Attachment D: GHSC-PSM Service Level Objectives

Chapter 1. PSM MIS Service Level Objectives (SLOs)

1. Overview of PSM MIS SLOs

The following sections summarize the GH Rx SLOs for IBM’s Supply Chain Management Information Subsystem.

1.1. Business Hours

Standard business hours are 8:00 a.m. until 5:00 p.m. Eastern Time Monday through Friday, except federal and IBM holidays, unless stated otherwise. One FIMS business day is equivalent to nine business hours for the purposes of any service level objectives. Beyond standard business hours, 24/7 support will be provided for the PSM MIS to address system outages and emergencies.

1.2. Definitions of Customer and Partner

Customer. The customer for the PSM MIS SLOs is USAID. USAID will directly use the PSM MIS, and these SLOs should provide objectives on up-time and reliability.

Partner. IBM, K+N, and Chemonics are all partners providing service and systems that support the global health supply chain.

1.3. Service Level Objectives

SLOs listed represent targets that Chemonics is confident can be met under normal circumstances. “Availability percentage” is defined as the amount, expressed as a percentage, equal to one year minus the qualifying outage time, divided by one year. The following will be excluded from the calculation of a performance metric (hereafter referred to as “standard exclusions”):

- Scheduled maintenance or a scheduled outage
- Any event outside of control of IBM, including the following examples:
  - Customer’s access to internet from customer location
  - System administration, commands, file transfers performed by customer representatives, including errors associated with improper use of services (such as improper or compromised credentials, user IDs, call sequences, formatting)
  - Other activities customer directs, denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and FIMS’ other suppliers), and other force majeure events
  - Customer’s breach of its material obligations under the agreement, including non-payment of valid invoices
Customer was not available to support PSM MIS' diagnosis and resolution of an incident, including lack of availability or untimely response time of customer to respond to incidents that require its participation for source identification or resolution.

Adverse impacts to PSM MIS service levels arising from actions, or lack of action, taken by partners other than IBM itself.

1.4. Incident Definitions

PSM MIS support practices follow the ITIL® definition of an incident as “An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident.” The PSM MIS Service Desk will classify the incidents with an appropriate severity level based on the severity tables below. The Service Desk will review the incident and problem information provided by the customer and validate the severity level of the problem. The modules referenced in the severity level descriptions below include WebSphere Commerce, Sterling Order Management, iLOG, Cognos, and the Integration Bus. The PSM MIS team may reclassify the severity level of a service ticket. Based upon the severity level, the PSM MIS team will initiate service on a service ticket within the specified response time.

<table>
<thead>
<tr>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Extensive/Widespread</td>
<td>Majority of PSM MIS modules affected (More than 3/4 of individuals, sites, or devices)</td>
</tr>
<tr>
<td>2 - Significant/Large</td>
<td>Multiple PSM MIS modules affected (Between 1/2 and 3/4 of individuals, sites, or devices)</td>
</tr>
<tr>
<td>3 - Moderate/Limited</td>
<td>Single module and/or multiple users affected (Between 1/4 and 1/2 of individuals, sites, or device)</td>
</tr>
<tr>
<td>4 - Minor/Localized</td>
<td>A single user is affected (Less than 1/4 of individuals, sites, or devices)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Critical</td>
<td>Primary business function is stopped with no redundancy or backup. Immediate impact on the global health supply chain’s ability to procure and deliver health commodities exists.</td>
</tr>
<tr>
<td>2 - High</td>
<td>Primary business function is severely degraded or supported by a backup or redundant system. Probable financial impact on the global health supply chain’s ability to procure and deliver health commodities exists.</td>
</tr>
<tr>
<td>3 - Medium</td>
<td>Non-critical business function is stopped or severely degraded. Possible financial impact to the business exists.</td>
</tr>
<tr>
<td>4 - Low</td>
<td>Non-critical business function is degraded. Little or no impact on the global health supply chain’s ability to procure and deliver health commodities exists.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Priority Determination</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.5. Incident Response Time SLOs

"Response time" means the time elapsed between when a service ticket is assigned in the PSM MIS ticketing system, signaling that Chemonics has acknowledged the service incident and severity level, to the point in time when the first activity is posted to the service ticket, indicating Chemonics has activated the response process. The PSM MIS team will update the status of a service ticket in the PSM MIS ticketing system.

