Cloud Architectures and Deployment Models

Table of Contents

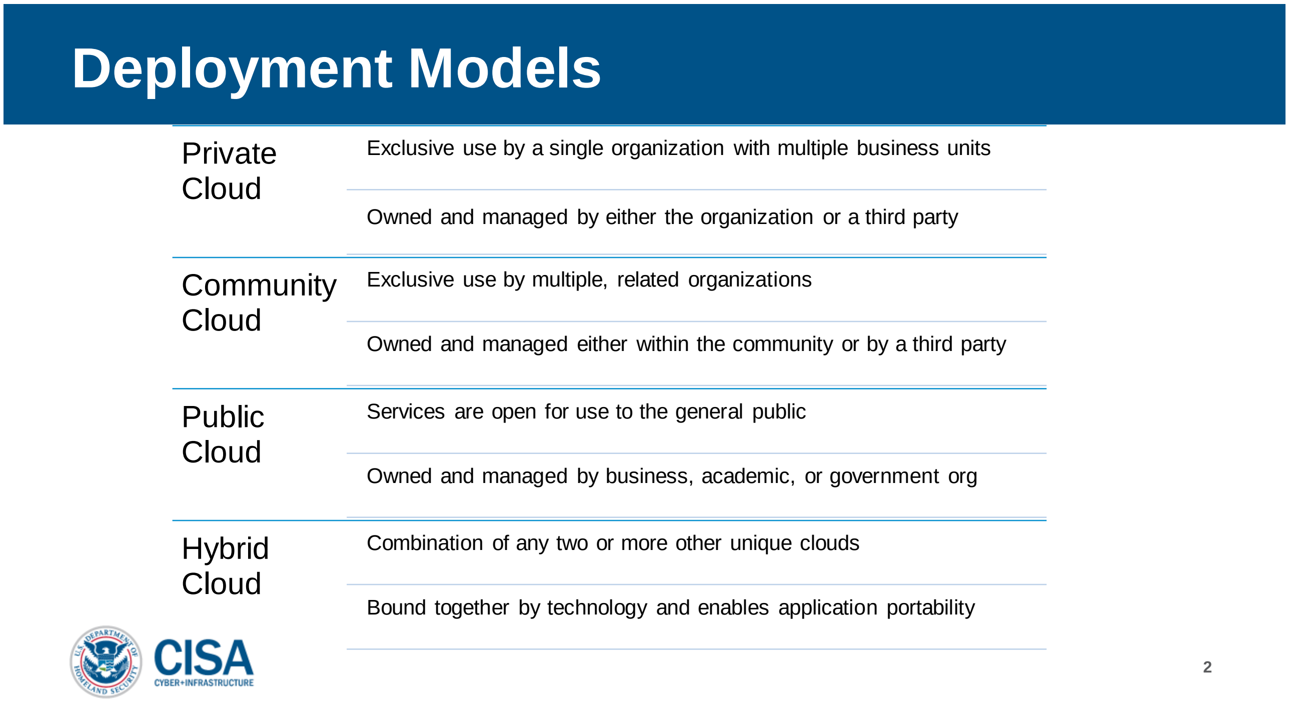
Cloud Architectures and Deployment Models

Cloud Architectures and Deployment Models

1

**001 Instructor: In this section, we will talk about different cloud architectures as well as the different goals involved in those cloud architectures.

Deployment Models



Deployment Models

Private Cloud	Exclusive use by a single organization with multiple business units
	Owned and managed by either the organization or a third party
Community Cloud	Exclusive use by multiple, related organizations
	Owned and managed either within the community or by a third party
Public Cloud	Services are open for use to the general public
	Owned and managed by business, academic, or government org
Hybrid Cloud	Combination of any two or more other unique clouds
	Bound together by technology and enables application portability

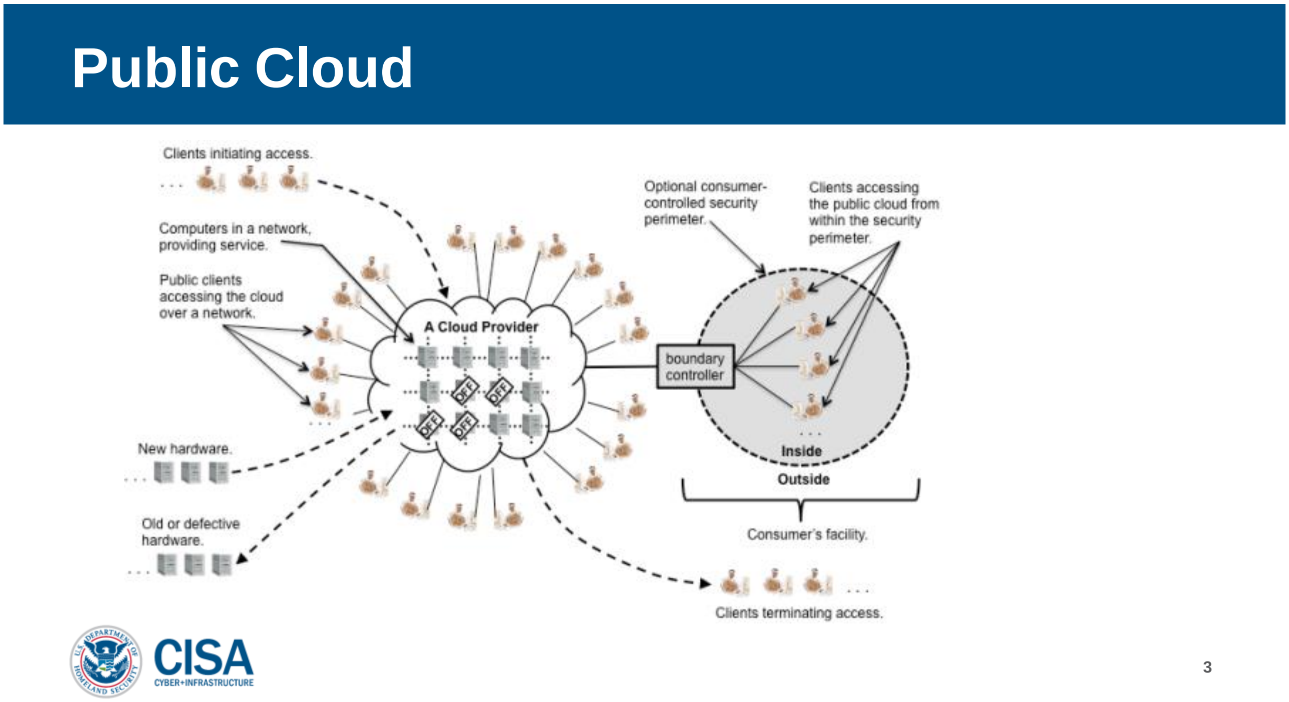
**002 First, there are four different major deployment models here. The first is a private cloud. And this is where a single organization has multiple different business units and establishes and resources their own private cloud. So only that organization can use the cloud resources. So it's owned and managed by that organization.

