Ernst & Young LLP
Ernst & Young Tower
One Renaissance Square
Suite 2300
2 North Central Avenue
Phoenix, AZ 85004

Tel: +1 602 322 3000
Fax: +1 602 322 3023
ey.com

Report of Independent Accountants

Management of NTT America, Inc.

Approach

We have examined management's assertion that NTT America, Inc. (NTT America) maintained effective controls to provide reasonable assurance that:

- NTT America's Colocation, Managed Web Hosting and Hybrid Cloud Services System was protected against unauthorized access, use, or modification to achieve NTT America's commitments and system requirements
- NTT America's Colocation, Managed Web Hosting and Hybrid Cloud Services System was available for operation and use to achieve NTT America's commitments and system requirements

during the period October 1, 2017 through September 30, 2018 based on the criteria for security and availability in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of NTT America's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of NTT America's relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating NTT America's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security and availability are achieved.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Building a better working world

Opinion

In our opinion, NTT America's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security and availability.

Ernst & Young LLP

December 7, 2018

Management's Assertion Regarding the Effectiveness of Its Controls Over the NTT America, Inc. Colocation, Managed Web Hosting and Hybrid Cloud Services System Based on the Trust Services Principles and Criteria for Security and Availability

December 7, 2018

We, as management of NTT America, Inc. (NTT America), are responsible for designing, implementing and maintaining effective controls over the NTT America Inc. Colocation, Managed Web Hosting and Hybrid Cloud Services System (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period October 1, 2017 to September 30, 2018, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security and availability (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that:

- the System was protected against unauthorized access, use or modification to achieve NTT America's commitments and system requirements
- the System was available for operation and use to achieve NTT America's commitments and system requirements based on the Control Criteria.

based on the Control Criteria.

Our attached description of the boundaries of the Colocation, Managed Web Hosting and Hybrid Cloud Services System identifies the aspects of the Colocation, Managed Web Hosting and Hybrid Cloud Services System covered by our assertion.

Very truly yours,

NTT America, Inc.

NTT Communications Group
NTT America, Inc.

Description of NTT America, Inc.'s Colocation, Managed Web Hosting and Hybrid Cloud Services System Company Overview

NTT America is North America's natural telecommunications gateway to the Asia-Pacific region, with strong capabilities in the U.S. market. NTT America is the U.S. subsidiary of NTT Communications Corporation (NTT Communications), the global hosting, data and IP services arm of the Fortune Global 500 telecom leader, Nippon Telegraph & Telephone Corporation (NTT). NTT America provides cloud and hosting solutions, network and IP networking for global enterprises and service providers.

NTT America's Global Enterprise Solutions product portfolio and service platforms include the following:

- Public, Private and Hybrid Cloud
- Dedicated Hosting
- Load Balancing
- Monitoring Services
- Professional Services
- Enterprise Customer Care
- Colocation
- Virtualization Services
- Managed Security
- Managed Storage
- Smart Content Delivery

Data Center Services offered through NTT America provide secure facilities to host a variety of web-enabled solutions in an environment engineered for reliable operations and dedicated high-speed internet connections. See www.us.ntt.com for more information.

NTT Communications Global IP Network (GIN Network)

Each Data Center is connected to the NTT Communications Global IP Network (the GIN network). The GIN network was designed and built by NTT Communications engineers using the latest technologies to provide fast, efficient and accurate data transport. The GIN network is designed with numerous direct paths, routing options and private peering points.

