CBEYOND COMMUNICATIONS LLC

INDEPENDENT PRACTITIONER’S TRUST SERVICES REPORT
FOR THE TOTALCLOUD DATA CENTER AND TOTALCLOUD
FOUNDATION SYSTEM

FOR THE PERIOD OF OCTOBER 1, 2013, TO DECEMBER 31, 2013

Attestation and Compliance Services

Proprietary & Confidential
Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.
INDEPENDENT PRACTITIONER’S TRUST SERVICES REPORT

To the Management of Cbeyond Communications LLC:

We have examined management’s assertion that during the period October 1, 2013, to December 31, 2013, Cbeyond Communications LLC ("Cbeyond") maintained effective controls over the TotalCloud Data Center and TotalCloud Foundation system for the security and availability principles set forth in TSP section 100A, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (applicable trust services criteria), to provide reasonable assurance that

- the system was protected against unauthorized access (both physical and logical); and
- the system was available for operation and use, as committed or agreed.

Cbeyond’s management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management’s description of the TotalCloud Data Center and TotalCloud Foundation system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Cbeyond’s relevant controls over the security and availability of the TotalCloud Data Center and TotalCloud Foundation system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, Cbeyond’s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, management’s assertion referred to above is fairly stated, in all material respects, based on the AICPA and CICA applicable trust services criteria.

Cbeyond’s use of the SOC 3SM SysTrust for Service Organizations seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Tampa, Florida
March 24, 2014
MANAGEMENT’S ASSERTION

March 24, 2014

During the period October 1, 2013, through December 31, 2013, Cbeyond Communications LLC ("Cbeyond") maintained effective controls over the TotalCloud Data Center and TotalCloud Foundation system for the security and availability principles set forth in TSP section 100A, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (applicable trust services criteria), to provide reasonable assurance that:

- the platform was protected against unauthorized access (both physical and logical); and
- the platform was available for operation and use, as committed or agreed;

The attached system description identifies the aspects of the TotalCloud Data Center and TotalCloud Foundation system covered by the assertion.

Tim Myers
Senior Vice President, Chief Information Officer
SYSTEM DESCRIPTION OF THE TOTALCLOUD DATA CENTER AND TOTALCLOUD FOUNDATION SYSTEM

Company Background

Cbeyond Communications LLC, a publicly traded company, provides a suite of cloud virtual and physical hosting services, and is headquartered in Atlanta, Georgia. Founded in 1999, Cbeyond provides small- and medium-sized businesses with managed and unmanaged technology services. Cbeyond is comprised of approximately 2,100 employees and utilizes data centers in Louisville, Kentucky, and Norcross, Georgia.

Description of Services Provided

Cbeyond’s TotalCloud Data Center and TotalCloud Foundation services are virtual hosting service options that clients can select based upon their business, storage and managed security needs. These services include multiple service level options and configurable selections within each customer’s environment for memory, storage, networking and security, 24/7 proactive monitoring, daily backup and support of the cloud infrastructure and the client’s environment. Depending on the hosting service option selected, Cbeyond performs a variety of provisioning, monitoring and/or management responsibilities for their clients. The hosting options and brief summary of Cbeyond’s responsibilities for each are as follows:

TotalCloud Data Center (TCDC)

The Cbeyond TCDC platform is a fully-managed private virtualized cloud environment built upon enterprise-class Cisco UCS servers, EMC VNX Storage Area Network (SAN) storage, Cisco Nexus switching, and VMware virtualization software. This platform provides integrated security and scalability to handle customers’ production applications. Cbeyond provisions, monitors, and manages the following:

- Virtualization/Hypervisor - VMware
- SAN storage
- Private network
- Operating system (OS) (Guest)
- OS – Windows
- Private virtual firewall
- Antivirus
- Backups
- Patching

TotalCloud Foundation (TC Foundation)

The Cbeyond TC Foundation solution provides the same type of deployment options as the TCDC solution. The TC Foundation solution differs from the TCDC solution in that management of the client environment is performed by the client rather than Cbeyond. Cbeyond provisions, monitors, and manages the following:

- Virtualization/Hypervisor - VMware
- SAN storage
- Private network
- Private virtual firewall
- Guest management and Other services are optional
Components of TotalCloud Services

The overall TotalCloud services described above are comprised of varying components that Cbeyond incorporates for the purpose of providing the clients’ selected services. Below is a brief description of the components utilized across the varying TotalCloud services options.

