

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Robert M. Franklin, Transferor	)	IB Docket No. 08-143
	)	
and	)	DA 08-1659
	)	
Inmarsat plc, Transferee	)	File Nos. ITC-T/C-20080618-00276
	)	ITC-T/C-20080618-00275
Consolidated Application for	)	SES-T/C-20080618-00818
Consent to Transfer Control of	)	SES-T/C-20080618-00819
Stratos Global Corporation and Its	)	SES-T/C-20080618-00820
Subsidiaries from an Irrevocable	)	SES-T/C-20080618-00821
Trust to Inmarsat plc	)	0003453455
	)	ISP-PDR-20080618-00013

**PETITION TO ADOPT CONDITIONS ON TRANSFER OF CONTROL**

Pursuant to Section 1.41 of the Federal Communications Commission’s (“Commission”) rules,<sup>1</sup> the Department of Justice (“DOJ”), including the Federal Bureau of Investigation, and Department of Homeland Security (“DHS”), (collectively, the “Agencies”), hereby submit this Petition to Adopt Conditions on the above-referenced consolidated application for transfer of control (“Petition”). Through this Petition, the Agencies advise the Commission that they have no objection to the Commission consenting to the above-referenced transfer of control, provided that the Commission conditions its consent on the agreement of Inmarsat plc and its direct and indirect

---

<sup>1</sup> 47 C.F.R. § 1.41.

subsidiaries (collectively, "Inmarsat") to abide by the commitments and undertakings set forth in the Network Security Agreement dated September 23, 2008 between Inmarsat Global Limited and Inmarsat Hawaii and the Agencies ("Inmarsat Agreement"), a copy of which is attached hereto as Exhibit A. A proposed condition is attached as Exhibit A to the Agreement.

In the above-captioned matter, applicants Robert M. Franklin and Inmarsat plc seek approval of a series of applications filed pursuant to Sections 214 and 310(d) of the Communications Act of 1934, as amended ("Act") for consent to the indirect transfer of control of Stratos Global Corporation ("Stratos Global") and its wholly-owned subsidiaries that hold licenses and authorizations from the Commission from an irrevocable trust, for which Mr. Franklin is the trustee, to Inmarsat. The applicants also request a declaratory ruling under Section 310(b)(4) of the Act<sup>2</sup> that allowing up to one-hundred percent indirect foreign ownership of Stratos Global and its wholly-owned subsidiaries that hold licenses and authorizations from the Commission is consistent with the public interest.

In December 2007, the Commission approved the transfer of control of Stratos Global to an irrevocable trust established by CIP Canada Investment Inc. ("CIP Canada"), a wholly-owned subsidiary of CIP UK Holdings Limited ("CIP UK"), which, in turn, is a wholly-owned subsidiary of Communications Investment Partners Limited

---

<sup>2</sup> 47 U.S.C. § 310(b)(4).

("CIP").<sup>3</sup> The trust currently holds the shares of Stratos Global for the benefit of CIP Canada, with Mr. Franklin, the Trustee, currently holding the voting power for those shares. CIP previously granted Inmarsat an option to acquire the shares of CIP UK, which Inmarsat has decided to exercise. Upon Inmarsat's exercise of its option, the trust will terminate, CIP Canada will become the holder of the shares of Stratos Global, and Inmarsat will indirectly own and control CIP UK, CIP Canada, and Stratos Global.

As the Commission is aware, the Agencies have taken the position that their ability to satisfy their obligations to protect the national security, enforce the laws, and preserve the safety of the public could be impaired to the extent that foreign entities own or operate a part of the U.S. telecommunications system, or foreign-located facilities are used to provide domestic telecommunications services to U.S. customers. The Commission has long recognized that national security, law enforcement, and public safety issues and concerns are part of its public interest analysis in matters such as this,<sup>4</sup> and has accorded deference to the views of other U.S. government agencies

---

<sup>3</sup> *Stratos Global Corporation, Transferor, Robert M. Franklin, Transferee, Consolidated Application for Consent to Transfer of Control, Memorandum Opinion and Order and Declaratory Ruling, WC Docket No. 07-73, FCC 07-213, 22 FCC Rcd 21328 (2007) ("Stratos Order").*