<table>
<thead>
<tr>
<th>Incident</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical incident</td>
<td>95% within 30 minutes response time</td>
<td></td>
</tr>
<tr>
<td>High incident</td>
<td>95% within 4 business hours response time</td>
<td>Standard</td>
</tr>
<tr>
<td>Medium</td>
<td>95% within 9 business hours response time</td>
<td>(see 1.3)</td>
</tr>
<tr>
<td>Low incident</td>
<td>95% within 18 business hours response time</td>
<td></td>
</tr>
</tbody>
</table>

1.6. Maintenance Windows

The monthly PSM MIS standard maintenance windows are to be agreed upon.

2. Cloud Services – Cloud Infrastructure as a Service (IaaS)

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server availability</td>
<td>99.5%</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td>Network availability</td>
<td>99.5%</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td>Virtual machine provisioning requests for existing environments</td>
<td>99% fulfilled within 18 business hours. Measured from time ticket was assigned to PSM MIS VM team.</td>
<td>Standard exclusions (see 1.3) and scheduled VM/environment changes that are to occur at a future time or during transition periods</td>
</tr>
<tr>
<td>Virtual machine/virtual environment resource requests for existing environments</td>
<td>99% fulfilled within 18 business hours. Measured from time ticket was assigned to PSM MIS VM team.</td>
<td></td>
</tr>
</tbody>
</table>

3. Hosting Services

3.1. Cloud Storage and Storage Management
### 3.2. Backup Management

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup infrastructure</td>
<td>99%</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td>Recovery point objective (RPO)*</td>
<td>24 hours</td>
<td>N/A</td>
</tr>
<tr>
<td>Recovery time objective (RTO)**</td>
<td>99% in 18 business hours</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td>Data recovery***</td>
<td>48 hours for targeted data recovery (for previous 7 days)</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td></td>
<td>5 days for targeted data recovery (for greater than previous 7 days)</td>
<td></td>
</tr>
</tbody>
</table>

* Recovery Point Objective is applicable for cases of data related failure during operation of the system. PSM MIS operational processes are designed to bring the subsystem’s data back to a state that is equivalent to a point in time within the stated time period immediately preceding the failure event.

** Should any server’s data set exceed the design parameter of one (1) TB, then both the RPO and RTO SLOs will need to be revised under a project change request to address adjustment of data backup and restore strategy, provisions and practices.

*** Data recovery requests are subject to evaluation by the PSM MIS team to determine the potential for impact to the operational data that may be present in PSM MIS at any time, and to the set of maintained data backups. For purposes of measurement, the elapsed time to be measured for the performance of data recovery does not commence until the SCIMS team has evaluated a specific data recovery request and indicated its acceptance for fulfillment within the PSM MIS service desk application. The PSM MIS team will arrive at determination within 48 hours of the receipt of the request for targeted data recovery.

### 3.3. Remote Access VPN

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN authentication system availability</td>
<td>99.5%</td>
<td>Standard exclusions (see 1.3) and issues with</td>
</tr>
</tbody>
</table>
VPN account creation, modification, or removal time | 95% in 18 business hours | customer-provided VPN concentrators

Standard exclusions (see 1.3), account creation during transition, and adds/modifications/removals pre-scheduled to occur at a specific time

### 3.4. Systems Administration

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Administrator account unlock/ password reset</td>
<td>99% completed within 4.5 business hours</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td>OS Administrator account creation</td>
<td>99% completed within 9 business hours</td>
<td></td>
</tr>
<tr>
<td>Server availability (percent of time the server and OS are available in production environment)</td>
<td>99.5%</td>
<td>Standard exclusions (see 1.3) and outages not attributed to OS</td>
</tr>
</tbody>
</table>

### 3.5. System Monitoring

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server monitoring infrastructure availability (%)</td>
<td>99.5%</td>
<td>Standard exclusions (see 1.3) and scheduled changes</td>
</tr>
<tr>
<td>Network monitoring infrastructure availability (%)</td>
<td>99.5%</td>
<td></td>
</tr>
</tbody>
</table>

