to ensure sufficient protection of confidentiality, integrity, and availability of information and information systems.

The NIST Cybersecurity Framework (CSF) is supported by governments and industries worldwide as a recommended baseline for use by any organization, regardless of its sector or size. According to Gartner, in 2015 the CSF was used by approximately 30 percent of US organizations, and usage is projected to reach 50 percent by 2020. Since Fiscal Year 2016, federal agency FISMA metrics have been organized around the CSF, and agencies are now required to implement the CSF under the Cybersecurity Executive Order.

AWS and NIST 800-53

AWS Cloud infrastructure and services have been validated by third-party testing performed against the NIST 800-53 Revision 4 controls and additional FedRAMP requirements. AWS has received FedRAMP ATOs from multiple authorizing agencies for both AWS GovCloud (US) and the AWS US East/West Regions. For more information, see the <u>AWS FedRAMP compliance</u> webpage, or the following FedRAMP Marketplace webpages:

- AWS East/West Region complete list of authorizing agencies
- AWS GovCloud (US) complete list of authorizing agencies
- AWS GovCloud JAB P-ATO at the high baseline

NIST 800-53 for APN Partners

Under NDA, AWS provides an AWS FedRAMP SSP template based upon NIST 800-53 Rev. 4, which is prepopulated with the applicable NIST 800-5 Rev. 4 Low/Moderate/High control baseline. Control responsibility is as follows:

- **Shared Responsibility** You will provide security and configurations of your software components, and AWS will provide security for its infrastructure.
- Customer-Only Responsibility You are fully responsible for guest operating systems, deployed applications, and select networking resources (for example, firewalls). More specifically, you are solely responsible for configuring and managing your security *in* the cloud.

 AWS-Only Responsibility – AWS manages the cloud infrastructure, including the network, data storage, system resources, data centers, physical security, reliability, and supporting hardware and software. Applications built on top of the AWS system inherit the features and configurable options that AWS provides. AWS is solely responsible for configuring and managing security of the cloud.

For security authorization purposes, compliance with the FedRAMP requirements (based on NIST 800-53 rev 4 Low/Moderate/High control baseline) is contingent upon AWS fully implementing AWS-only and shared controls and you implementing customer-only and shared controls. A FedRAMP-accredited 3PAO has assessed and authorized AWS implementation of our control responsibility. The portion of shared controls that you are responsible for and the controls related to applications you implement on top of the AWS infrastructure must be separately assessed and authorized by you in agreement with NIST 800-37 and your specific security authorization policies and procedures.

AWS FedRAMP-compliant systems have been granted authorizations, have addressed the FedRAMP security controls (NIST 800-53), use the required FedRAMP templates for the security packages posted in the secure FedRAMP Repository, have been assessed by an accredited independent 3PAO, and maintain the continuous monitoring requirements of FedRAMP.

You can use the <u>NIST CSF whitepaper</u> to assess your AWS environment against the NIST CSF and improve the security measures you implement and operate. The whitepaper also provides a third-party auditor letter attesting to the AWS Cloud services' conformance to NIST CSF risk management practices.

9.3.5 Uptime Institute Tiers

The <u>Uptime Institute</u> created the standard Tier Classification System to evaluate various data center facilities in terms of potential site infrastructure performance, or uptime. Uptime Institute has not authorized other organizations to certify data centers under its Tier Classification System. Uptime Institute does not design, build, or operate data centers.

AWS and Uptime Institute Tiers

AWS operates our data centers in alignment with the Tier III+ guidelines, but we have chosen not to have a certified Uptime Institute-based tiering level so that we have more flexibility to expand and improve performance. AWS's approach to infrastructure performance acknowledges Uptime Institute's tiering guidelines and applies them to our global data center infrastructure design to ensure the highest level of performance and availability for our customers. AWS then improves on the guidelines provided by the Uptime Institute to scale for global operations and produce an operating outcome for availability and performance that far exceeds that which would be achieved through the



Uptime Institute tiering guidelines alone. Although we do not claim alignment with Tier IV, we can ensure that our systems have a fault tolerant sequence of operations with self-correcting mitigations in place.

AWS has identified critical system components required to maintain the availability of the system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Availability Zones are connected to each other with fast, private fiber-optic networking, enabling you to easily architect applications that automatically fail-over between Availability Zones without interruption.