<sup>4</sup> *See Rules and Policies on Foreign Participation in the U.S. Telecommunications Market, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23919-21 ¶¶ 61-66 (1997) ("Foreign Participation Order"); see also Amendment of the Commission's Regulatory Policies to Allow Non-U.S. Licensed Space Stations to Provide Domestic and International Satellite Service in the United States, Report and Order, 12 FCC Rcd 24094, 24100 ¶ 15 (1997) ("DISCO II").*

with expertise in those areas.<sup>5</sup>

As noted above, the Agencies have had an Agreement in place with various Stratos Global subsidiaries since August 2001 to help to ensure that the Agencies and other entities with responsibility for enforcing the law, protecting the national security, and preserving public safety can proceed appropriately to satisfy those responsibilities. In consenting to the transfer of control of Stratos Global to the irrevocable trust, the Commission expressly conditioned its consent on the agreement of Stratos Global to continue to abide by the commitments and undertakings set forth in the Network Security Agreement dated August 7, 2001 between various Stratos Global subsidiaries and the Agencies (“Stratos Agreement”), as amended by Amendment No. 1 dated August 14, 2007,<sup>6</sup> copies of which are attached hereto as Exhibits B and C, respectively. After discussions with representatives of Inmarsat, the Agencies have concluded that the commitments set forth in the Inmarsat Agreement will also help to ensure that the Agencies and other entities with responsibility for enforcing the law, protecting the national security, and preserving public safety can proceed appropriately to satisfy those responsibilities. Accordingly, the Agencies hereby advise the Commission that they have no objection to the Commission consenting to the above-referenced transfer of control application provided that the Commission conditions its consent on

---

<sup>5</sup> See *Foreign Participation Order* at 23919-20 ¶¶ 62-63; see also *DISCO II* at 24179-80 ¶¶ 179-80.

<sup>6</sup> *Stratos Order* at 21373, ¶¶ 110-11.

compliance by Inmarsat with the commitments set forth in the Inmarsat Agreement, and the continued compliance by Stratos Global and its subsidiaries with the Stratos Agreement, as amended.

The Agencies are authorized to state that the applicants do not object to the grant of this Petition.

Respectfully submitted,

          /s/ Richard C. Sofield            
Richard C. Sofield  
Director  
Foreign Investment Review Staff  
National Security Division  
United States Department of Justice  
950 Pennsylvania Avenue, N.W.  
Washington, DC 20530

          /s/ Stewart A. Baker            
Stewart A. Baker  
Assistant Secretary for Policy  
U.S. Department of Homeland Security  
3801 Nebraska Avenue, N.W.  
Washington, DC 20528

December, 2008

# **EXHIBIT A**

## AGREEMENT

This AGREEMENT (“Agreement”) is made as of the Effective Date by and between Inmarsat Global Limited, a company organized under the laws of England and Wales and headquartered in London, England, and all of its Affiliates and subsidiaries including Inmarsat Hawaii Inc. (collectively, “Inmarsat”), on the one hand, and the U.S. Department of Justice (“DOJ”) and the U.S. Department of Homeland Security (“DHS”), on the other hand (DOJ and DHS are referred to collectively as “the Government Parties,” and all of the Parties to this Agreement are referred to collectively as the “Parties”).

## RECITALS

WHEREAS, U.S. communications systems are essential to the ability of the U.S. government to fulfill its responsibilities to the public to preserve the national security of the United States, to enforce the laws, and to maintain the safety of the public;

WHEREAS, the U.S. government has an obligation to the public to ensure that U.S. communications and related information are secure in order to preserve the national security of the United States, protect the privacy of U.S. persons and to enforce the laws of the United States;

WHEREAS, it is critical to the well being of the nation and its citizens to maintain the viability, integrity, and security of the communication systems of the United States (*see, e.g.*, Executive Order 13231, Critical Infrastructure Protection in the Information Age, Presidential Decision Directive 63, Critical Infrastructure Protection, and Presidential Homeland Security Directive / HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection);

WHEREAS, protection of Classified and Sensitive Information is also critical to U.S. national security;

WHEREAS, Inmarsat is a wholly-owned subsidiary of Inmarsat plc, a public company listed on the London Stock Exchange;

WHEREAS, Inmarsat maintains a global network consisting of geostationary communications satellites and earth stations, through which it will provide Broadband Global Area Network (“BGAN”) Service to independent distributors who will in turn distribute such service to individual customers, and through which Inmarsat may also in the future distribute such services to its own customers;

WHEREAS, Inmarsat’s BGAN Service enables users to send and receive data, voice, or other communications to and from mobile terminals from anywhere within the United States, and elsewhere;

WHEREAS, Domestic Communications sent and received via BGAN Service are, as of the date of this agreement, routed by Inmarsat’s network from mobile terminals within the United States to Inmarsat satellites, and through Inmarsat earth stations currently located outside of the

United States, but are expected in the future to be routed through Inmarsat earth stations located in the United States;

