Section III - International Business Machines Corporation's Description of its IBM Cloud Infrastructure as a Service (IaaS) System

III. International Business Machines Corporation's Description of its IBM Cloud Infrastructure as a Service (IaaS) System

A. System Overview

Background

International Business Machines Corporation, also referred to as "IBM Cloud IaaS" provides on-demand cloud infrastructure as a service to its customers, allowing them to create scalable bare metal server, virtual server, or hybrid computing environments, via IBM Cloud IaaS's Customer Portal, leveraging global data centers and points of presence (PoP).

IBM Cloud IaaS is built using a Network-Within-A-Network topology that provides remote access to allow customers the ability to build and manage computing environments remotely. IBM Cloud IaaS's "Network-Within-A-Network" configuration includes three (3) network interfaces. Public, private, and management traffic travel across separate network interfaces, segregating and securing traffic while streamlining management functions.

- Public Network - Network traffic from anywhere in the world will connect to the closest network PoP, and it will travel directly across the network to its data center, minimizing the number of network hops and handoffs between providers.
- Private Network - Provides a connection to the customer's servers (bare metal or virtual) in IBM Cloud IaaS data centers around the world. Data can be moved between servers through the private network; and customers can utilize various services, update and patch servers, software repositories, and backend services, without interfering with public network traffic.
- Management Network - Each server within the IBM Cloud IaaS is connected to the management network. This out-of-band management network, accessible via VPN, allows access to each server for maintenance and administration, independent of its CPU and regardless of its firmware or operating system.

The following products and services are delivered within the IBM Cloud IaaS system boundaries:

- Networking: IBM Cloud Load Balancer, IBM Cloud Direct Link "1.0", Hardware Firewall, Gateway Appliance, IPSec VPN, Fortigate Security Appliance
- Storage: IBM Cloud File Storage, IBM Cloud Block Storage, IBM Cloud Backup, IBM Cloud Object Storage (IaaS), Storage Area Network (SAN)
- Compute: IBM Cloud Bare Metal, IBM Cloud Hardware Security Module, SAP-Certified Cloud Infrastructure, IBM Cloud Virtual Servers

IBM Cloud IaaS delivers its products and services through the Internal Management System (IMS), which is an internally developed customer relationship management (CRM) system used to track customers' hardware and services. IMS allows customers to manage their cloud environments. Customer capabilities include management of system and network devices provisioned by the customer, account management, ordering and deployment, and customer support.

IMS has two components: IMS, as viewed by internal employees, and the Customer Portal, as available to users of IBM Cloud IaaS. The Customer Portal allows customers to:

- Create and manage tickets for incident response and resolution
- Review account information

- View information and certain configuration data regarding their purchased solutions
- Perform functions such as OS reloads, and access RescueLayer
- Maintain customer provisioned firewall and DNS configurations that affect their bare metal servers
- Purchase or upgrade services to initiate the automated provisioning process for new systems

IBM Cloud IaaS personnel also have access to IMS to set up and configure purchased solutions, assist in troubleshooting technical issues, and respond to customer requests.

Service Commitments and System Requirements

Customers are provided and required to agree to a Cloud Service Agreement (CSA) during the ordering process. The CSA is available to customers through the customer portal and acts as the formal contract and usage policy for customer users of the IBM Cloud IaaS system. The CSA documents the contractual obligations of IBM Cloud and the customers using IBM Cloud IaaS, including principal service commitments and system requirements. Any updates to the CSA are communicated to the existing customers through the IBM Customer Portal.

Only the principal service commitments and system requirements relevant to the applicable trust services criteria are within the boundaries of the system. Security and availability commitments include but are not limited to the following:

- Security and availability commitments to user entities are documented and communicated in contracts and customer agreements as well as in the description of the service offering that is available to customers
- Security and availability risk assessments of the IBM Cloud Services are performed at least annually
- Monitoring controls are in place to provide oversight of controls and processes within the operation of the system
- Use of encryption technologies to protect customer data both at rest and in transit
- Security and availability categories within the fundamental design of the system are designed to permit system users least privileged access based on job responsibilities
- Physical access to facilities and restriction of protected information assets to authorized personnel
- Tone at the top, annual trainings and recertifications of skills development
- Monitoring controls are in place to assess, test, and apply security advisory patches to the IBM Cloud services and associated systems, networks, applications, and underlying components within the scope of services
- Policies and procedures are designed to manage risks associated with the application of changes
- A backup process is performed and available to allow restoration in the event of data loss or downtime