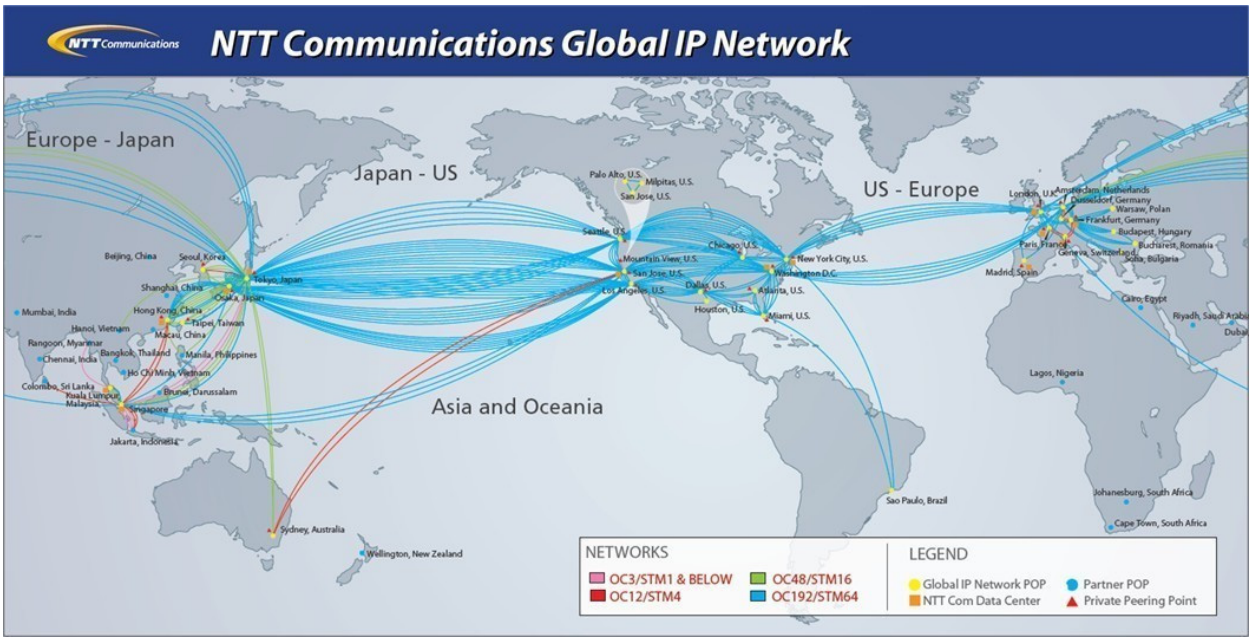
The GIN network is built upon 10GE and 100GE circuits, along with Cisco and Juniper Network routers. The GIN network carries only data; there are no voice "ride alongs" to inhibit data traffic. Regular upgrades are performed to help ensure that network performance meets customer expectations.

The GIN network features densely meshed paths between most major network points, both domestically and internationally. From the beginning, redundancy has been the main focal point in building connections. Connections are provided by different carriers at many of the major points in the GIN network and are not reliant on one vendor. These geographic and carrier redundancies help ensure that data will keep moving, even if a link fails.

The GIN network has multiple, highly secure, carrier-class Points-of-Presence (POP). As a global Tier One internet service provider (ISP), NTT Communications maintains private peering relationships with other U.S. and global Tier One ISPs. These private peering relationships provide multiple routing paths for continuous, uninterrupted transport of customer data.

NTT Communications Group
NTT America, Inc.

NTT Communications Global IP Network (GIN Network)



System security and availability

Policies

Formal processes related to system security and availability are fundamental to NTT America's internal control structure.

Each department or group critical to the security and availability of NTT America's services has created policies to help govern and instruct personnel in the performance of their duties. Policies are created by the applicable business or operations team and are approved by the director or vice president overseeing those departments.

Policies cover access to Data Centers, POP servers, Network Operations Center (NOC), diagnostic measurement servers, network, data center routers, cloud systems and backup systems. Policies and escalation procedures are also in place for monitoring of environmental equipment and network components related to network security and availability.

Communications

NTT America has established several means of communication with both customers and their employees. Availability information and service-level agreements (SLAs) are posted on the NTT America website and the Global Customer Portal. The SLAs establish performance objectives in the following four areas: Availability, Latency, Packet Loss and Jitter. Measurements for the SLAs are reported on the us.ntt.com/support/service-level-agreements website, along with a mechanism to apply for a credit.

NTT Communications Group
NTT America, Inc.

The Certified Engineering Team provides 24/7/365 assistance to customers through Monitoring, Technical Support, Customer Service, System Administration and Network Administration functions. The Certified Engineering Team is staffed 24/7/365 with professionally trained and certified Windows, Exchange, Solaris, Linux and Network administrators. In addition to contacting the Certified Engineering Team, customers can also report problems and check on system status through their Global Customer Portal.

An intranet site is used to post NTT America's policies and is accessible to all employees. Weekly and monthly meetings are held by management and department members to help ensure policies are being followed and issues are addressed and escalated when appropriate. These periodic meetings are held with the Data Centers, NOC and IP Engineering groups.

The NTT America Global Customer Portal is used by NTT America to communicate incidents, maintenance windows, downtime and other pertinent changes and information to its customers relating to the services for which each individual customer has contracted with NTT America.

People

The NTT Communications Global IP Network, NTT America Data Centers and network environments are maintained by the following groups:

- The IP Operations group oversees the Global NOC and the Security Abuse Team (SAT). The NOC is responsible for monitoring the global backbone network, as well as the U.S. regional networks, 24 hours a day. The NOC is also responsible for maintenance of the network and for tracking and escalating outages. SAT is responsible for handling various security, abuse and compliance issues, such as monitoring network traffic for possible attacks and taking action against identified attackers.
- IP Engineering and the NTT America Network Engineers are responsible for the configuration, security and maintenance of the network and IP backbone routers.
- The Network Engineering group is responsible for the configuration, security and maintenance of the routers within the Data Centers.
- The Vice President of Service Delivery oversees the Data Center Operations (DCO). Within the Data Center, the Director of Technical Operations and staff are responsible for the day-to-day operations, including the provisioning of new customer orders, in addition to the maintenance and security of the Data Center and environmental equipment. The Certified Engineering Team monitors customer servers and the Network, resolves customer issues through their Tier 2 technical support team, and provides system and network administration.