WHEREAS, it is critical to the law enforcement, national security, and public safety interests of the United States government that such Domestic Communications, and any related Call Associated Data, Transactional Data, or Subscriber Information are made available pursuant to Lawful U.S. Process, including but not limited to the context of a real-time lawfully authorized Electronic Surveillance, within the United States in a timely, secure, and reliable manner;

WHEREAS, the cooperation and assistance of Inmarsat is necessary to ensure the above-mentioned critical interests, and to facilitate lawful access within the United States to certain information;

WHEREAS, Inmarsat holds an experimental authorization originally granted by the Federal Communications Commission (“FCC” or “Commission”) on February 23, 2006, and which has subsequently been renewed, pursuant to which Inmarsat may conduct tests and demonstrations of BGAN Service; and

WHEREAS, Inmarsat’s BGAN Service is also being provided in the U.S. by independent distributors, who originally received special temporary authorizations from the Commission in 2006 and 2007 (which have subsequently been renewed as necessary), and have pending applications for permanent authority;

NOW THEREFORE, the Parties are entering into this Agreement to address certain U.S. national security, law enforcement, and public safety concerns with respect to the provision or facilitation of BGAN Service in the United States.

## **ARTICLE 1: DEFINITION OF TERMS**

As used in this Agreement:

1.1 “Affiliate” means any entity that Inmarsat owns or Controls.

1.1.A. “BGAN Service” means Broadband Global Area Network Service (or any successor service) that provides voice and broadband data service, accessed by MESs communicating with Inmarsat-4 satellites, which are communicating with Inmarsat land earth stations linked to terrestrial networks.

1.2 “Call-Associated Data” or “CAD” means any information relating to a communication or relating to the sender or recipient of that communication and includes, without limitation, subscriber identification, called party number, calling party number, start time, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, post cut-through dual-tone multifrequency (dialed digit extraction), in-band and out-of-band signaling, party add, drop and hold, and any other call-identifying information, as defined in 47 U.S.C. § 1001(2).

1.3 “Classified Information” shall have the meaning indicated in Executive Order 12958, as



amended by Executive Order 13292, or any successor executive order, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act of 1954.

1.4 “Control” and “Controls” mean the power, direct or indirect, whether or not exercised, and whether or not exercised or exercisable through the ownership of a majority or a dominant minority of the total outstanding voting securities of an entity, or by proxy voting, contractual arrangements, or other means, to determine, direct, or decide matters affecting an entity or facility; in particular, but without limitation, to determine, direct, take, reach or cause decisions regarding:

- (a) the sale, lease, mortgage, pledge, or other transfer of any or all of the principal assets of the entity, whether or not in the ordinary course of business;
- (b) the dissolution of the entity;
- (c) the closing and/or relocation of the production or research and development facilities of the entity;
- (d) the termination or non-fulfillment of contracts of the entity;
- (e) the amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in Section 1.4(a) through (d); or
- (f) Inmarsat’s obligations under this Agreement.

1.4.A. “Customer Proprietary Network Information” or “CPNI” is defined in 47 U.S.C. § 222(h)(1).

1.5 “De facto” and “de jure” control have the meanings provided in 47 C.F.R. § 1.2110.

1.6 “DHS” means the U.S. Department of Homeland Security.

1.7 “DOJ” means the U.S. Department of Justice.

1.8 “Domestic Communications” means (a) Wire Communications or Electronic Communications (whether stored or not) originating at one U.S. location and terminating at another U.S. location, and (b) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates from or terminates at a U.S.-Licensed MES.

1.9 “Domestic Communications Infrastructure” means (a) transmission, switching, bridging and routing equipment (including software and upgrades) used by or on behalf of Inmarsat to provide, process, direct, control, supervise or manage Domestic Communications; (b) facilities and equipment used by or on behalf of Inmarsat that are physically located in the United States; and (c) facilities used by or on behalf of Inmarsat to control the equipment described in (a) and (b) above. Domestic Communications Infrastructure does not include equipment or facilities used by service providers other than Inmarsat or its Affiliates that are:

- (1) interconnecting communications providers; or

- (2) providers of services or content that are
  - (A) accessible using the communications services of Inmarsat or its Affiliates, and
  - (B) available in substantially similar form and on commercially reasonable terms through communications services of companies other than Inmarsat or its Affiliates.

The phrase “on behalf of” as used in this Section does not include entities with which Inmarsat or any of its Affiliates has contracted for peering, interconnection, roaming, long distance, resale, or distribution of BGAN Service.

1.10 “Effective Date” means the date this Agreement has been duly signed by all of the Parties, unless otherwise specified herein.

1.11 “Electronic Communication” has the meaning given it in 18 U.S.C. § 2510(12).