We have none of the concerns about who owns the data? Where is the data being stored? Is the data being handled correctly according to our business regulations and laws? None of those concerns exist because the organization still controls all of the cloud resources. You don't have to go out to that cloud provider. Community cloud is where related organizations get together and pool their resources to buy that physical hardware and maintain and operate that physical hardware. So different organizations will have a piece of the cloud that will maintain and operate and provide those cloud resources. A third party can come in and manage those resources on behalf of those organizations. But only those organizations will have access to those cloud resources. A public cloud is open for general use, to the public.

So you don't have to be a member of the specific organization. You don't have to be a member of a group of organizations. Anybody can go and create an account on the public cloud. An example here maybe Dropbox or Evernote, or any number of the different providers on the Internet. These public clouds are owned and managed by businesses such as Google and Microsoft. It could be academic because it could be a university-based cloud. Or maybe it's a government-based cloud. A government organization can host this public cloud. The difference between the public cloud and the private cloud, the public cloud is accessible to the general public. Then finally, we have hybrid cloud which is just a combination of two or more of these other models. And they do have to be a unique cloud.

So two community clouds together would just be one giant community cloud. It wouldn't be considered a hybrid cloud. But if you have a public cloud on a community cloud that would be a hybrid cloud. So these cloud models are typically bound together by some technology interface and it does enable a portability of applications. So should one cloud section go down, maybe that community cloud goes down, the public cloud can pick up that application and still provide that service and provide that functionality.

Public Cloud

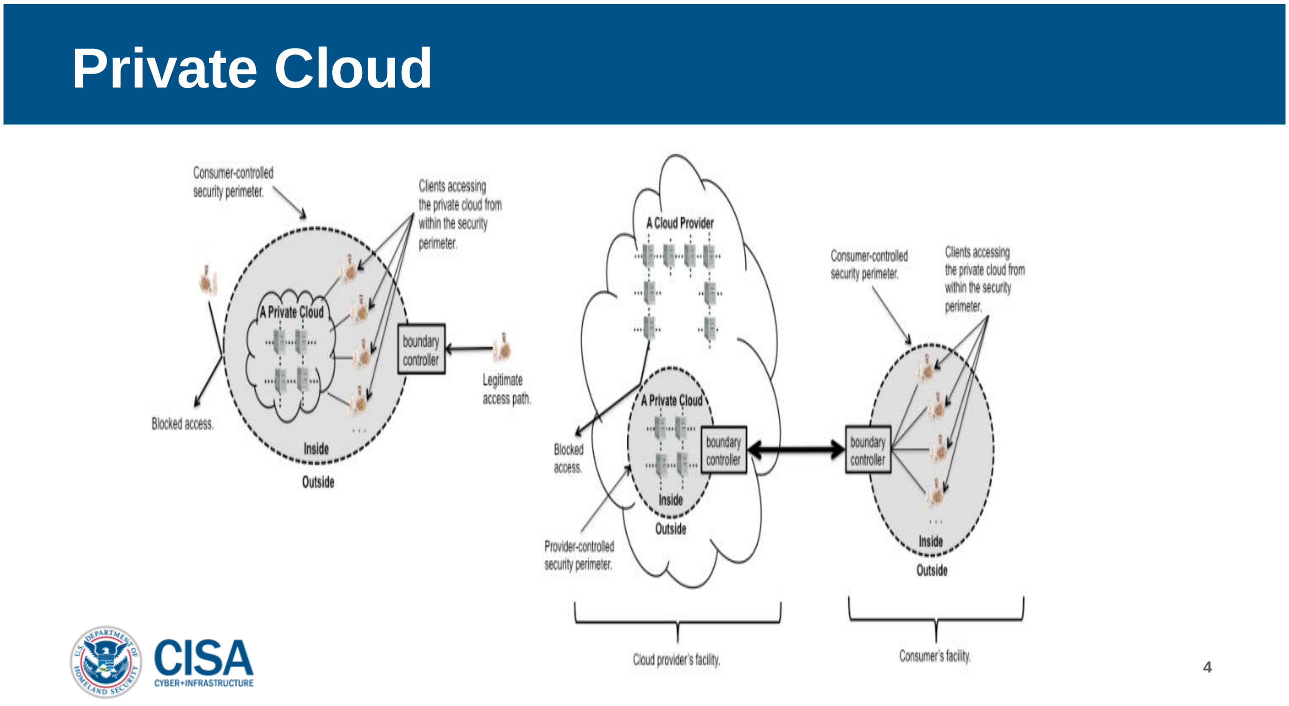


Public Cloud

Clients initiating access.
Computers in a network, providing service.
Public clients accessing the cloud over a network.
A Cloud Provider
OFF
OFF
OFF
OFF
New hardware.
Old or defective hardware.
Optional consumer-controlled security perimeter.
Clients accessing the public cloud from within the security perimeter.
boundary controller
Inside
Outside
Consumer's facility.
Clients terminating access.
CISA
CYBER+INFRASTRUCTURE
3

**003 Now here are some diagrams to make that make a little bit more sense. For a public cloud, here, we have our cloud provider that manages all of the hardware, it brings in new hardware. It takes out the old hardware. And here, we have clients that are connecting and clients are terminating access. And this inside outside diagram, this could be an organization or this could be someone's house. So here, we have the clients accessing the public cloud from within some kind of security perimeter. That could be an organization perimeter or that could just be a regular home or maybe a hotel perimeter. It doesn't really matter.