Virtual Server

Cbeyond provisions and configures virtual servers with the specified sizing along with an OS. Each virtual server is a portion of the larger pool of pre-installed and integrated compute, storage, network and security infrastructure resources. Customers have access to the virtual server. Each virtual server will reside within a physical group of server clusters that are networked together into a resource group with high availability and automated resource management.

OS Management

Cbeyond’s TCDC services include OS management for the day-to-day support of the virtual server/guest OS as identified in the schedule. As part of this service, customers’ virtual servers are installed with a Microsoft OS, patched, and managed/monitored on an ongoing basis. The initial provisioning of the OS creates an administrator account with a randomly generated password. Customers are provided this login information and are responsible for changing upon their first login.

Network Configuration

Customers utilizing the private option receive one private virtual local area network (LAN) as part of the TCDC service and have the option of purchasing dedicated private virtual LANs for an additional charge. The service includes network configuration and Internet Protocol (IP) allocations per each service profile. The network topology is pre-defined for each service profile and the provisioning of this design is automated during the build process.

Virtual Firewall Services

The TotalCloud managed firewall is a bundled service, which is included for customers as part of their TCDC Private bundle and/or TC Foundation bundle. Cbeyond’s managed firewall provides for the day-to-day support of redundant high-availability firewall and security services.

Monitoring

Cbeyond’s TCDC services include monitoring of customer infrastructure elements as well the shared infrastructure used to support the customers. This monitoring service detects system level events that indicate immediate or potential failures. Each OS deployed on a TCDC platform includes a Cbeyond monitoring agent. This agent monitors the central processing unit (CPU) and memory utilization as noted in the OS management section.

Infrastructure

The in-scope infrastructure consists of virtual machine hosts, network devices and supporting tools as shown in the table below:

<table>
<thead>
<tr>
<th>Supporting Systems Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Name</strong></td>
</tr>
<tr>
<td>OS</td>
</tr>
<tr>
<td>Firewalls</td>
</tr>
</tbody>
</table>
### Supporting Systems Infrastructure

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Description</th>
<th>OS/ Platform</th>
<th>Physical Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Servers</td>
<td>Automated backup system software and network of servers that provide backup and recovery for subscribing customers.</td>
<td>EMC VNX SAN</td>
<td>Louisville Data Center</td>
</tr>
<tr>
<td>Virtual hypervisor</td>
<td>VMware vCenter server that provides authentication and restricts access to customer virtual environments.</td>
<td>VMware vSphere</td>
<td>Louisville Data Center</td>
</tr>
<tr>
<td>VMware hosts</td>
<td>VMware ESX hosts for running client virtual machines</td>
<td>VMware ESX</td>
<td>Louisville Data Center</td>
</tr>
<tr>
<td>Routers and Switches</td>
<td>Routers and switches are utilized to route network traffic.</td>
<td>Cisco</td>
<td>Louisville Data Center</td>
</tr>
</tbody>
</table>

### Software

The following applications are utilized to perform the TCDC and TC Foundation services:

- Biometric, physical key and badge/key fob access systems – Physical access control systems are linked to uniquely identifiable characteristics and personal information about the user.
- Virtualization software – Virtual machine and hypervisor management software are utilized to create, modify and delete virtual machines.
- Support applications – Automated tools are utilized to allow Cbeyond TotalCloud personnel to access customer systems remotely to provide support services.
- Backup solution – Veeam backup is utilized to schedule and execute backup jobs. These jobs back up customer data to a SAN.
- Antivirus – Symantec EndPoint Protection antivirus software is used to manage the central antivirus server.
- Intrusion Prevention System (IPS) – Hewlett Packard TippingPoint IPS is utilized to monitor the network traffic and alert operations personnel via onscreen and e-mail alert notifications when any type of malicious traffic is detected.