Uptime Institute Tiers for APN Partners

AWS customers can build highly resilient systems in the cloud by employing multiple instances in multiple Availability Zones plus data replication to achieve extremely high recovery time and recovery point objectives, as well as service availability of 99.999% and more. Service availability is therefore a function of the design; customers who care about the availability and performance of their applications want to deploy these applications across multiple Availability Zones in the same region for fault tolerance and low latency. Some AWS Cloud services, such as Amazon S3, are built to leverage all Availability Zones within the region and have a durability objective of 99.999999999%.

10.0 Managing your AWS Resources

With the AWS Cloud, customers can easily provision, manage, and monitor all of their IT resources through a "single pane of glass" with the tool that best fits their unique needs. This helps you know what is going on in your cloud environment, such as instance health, logs of user actions, and ways you can save money. AWS Cloud services are driven by robust APIs that allow for a wide variety of monitoring, management and developer tools to integrate easily with AWS Cloud resources. Common tools from vendors such as Microsoft, VMware, BMC Software, Okta, RightScale, Eucalyptus, CA, Xceedium, Symantec, Racemi, and Dell are supported on AWS. Below are some AWS-native management options, which can be used alongside familiar management tools available on <u>AWS Marketplace</u>.

10.1 AWS Management Console

The <u>AWS Management Console</u> is a single destination for managing all AWS resources. Customers can use the AWS Management Console to perform any number of tasks (e.g., deploying new applications, monitoring the health of applications, accessing monthly spending by service, and managing security credentials). The AWS Management Console supports all <u>AWS Regions</u> and lets customers provision resources across multiple Regions.

10.2 Command Line Interface

The <u>AWS CLI</u> is a unified tool used to manage AWS Cloud services. With just one tool to download and configure, customers can control multiple AWS resources from the command line and automate them through scripts. The AWS CLI introduces a new set of simple <u>file commands</u> for efficient file transfers to and from <u>Amazon S3</u>.

10.3 AWS Developer Tools

AWS offerings are provided with a range of <u>supporting components</u> like developer tools, toolkits, and command line tools for developing and managing your AWS applications:

The <u>AWS Developer Tools</u> help you securely store and version control your application's source code and automatically build, test, and deploy your application to AWS or your on-premises environment, <u>including tools for continuous integration and</u> <u>continuous delivery</u>. Our developer tools include the following:

- <u>AWS Cloud9</u> Write, run, and debug code in a cloud integrated development environment (IDE)
- <u>AWS CodeBuild</u> Build and test code
- <u>AWS CodeCommit</u> Store code in private Git repositories
- <u>AWS CodeDeploy</u> Automate code deployments
- <u>AWS CodePipeline</u> Release software using continuous integration and delivery
- <u>AWS CodeStar</u> Develop, build, and deploy applications on AWS
- <u>AWS X-Ray</u> Analyze and debug production applications

10.4 Management Tools

AWS provides <u>management tools</u> that allows you to programmatically provision, monitor, and automate all the components of your cloud environment. Using these tools, you can maintain consistent controls without restricting development velocity. These services all work together and are integrated with every part of the AWS platform, allowing you to have greater insight into your cloud environment as well as maintain logs necessary for audits. Our management tools include the following:

- <u>AWS CloudFormation</u> Model and provision—in an automated and secure manner—all the resources needed for your applications across all regions and accounts
- <u>AWS Service Catalog</u> Create and manage catalogs of IT services that are approved for use on AWS
- <u>AWS Systems Manager</u> Quickly view and monitor all your resources and automate common operational tasks
- <u>AWS OpsWorks</u> Host and scale Chef Automate and Puppet Enterprise servers
- <u>AWS Config</u> Inventory all configurations across your resources



- <u>AWS CloudTrail</u> Automatically log, continuously monitor, and retain account activity related to actions across your AWS infrastructure
- <u>Amazon CloudWatch</u> Collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources

11.0 Back-up and Disaster Recovery

The AWS Cloud enables a lightweight approach to backup and recovery. With the cloud, computers are virtual abstract resources instantiated via code rather than being hardware-based (i.e., infrastructure as code). This means that capacity is available at incremental cost rather than upfront cost, resource provisioning takes place in minutes, and server images are available on demand. These characteristics offer customers opportunities to recover deleted or corrupted data with less infrastructure overhead.