Private Cloud

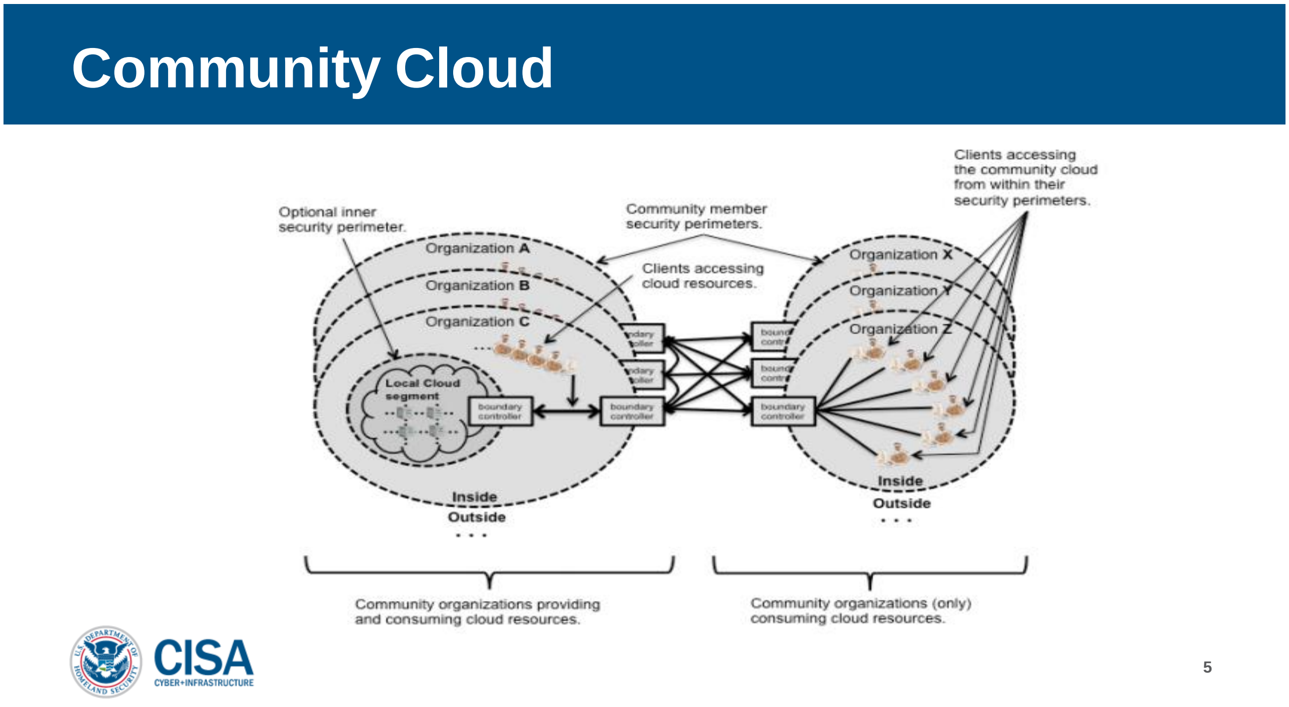


Private Cloud

Consumer-controlled security perimeter.
Clients accessing the private cloud from within the security perimeter.
A Private Cloud
boundary controller
Legitimate access path.
Blocked access.
Inside
Outside
A Cloud Provider
Consumer-controlled security perimeter.
Clients accessing the private cloud from within the security perimeter.
A Private Cloud
boundary controller
boundary controller
Blocked access.
Provider-controlled security perimeter.
Inside
Outside
Inside
Outside
Cloud provider's facility.
Consumer's facility.
CISA
CYBER+INFRASTRUCTURE
4

**004 Next up is private cloud. There's two basic models here. First model is that it's completely controlled within the organization. So there is no resource outside of this organizational boundary. There's nothing outside, other than maybe a user connecting in through a controlled interface. Or, an organization can rent some space through a cloud provider, but this, these cloud resources are considered to be belonging to that specific organization. This cloud provider manages resources on behalf of the organization but these resources are not shared with any other tenant. They are solely belonging to that one organization.

Community Cloud

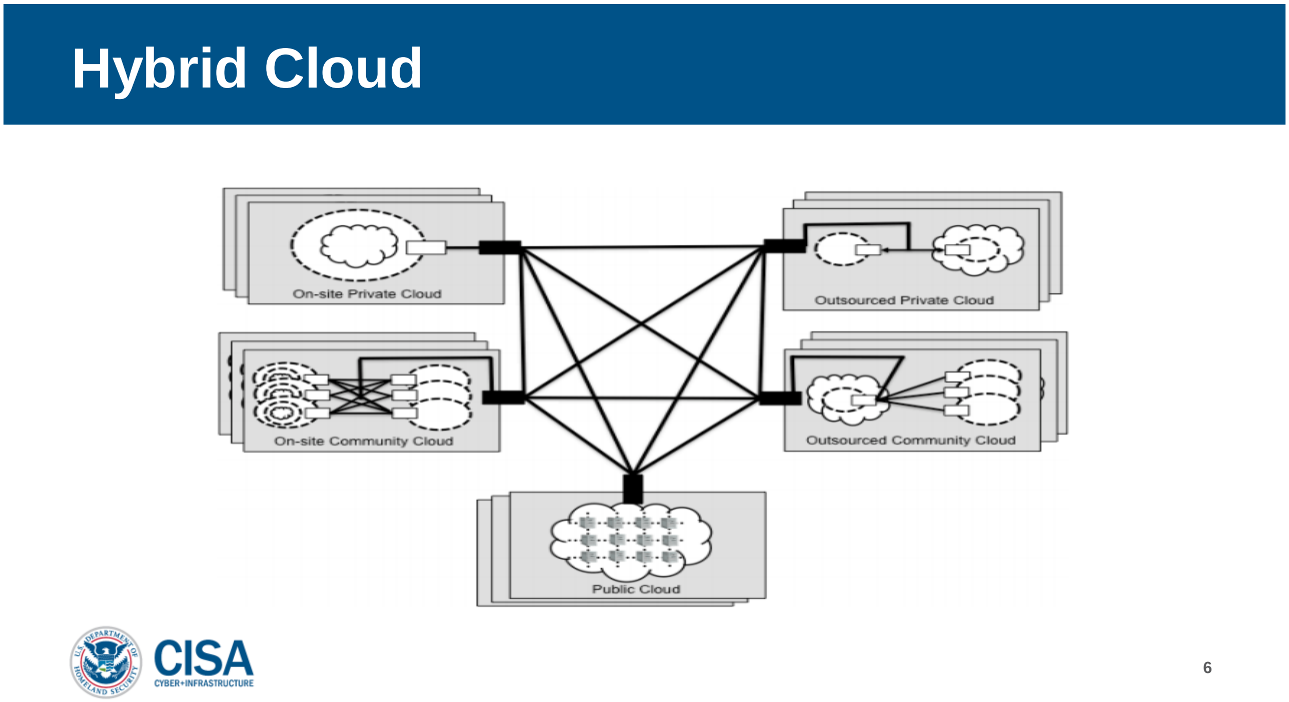


Community Cloud

Clients accessing the community cloud from within their security perimeters.
Optional inner security perimeter.
Community member security perimeters.
Organization A
Organization B
Organization C
Clients accessing cloud resources.
Organization X
Organization Y
Organization Z
Local Cloud segment
boundary controller
boundary controller
boundary controller
Inside
Outside
Inside
Outside
Community organizations providing and consuming cloud resources.
Community organizations (only) consuming cloud resources.
CISA
CYBER+INFRASTRUCTURE
5

**005 Now a community cloud will have a set of organizations that are both providing and consuming cloud resources. So the organizations A, B, and C here are both providing and consuming resources; versus the organizations X, Y, and Z. These are only consuming those cloud resources. They are not necessarily providing any resources themselves, they're just taking advantage of the resources provided by the other organizations.

