

AGREEMENT

AMENDMENT 1

This AGREEMENT – AMENDMENT 1 (“AMENDMENT 1”) is made as of the date of the last signature affixed hereto by and among Global Crossing Limited (“GCL”), formerly known as GC Acquisition Limited (“New GX”), and Singapore Technologies Telemedia Pte Ltd (“ST Telemedia”), on the one hand, and the Federal Bureau of Investigation (“FBI”), the U.S. Department of Justice (“DOJ”), the Department of Defense (“DOD”), and the Department of Homeland Security (“DHS”), on the other (referred to individually as a “Party” and collectively as the “Parties”).

RECITALS

WHEREAS, the Parties entered into an Agreement dated as of September 24, 2003, to address national security, law enforcement, and public safety issues arising from ST Telemedia’s investment in GCL (“Agreement”);

WHEREAS, on October 25, 2006, GCL, GC Crystal Acquisition, Inc. (“GC Crystal Acquisition”), a newly established Delaware corporation and an indirect wholly owned subsidiary of GCL, and Impsat Fiber Networks, Inc. (“Impsat”) entered into an agreement and plan of merger (“Merger Agreement”), pursuant to which Impsat will merge into GC Crystal Acquisition, with Impsat continuing as the surviving corporation under its existing name;

WHEREAS, GCL, upon consummation of the merger, will become the indirect parent of Impsat’s U.S. subsidiary, Impsat USA, Inc. (“Impsat USA”), and Impsat USA will become a “Domestic Communications Company” as defined in the Agreement;

WHEREAS, Impsat USA maintains space in one of its facilities that may be used for the provision of Hosting Services to certain U.S. Hosting Services Customers;

WHEREAS, GCL and Impsat have filed applications with the Federal Communications Commission (“FCC”) (in WC Docket No. 06-215, File No. ITC-T/C-20061128-00533, File No. SES-T/C-20061128-02052, and File No. SCL-T/C-20061128-00011) requesting consent to the transfer of control of Impsat USA to GCL;

WHEREAS, the Parties are entering into this AMENDMENT 1 in light of the Merger Agreement and also in light of certain requirements relating to security clearances in the Agreement;

NOW THEREFORE, the Parties agree to amend the Agreement as follows:

1. **Hosting Services**

(a) Article 1 of the Agreement is amended to include the following defined terms:

1.4.1. “Data Center” means (a) equipment (including firmware, software, and upgrades), facilities, and premises used by (or on behalf of) GCL in connection with Hosting Services (including data storage and provisioning, control, maintenance, management, security, selling, billing, or monitoring of Hosting Services), and (b) equipment hosted by GCL that is leased or owned by a Hosting Services customer.

1.18.1. “Hosting Services” means web hosting (whether shared or dedicated, and including design, server management, maintenance and telecommunications services), web site traffic management, electronic commerce, streamed media services, server collocation and management, application hosting, and all other similar services offered by GCL.

1.35.1. “U.S. Hosting Data” means all data, records, documents or information (including Domestic Communications, other Wire or Electronic Communications, Subscriber Information and Transactional data in any form (including but not limited to paper, electronic, magnetic, mechanical, or photographic) transmitted, received, generated, maintained, processed, used by or stored in a Data Center for a U.S. Hosting Services Customer.

1.35.2. “U.S. Hosting Services Customer” is a customer or subscriber that receives Hosting Services from a Domestic Communications Company and that is U.S.-domiciled or holds itself out as being U.S.-domiciled. A customer or subscriber will be considered to be U.S.-domiciled if (i) it has its principal office(s) or place(s) of business in the United States, (ii) it is incorporated in the United States, (iii) it receives Hosting Services facilitated by a Data Center that is physically located in the United States, or (iv) other criteria tend to indicate that it is U.S.-domiciled.

(b) A new Section 2.12 and Section 2.13 are added to the Agreement, as follows:

2.12. Data Centers and Access to Communications. Except to the extent and under conditions concurred in by the DHS, DOJ, DOD and FBI in writing:

- (i) all Data Centers used to provide Hosting Services to U.S. Hosting Services Customers shall at all times be located in the United States; and
- (ii) GCL shall, upon service of appropriate Lawful U.S. Process, ensure that Wire or Electronic Communications of a specified U.S. Hosting Services Customer that are transmitted to, from or through a Data Center shall be accessible from or pass through a facility under the control of GCL and physically located in the United States, from which Electronic Surveillance can be conducted in a timely manner. GCL will provide technical or other assistance to facilitate such Electronic Surveillance.