11.1 Disaster Recovery on AWS

Any event that has a negative impact on an organization's operational continuity or finances could be termed a disaster. This includes hardware or software failure, a network outage, a power outage, physical damage to a building like fire or flooding, human error, or some other significant event. AWS can enable customers to cost-effectively operate multiple DR strategies. **Figure 8** shows a spectrum of scenarios— "backup and restore," "pilot light," "warm standby," and "multi-site"—arranged by how quickly a system can be available to users after a DR event.



Figure 8 – Spectrum of DR Options

Each DR option is discussed in more detail below:

 Backup and Restore – In most traditional environments, data is backed up to tape and sent off-site regularly. Recovery time will be the longest using this method, and lack of automation leads to increased costs. Using <u>Amazon S3</u> is ideal for backup data, as it is designed to provide 99.999999999% durability of objects over a given year. Transferring data to and from Amazon S3 is typically done via the network, and it is therefore accessible from any location. Also, with <u>AWS Storage Gateway</u>, customers can automatically back up on-premises data to Amazon S3. In addition, using <u>AWS Backup</u>, you can centrally configure backup policies and monitor backup activity for AWS resources such as Amazon EBS volumes, Amazon RDS databases, Amazon DynamoDB tables, Amazon EFS file systems, and AWS Storage Gateway volumes.

- Pilot Light for Simple Recovery into AWS Warm Standby Solution The idea of the pilot light is an analogy that comes from the gas heater. In a gas heater, a small idle flame that's always on can quickly ignite the entire furnace to heat up a house as needed. This scenario is analogous to a backup and restore scenario; however, customers must ensure that they have the most critical core elements of their system already configured and running in AWS (the pilot light). When the time comes for recovery, customers would rapidly provision a full-scale production environment around the critical core.
- Warm Standby Solution in AWS The term "warm standby" is used to describe a DR scenario in which a scaled-down version of a fully functional environment is always running in the cloud. It further decreases recovery time because, in this case, some services are always running. By identifying organizational-critical systems, customers could fully duplicate these systems on AWS and have them always on.
- Multi-Site Solution Deployed on AWS and On-Site A multi-site solution runs in AWS as well as on a customer's existing on-premises infrastructure in an active-active configuration. During a disaster situation, an organization can simply send all traffic to AWS servers, which can scale to handle their full production load.

12.0 Security Questionnaires

Under the Shared Responsibility Model, AWS is responsible for security *of* the cloud: protecting the infrastructure that runs all of the services offered in the AWS Cloud. All other security *in* the cloud is dependent on your management of your account(s) and your solution. AWS personnel cannot fill out Security Questionnaires on behalf of our APN Partners. We have the following resources to assist with understanding security on AWS. If you have additional questions about a specific requirement, please reach out and we will try to provide further information.

- <u>Shared Responsibility Model</u> Describes AWS responsibility and customer/APN Partner responsibility
- <u>Our Data Centers</u> Provides a virtual tour of one of our data centers
- Our Controls Provides insight into some of our physical and environmental controls to help you fulfill your own audit and regulatory requirements
- <u>Data Privacy</u> Details our approach to data privacy
- <u>CSA Consensus Assessments Initiative Questionnaire</u> AWS responses to a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider
- <u>AWS Answers to Key Compliance Questions</u> Addresses common cloud computing compliance questions as they relate to AWS
- <u>AWS Compliance Quick Reference Guide</u> Provides an overview of our assurance programs and how to secure your content on the AWS Cloud

13.0 AWS Public Sector Access Policy – Instructions

If this opportunity requires the resale of AWS offerings, you must include the AWS Public Sector Access Policy ("Access Policy") in your response and incorporate the Access Policy in any agreement regarding such resale, per your Reseller Agreement, as amended. The Access Policy sets out rules, conditions, and restrictions regarding use of the AWS cloud services and can be accessed at: <u>https://s3-us-west-</u>

2.amazonaws.com/solution-provider-program-legaldocuments/AWS+Public+Sector+Access+Policy.pdf



14.0 Industry Analyst Reports on AWS Market Position [Note: "Do not edit content in this section, or use in a public document other than a direct RFx response. And, please include all citations and disclaimers outlined below."]

Gartner, Inc., a leading information technology research company, released its 2018 <u>Magic Quadrant for Cloud Infrastructure as a Service (IaaS), Worldwide</u>¹ report, where AWS is positioned highest in execution and furthest in vision within the Leaders Quadrant.