Hybrid Cloud

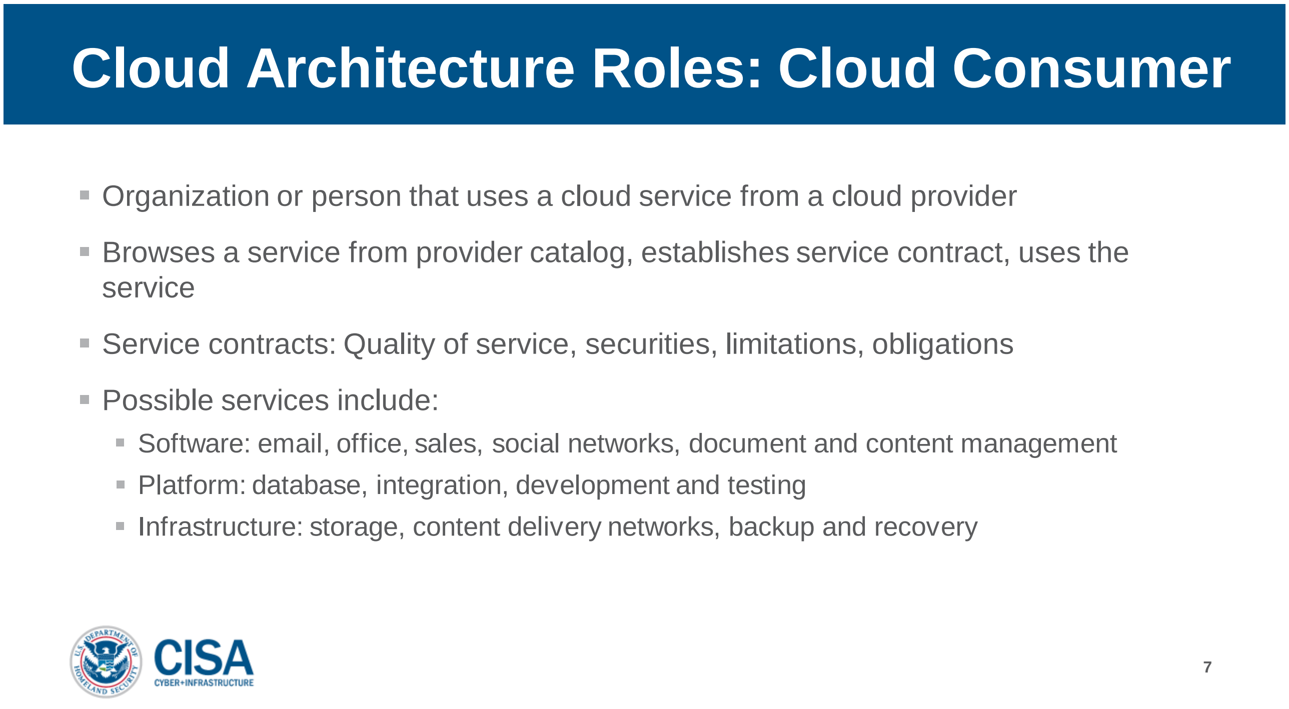


Hybrid Cloud

6

**006 And then here we have hybrid cloud. Where it's a combination of the different cloud models.

Cloud Architecture Roles: Cloud Consumer



Cloud Architecture Roles: Cloud Consumer

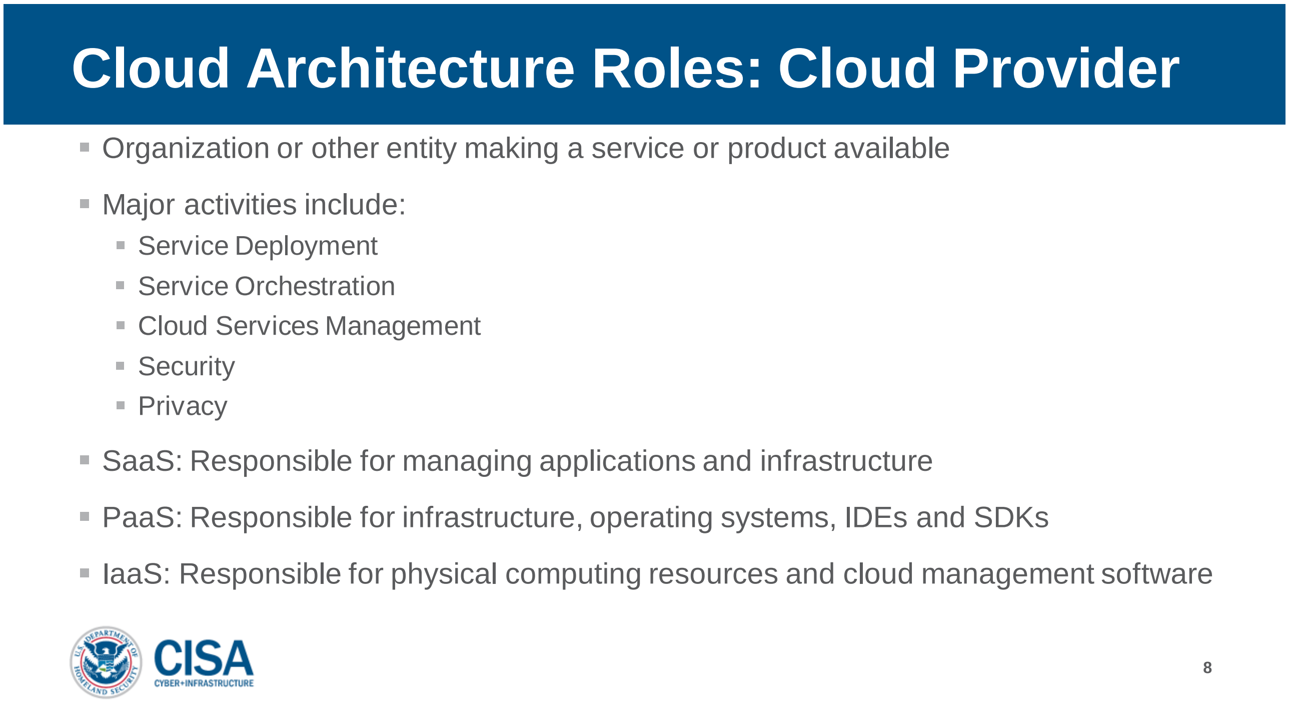
- Organization or person that uses a cloud service from a cloud provider
- Browses a service from provider catalog, establishes service contract, uses the service
- Service contracts: Quality of service, securities, limitations, obligations
- Possible services include:
  - Software: email, office, sales, social networks, document and content management
  - Platform: database, integration, development and testing
  - Infrastructure: storage, content delivery networks, backup and recovery