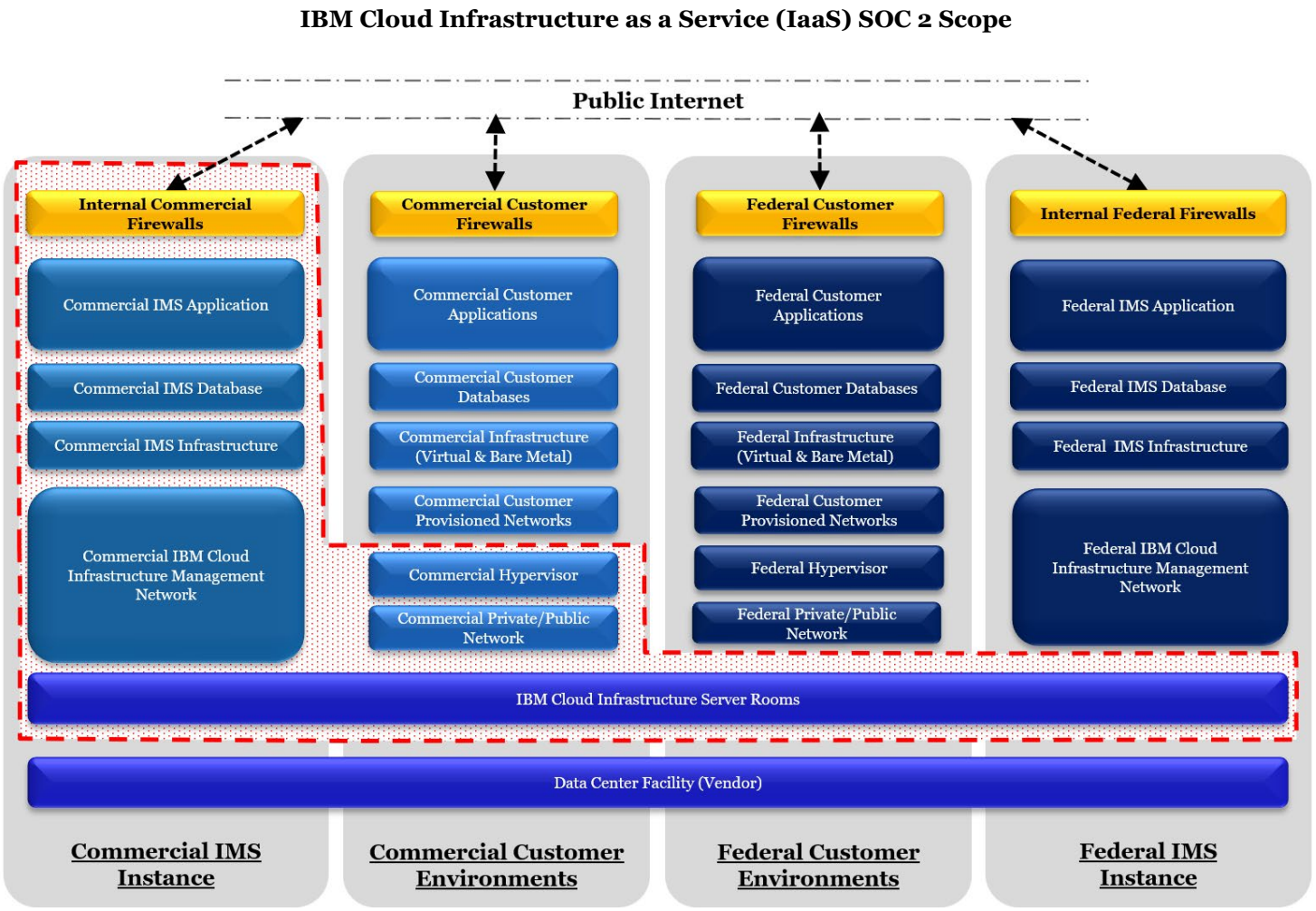
The relevant service commitments and system requirements are also included within the following sections of the CSA:

1. Cloud Services
2. Content and Data Protection
   Included within paragraph d. of the Content and Data Protection section is a link to IBM's Data Security and Privacy Principles for IBM Cloud Services (DSP). Relevant service commitments and system requirements are included within the following sections of the DSP:
   - Data Protection
   - Security Policies
   - Security Incidents
   - Physical Security and Entry Control
   - Access, Intervention, Transfer and Separation Control
   - Service Integrity and Availability Control
9. General

The CSA encompasses the full list of service commitments and system requirements delivered to IBM Cloud customers, which may include services outside the scope of the report. As such, the CSA should be read in conjunction with the system boundaries and applicable trust services criteria outlined below. All other service commitments and system requirements described within the CSA are not in scope for this report.

Principal service commitments and system requirements within the boundaries of the system are outlined further in the sections below. Additionally, aspects of the system description that reflect the boundaries of the IBM Public Cloud Platform system are posted online for customers and prospective customers in the IBM Cloud Terms of Use within the IBM Customer Portal.