### 3.6. Service Desk

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticketing system password reset</td>
<td>90% complete within 3 business hours</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td>Ticketing system re-enable disabled account</td>
<td>90% complete within 3 business hours</td>
<td></td>
</tr>
</tbody>
</table>

### 3.7. Infrastructure Availability

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of PSM MIS infrastructure</td>
<td>99.5%</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
</tbody>
</table>
4. Security Services

4.1. Security Governance Support

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-time delivery of standard quarterly</td>
<td>90% within 27 business hours of due date over contract period</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td>monitoring reports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-time resolution of POA&amp;M items</td>
<td>90%</td>
<td>Standard exclusions (see 1.3) and items for which the resolution date was not agreed to in advance by IBM</td>
</tr>
</tbody>
</table>

4.2. Security Engineering

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-priority firewall access list change request completion</td>
<td>98% of requests completed within 9 business hours</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td>Medium-priority firewall access list change request completion</td>
<td>98% of requests completed within 18 business hours</td>
<td>Standard exclusions (see 1.3) and scheduled wait times</td>
</tr>
<tr>
<td>Low-priority firewall access list change request completion</td>
<td>98% of requests completed within 36 business hours</td>
<td></td>
</tr>
</tbody>
</table>

4.3. Security Operations

<table>
<thead>
<tr>
<th>Measure</th>
<th>Target</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM notification to Chemonics of Critical security incident</td>
<td>95% within 15 minutes of identification* of confirmed Critical incident</td>
<td>Standard exclusions (see 1.3)</td>
</tr>
<tr>
<td>Customer requested scans **</td>
<td>98% of requests completed within 24 hours</td>
<td></td>
</tr>
</tbody>
</table>

* Identification is defined as when the incident is verified by IBM as a valid Critical security incident.

** Customer may request vulnerability scans and uncorrelated reviews of firewall and server logs.

5. Abbreviations and Acronyms

AD active directory

ARS Action Request System
ATO authorization to operate
COOP Continuity of Operations Plan
ESM Enterprise System Monitoring
FDC IBM Federal Data Center
FIMS Federal Infrastructure Managed Services
GB gigabyte
GPO group policy objects
IaaS Infrastructure as a Service
ICR internal control review
ISSO information system security officer
ITCS IBM Technical Configuration Standard
ITIL® Information Technology Infrastructure Library
ITM IBM Tivoli Monitoring
ITNM IBM Tivoli Network manager
NAS network attached storage
NIDS Network Intrusion Detection System
NIST National Institute of Standards and Technology
OS operating system
POA&M Plan of Actions and Milestones
POC point of contact
RPO recovery point objective
RTO recovery time objective
SAN storage area network
PSM MIS Procurement and Supply Management Information Subsystem
SIEM Security Information and Event Management
SLO service level objective
SOC Security Operations Center
TEPS Tivoli Enterprise Portal Server
TIP Tivoli Integrated Portal
VLAN virtual local area network
VM virtual machine
VPN virtual private network
Chapter 2. Overview of the Cloud Service hosting PSM MIS Applications

This Cloud Service description provides the description of available services options that Chemonics will provide for PSM MIS.

1. Definitions

The following additional definitions apply for the Services.

Authorized point(s) of contact. a person(s) Customer assigns who can oversee the use of the Cloud Service for PSM MIS and who has the authority to act on Customer’s behalf regarding the Cloud Service, including ordering Cloud Service, enabling and disabling the Cloud Service.

Cloud base infrastructure. the components of the Cloud Service computing infrastructure that are potentially shared by all Instances and Customers, including physical servers, network, storage, and security components and cloud management components.

Customer. the Government Agency identified in the Customer information section of this Agreement and its End Users. The term Customer is a broad term and includes not only the reference to a Government Agency but all the specific employees from that Agency involved in use of the Cloud Service (i.e., Account Administrator, End Users).

End user. Those who access or use the Services using user account identification to access the Cloud Service.

