SPIRENT
Federal Systems

White Paper

# Impact of DoD Cloud Strategy and FedRAMP on CSP, Government Agencies and Integrators.

# Table of Contents

# 1.0 DoD Cloud Strategy Impact

The DoD Cloud Computing Strategy impacts all Cloud Service Providers (CSP) at government agencies and integrator facilities as well as customers procuring cloud services. The Strategy has accelerated the move to consolidate thousands of government data centers and enterprise services into a small number of clouds. These clouds are being built and managed by government, integrators, and commercial CSP like Amazon, IBM, Microsoft and Oracle.

All the cloud computing benefits that DoD envisions; efficiency, effectiveness and security present service and security challenges to government, service providers, service consumers and third party assessors. Cloud service requirements for broad network access, rapid elasticity, resource pooling, on-demand services and measured services impact the type of test cloud solutions used to validate CSPs. To meet these challenges, the DoD is leveraging the Federal Risk and Authorization Management Program (FedRAMP).

## 1.1 DoD Cloud Strategy

The Strategy was developed to foster adoption of cloud computing, optimize data center consolidation, establish DoD Enterprise Cloud Infrastructure and deliver cloud services. The Strategy encourages DoD Components to use cloud services offered by other DoD Components, Federal Government Agencies, mission partners and commercial vendors. Cloud Service Providers must comply with DoD Information Assurance (IA), cybersecurity, COOP and other policies.

In compliance with DoD IA and security directives, the Strategy calls for separate Cloud Service Providers for Nonsecure Internet Protocol Router Network (NIPRNet), Secure Internet Protocol Router Network (SIPRNet) and Top Secret Sensitive Compartmentalized Information (TS SCI) security domains.

The Strategy emphasizes that cloud services are a key component that will enable it to achieve DoD's Joint Information Environment (JIE) goals. JIE will deliver and increase collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location. JIE will help transform the way DoD acquires, operates and manages IT resources. The Department's goal is to achieve an increase in efficiency, effectiveness and security.

### 1.2 Federal Risk & Authorization Management Program

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. It establishes a set of requirements to test, assess and authorize cloud infrastructures and services for government agencies. FedRAMP impacts any government or corporate organization that wants to establish and provide cloud infrastructures and services for the federal government. Prior to deployment, CSP need to comply with FedRAMP to test and assess the three basic cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

As of the date of this white paper, four cloud services have received full FedRAMP authorizations and eleven services have received provisional authorizations. Services that have been granted FedRAMP authorization include:

- Amazon AWS GovCloud IaaS
- Amazon AWS East/West IaaS
- USDA National Information Technology Center (NITC) IaaS
- eCase SaaS

Other services that have been granted provisional FedRAMP authorization include:

- Akamai Content Delivery IaaS
- Oracle Federal Managed Cloud Services PaaS
- AT&T Storage as a Service (StaaS)
- IBM Smart Cloud for Government IaaS
- HP Enterprise Cloud Services - Virtual Private Cloud IaaS
- Lockheed Martin Solutions as a Service (Solas)
- Microsoft Cloud Infrastructure IaaS
- Microsoft Windows Azure Public Cloud Solution PaaS

#### 1.2.1 Cloud Assessment Organizations

FedRAMP accredits third party assessors to provide verification for cloud services. Such assessors are known as Third Party Assessment Organizations (3PAO). A 3PAO performs the functions of a cloud auditor for pre deployment and post deployment operations. Cloud CSP have to comply with FedRAMP 3PAO requirements and perform the following functions:

- Develop Security Assessment Plan
- Perform initial assessments of CSP security controls
- Conduct security tests
- Develop a Security Assessment Report

# 2.0 Cloud Service Roles & Models

This section describes the Strategy cloud service roles and cloud models.

### 2.1 Cloud Service Roles

#### 2.1.1 Service Consumer

The Strategy defines the role of Service Consumer as organization that decides to move certain IT resources from the confines of their enterprise to one or more external partners allowing them to focus resources on mission critical needs.