Figure 9 – Gartner 2018 Magic Quadrant for Cloud IaaS, Worldwide

¹ GartnerGartner, Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, Dennis Smith, Lydia Leong, Bala, Raj, Lowery, Craig, Smith, Dennis, published 23 May 2018 - ID G00336148. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from AWS: http://www.gartner.com/doc/reprints?id=1-2G205FC&ct=150519&st=sb. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organisation and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

All statements in this report attributable to Gartner represent AWS's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this proposal). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.



AWS, for the fourth consecutive year, is also positioned highest in execution and furthest in vision within the Leaders Quadrant of Gartner's 2018 <u>Magic Quadrant for</u> <u>Public Cloud Storage Services, Worldwide</u>² report.



Figure 10 – Gartner 2018 Magic Quadrant for Public Cloud Storage Services, Worldwide

More analyst reports can be found at AWS in Analyst Research.

² Gartner, Magic Quadrant for Public Cloud Storage Services, Worldwide, Raj Bala (Sr Director, Analyst), Julia Palmer (Sr Director, Analyst), published 31 July 2018 - ID G00340206.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from: https://www.gartner.com/doc/reprints?id=1-21H2LGI&ct=150626&st=sb

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organisation and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. All statements in this report attributable to Gartner represent AWS's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this proposal). The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.



AWS Overview

- What is Cloud Computing: <u>https://aws.amazon.com/what-is-cloud-</u> <u>computing/</u>
- Types of Cloud Computing: <u>https://aws.amazon.com/types-of-cloud-</u> <u>computing/</u>
- Choosing a Cloud Platform: <u>https://aws.amazon.com/choosing-a-cloud-platform/</u>
- About AWS: <u>https://aws.amazon.com/about-aws/</u>
- AWS Global Infrastructure: <u>https://aws.amazon.com/about-aws/global-infrastructure/</u>

AWS Solutions

- Websites and Web Hosting: <u>https://aws.amazon.com/websites/</u>
- Development and Test: <u>https://aws.amazon.com/dev-test/</u>
- Backup and Recovery: <u>https://aws.amazon.com/backup-recovery/</u>
- Data Archive: <u>https://aws.amazon.com/archive/</u>
- Disaster Recovery: <u>https://aws.amazon.com/disaster-recovery/</u>
- Big Data: <u>https://aws.amazon.com/big-data/</u>
- High Performance Computing: <u>https://aws.amazon.com/hpc/</u>
- Internet of Things: <u>https://aws.amazon.com/iot/</u>
- Financial Services: <u>https://aws.amazon.com/financial-services/</u>
- Health
 <u>https://aws.amazon.com/health/</u>

- Life Sciences:
 <u>https://aws.amazon.com/health/life-</u>sciences/
- Genomics: https://aws.amazon.com/health/genomics/
- Business Applications: <u>https://aws.amazon.com/business-applications/</u>
- <u>DevOps:</u> <u>https://aws.amazon.com/devops/</u>

AWS Products and Services

- List of all AWS cloud services: <u>https://aws.amazon.com/products/</u>
- AWS Marketplace: https://aws.amazon.com/marketplace/
- AWS service documentation: http://aws.amazon.com/documentation/

AWS in the Public Sector

- AWS Public Sector Homepage: <u>https://aws.amazon.com/government-</u> education/
- U.S. Federal Government: https://aws.amazon.com/federal/
- State and Local Government: <u>https://aws.amazon.com/stateandlocal/</u>
- Defense and Aerospace: <u>https://aws.amazon.com/government-</u> education/defense/
- Education: <u>https://aws.amazon.com/education/</u>
- AWS Educate: <u>https://aws.amazon.com/education/awsedu</u> <u>cate/</u>
- Nonprofit Organizations
 <u>https://aws.amazon.com/government-</u>
 <u>education/nonprofits/</u>

- AWS GovCloud (US) Region: <u>http://aws.amazon.com/govcloud-us/</u>
- AWS Government Partners: <u>https://aws.amazon.com/partners/governm</u> <u>ent/</u>
- AWS Public Sector Blog: <u>https://aws.amazon.com/blogs/publicsector</u>
 /

AWS Partner Community

- AWS Partner Network: <u>https://aws.amazon.com/partners/</u>
- AWS Partner Directory: <u>http://www.aws-partner-directory.com/</u>
- AWS Partner Programs: <u>https://aws.amazon.com/partners/programs</u>
 <u>l</u>

