ENHANCED SECURITY PLAN FOR U.S.-BASED CUSTOMERS' DOMESTIC COMMUNICATIONS INFRASTRUCTURE

Overview of Plan

1. Security Policies and Procedures

a. Security Director. Netcracker Technology Corporation (NTC) shall designate and maintain a Security Director. The Security Director shall possess demonstrated expertise in assessing the security of computer code and network provisioning services, and shall:

i. Be subject to the Offices' review and approval.

ii. Possess a U.S. security clearance of at least a Top Secret level.

iii. Act as the liaison with and point of contact for the Offices on behalf of NTC.

iv. Be a corporate officer with appropriate authority, reporting lines, independence, skills, and resources to ensure compliance with the Enhanced Security Plan.

b. Security Policy. NTC shall create and implement a Security Policy. The Security Policy shall detail the specific procedures by which NTC shall comply with the Enhanced Security Plan, and shall:

i. Be subject to the Offices' review and approval.

ii. Establish user identity and access management policies that set forth rights of "Access" (as defined in the Enhanced Security Plan) by NTC to U.S.-Based Customers' Domestic Communications Infrastructure and controls over such Access in order to detect anomalous user behavior.

iii. Ensure that a monitoring system provides alerts to identify, prevent, and contain unauthorized attempts to access U.S.-Based Customers' Domestic Communications Infrastructure through NTC from all sources, including remote access, network segmentation, and tiered access.

iv. Include personnel screening procedures, including background checks, for all NTC employees who provide services to U.S.-Based Customers' Domestic Communications Infrastructure.

v. Be disseminated to NTC's U.S.-Based Customers along with annual reports describing NTC's security policy.

c. Code Security.

i. NTC shall authenticate all software delivered to its U.S.-Based Customers through code signing or other technical means.

ii. NTC shall maintain sufficient controls and documentation to trace every change to the Netcracker Product Suite Source Code or code developed by NTC for a U.S.-Based Customer that changes, adds, or removes product functionality.

iii. NTC shall identify and maintain a Configuration Management System that tracks all changes to the Netcracker Product Suite Source Code or code developed by NTC for its U.S.-Based Customers.

iv. NTC shall provide the Netcracker Product Suite Source Code for the latest available major release of the Netcracker Product Suite components contracted for use on U.S.-Based Customers' Domestic Communications Infrastructure, including any customization or project code for U.S.-Based Customers, to the Offices (or third-party identified by the Offices) for review and testing at intervals set by the Enhanced Security Plan.

v. NTC shall work with the Offices and the Security Director to enhance security around its source code.

2. U.S.-Based Infrastructure and Security, and Access Consent

a. U.S.-Based Infrastructure. NTC shall move to the United States (or maintain in the United States) the following infrastructure used to provide services to U.S.-Based Customers, and shall not access this infrastructure from outside the United States except as provided in the Enhanced Security Plan:

i. File storage and shared drives server, such as File Transfer Protocol Servers.

ii. Servers for internal and external SharePoint portals.

iii. Internal server cloud (for development and test environments).

iv. Servers for the issue and support ticketing systems.

v. Configuration management, version control, and build infrastructure, including Subversion and build automation servers.

vi. Systems used to provision, manage, configure or otherwise Access any Domestic Communication Infrastructure network element.

vii. Servers associated with a Public Key Infrastructure, key or secret management or code signing.

viii. Any system or portion of system providing security or incident and event management including audit log management or access to Security-Relevant Information for the above systems.

b. U.S.-Based Security. NTC will move to the United States (or maintain in the United States) certain supervisory security functions, including management of the employee screening functions and the office of the Security Director to oversee work performed

by NTC personnel or any NTC subcontractors in relation to U.S.-Based Customers' Domestic Communications Infrastructure, regardless of the location of such personnel.

c. Access Consent. NTC will not Access U.S.-Based Customers' Domestic Communications Infrastructure from any location outside the physical control of the U.S.-Based Customer without obtaining the prior, informed, and express written consent of the U.S.-Based Customer.

3. Restrictions on Transferring Sensitive Data Outside of the United States

a. Sensitive Individual Data and Sensitive Network Data. NTC shall not route or transfer Sensitive Individual Data or Sensitive Network Data (defined in the Enhanced Security Plan) outside the United States except as provided in the Enhanced Security Plan.

b. Presentation Layer Remote Desktop. Under the direction of the Security Director, and subject to other limitations defined in the Enhanced Security Plan, NTC may utilize presentation layer access to Sensitive Individual Data through a PCI DSS-compliant remote desktop or similar solution—meaning the transfer consists solely of images of the user interface and the keystrokes and mouse activity of the user—for the purpose of carrying out NTC's billing services, and customer order and management services.

c. Routing Consent. NTC shall not route or transfer Sensitive Individual Data or Sensitive Network Data outside the United States without anonymizing such Data and obtaining the prior, informed, and express written consent of the U.S.-Based Customer.

d. Logging. NTC shall record access by NTC to Sensitive Network Data and Sensitive Individual Data, and shall record access to and activity on systems capable of accessing Sensitive Network Data or Sensitive Individual Data in sufficient detail to enable the Security Director and/or Third Party Auditor to detect unauthorized activity.

e. Encryption. NTC shall ensure its U.S.-Based Customers have the means, without assistance from or notification to NTC, to monitor and inspect the contents of any data transfers that NTC makes through any Access granted to NTC by the Customers. In the event that NTC chooses to add encryption not supplied by the Customers, NTC shall make relevant encryption keys available to the Customers before NTC transfers data.

4. The Third-Party Auditor and Rights to Third-Party Audits

a. NTC shall engage and make available to the Security Director and the Offices a Third-Party Auditor to ensure compliance with the Enhanced Security Plan.

b. As part of his/her responsibilities, the Third-Party Auditor will undertake annual Third-Party Audits of NTC's compliance with the terms of the Enhanced Security Plan.

5. Site Visits and Interviews

a. NTC shall provide the Offices with access to NTC's global infrastructure used to provide services to U.S.-Based Customers for the purpose of verifying compliance with the terms of the Enhanced Security Plan.

b. NTC shall use its best efforts to make available to the Offices for interview officers or employees of NTC to verify compliance with the Enhanced Security Plan.

###