CISA CYBER+INFRASTRUCTURE

7

**007 Now there are five basic cloud roles. The first role is a cloud consumer. And this is the person or the organization who uses the cloud service, usually a cloud consumer will pay some kind of money to access that cloud service. Or maybe that service is being offered free of charge and the consumer just sees advertisements on the service. Somehow the cloud provider is making money, guarantee that one. So the cloud consumer browses the service from the provider catalog, establishes the service contract and actually uses the service. This could be mail, this could be software, this could be storage. Whatever it is, the cloud consumer has some kind of service contract with the cloud provider. So the cloud software as a service, that's typically what we're going to see here. It could be email, it could be office, it could be sales, social networks could also be considered software as a service. Platform and infrastructure as a service is also possible, though when you get into infrastructure as a service, it's more than likely going to be an organization rather than a person purchasing infrastructure as a service.

Cloud Architecture Roles: Cloud Provider



Cloud Architecture Roles: Cloud Provider

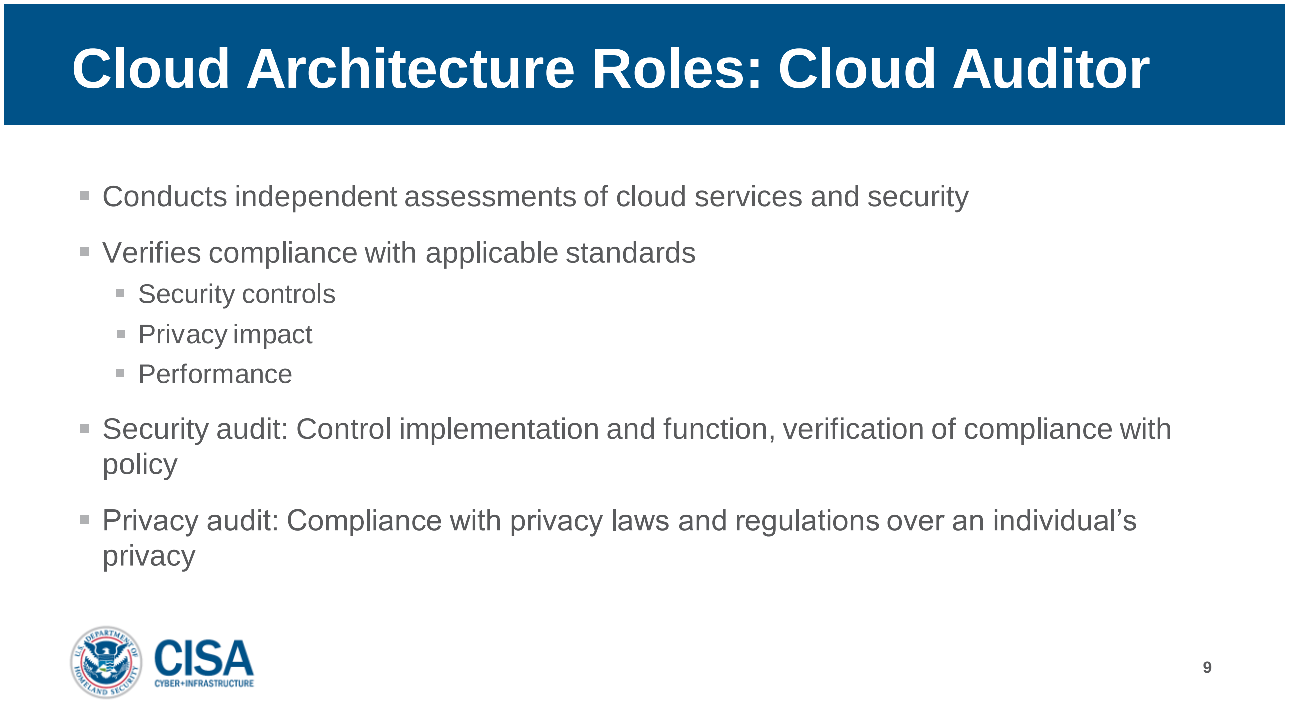
- Organization or other entity making a service or product available
- Major activities include:
  - Service Deployment
  - Service Orchestration
  - Cloud Services Management
  - Security
  - Privacy
- SaaS: Responsible for managing applications and infrastructure
- PaaS: Responsible for infrastructure, operating systems, IDEs and SDKs
- IaaS: Responsible for physical computing resources and cloud management software

CISA
CYBER+INFRASTRUCTURE

8

**008 Now a cloud provider is the other side of that coin. And it is another role. And it is the organization or the entity that is making that product available. It is making that service available. So the cloud provider is responsible for managing that cloud interface. It's responsible for managing the physical software and hardware of that particular cloud. And depending on the cloud model; software, platform or infrastructure as a service, depends on how much responsibility that cloud provider has.