AWS Professional Services

- AWS Professional Services: <u>https://aws.amazon.com/professional-services/</u>
- AWS Cloud Adoption Framework: <u>https://aws.amazon.com/professional-services/CAF/</u>
- AWS Enterprise Accelerators: <u>https://aws.amazon.com/professional-</u> <u>services/enterprise-accelerators/</u>

AWS Pricing

- AWS Pricing Overview: <u>http://aws.amazon.com/pricing/</u>
- Pricing for each service: <u>https://aws.amazon.com/pricing/services/</u>
- AWS Economics Center: <u>https://aws.amazon.com/economics/</u>
- Cost Optimization:



AWS Partner Package

https://aws.amazon.com/pricing/costoptimization/

- AWS Simple Monthly Calendar: <u>http://calculator.s3.amazonaws.com/index.</u> html
- AWS TCO Calculator: <u>http://aws.amazon.com/tco-calculator/</u>

AWS Billing

- AWS Billing and Cost Management: <u>http://docs.aws.amazon.com/awsaccountbil</u> ling/latest/aboutv2/billing-what-is.html
- Consolidated Billing: <u>http://docs.aws.amazon.com/awsaccountbil</u> ling/latest/aboutv2/consolidated-billing.html
- Cost Explorer: <u>http://docs.aws.amazon.com/awsaccountbil</u> <u>ling/latest/aboutv2/cost-explorer-what-</u> <u>is.html</u>
- AWS Budgets and Forecasts: <u>http://docs.aws.amazon.com/awsaccountbil</u> <u>ling/latest/aboutv2/budgets-managing-</u> <u>costs.html</u>

AWS Security and Compliance

- AWS Security Center: <u>http://aws.amazon.com/security/</u>
- AWS Shared Responsibility Model: <u>http://aws.amazon.com/security/sharing-</u> <u>the-security-responsibility/</u>
- AWS Security Features: <u>http://aws.amazon.com/security/aws-</u> <u>security-features/</u>
- AWS Compliance: <u>http://aws.amazon.com/compliance/</u>
- AWS Compliance FAQs: <u>http://aws.amazon.com/compliance/pci-</u> <u>data-privacy-protection-hipaa-soc-fedramp-</u> <u>faqs/</u>

- AWS Data Privacy: http://aws.amazon.com/compliance/dataprivacy-faq/
- Access Control: <u>http://aws.amazon.com/iam/</u>
- AWS Security Blog: <u>https://blogs.aws.amazon.com/security/</u>

AWS Support

- AWS Support Tiers: <u>https://aws.amazon.com/premiumsupport/</u>
- Support Knowledge Center: <u>https://aws.amazon.com/premiumsupport/k</u> <u>nowledge-center/</u>
- AWS Trusted Advisor: <u>https://aws.amazon.com/premiumsupport/tr</u> <u>ustedadvisor/</u>

AWS Training and Best Practices

- AWS Training and Certification: <u>http://aws.amazon.com/training/</u>
- AWS Architecture Center: <u>http://aws.amazon.com/architecture/</u>
- AWS Test Drive: http://aws.amazon.com/testdrive/

Industry Analysis

- Analyst Reports: <u>http://aws.amazon.com/resources/analyst-reports/</u>
- Gartner Magic Quadrant for Cloud Infrastructure as a Service (August 2016): <u>https://www.gartner.com/doc/reprints?id=1-</u> 2G2O5FC&ct=150519&st=sb
- Gartner Magic Quadrant for Public Cloud Storage Services (July 2016): <u>https://www.gartner.com/doc/reprints?id=1-</u> <u>2IH2LGI&ct=150626&st=sb</u>
- Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014:

http://www.forrester.com/pimages/rws/reprints/document/113065/oid/1-SBOUWE

 IDC Report: Quantifying the Business Value of Amazon Web Services: <u>http://d0.awsstatic.com/analyst-</u> <u>reports/IDC_Business_Value_of_AWS_Ma</u> y 2015.pdf

AWS Case Studies

- AWS Case Studies: <u>https://aws.amazon.com/solutions/case-</u> <u>studies/</u>
- Public Sector Case Studies: <u>http://aws.amazon.com/solutions/case-</u> <u>studies/government-education/</u>

Procurement

- AWS Public Sector Contract Center: <u>http://aws.amazon.com/contract-center/</u>
- 10 Considerations for a Cloud Procurement Whitepaper: <u>http://d0.awsstatic.com/whitepapers/10-</u> considerations-for-a-cloud-procurement.pdf
- How to Buy Cloud Computing Services for your Agency (Webinar): <u>https://aws.amazon.com/webinars/buyingcloud-computing-services/</u>