#### 2.1.2 Service Provider

The Strategy defines the role of Service Providers as organizations that decide to specialize in offering an IT service to multiple consumers over a network. Service providers invest in transitioning enclave IT capabilities into cloud services by implementing scalable and dependable infrastructures. CSP infrastructures enable customer self-service and metered utilization through automation.

### 2.2 Service Models

The Strategy defines three basic cloud service models; Software as a Service (SaaS) Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

#### 2.2.1 Software as a Service (SaaS)

The Strategy defines SaaS as the capability provided to the consumer by a CSP to use applications hosted on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface such as a web browser or a program interface.

In a SaaS model, the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

#### 2.2.2 Platform as a Service (PaaS)

The Strategy defines PaaS as the capability provided to the consumer to deploy consumer created or acquired applications into the cloud infrastructure. The CSP supports the applications programming languages, libraries, services, and tools.
In a PaaS service model, the consumer does not manage or control the underlying cloud infrastructure including the network, servers, operating systems, or storage. The consumer only has control over the deployed applications and configuration settings for the application environment.

### 2.2.3 Infrastructure as a Service (IaaS)

The Strategy defines IaaS as the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources. In an IaaS service model, the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

In an IaaS service Model, the consumer does not manage or control the underlying cloud infrastructure such as the hypervisors, but has control over operating systems, storage, and deployed applications. The consumer could have limited control of select networking components such as host-based firewalls.

# 3.0 Cloud Data & Service Requirements

In order to understand the challenges in government cloud deployments for Big Data Analytics we first need to understand Big Data.

### 3.1 Cloud Data Analytics Requirements

The term "Big Data" describes how organizations use data mining applications to analyze data and establish relationships between data. Leveraging new database and file systems technology, enterprises and government agencies can correlate petabytes of data to try to predict future events and behaviors; and analyze historical data. Cloud test tools need to be able to generate petabytes and petabytes of data that can be used by data mining applications. Data generated by cloud test tools need to support Big Data databases, file systems and protocols. In the past Oracle, Microsoft and IBM have accounted for more than 80% of the relational database market. The Structured Query Language (SQL) is still the most popular relational database programming language. SQL databases store data in multiple tables where users can insert, delete or modify the data. Today, there are new database options for data mining and analytics applications. Many of these options do not use SQL. As the name implies "Not Only SQL" or NoSQL are databases that don't use SQL. NoSQL databases are very good at processing unstructured content found in social networks like twitter, facebook and linkedIn. The most popular NoSQL databases used for data mining and analytics are Cassandra, MongoDB, CouchDB and Hadoop. Retrieving and analyzing data requires vast computing resources. This is where the NoSQL and Hadoop file systems play an important role.

### 3.1.1 Hadoop

Hadoop is a framework for distributed computing of large data sets across multiple datacenters and computer clusters. It was designed to handle petabytes of both unstructured and structured data. Unlike centralized databases, Hadoop is designed to run on a large number of servers that don't share memory or disk storage. Hadoop can scale from one server to thousands of servers with each server providing processing resources. The Hadoop framework includes multiple elements that include common utilities, a distributed file system, a simple job scheduler, and a parallel processing job scheduler known as MapReduce.

The framework and Hadoop Distributed File System (HDFS) is being widely adopted by hundreds of organizations. It is being used by IBM, eBay, Rackspace, Facebook, Google, Yahoo, Twitter and LinkedIn. According to Apache, Yahoo is running Hadoop on more than 40,000 computers with over 100,000 CPUs. Twitter uses it to store and process tweets and log files. LinkedIn is using it on more than 4,000 computers. Facebook uses it on more than 1,400 computer clusters with over 11,000 cores.

### 3.1.2 Cassandra

Cassandra is a NoSQL open source distributed database system with strong support for clusters and data centers. It is designed to process large amount of data in a distributed environment. The ability to replicate data across multiple servers increases availability and prevents a single point of failure. Cassandra was developed by Facebook to support their search features. It is now maintained and distributed by Apache.