Boundaries of the System



Note: Area within the dashed line is within the boundaries of the system.

The boundaries of the system covers the services managed by IBM Cloud IaaS, including global data center physical locations, the IMS portal and the supporting infrastructure devices. This also includes the network devices that are managed by IBM Cloud IaaS and infrastructure (including hypervisors) that support customer environments.

Customers are responsible within their commercial customer environment for management of the customer provisioned network devices, infrastructure (bare metal and virtual servers), databases, applications, and other systems/devices including the implementation, configuration, and maintenance of such, and are not included within the scope of this report.

The following products and services are delivered from within the IBM Cloud IaaS scope and are provisioned via IMS. Customers are responsible for the implementation, configuration, and maintenance within their environment.

Networking

- **IBM Cloud Load Balancer** enables customers to utilize public (internet facing) and private (internal) load balancing to distribute traffic between application servers deployed locally within an IBM Cloud data center.

- **IBM Cloud Direct Link "1.0"** enables customers to establish a point-to-point connection from their location to the cloud infrastructure terminating at IBM network points of presence (PoPs); it is delivered from within the security scope via a series of Layer 3 switches and routers (XCS/XCR/MBR/BCR/BAS/BCS). Customers are responsible for ordering their single mode fiber cross-connections and are responsible for the configuration of their routers. Customers are provided with an IP allocation for point-to-point connection configuration; additionally, they will be assigned a /24 (254 usable IPs) for their remote hosts.

- **Hardware Firewall** is a Fortigate device which allows customers to protect multiple VLANs using firewall rules, application control, anti-malware, and advanced inspection technologies.

- **Gateway Appliance** is a customer managed offering providing a selection of AT&T Vyatta 5600 vRouters or a Juniper vSRX device which allows the customer to manage their physical and virtual networks for VLAN routing, firewall and VPN management and traffic shaping.

- **IPSec VPN** is a service available to customers to facilitate management of their environment using an encrypted VPN tunnel.

- **Fortigate Security Appliance** is a customer managed, high throughput firewall that provides them with enhanced granular control over their networks.

Storage

- **IBM Cloud File Storage** is a flash-backed NFS-based file storage system that allows customers to increase storage capacity and adjust performance based on workload demands.

- **IBM Cloud Block Storage** is a persistent storage option available for Cloud Virtual and Bare Metal Servers.

- **IBM Cloud Backup** is a recovery system the customer manages, enabling customer to securely backup data between IBM servers in one or more IBM Cloud data centers.

- **IBM Cloud Object Storage (IaaS)** is a cross-regional, unstructured, scalable, and persistent data storage service designed to support exponential data growth.

- **Storage Area Network (SAN)** is architected to attach remote computer storage devices to servers in such a way that, to the operating system, the devices appear as locally attached.

Compute

- **IBM Cloud Bare Metal** is a dedicated physical server. Bare metal servers allow direct access to physical hardware to support high demand and processor-intensive workloads.

- **IBM Cloud Hardware Security Module** is a standalone appliance that provides dedicated single-tenant encryption and key management.

- **SAP-Certified Cloud Infrastructure** is a dedicated physical server purpose-built for SAP workloads.

- **IBM Cloud Virtual Servers** are computing "instances" that are a complete computing environment that includes a full hardware and software stack accessed and controlled over the Internet. The computing resources can be scaled on demand, adding or resizing instances as needed, but without having to purchase physical systems. Public and private virtual nodes are available.

This report does not extend to the workloads (data, files, information) sent by IBM Cloud IaaS customers to the IBM Cloud IaaS system. The integrity and conformity with regulatory requirements of such data are solely the responsibility of the applicable IBM Cloud IaaS customer. Additionally, the boundaries of the system do not extend to business process controls, automated application controls, or key reports.

IBM Cloud IaaS provides services to the Federal government and Department of Defense (DoD) via the FedRAMP and Defense Information Systems Agency (DISA)/DoD programs in two data centers (DAL08 and WDC03). A separate instance of IMS (FedIMS) provides provisioning functionality and infrastructure management. These data center facilities are included within the physical security boundaries of the system, however, other aspects of the services including the FedIMS system and its processes, are not included within the boundaries of the system.

The accompanying description includes only those controls directly impacting IBM Cloud IaaS and customers' hosting environments utilizing IBM Cloud IaaS services detailed in this report. IBM Cloud IaaS also provides enterprise-class tools to help mitigate potential security risks and ensure availability. Tools provided by IBM Cloud IaaS include, but are not limited to, load balancing, intrusion detection and prevention, standard and dedicated hardware firewalls, anti-virus, anti-spyware, anti-malware, VeriSign® and GeoTrust® SSL Certificates. This report does not extend to controls over IBM Cloud IaaS's other services and tools.