Legal

•

- AWS Customer Agreement: http://aws.amazon.com/agreement/
- AWS Service Terms: <u>https://aws.amazon.com/service-terms/</u>
- AWS Acceptable Use Policy: <u>http://aws.amazon.com/aup/</u>
- AWS Trademark Guidelines: <u>http://aws.amazon.com/trademark-guidelines/</u>
- AWS Site Terms: http://aws.amazon.com/terms/



AWS Partner Package

aws

- AWS Privacy Policy: <u>https://aws.amazon.com/privacy/</u>
- AWS Tax Help: <u>http://aws.amazon.com/tax-help/</u>

Additional Resources

- AWS Blog: <u>https://aws.amazon.com/blogs/aws/</u>
- AWS Discussion Forums: <u>https://forums.aws.amazon.com/index.jspa</u>
- What's New from AWS: <u>http://aws.amazon.com/new/</u>
- AWS YouTube Channel: <u>https://www.youtube.com/user/AmazonWe</u> <u>bServices</u>
- AWS Twitter Feed: <u>https://twitter.com/awscloud</u>
- AWS on SlideShare: <u>http://www.slideshare.net/AmazonWebServ</u> <u>ices</u>
- Events and Webinars
 <u>https://aws.amazon.com/about-aws/events/</u>
- An E-Book of Cloud Best Practices: <u>https://medium.com/aws-enterprise-</u> <u>collection/an-e-book-of-cloud-best-</u> <u>practices-for-your-enterprise-</u> 4a211840c55b#.corzpjf3m

AWS Whitepapers

- AWS Whitepapers: <u>http://aws.amazon.com/whitepapers/</u>
- Overview of AWS Whitepaper: <u>http://d0.awsstatic.com/whitepapers/aws-overview.pdf</u>
- Security Resources and Whitepapers: <u>http://aws.amazon.com/security/security-resources/</u>
- Introduction to AWS Security Processes: <u>https://d0.awsstatic.com/whitepapers/Security/Intro_Security_Practices.pdf</u>

- AWS Compliance whitepapers: <u>http://aws.amazon.com/compliance/aws-</u> <u>whitepapers/</u>
- AWS Risk and Compliance Whitepaper: <u>https://d0.awsstatic.com/whitepapers/compl</u> <u>iance/AWS Risk and Compliance Whitep</u> <u>aper.pdf</u>
- AWS Storage Services Overview: <u>https://d0.awsstatic.com/whitepapers/Stora</u> <u>ge/AWS%20Storage%20Services%20Whit</u> <u>epaper-v9.pdf</u>
- Backup and Recovery Approaches Using AWS: <u>https://d0.awsstatic.com/whitepapers/Stora</u> <u>ge/Backup and Recovery Approaches_U</u> sing AWS.pdf

AWS Billing

- AWS Billing and Cost Management: <u>http://docs.aws.amazon.com/awsaccountbil</u> ling/latest/aboutv2/billing-what-is.html
- Consolidated Billing: <u>http://docs.aws.amazon.com/awsaccountbil</u> <u>ling/latest/aboutv2/consolidated-billing.html</u>
- Cost Explorer: <u>http://docs.aws.amazon.com/awsaccountbil</u> <u>ling/latest/aboutv2/cost-explorer-what-</u> <u>is.html</u>
- AWS Budgets and Forecasts: <u>http://docs.aws.amazon.com/awsaccountbil</u> <u>ling/latest/aboutv2/budgets-managing-costs.html</u>

AWS Security and Compliance

- AWS Security Center: <u>http://aws.amazon.com/security/</u>
- AWS Shared Responsibility Model: <u>http://aws.amazon.com/security/sharing-</u> <u>the-security-responsibility/</u>

- AWS Security Features: <u>http://aws.amazon.com/security/aws-</u> <u>security-features/</u>
- AWS Compliance: <u>http://aws.amazon.com/compliance/</u>
- AWS Compliance FAQs: <u>http://aws.amazon.com/compliance/pci-</u> <u>data-privacy-protection-hipaa-soc-fedramp-</u> <u>faqs/</u>
- AWS Data Privacy: <u>http://aws.amazon.com/compliance/data-privacy-faq/</u>
- Access Control: <u>http://aws.amazon.com/iam/</u>
- AWS Security Blog: <u>https://blogs.aws.amazon.com/security/</u>