Procedures

Security and availability of NTT America's systems are critical to its customers. The Data Centers are equipped with environmental systems, including cooling systems, UPS (uninterruptible power supply) devices, fire suppression and/or detection systems, backup generators and electrical distribution systems to help ensure customer systems remain available in the event of an emergency or power loss. NTT America contracts with external service firms to perform regular preventive and corrective maintenance of the environmental infrastructure equipment to help identify equipment in need of maintenance or replacement prior to an actual failure.

System availability is measured and monitored using the following tools:

- Netcool is a tool that monitors various systems, including network devices. Netcool is used by NTT America to monitor and alert the Certified Engineering team and the NTT America NOC of any potential events. Netcool incorporates probes that scan network devices periodically to detect early warnings of system problems. When a probe identifies a problem (e.g., router is not responsive), it creates an event in the Netcool Object Server. The Netcool client software, in turn, displays a visual event, color-coded based on criticality. After each event is verified, the Certified Engineering team opens a problem ticket, which is automatically populated with the details of the event from Netcool. The Certified Engineers and Network Engineers continually monitor Netcool for reported events and respond accordingly. DataTrax monitors Data Center environmental systems in order to identify any systems operating outside of a preset tolerance window. If any abnormalities are detected, DataTrax alerts NTT America personnel to the problem via automated emails and text pages. DataTrax monitors environmental systems, including cooling systems, UPS devices, fire suppression and/or detection systems, backup generators and electrical distribution systems.
- Measurements for SLA statistics are recorded by Indicative agents at 31 of NTT America's major POP locations. Indicative is a licensed software tool, developed by Agilent Technologies, which runs on the Diagnostic Measurement Server (DMS) to monitor network performance. The DMS compiles the measurement information obtained from these 31 agent locations. Each of these 31 locations has an integrated system of agents, switches and routers that are connected directly to the layer 2 backbone switches in the POP. The architecture is fully redundant so that a failure in any given agent, switch or router will not cause loss of data or availability.

IP Backbone Network

The core architecture of the IP backbone network includes Cisco and Juniper routers. Redundancy has been built into the architecture to help eliminate a single point of failure with these devices. NTT America has developed a unified management system which act as the primary interface between the IP Engineers and the IP backbone and helps ensure all routers are configured accurately and consistently.

Access to these IP backbone devices is restricted to authorized personnel in the IP Engineering Operations group and the NTT America Customer Engineers. The Director of IP Engineering Operations approves any changes in access for new and existing users. Formal change control, configuration standards and administration procedures are followed to help ensure router and switch devices are configured in a consistent manner in order to provide optimal service and security.

Approved users must authenticate to the routers through an access control server called Terminal Access Controller Access – Control System Plus (TACACS+). The TACACS+ server requires all users to have a unique username and password. The TACACS+ server logs all user activity, including failed login attempts. The log file is reviewed periodically by the IP Engineering Operations group for unusual activity.

If the TACACS+ server is down or fails, each device has a backup account, which all of the authorized NTT America IP Engineering and Network Engineers can access. The backup account has an encrypted password that uses a high-level encryption algorithm for added protection. The router and switch configurations have activated the "enable secret" service to require an additional password for administrative-level (i.e., root) access. These passwords also use a sophisticated encryption algorithm.

Each device uses Access Control Lists (ACLs) to filter source and destination data traffic. For example, one ACL allows only specific IP addresses to authenticate to the router using secure shell (SSH). Another ACL restricts SNMP to specific servers. The ACLs, as with all configurations, are maintained in the unified management system.

Changes to router and switch configurations follow Methods and Procedures and are tracked and logged by a third-party software package called RANCID which automatically records all device configurations at regular intervals. When a configuration change is detected, RANCID automatically sends an email notification to a predefined list of administrators, including the Director of IP Engineering, who will follow up on any unusual activity. The email provides a detailed description of the device and the changes that were made. This monitoring tool would identify all changes made, including those considered "emergency" changes.

Global Enterprise Solutions Network

The Network Engineering group maintains the routers within the Data Centers. The core architecture at the Data Centers includes Cisco routers, which connect to NTT Communications' GIN network. Access to the network devices is restricted to authorized personnel in the Network Engineering group through a TACACS+ server, where each authorized user must have a unique ID and password. The manager of Network Engineering approves any changes in access for new and existing users.