1.12 “Electronic Surveillance” means (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (b) access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 *et seq.*; (c) acquisition of dialing, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 *et seq.* and 50 U.S.C. § 1841 *et seq.*; (d) acquisition of location-related information concerning a service subscriber or facility; (e) preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (f) access to, or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (a) through (e) above and comparable State laws.

1.13 [NOT USED].

1.14 “FCC” or “Commission” means the Federal Communications Commission.

1.15 “Foreign” where used in this Agreement, whether capitalized or lower case, means non-U.S.

1.16 “Governmental Authority” or “Governmental Authorities” mean any government, or any governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau, or political subdivision and any court, tribunal, judicial, or arbitral body.

1.16.A. “Government Parties” means DOJ and DHS.

1.16.B. “Implementation Plan” is defined in Section 2.1 herein.

1.17 “Intercept” or “Intercepted” has the meaning defined in 18 U.S.C. § 2510(4).

1.18 “Lawful U.S. Process” means U.S. federal, state, or local Electronic Surveillance or other

court orders, processes, or authorizations issued under U.S. federal, state, or local law for physical search or seizure, production of tangible things, or access to or disclosure of Domestic Communications, Call Associated Data, Transactional Data, or Subscriber Information.

1.19 “MES” means a mobile earth station, a mobile earth terminal or “MET” (*i.e.*, a hand-held, portable, or other mobile terminal capable of receiving and/or transmitting Wire Communications or Electronic Communications by satellite), and includes a mobile earth terminal capable of receiving and/or transmitting Inmarsat services.

1.20 “Non U.S.-Licensed MES” means an Inmarsat MES other than a U.S.-Licensed MES.

1.21 “Outsourcing Contract” means a contract between Inmarsat and an individual or entity to perform functions covered by this Agreement and related to Domestic Communications which are normally performed by employees of companies in the business of providing those communications services that Inmarsat provides. Outsourcing Contract also includes any contract to perform a specific activity that is required to be performed by Inmarsat under the express terms of this Agreement. The contractor designated by Inmarsat for operation of the U.S. POP required by this Agreement is referred to herein as the “Outsourcing Contractor.”

1.22 “Party” or “Parties” have the meanings given them in the Preamble.

1.23 “Pro forma assignments” or “pro forma transfers of control” are transfers or assignments that do not involve a substantial change in ownership or control as provided by Section 63.24 of the FCC’s Rules (47 C.F.R. § 63.24).

1.24 “Sensitive Information” means information that is not Classified Information regarding (a) the persons or facilities that are the subjects of Lawful U.S. Process, (b) the identity of the government agency or agencies serving such Lawful U.S. Process, (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance pursuant to Lawful U.S. Process, (d) the means of carrying out Electronic Surveillance pursuant to Lawful U.S. Process, or (e) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process; as well as all other information that is not Classified Information but is designated in writing by an authorized official of a federal, state or local law enforcement agency or a U.S. intelligence agency as “Sensitive Information” of some type recognized by the agency involved. The designation “Sensitive” as used in this paragraph may refer to information marked or labeled “Official Use Only,” “Limited Official Use Only,” “Law Enforcement Sensitive,” “Sensitive Security Information,” “Sensitive but Unclassified,” “Controlled Unclassified Information” or other similar designations, and all such information shall be deemed “Sensitive Information” for purposes of this Agreement.

1.25 “Subscriber Information” means information relating to subscribers or customers of Inmarsat of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709. Such information shall also be considered Subscriber Information when it is sought pursuant to the provisions of other Lawful U.S. Process.

1.26 “Transactional Data” means:

- (a) “call identifying information,” as defined in 47 U.S.C. § 1001(2), including without limitation the telephone number or similar identifying designator associated with a Domestic Communication;
- (b) any information possessed by Inmarsat, or an entity acting on behalf of Inmarsat, relating specifically to the identity and physical address of a customer or subscriber, or account payer, or the end-user of such customer or subscriber, or account payer, or associated with such person relating to all telephone numbers, domain names, Internet Protocol (“IP”) addresses, Uniform Resource Locators (“URLs”), other identifying designators, types of services, length of service, fees, usage including billing records and connection logs, and the physical location of equipment, if known and if different from the location information provided under (d) below;
- (c) the time, date, size, or volume of data transfers, duration, domain names, Media Access Control (“MAC”) or IP addresses (including source and destination), URL’s, port numbers, packet sizes, protocols or services, special purpose flags, or other header information or identifying designators or characteristics associated with any Domestic Communication, including electronic mail headers showing From: and To: addresses; and
- (d) as to any mode of transmission (including mobile transmissions), and to the extent permitted by U.S. laws, any information indicating as closely as possible the physical location to or from which a Domestic Communication is transmitted.