2.13. U.S. Hosting Data Storage and Access. GCL shall have the ability to provide in the United States stored U.S. Hosting Data (whether in “electronic storage” as defined in 18 U.S.C. § 2510(17) or stored in any other manner) except for stored U.S. Hosting Data located on equipment that is owned or controlled by a U.S. Hosting Services Customer and is collocated in GCL-controlled space in a data center. GCL shall ensure that such data shall not be stored outside the United States. In any event, GCL shall take all technically feasible steps to ensure that such data is stored in a manner not subject to mandatory destruction under any foreign laws.

(c) Section 2.4 of the Agreement is hereby amended to read in its entirety as follows:

2.4. Billing Records. Domestic Communications Companies shall store for at least 18 months all billing records described in Section 2.3(v) above, including billing records related to U.S. Hosting Services. Nothing in this paragraph shall require a Domestic Communications Company to store such records for longer than 18 months.

(d) Section 2.7 of the Agreement is hereby amended to read in its entirety as follows:

2.7. Routing of Domestic Communications and U.S. Hosting Data. Except for routing of traffic (i) to U.S. states, territories and possessions outside the Continental United States, (ii) to avoid network disruptions, (iii) consistent with least-cost routing practices that are implemented pursuant to policies reviewed and approved by the third-party auditor selected pursuant to Section 5.8 of this Agreement, and (iv) as otherwise may be agreed by the DOJ, FBI, DOD, and DHS, Domestic Communications Companies shall not route Domestic Communications and U.S. Hosting Data outside the United States.

2. **Screening of Personnel**

A new Section 3.12(vi) is added to the Agreement, as follows:

(vi) All personnel employed by any entity of which GCL acquires control (“New Domestic Communications Company”), including but not limited to the employees of Impsat USA, and who are subject to the screening procedures set forth in the Agreement, must satisfy such procedures before they are permitted access to any Domestic Communications Infrastructure or to Transactional Data, Call Associated Data, or Subscriber Information, other than such portion of the Domestic Communications Infrastructure, and such portion of the Transactional Data, Call Associated Data, or Subscriber Information, that pertain solely to the New Domestic Communications Company.

3. **Technical Changes**

The Agreement is hereby amended to include the following technical changes that are not intended to modify the obligations of the Domestic Communications Companies:

(a) In Section 3.8 of the Agreement, the individuals designated as nominees are required to be eligible for a U.S. security clearance and their applications for such clearances must have been submitted to DoD. The Domestic Communications Companies shall collect and review such applications and determine that the individuals meet company security standards and, in their opinion, meet the requirements for a U.S. security clearance. The Domestic Communications Companies shall offer to forward such applications to the FBI, DOJ, DOD and DHS. The FBI, DoJ, DOD and DHS may choose not to receive, process or complete action on such clearance applications unless and until they deem necessary. All other requirements and undertakings of paragraph 3.8 continue to apply.

(b) In Section 3.13, the Head of Network Operations and Head of Global Security for Domestic Communications Companies are required to possess or apply for a U.S. security clearance. The Domestic Communications Companies shall collect and review such clearance applications and determine that the individuals meet company security standards and, in their opinion, meet the requirements for a U.S. security clearance. The Domestic Communications Companies shall offer to forward such applications to the FBI, DOJ, DOD and DHS. The FBI, DoJ, DOD and DHS may choose not to receive, process or complete action on such clearance applications unless and until they deem necessary. All other requirements and undertakings of paragraph 3.13 continue to apply.

(c) In Section 3.14, the Human Resources executive responsible for hiring and screening and the General Counsel are required to possess or apply for a U.S. security clearance. The Domestic Communications Companies shall collect and review such clearance applications and determine that the individuals meet company security standards and, in their opinion, meet the requirements for a U.S. security clearance. The Domestic Communications Companies shall offer to forward such applications to the FBI, DOJ, DOD and DHS. The FBI, DoJ, DOD and DHS may choose not to receive, process or complete action on such clearance applications unless and until they deem necessary. All other requirements and undertakings of paragraph 3.14 continue to apply.