Administration and maintenance of network devices are tracked through the ticketing system. Maintenance is conducted during off-peak hours. Configuration standards are stored on a separate "configuration server," and changes to baseline configurations are tracked using a version control system. ACLs are utilized at several levels to restrict network traffic. All hosts are automatically denied access to NTT America network devices unless they are defined to an ACL. SSH and Telnet access is only allowed from known NTT Communications or NTT America addresses.

Hybrid Cloud Services

Hybrid Cloud is architected on the VMware vSphere platform, which is designed to provide a consistent configuration across cloud host clusters. Each host is installed via a master image, which provides consistent software installation. Access to modify the templates used in the imaging process is restricted to authorized NTT America personnel via secure access control mechanisms. After installation, the vSphere feature, Host Profiles, is used to apply a configuration package consistent with the requirements of the cluster the host is joining. The host configuration is checked for compliance with build specifications via an automated daily process. In the event a host is out of compliance, an alert is sent to the administrative group, which investigates and remediates as required.

The management infrastructure for Hybrid Cloud utilizes centralized authentication via Active Directory (AD) for Windows-based components, as well as ESX systems. User rights are assigned to individual users by groups associated with their job role. Default administrative accounts are disabled for remote access, and privilege escalation is needed after login to access administrative functions. All authentication communication between systems and all administrative user access are encrypted. Logging within the environment, including logging of all administrative activity, is handled by sending the logs to an isolated logging server. Logs are maintained for a year to be available in the event they are needed. User access to the cloud environment is approved by the cloud manager through email communication. The cloud manager also reviews cloud access on a quarterly basis to help ensure that current access levels within the cloud environment remain commensurate with associate job functions. Terminated user access is communicated by HR and removed by cloud administrators upon notification.

NTT Communications Group
NTT America, Inc.

To enhance security and provide isolation in the event of a breach, Hypervisor/Management Network segments are divided into multiple layer 2 segments (VLAN).

An actively managed firewall controls access to all management systems; these management segments are only accessible from NTT America management networks.

Each host (Hypervisor) within the environment employs a software firewall on the management interface, which supplements the hardware firewall. Authentication to the host is provided via the AD system.

Individual Active Directory accounts are used by each user to log into the Hybrid Cloud portal. NTT America will enable access to the portal for customers who elect to use their existing compatible system for authentication.

Customer data is segregated at the Hypervisor and cloud manager layer by built-in access controls within a shared environment. Further separation at the data logical unit level (LUN) is provided within a dedicated environment.

Managed Recovery Services

Managed Recovery Services allow customers to specify schedules for the backup of data from their servers to NTT America's in-house backup infrastructure. Based on the plan purchased, customers have the option of choosing which servers and data to back up, the retention period and the window of time when backups are initiated.

Data backup provisioning takes place during the final install phase of the provisioning process. The backup software is installed on the customer server and connected to the NTT America infrastructure through the secondary network. DCO then activates the policy and creates a NetBackup client in GMP. GMP tests connectivity and status by attempting to perform a full backup under the constraints set by the client. The results of the test backup are then emailed to GMP users. For any unsuccessful or failed backups, DCO will troubleshoot and escalate as necessary until the issue is resolved and backups are successful.

Recovery services are performed for the customer servers using the Veritas NetBackup application and can be performed by either the customer or the Certified Engineering Team, at the customer's request only. The request is documented in the Siebel ticketing system. The Certified Engineering Team can initiate the restoration by accessing the NetBackup client on the customer's server or via the master server. Once a successful restoration is completed, the customer is notified and the Siebel ticket is closed. Any failed restorations are escalated as necessary until the issue is resolved.

Monitoring

Tools

Network events are identified and monitored through the use of Netcool and other monitoring tools or through communications with customers. These events are tracked using ticket management software that helps ensure timely resolution of each ticket. NTT America personnel are responsible for managing event resolution to its conclusion.

NTT Communications Group
NTT America, Inc.

Netcool, working in conjunction with other utilities, is a tool used by NTT America to monitor various systems and alert the Certified Engineering Team of any potential NTT Communications backbone network events and any potential internal, storage or customer network events. Netcool incorporates probes that scan network devices periodically to look for signs of possible problems. When a probe identifies a problem, it reports the event to the Netcool Object Server. The Netcool client software, in turn, displays the event, which is color-coded based on criticality, to the individuals monitoring the system.

Indicative, running on the DMS, monitors the polling agents. It sends emails to Internet Security Systems (ISS) and SNMP traps to the NOC. It is reviewed by NOC personnel to make sure measurements are taken by the agents. The DMS compiles the measurement information obtained from 31 different agents running on the POPs. Nightly SLA reports are sent out to the NOC and representatives from each department within GIN network. The report notes anomalies detected by the SLA agents. Issues are documented in a ticketing system and escalated as needed.

Various tools and scripts are used to help detect when changes have been made to the IP backbone and Data Center routers. Results are reviewed by the Network Engineering Manager or IP Engineering.