### People

Cbeyond utilizes the specific functional areas of operations within the TotalCloud services including the following:

- Executive management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives
- IT department – manages, monitors, and supports users’ information and systems from unauthorized access and use while maintaining integrity and availability
- Support operations center (SOC) – division of IT department responsible for monitoring and incident response
- Finance – performs financial management and accounting functions
- Sales and marketing – performs sales, marketing, and business development functions
- Sales and support engineering – pre and post-sales engineering including customer support
- Infrastructure engineering – oversees managed infrastructure and deployment
- Quality assurance – performs all testing and quality assurance functions
- Security – oversees security and compliance activities for the company as well as the services

Procedures

Cbeyond has implemented procedures and control activities to help achieve its business objectives. These controls are implemented with a risk-based approach. Once the likelihood and impact of relevant risks have been analyzed, procedures and controls are designed and implemented to meet the overall business objectives of the organization.

Physical Security

All TotalCloud infrastructure is hosted within the Louisville data center. Access to the building and office space is granted through proximity badges, and the badge access system is administered by authorized personnel. Once inside the building, a biometric scanner and badge must be used to enter the data center housing TotalCloud infrastructure. Visitors to the data center must provide a government issued photo ID, sign a log book and are assigned a visitor badge. Visitor badges have no electronic access within the building, and as such, visitors must be escorted at all times while on site by authorized personnel. Data center ingress and egress points as well as sensitive sections of the building are under camera surveillance 24 hours a day.

Environmental Security

The data center is equipped with fueled electric power generators and redundant uninterruptable power supply (UPS) units to provide continuous power in the event of an outage. The generators and UPS systems are inspected for maintenance by a third party on a quarterly basis. Management retains the inspection reports for maintenance. The data center is additionally equipped with fire and smoke detectors which trigger visible and audible alarms in the event of a fire. Dry-pipe water sprinklers are present at each location along with hand-held fire extinguishers to allow for prompt suppression of fire. Management contracts with third party specialists to inspect the fire detection and suppression systems on a quarterly basis, and the inspection report is retained as evidence of completion.

The data center is equipped with multiple air-conditioning units to regulate temperature and humidity. Management contracts with third party specialists to inspect the air-conditioning units on a quarterly basis and the inspection report is retained as evidence of completion. The data center is equipped with water detection devices to detect and mitigate water damage in the event of a flood or water leak. These water detection units are placed under the raised floor.

Logical Access

Users may connect to the Cbeyond management network in one of two ways:

1) Directly – users may connect directly to the network by being physically present at the Louisville data center.

2) Remotely – users must authenticate to the corporate network domain and subsequently authenticate to the management network via a jump host, using two-factor authentication.

Within the management network, several tools allow access to customers' virtual machines. Cbeyond provisions each customer OS within the virtual environment, but customers change the password upon first access to the system. Customer support OS user accounts and passwords are stored in the Spooler Password Page application on the management network. If a Cbeyond administrative user has access to the Spooler Password Page application, along with the Net IQ remote access application used to remotely view the customers virtual instance of the OS, the Cbeyond administrative user can use the customer support user account and password to access the customer virtual server. Additionally, the vCenter hypervisor management application allows privileged users to create, modify and delete virtual machines.

Access to the above applications is controlled strictly through Active Directory groups. In order to be provisioned access to these systems, a user must submit a formal request and gain approval from infrastructure engineering management. Additionally, upon termination, the human resources department initiates an automated process to
have the employee’s account removed from Cbeyond systems. This process generates a series of tickets which are routed to the corresponding system administrators to ensure that access is removed or disabled.

Users of supporting tools and infrastructure are authenticated against Active Directory. As a result, password parameters are controlled at the network domain level by a group policy.