Normal business hours. 8 a.m. to 5 p.m. Eastern Time Monday through Friday, excluding federal holidays, unless otherwise stated. Beyond normal business hours, 24/7 support will be provided for the Cloud Service to address Critical incidents.

Response time. The time elapsed between when a service ticket is assigned in the PSM MIS ticketing system signaling Chemonics has acknowledged the service incident and severity level, to the point in time when the first activity is posted to the service ticket indicating Chemonics’ activation of the resolution process. Chemonics will update status of a service ticket in the ticketing system.

2. Description of Services

Delivered by multiple FISMA-compliant, green data centers across the United States employing standards-based processes (ITIL and NIST) and best practices, these Services are designed to provide the Customer the ability to utilize virtual computing resources to support the Customer’s computing, development, and testing needs. Security services provide the Customer with assistance engineering, monitoring, and maintaining infrastructure to meet FISMA standards and achieve U.S. Department of Defense compliance.

The Cloud Service architecture is consistent with the IBM reference architecture for cloud and supports hosting services as well as security services. The Cloud Service adheres to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145
definition for cloud of a "model for enabling convenient, on-demand network access to a shared pool of configuration computing resources, such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction."

3. Cloud Services

3.1. Cloud Infrastructure as a Service (IaaS)

3.1.1. Description

Cloud IaaS provides compute resources for client virtual environments. Configurations are available with Customer-specified virtual CPU, memory, and OS instances, such as those depicted in the examples in this subsection. This allows for elasticity of demand so that the Customer pays only for allocated cloud resources. Additional resources can be purchased on demand and de-provisioned when no longer required. Both Linux® and Windows® operating systems are supported. Charges are based on the allocated number of vCPU GHz, gigabytes (GB) of RAM, and OS instances.

The Cloud Service will provide up to 10,000 GB/month of network bandwidth for inbound and outbound data transfers to cloud instances. Additional bandwidth may be requested through project change control.

<table>
<thead>
<tr>
<th>Example-Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Small Resource Pool</strong></td>
</tr>
<tr>
<td>50GHz vCPU</td>
</tr>
<tr>
<td>30GB RAM</td>
</tr>
<tr>
<td>10 OS instances</td>
</tr>
</tbody>
</table>

The following Guest OS instances are supported:

Red Hat® Enterprise Linux®

3.1.2. IBM Responsibilities

a. Provision Customer virtual environment compute resources and/or provide self-service portal

b. Provision VLANs and associated VM networks

c. Patch OS

d. Maintain & support cloud infrastructure hardware

3.1.3. Chemonics Responsibilities
a. Obtain internet access or other network connectivity necessary for use of the Services.

b. Manage Services usage, coordinate, educate, and be responsible for the activities of all End Users and their compliance with the terms of the Agreement.

3.2. Base Configuration

PSM MIS Virtual Machines are identified in the Infrastructure and Software as a Service (IaaS and SaaS) Commercial Terms for SoftLayer Services.

3.2.1. Additional Memory

Additional memory blocks are available to a VM if required for the service.

3.2.2. Additional Storage

Additional cloud storage can be added to the Cloud instances. Common amounts are 250GB, 500GB, and 1 terabyte (TB).

4. Additional Services

4.2. Backup Management

4.2.1. Description

The Backup Management Services provides backup and restoration of Customer data. This includes configuration of the backup storage (scheduling, encryption), as well as management of sequential media and coordination of offsite storage. Charges are based on the disk storage for the backup. Additional backup disk storage may be addressed through project change control.

Backup Browser based User Interface

Client has two major customers that send orders. System must support multi-client tenancy on a single instance Implementation:

By default, backups are performed, held, and migrated off-site on the following schedule. Changes to this schedule or data retention outside of the standard policy may incur additional costs.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Backup Type</th>
<th>Offsite Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>Incremental</td>
<td>Moved offsite daily</td>
</tr>
<tr>
<td>Weekly</td>
<td>Full</td>
<td>Moved offsite weekly, one (1) monthly cycles are retained offsite</td>
</tr>
</tbody>
</table>
4.2.2. IBM Responsibilities

a. Configure/manage backup schedules

b. Manage capacity of disk media

c. Manage backup infrastructure

d. Monitor backup processes

e. Provide logistical support for off-site disk media

f. Add, modify, and remove backups

4.2.3. Chemonics Responsibilities

a. Cost of disk media

b. Define retention requirements if outside of standard offering

4.4. Systems Administration

4.4.1. Description

The System Administration Service provides ongoing support of Customer servers up to and including the Operating System (OS). IBM can administer virtual and physical systems to provide a foundation upon which the PSM MIS applications can be managed. This includes keeping the OS up to date and patched from vulnerabilities as well as basic system configuration. Charges are based on the production and non-production environments.