Cloud Architecture Roles: Cloud Auditor



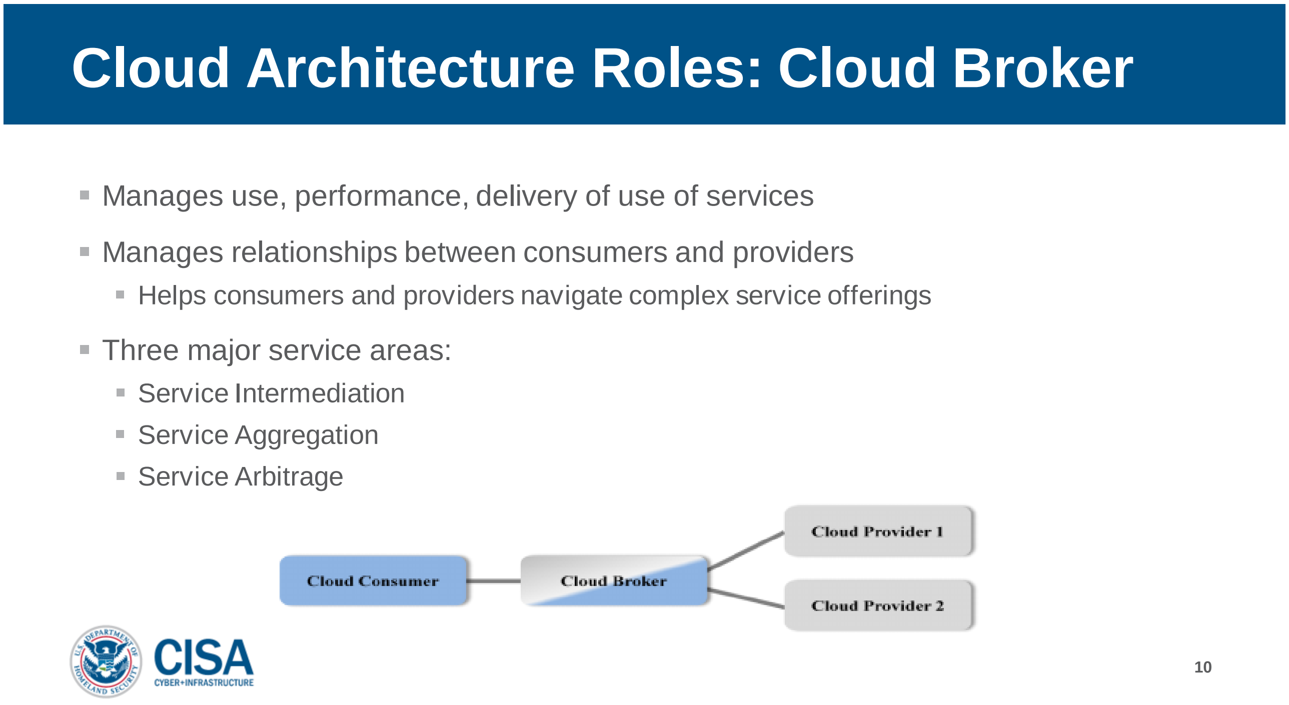
Cloud Architecture Roles: Cloud Auditor

- Conducts independent assessments of cloud services and security
- Verifies compliance with applicable standards
  - Security controls
  - Privacy impact
  - Performance
- Security audit: Control implementation and function, verification of compliance with policy
- Privacy audit: Compliance with privacy laws and regulations over an individual’s privacy

**009 The next role is the cloud auditor. And this is a third-party assessment that comes in and assesses the security and functionality and privacy of the cloud services. It could be a security audit, it could be a privacy audit, it could be a functionality audit. It could be all of the above. It could be a combination of the above. It depends on what kind of audit is being performed. So a cloud auditor will verify that the cloud provider's functionality claims are legitimate.

That their security level is adequate for a particular level of security or that their privacy level is adequate for particular level of privacy. And these are things that cloud consumers can expect the cloud providers to maintain because that means the cloud consumer has some kind of level of trust in the cloud provider, thanks to the cloud auditor.

Cloud Architecture Roles: Cloud Broker



Cloud Architecture Roles: Cloud Broker

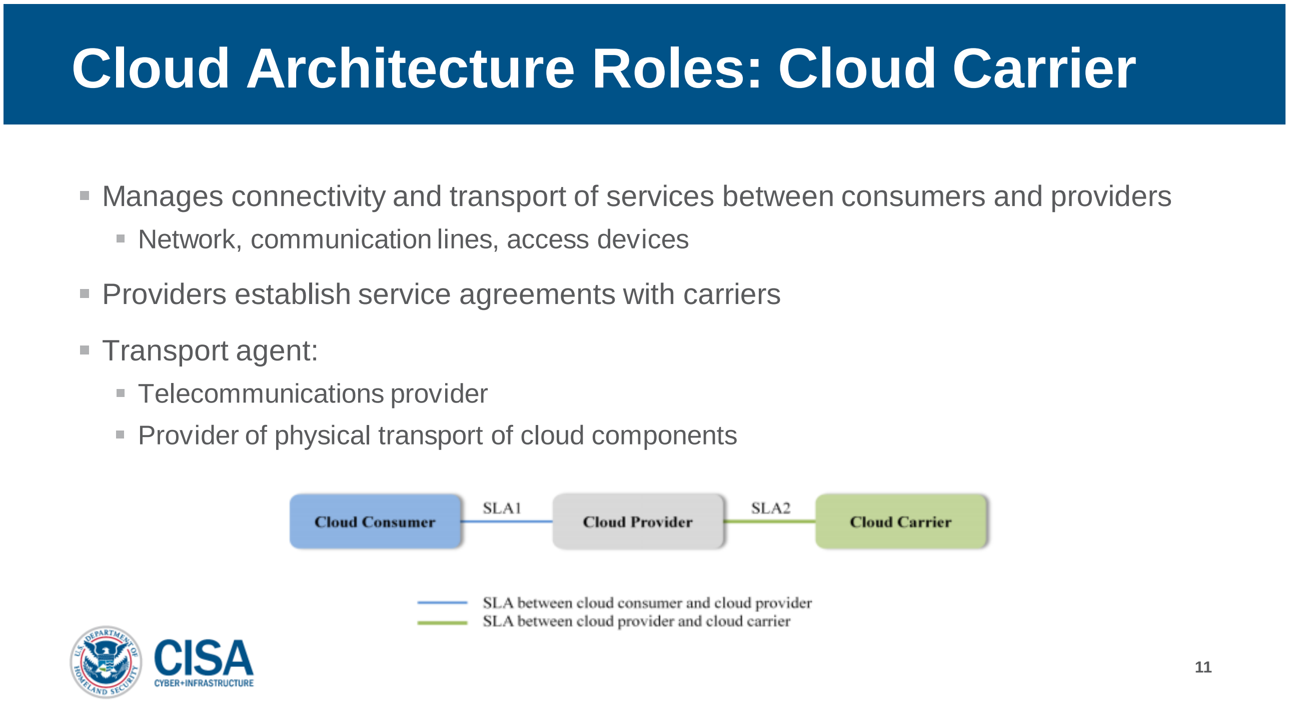
- Manages use, performance, delivery of use of services
- Manages relationships between consumers and providers
  - Helps consumers and providers navigate complex service offerings
- Three major service areas:
  - Service Intermediation
  - Service Aggregation
  - Service Arbitrage