### 3.1.3 MongoDB

MongoDB is a NoSQL open source document-oriented database system. Document oriented databases are designed for storing, retrieving, and managing semi-structured data. MongoDB uses multiple encodings including XML and JavaScript Object Notation (JSON). MongoDB is used by Craigslist and eBay.

### 3.1.4 Couch DB

CouchDB is another NoSQL open source document-oriented database system. It stores data as documents. CouchDB uses JavaScript Object Notation (JSON) to store data and JavaScript as its query language.

### 3.2 Cloud Service Requirements

The Strategy defines cloud service characteristics that are essential for DoD and which need to be tested by auditors and Cloud Service Providers.

### 3.2.1 Broad Network Access Requirements

Broad network access is the ability of the CSP to provide network access through standard mechanisms that promote use by heterogeneous thin or thick client platforms. Thin client platforms include mobile phones and tablets while thick client platforms refer to desktops and laptops.

Auditors need to be able to assess if cloud services are capable of providing access to mobile devices and fixed devices for both thin and thick clients. Test tools should be able to simulate thousands of mobile and fixed clients from smartphones, tablets, laptops and desktops. Assessments should include generating multiple network, transport and application protocols while generating security exploits to ensure the resiliency of the CSP infrastructure and services.

### 3.2.2 Rapid Elasticity Requirements

Elasticity is nothing more than the ability to add and remove computer resources in order to meet the size and time requirements for workloads. In other words, you may have a data analytics task that requires more computer servers, memory and CPU cores. Cloud environments that leverage virtualization of servers and network devices can add or remove computing resources in a matter of minutes. Without virtualization, it could take days and weeks to add and provision physical servers, memory, cores, storage and network resources.

Auditors need to be able to test rapid elasticity by generating load traffic that simulates thousands of concurrent users and connections per second. The test loads should assess the resiliency of virtual hypervisors and virtual images to operate under loads that meet and exceed their specifications. In addition, the load and test traffic should simulate enterprise services including email services, relational databases, NoSQL data analytics databases, web services, video and voice services. The test profiles should generate thousands of application level protocols for SQL and NoSQL data analytics applications including SSL, TLS, HTTP, SMTP, MySQL, Cassandra, MongoDB, CouchDB and Hadoop.

### 3.2.3 Resource Pooling Requirements

Resource pooling is defined as the ability to re-allocate computing resources to serve multiple DoD organizations using a multi-tenant model. In this model providers are able to pool different physical and virtual resources dynamically and assigned and reassigned them according to consumer demand.

The difference between resource pooling and rapid elasticity is that with resource pooling, providers are assigning and reassigning existing resources where in rapid elasticity providers are adding and removing computing resources. Computing resources include storage, processing, memory, network bandwidth, and virtual machines.

### 3.2.4 On Demand Self Service Requirements

On demand self-service is defined as the ability for consumers to unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with Cloud Service Providers.

### 3.2.5 Measured Service Requirements

Measured service is defined as the ability for cloud systems to automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of Service. Measured or metered services can include storage, processing, bandwidth, and active user accounts. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

### 3.2.6 Security Requirements

The Strategy dictates that Cloud Service Providers need to comply with all DoD security policies, instructions and directives. Ensuring the confidentiality, integrity and availability of cloud infrastructure and services is a top priority for the Department mission critical applications and networks.

# 4.0 Cloud Assessment & Test Requirements

### 4.1 Cloud Test Providers

Cloud test tools should reside in the cloud just like any other cloud application. In order to measure the impact of latency and meet elasticity and COOP requirements, Cloud Test Providers should have more than one cloud Point of Presence (POP) in the country and the world.

### 4.2 Cloud Test Virtual Machines

In order to protect your capital investments, cloud assessment applications should be virtualized and like any Virtual Machine (VM) it should run on any hypervisor. It should not matter if the hypervisor vendor is IBM, HP or Vmware. Consumers should be able to move cloud assessment applications from one CSP to another one in minutes; from Amazon to Rackspace; IBM to Microsoft or Lockheed to Raytheon.