Systems Administration includes the following:

a. OS patching (including OS vulnerability remediation)

b. Administration of local accounts and groups

c. Administration of basic Lightweight Directory Authentication Protocol (LDAP) services (objects, domain controllers, user accounts, Group Policy Objects)

d. Support of systems management agents such as backup and monitoring
e. Basic configuration of local disks and virtual machines

Supported operating systems:

Red Hat® Enterprise Linux®

4.4.2. IBM Responsibilities

a. Provide administration of OS, accounts and groups, Present storage to OS

b. Resolve any and all technical issues with the service related to OS, and management agents

c. Respond to monitored system incidents

d. Respond to virtual machine (VM) related incidents

e. Respond to network-related incidents

4.4.3. Chemonics Responsibilities

Provide a supported remote access client device (such as a laptop or desktop computer) for remote access to PSM MIS. End User oriented VPN access is not included, but should such requirement arise then it may be addressed through project change control.

4.5. System Monitoring (SM)

4.5.1. Description

SM provides the core functions of availability, performance, and event management. SM includes 24x7x365 automated monitoring of networks, systems and critical business services with real-time alerting, ticketing, notification, and reporting capabilities.

Event Management supports analysis of events from event sources and supports incident ticketing. Industry best practices are used to provide aggregated views and reporting capabilities through a web-based portal as the Customer’s single point of view. SM charges are based on the number of virtual machines registered in the monitoring system, actively monitored.

SM includes:

a. 24x7x365 automated monitoring of Linux systems monitoring
b. Network and Server up/down monitoring

c. Cloud Service portal pages, views and access support for incident display

d. Availability and performance reporting

e. Incident ticketing and notification

4.5.2. IBM Responsibilities

a. Server monitoring support

b. Setup and support monitoring situations to include minor changes to thresholds, occurrences, and timing

c. Setup and support user access for Cloud Service portal

d. Network Monitoring Support

e. Event Management Support

f. Handle adds, modifications, and removals of user accounts on Cloud Service portal

4.6. Security Engineering

4.6.1. Description

The Security Engineering Service provides management and administration of security systems, security devices, and security zones. The Security Engineering offering covers administration of system controls that may be necessary to meet compliance requirements. Included is management and administration of:

a. Dedicated security devices and software

b. Physical and virtual firewalls

c. Intrusion detection systems

d. Security zones

Charges are based on the number of dedicated security systems and devices (e.g., physical and virtual firewalls, VPN, network intrusion detection systems (NIDS), servers, etc.), and the number of security zones.
4.6.2. IBM Responsibilities

a. Implement changes to managed systems following standard ITIL-aligned change control processes

b. Resolve technical issues associated with PSM MIS

c. Respond to alerts associated with PSM MIS

d. Perform standard maintenance, patching, and upgrades to managed cloud infrastructure per ITIL-aligned standard processes

e. Resolve identified security vulnerabilities as allowed by Customer technical requirements

4.7. Security Operations (SO)

4.7.1. Description

The goal of the Security Operations is to be the Customer’s central resource for PSM MIS security monitoring and notification, as well as threat prevention. The SO service includes monitoring focused on identifying possible security incidents, logging information about them, attempting to stop them, and reporting them to security administrators. Chemonics will also use SO reporting to identify problems with security policies, document threats, and deter security policy violations.

The SO provides 24x7x365 monitoring and tuning for intrusion prevention as well as security and vulnerability scanning, system log monitoring, security event and security incident escalation, security incident response support services, and standard reporting. SO Service charges are based on labor for monitoring devices including firewalls, intrusion detection and prevention systems, servers, and network devices.