Change Management

Cbeyond customers may request infrastructure or other changes via a customer service web portal. Cbeyond SOC personnel execute these changes per customer request and track the changes within tickets in the portal. These types of changes are considered pre-approved as Cbeyond must perform them to comply with customer agreements.

Internally requested changes affecting customer systems, such as patches, firewall changes, and provisioning of memory, are requested and tracked within the ServiceNow ticketing system. These types of changes require approval from a manager as well as documentation of a backout plan and any necessary regression testing. As no application source code exists, testing is generally not required for TCDC and TC Foundation changes.

All emergency changes, whether requested by the customer or internal personnel, follow the same process as standard changes. These changes may undergo a shorter change management cycle, but approval and documentation within the ticketing system must be established prior to implementation of the change.

Security Monitoring

A Hewlett Packard TippingPoint IPS is used to monitor the overall network security of system housed within the Louisville data center. This IPS is continuously monitored by SOC personnel, and daily reports of high-severity items are sent to network security personnel. Incident response procedures are in place in the event that a breach of system security occurs. The security incident is logged in a ticketing system, and essential personnel are notified to help resolve the issue. The incident response policies and procedures are tested and modified as necessary on an annual basis. Additionally, security violations can be reported to a third party whistleblower hotline, which sends a ticket for tracking to key security personnel.

Additional monitoring of the security and availability of customer systems occurs at a higher level on a quarterly basis in the form of formal risk assessments. Management examines the security and availability risks that impact the business of the company as part of quarterly comprehensive risk assessment. Additional periodic assessments take place in the form of quarterly audit meetings and weekly security meetings.

Antivirus

Cbeyond utilizes Symantec Endpoint Protection on a central antivirus server to download and deploy antivirus definitions to production virtual machines. The antivirus software is configured to update virus definitions on a daily basis and perform virus scans on a weekly basis.

Backup and Recovery

A Veeam backup solution is utilized to back up data on customer machines to an EMC VNX SAN to allow customer data to be striped across an array of disks. Backups are periodically restored as part of normal business operations. Off-site replication of data and other disaster recovery processes are not included as part of Cbeyond’s suite of TotalCloud services. Cbeyond customers are responsible for ensuring that a business continuity plan is in place in the event of a disaster.

Data

Various primary and supporting systems infrastructure data are analyzed and used to support Cbeyond’s TCDC and TC Foundation systems. Specific data includes, but is not limited to, the following:

- Activity logs of badge card and finger / hand print access attempts, including denied access attempts from the badge card access system and the biometric recognition access system
- Activity logs from the corporate firewalls
- Alert notifications of failed and successful data backups received from automated backup system
- Incidents and issue reports documented within the automated ticketing system

Customer data is not included within the scope of the TCDC or TC Foundation systems.

**Significant Changes During the Review Period**

No relevant changes to the TCDC or TC Foundation systems occurred during the review period.

**System Boundaries**

The boundaries of the system are limited to the TCDC and TC Foundation services provided by Cbeyond. The system does not include customer end-point data sources that send data to Cbeyond. It also does not include the corporate application systems, the individual customer virtual environments, or network connections outside of the Cbeyond data center.

**Trust Services Criteria Not Applicable to the In-Scope System**

The Trust Services criteria presented below are not applicable to the TotalCloud Data Center and TotalCloud Foundation systems within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted applicable trust services criteria. The following table presents the trust services criteria that are not applicable for the TotalCloud Data Center and TotalCloud Foundation systems at Cbeyond.

<table>
<thead>
<tr>
<th>Criteria #</th>
<th>Reason for Omitted Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP.1.2.n</td>
<td>The in-scope Cbeyond system does not provide for the sharing of information related to TCDC and TC Foundation services with third parties.</td>
</tr>
<tr>
<td>AP.3.3</td>
<td>This criterion is partially applicable. Cbeyond does not provide off-site media storage or disaster recovery services as part of the TCDC and TC Foundation services.</td>
</tr>
</tbody>
</table>