(d) In Section 3.15, the Security Directors are required to possess or apply for a U.S. security clearance. The Domestic Communications Companies shall collect and review such clearance applications and determine that the individuals meet company security standards and, in their opinion, meet the requirements for a U.S. security clearance. The Domestic Communications Companies shall offer to forward such applications to the FBI, DOJ, DOD and DHS. The FBI, DoJ, DOD and DHS may choose not to receive, process or complete action on such clearance applications unless and until they deem necessary. All other requirements and undertakings of paragraph 3.15 continue to apply.

4. FCC Approval

Upon the execution of this AMENDMENT 1 by all the Parties, the DOJ, FBI, DOD, and DHS shall promptly notify the FCC that they have no objection to the FCC's grant of the applications filed with the FCC in WC Docket No. 06-215, File No. ITC-T/C-20061128-00533, File No. SES-T/C-20061128-02052, and File No. SCL-T/C-20061128-00011, provided such grant is conditioned on compliance with the Agreement, as amended hereby.

This AMENDMENT 1 is executed on behalf of the Parties:

Global Crossing Limited

Date: 1/25/07

By: John B. McShane
Printed Name: John B. McShane
Title: General Counsel

Singapore Technologies Telemedia Pte Ltd

Date: _____

By: _____
Printed Name: _____
Title: _____

United States Department of Justice

Date: _____

By: _____
Printed Name: _____
Title: _____

Federal Bureau of Investigation

Date: _____

By: _____
Printed Name: _____
Title: _____

United States Department of Defense

Date: _____

By: _____
Printed Name: _____
Title: _____

This AMENDMENT 1 is executed on behalf of the Parties:

Global Crossing Limited

Date: _____

By: _____

Printed Name:

Title:

Singapore Technologies Telemedia Pte Ltd

Date: 26 January 2007

By: 

Printed Name: PEK KOCK LAN

Title: COMPANY SECRETARY

United States Department of Justice

Date: _____

By: _____

Printed Name:

Title:

Federal Bureau of Investigation

Date: _____

By: _____

Printed Name:

Title:

United States Department of Defense

Date: _____

By: _____

Printed Name:

Title:

This AMENDMENT 1 is executed on behalf of the Parties:

Global Crossing Limited

Date: _____

By: _____

Printed Name:

Title:

Singapore Technologies Telemedia Pte Ltd

Date: _____

By: _____

Printed Name:

Title:

United States Department of Justice

Date: 2-2-07

By: 

Printed Name: Charles M. Steele

Title: Chief of Staff, National Security Division

Federal Bureau of Investigation

Date: _____

By: _____

Printed Name:

Title:

United States Department of Defense

Date: _____

By: _____

Printed Name:

Title:

This AMENDMENT 1 is executed on behalf of the Parties:

Global Crossing Limited

Date: _____

By: _____
Printed Name:
Title:

Singapore Technologies Telemedia Pte Ltd

Date: _____

By: _____
Printed Name:
Title:

United States Department of Justice

Date: _____

By: _____
Printed Name:
Title:

Federal Bureau of Investigation

Date: 2/1/07

By: /s/ ELAINE N. LAMMERT
Printed Name: Elaine N. Lammert
Title: Deputy General Counsel
Federal Bureau of Investigation

United States Department of Defense

Date: _____

By: _____
Printed Name:
Title:

This AMENDMENT 1 is executed on behalf of the Parties:

Global Crossing Limited

Date: _____

By: _____
Printed Name:
Title:

Singapore Technologies Telemedia Pte Ltd

Date: _____

By: _____
Printed Name:
Title:

United States Department of Justice

Date: _____

By: _____
Printed Name:
Title:

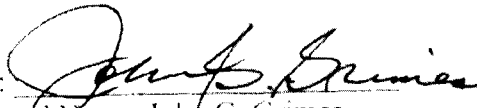
Federal Bureau of Investigation

Date: _____

By: _____
Printed Name:
Title:

United States Department of Defense

Date: 1/30/07

By: 
Printed Name: John G. Grimes
Title: Assistant Secretary of Defense for Networks
and Information Integration (ASD NII) /
Department of Defense Chief Information
Officer (CIO)

United States Department of Homeland Security

Date: February 1, 2007

By: Stephen Helfetz
Printed Name: Stephen Helfetz
Title: Director, Foreign Financial
+ Investment Issues