### 4.3 Application Layer & Load Realism

Cloud auditors and Cloud Service Providers need to understand and be concerned with the difference of cloud test tools, stand alone test tools and their features. For example, cloud test solutions that generate an HTTP have a low value if there is no variation for the HTTP header fields. These tools do not interact with an application server by using the server's responses and decide what to do next. Although they may indicate the number of HTTP Get transactions that the server is responding, they do not exercise all the logic of the HTTP web server application so the results are not reliable.
Cloud test solutions should mimic real clients such as browsers and their human interactions. At a minimum, they should allow customers to configure a list of usernames and passwords to authenticate users. Some tools use CVS lists but are very cumbersome to use because they usually rely only on regular expressions mechanisms to filter responses from the server. In today's environment, JavaScript Object Notation (JSON) is becoming the predominant data exchange format for client to server communications. An advanced cloud test solution should support and process JSON interactions between client and servers.

In order to achieve valid load realism on a server, cloud test solutions should be able to generate random request to multiple cloud services. The request could be against web servers, database servers or mail servers. If a web server is used, as an example, it is observed that web clients or users browse many pages at random. For most cloud test solutions, it is very difficult to develop such test cases that could involve saving multiple web pages and links, multiple cart products, creating arrays and selecting indexes. In those cases, the test users decide to create very simplistic scenarios that do not exercise the real load of those servers. This creates an illusion of load performance and test results.

Advanced cloud test solutions should be able to randomly pick a product or service from an enterprise site, fill out forms, emulate mobile devices along with their geo location, decide how much load should be served from a browser or database cache, and generate loads from multiple IPs and ports.

### 4.4 Network & Transport Layer Realism

CSP assessments should leverage cloud test tools that simulates real traffic. One of the characteristics of real traffic is randomization of source port and IP addresses. Generating traffic that simulates thousands of users can be implemented in multiple ways. Test tools could use one IP that generates thousands of transport UDP and TCP sessions with random source port allocation; or the tool may generate thousands of IP addresses with one or just a couple of transport sessions.

### 4.5 Security and Vulnerabilities

Cloud test solutions should be able to generate thousands of security attacks against cloud infrastructure servers and services. The attacks should map to the industry Common Vulnerabilities and Exposures. In addition, test solutions should be able to generate fuzzing traffic to discover new Zero-Day attacks.

# 5.0 Cloud Test Tools

Auditors and Cloud Service Providers are entrusted with ensuring the resiliency, confidentiality, integrity and availability of cloud infrastructures and services. For this reason, validation and verification of cloud requirements both prior to deployment and after deployment will have an impact on the security posture of cloud services. It is essential that Cloud Service Providers and auditors select the right cloud test solutions and tools.

## 5.1 Spirent Cloud Solutions

Spirent Federal delivers the most broad selection of government cloud test solutions, empowering government agencies, federal integrators, service providers and third party assessors to test multiple cloud service models. Spirent cloud test solutions allow customers to test SaaS, PaaS and IaaS cloud services.

With thousands of customers using our cloud test solutions, Spirent is the leading cloud test solution company in the world. Cloud Service Providers and 3rd Party FedRAMP assessors using Spirent cloud solutions do not have to choose between security and performance. Spirent's private cloud and managed cloud solutions leverage our Blitz and ArmorHub technology to generate application and security traffic to measure the resiliency, confidentiality, integrity and availability of cloud infrastructures.
Spirent test clouds generate client to server transactions for multiple protocols. Using Blitz technology, Spirent can measure the maximum number of users, client applications, server transactions for physical and virtual devices including servers, switches, routers, load balancers, firewalls, IDS/IPS and Data Loss Prevention (DLP) appliances. Spirent clouds allow customers to measure the computing resources of virtual and physical cloud components. Spirent clouds generate security traffic to assess the security posture of cloud infrastructures. Using ArmorHub technology, Spirent clouds generate traffic to scan servers for Common Vulnerabilities & Exposures (CVE).

Spirent Federal Systems
1402 W. State Rd.
Pleasant Grove, UT, 84062
801 785 1448
www.spirentfederal.com

SPIRENT
Federal Systems