Cloud Consumer
Cloud Broker
Cloud Provider 1
Cloud Provider 2

10

**010 The next role is the cloud broker. And the cloud broker helps the cloud consumer find, purchase and manage their cloud services. Because many companies are standing up clouds, they're calling their new software their, you know Acme cloud, just to make things a little bit more confusing for the consumer. Now the cloud broker is there to help the consumer navigate those waters. So the cloud consumer contracts with the cloud broker, says, 'hey, broker, I want these services. I want this functionality. I don't know what's best. I don't have time to sit down and sort through all the different providers. Just provide me with a solution.' The cloud broker goes, 'sure, I'll go out and do that research for you and then provide you with the solution.' And the cloud broker contacts the cloud providers that are most accurately needed for that particular consumer. And essentially brokers that deal.

Cloud Architecture Roles: Cloud Carrier



Cloud Architecture Roles: Cloud Carrier

- Manages connectivity and transport of services between consumers and providers
  - Network, communication lines, access devices
- Providers establish service agreements with carriers
- Transport agent:
  - Telecommunications provider
  - Provider of physical transport of cloud components

Cloud Consumer — SLA1 — Cloud Provider — SLA2 — Cloud Carrier

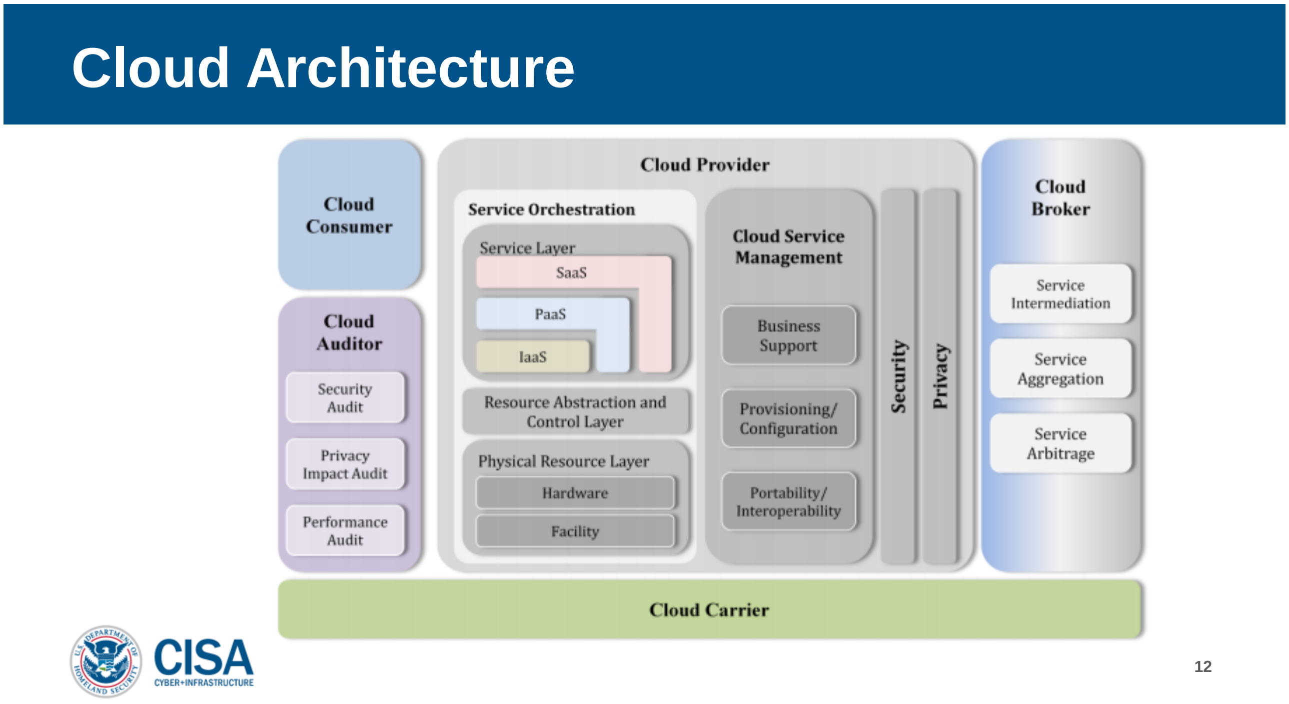
SLA between cloud consumer and cloud provider
SLA between cloud provider and cloud carrier

CISA
CYBER+INFRASTRUCTURE

11

**011 Then finally, we have a cloud carrier and this is essentially an additional layer of cloud. Because a cloud provider could be providing a software as a service, but themselves renting their own infrastructure as a service. So that cloud carrier manages that connectivity and manages the transport of services between the consumer and between the provider. So it does establish some service agreements with the providers. So this consumer has their own service agreement with the provider. As far as the consumer is concerned, everything stops here. Because they're just relying on the cloud provider. And the cloud provider can have an additional agreement with the cloud carrier, creating a chain of agreements that is required for that particular cloud to be functional.