AWS Support

- AWS Support Tiers: <u>https://aws.amazon.com/premiumsupport/</u>
- Support Knowledge Center: <u>https://aws.amazon.com/premiumsupport/k</u> <u>nowledge-center/</u>
- AWS Trusted Advisor: <u>https://aws.amazon.com/premiumsupport/tr</u> <u>ustedadvisor/</u>

AWS Training and Best Practices

- AWS Training and Certification: <u>http://aws.amazon.com/training/</u>
- AWS Architecture Center: <u>http://aws.amazon.com/architecture/</u>
 AWS Test Drive:
- http://aws.amazon.com/testdrive/

Industry Analysis

 Analyst Reports: <u>http://aws.amazon.com/resources/analyst-</u> reports/

AWS Partner Package

- Gartner Magic Quadrant for Cloud Infrastructure as a Service (August 2016): <u>https://www.gartner.com/doc/reprints?id=1-</u> 2G2O5FC&ct=150519&st=sb
- Gartner Magic Quadrant for Public Cloud Storage Services (July 2016): <u>https://www.gartner.com/doc/reprints?id=1-</u> <u>2IH2LGI&ct=150626&st=sb</u>
- Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014: <u>http://www.forrester.com/pimages/rws/reprints/document/113065/oid/1-SBOUWE</u>
- IDC Report: Quantifying the Business Value of Amazon Web Services: <u>http://d0.awsstatic.com/analyst-</u> <u>reports/IDC Business Value of AWS Ma</u> <u>y 2015.pdf</u>

AWS Case Studies

- AWS Case Studies:
 <u>https://aws.amazon.com/solutions/case-</u>
 studies/
- Public Sector Case Studies: <u>http://aws.amazon.com/solutions/case-</u> <u>studies/government-education/</u>

Procurement

- AWS Public Sector Contract Center: <u>http://aws.amazon.com/contract-center/</u>
- 10 Considerations for a Cloud Procurement Whitepaper:

http://d0.awsstatic.com/whitepapers/10considerations-for-a-cloud-procurement.pdf

 How to Buy Cloud Computing Services for your Agency (Webinar): <u>https://aws.amazon.com/webinars/buyingcloud-computing-services/</u>

Legal

- AWS Customer Agreement: <u>http://aws.amazon.com/agreement/</u>
- AWS Service Terms: <u>https://aws.amazon.com/service-terms/</u>
- AWS Acceptable Use Policy: <u>http://aws.amazon.com/aup/</u>
- AWS Trademark Guidelines:
 <u>http://aws.amazon.com/trademark-guidelines/</u>
- AWS Site Terms: <u>http://aws.amazon.com/terms/</u>
- AWS Privacy Policy: <u>https://aws.amazon.com/privacy/</u>
- AWS Tax Help: <u>http://aws.amazon.com/tax-help/</u>

Additional Resources

- AWS Blog: <u>https://aws.amazon.com/blogs/aws/</u>
- AWS Discussion Forums: <u>https://forums.aws.amazon.com/index.jspa</u>
- What's New from AWS: <u>http://aws.amazon.com/new/</u>

- AWS YouTube Channel: <u>https://www.youtube.com/user/AmazonWe</u> <u>bServices</u>
- AWS Twitter Feed: <u>https://twitter.com/awscloud</u>
- AWS on SlideShare: <u>http://www.slideshare.net/AmazonWebServ</u> <u>ices</u>
- Events and Webinars
 <u>https://aws.amazon.com/about-aws/events/</u>
- An E-Book of Cloud Best Practices: <u>https://medium.com/aws-enterprise-</u> <u>collection/an-e-book-of-cloud-best-</u> <u>practices-for-your-enterprise-</u> <u>4a211840c55b#.corzpjf3m</u>

AWS Whitepapers

- AWS Whitepapers: <u>http://aws.amazon.com/whitepapers/</u>
- Overview of AWS Whitepaper: <u>http://d0.awsstatic.com/whitepapers/aws-</u> overview.pdf
- Security Resources and Whitepapers: <u>http://aws.amazon.com/security/security-resources/</u>
- Introduction to AWS Security Processes: <u>https://d0.awsstatic.com/whitepapers/Security/Intro_Security_Practices.pdf</u>