Included in the SO offering are the following:

a. Monitoring and Response
   - 24x7x365 monitoring and analysis of events generated by the systems logs and monitoring toolsets
   - Support for monitoring of Linux hosts and log monitoring and scanning of network devices
   - Escalation of suspected or actual security incidents to Customer contact
   - Support for response to security incidents

b. Scanning
   - Analysis vulnerability scans of the monitored items
• Up to an estimated twenty (20) hours per month of technical support for vulnerability scan analysis

c. Systems
• Scanning managed and administered by IBM
• Log collection and analysis
• Intrusion detection and prevention monitoring

4.7.2. IBM Responsibilities

a. Administer the Cloud Service hosting PSM MIS applications.
b. Provide appropriate staff for 24x7x365 monitoring and analysis of monitored cloud infrastructure events
c. Complete and analyze vulnerability scans
d. Monitor and analyze events for potential security incidents
e. Escalate security incidents to appropriate Customer contacts

4.8. Dedicated Firewall

4.8.1. Description

The Dedicated Firewall provides a firewall that is managed by IBM and dedicated to a single Customer inside of the Cloud Service. The currently planned initial firewalls are:

• Fortinet Fortigate Security Appliance - stateful firewall, SSL VPN, intrusion detection/prevention, and
• Brocade Vyatta vRouter - stateful firewall, IPsec VPN, dynamic routing, NAT/DHCP, Denial of Service (DOS) attack mitigation.

4.8.2. IBM Responsibilities

a. Implement changes to managed systems following standard ITIL-aligned change control processes
b. Resolve technical issues associated with managed cloud infrastructure
c. Respond to alerts associated with managed cloud infrastructure
d. Perform standard maintenance, patching, and upgrades to managed cloud infrastructure per ITIL-aligned standard processes
e. Resolve identified security vulnerabilities as allowed by Customer technical requirements

4.9. Service Component Operating System

Each Instance is provisioned and pre-loaded with an Operating System (Red Hat Enterprise Linux). Charges for the operating system are included as part of the Instance monthly charge. Use of the Operating System Image is provided in accordance with Use and Access of the SoftLayer Services commercial terms.

Red Hat Enterprise Linux software is licensed from Red Hat to Customer under the Red Hat Enterprise Agreement found at http://www.redhat.com/licenses/.

5. Security

5.1. IBM Security Responsibilities

IBM will provide the following for the Cloud Base Infrastructure only:

a. Physical access security for Data Centers, which may include physical alarm systems, video surveillance, and motion detectors in applicable areas.

b. Cloud Base Infrastructure auditing and monitoring of internal privileged users. All users utilize unique identities and credentials. Infrastructure operated and managed by Chemonics uses IBM’s internal data center security policy.

d. Intrusion prevention system/intrusion detection system (IPS/IDS) monitoring of network traffic to and from Cloud Base Infrastructure to help detect incoming attacks, or malicious behaviors. Chemonics reserves the right to suspend, block, or delete any Instances that Chemonics thinks are being used in a malicious manner and to block any malicious traffic.

e. Weekly vulnerability scanning of the cloud base only.

Customer agrees that IBM shall have no liability for any security-related services or advice that IBM may voluntarily provide.

5.2. Chemonics Security Responsibilities

Customer will:

a. Participate in management and security of Instances once provisioned for Customer

b. Not access or attempt to access IBM’s secure internal network or the resources or information of other IBM Customers

d. Notify IBM when Customer is performing any technical security integrity review, penetration test, or vulnerability scan:

1) Only test, scan, or review the Customer IP addresses that are part of the Services

2) Only test, scan, or review the Customer Instances and not shared portions of the cloud
3) Maintain record of the date and time of any review, penetration test, or vulnerability scan and provide to IBM upon request
4) Not perform such reviews more than once per calendar quarter
5) Not perform or simulate denial-of-service attacks

e. Manage End User credentials for access to Instances and any Services

h. Use secure protocols and mechanisms for accessing Instances, such as the VPN service

i. Use Instances in accordance with the Acceptable Use Policy which includes not using in a malicious manner, including but not limited to botnet or malware hosting