Cloud Architecture

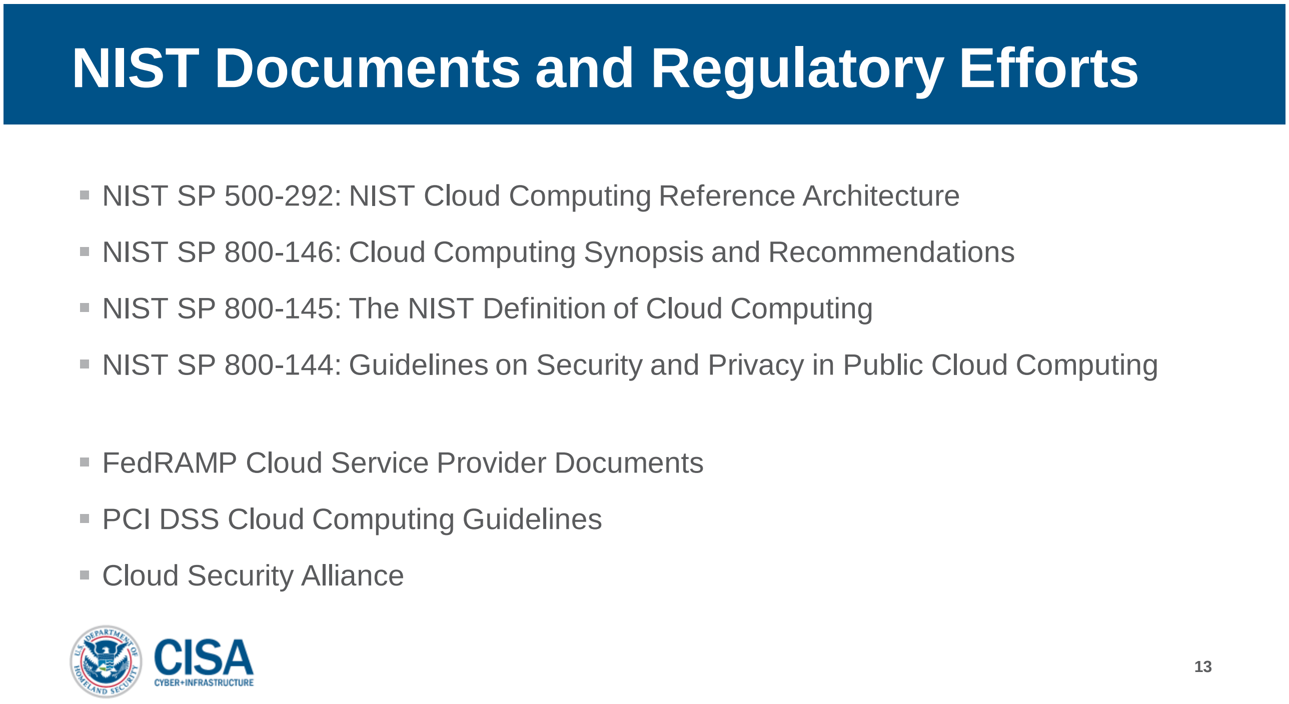


Cloud Architecture

12

**012 To group this all together, we have cloud consumer right at the top. We have cloud auditor over here on the side. And then, the cloud provider has the bulk of the responsibilities here, as far as cloud architectures. Because they have to set up infrastructure platform and service, and software as a service, as well as establish all of the hardware, establish the cloud server management, and have privacy and security controls in place. And then the cloud broker sits to the side there to offer that service implementation, that service aggregation, and that service arbitrage. Where's the cloud carrier? Sits right at the bottom and provides service to all of the other roles.

NIST Documents and Regulatory Efforts



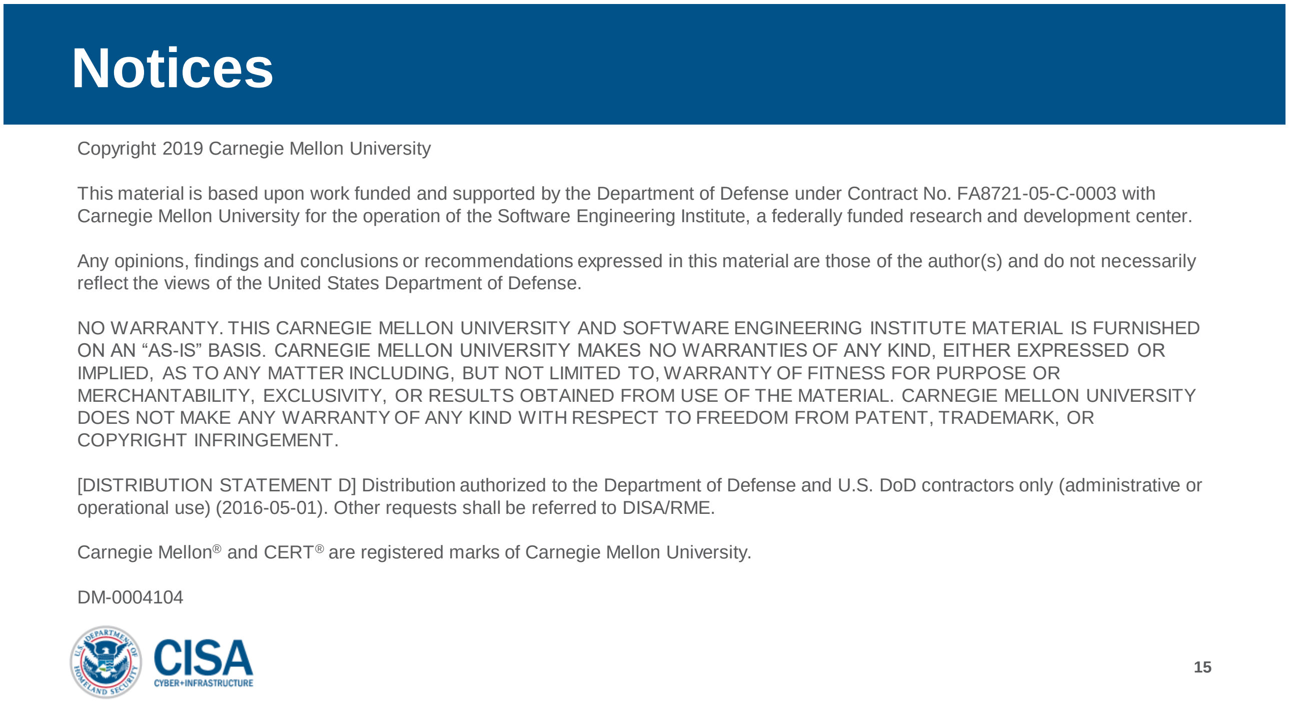
NIST Documents and Regulatory Efforts

- NIST SP 500-292: NIST Cloud Computing Reference Architecture
- NIST SP 800-146: Cloud Computing Synopsis and Recommendations
- NIST SP 800-145: The NIST Definition of Cloud Computing
- NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing

- FedRAMP Cloud Service Provider Documents
- PCI DSS Cloud Computing Guidelines
- Cloud Security Alliance

**013 Now there has been regulatory efforts for cloud computing, primarily through NIST, and NIST does have a series of special publications. So for more details on how to secure the cloud and more details on cloud architecture, definitely refer to these documents. FedRAMP for federal space also has some provider documents that are available. For the financial sector, PCI DSS has its own guidelines for cloud computing. And then finally the Cloud Security Alliance is an organization dedicated to the security of cloud computing.

Notices



Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT D] Distribution authorized to the Department of Defense and U.S. DoD contractors only (administrative or operational use) (2016-05-01). Other requests shall be referred to DISA/RME.

DM-0004104