The term includes all records or other information of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c) and (d) but does not include the content of any communication. The phrase “on behalf of” as used in this Section does not include entities with which Inmarsat has contracted for peering, interconnection, roaming, long distance, or resale of BGAN Service.

1.27 “United States,” “US” or “U.S.” means the United States of America, including all of its States, districts, territories, possessions, commonwealths, and the special maritime and territorial jurisdiction of the United States.

1.28 “U.S. LES” means a land earth station facility, located in any state of the United States, that is involved with the transmission of satellite communications and meets all other applicable requirements of this Agreement.

1.29 “U.S.-Licensed MES” means an MES licensed by the FCC to Inmarsat or Inmarsat’s distributors and utilizing the Inmarsat network, including to provide Inmarsat services.

1.30 “U.S. POP” or “POP” means a point of presence located in the United States through which communications are routed for purpose of switching and at which Electronic Surveillance can be conducted, and meeting all other applicable requirements of this Agreement.

1.31 “Wire Communication” has the meaning given it in 18 U.S.C. § 2510(1).

1.32 “Inmarsat” means Inmarsat Global Limited, a company organized under the laws of England and Wales and headquartered in London, England, and all of its Affiliates and subsidiaries.

1.33 Other Definitional Provisions. Other capitalized terms used in this Agreement and not defined in this Article 1 shall have the meanings assigned them elsewhere in this Agreement. The definitions in this Agreement are applicable to the singular as well as the plural forms of such terms and to the masculine as well as to the feminine and neuter genders of such terms. Whenever the words “include,” “includes,” “including,” or “such as” are used in this Agreement, they shall be deemed to be followed by the words “without limitation.”

## **ARTICLE 2: INFORMATION STORAGE AND ACCESS**

2.1 Implementation Plan. Certain of the rights and obligations of the Parties are set forth in further detail in an Implementation Plan dated \_\_\_\_\_, 2008 which is executed by all of the Parties and is hereby expressly incorporated in, and constitutes an integral part of, this Agreement. Wherever the term “Agreement” appears herein, it shall also be deemed to refer to and include the Implementation Plan.

2.2 Domestic Communications Infrastructure. Except to the extent and under conditions concurred in by the Government Parties in writing:

- (a) Point of Presence. Inmarsat will ensure as specified in the Implementation Plan that transmitted Domestic Communications, and Call Associated Data, and Transactional Data related to Domestic Communications that are carried by or on behalf of Inmarsat are transmitted to or through a U.S. POP, at which Electronic Surveillance can be conducted pursuant to Lawful U.S. Process. Inmarsat will ensure that Inmarsat and/or its Outsourcing Contractor provides technical or other assistance to facilitate such Electronic Surveillance.
- (b) Communications of a Non U.S.-Licensed MES. Inmarsat shall configure its network such that pursuant to Lawful U.S. Process, Electronic Surveillance of a Non U.S.-Licensed MES can be conducted in accordance with the Implementation Plan.

2.3 Compliance with Lawful U.S. Process. Inmarsat employees or agents in the United States, including the Outsourcing Contractor, shall have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with Lawful U.S. Process. Such employees or agents will further have such authority with regard to the following, as applicable:

- (a) the orders of the President in the exercise of his/her authority under § 706 of the Communications Act of 1934, as amended, (47 U.S.C. § 606), and under § 302(e) of the Aviation Act of 1958 (49 U.S.C. § 40107(b)) and Executive Order 11161 (as amended by Executive Order 11382); and

- (b) National Security and Emergency Preparedness rules, regulations and orders issued pursuant to the Communications Act of 1934, as amended (47 U.S.C. § 151 *et seq.*).

2.4 Information Storage and Access. Inmarsat shall make the following data and communications, if stored by or on behalf of Inmarsat for any reason, available in the United States:

- (a) Domestic Communications;
- (b) any Wire Communications or Electronic Communications received by, intended to be received by, or stored in the account associated with a U.S.-Licensed MES, or transmitted through a U.S. LES, or routed through a U.S. POP to or from a customer or subscriber of Inmarsat;
- (c) Transactional Data and Call Associated Data relating to Domestic Communications;
- (d) Subscriber Information concerning the customers and subscribers of services using U.S.-Licensed MESs, or who are known to be domiciled or holding themselves out as being domiciled in the United States, as well as Subscriber Information related to any Domestic Communication transmitted through a U.S. LES or routed through a U.S. POP; and
- (e) Billing records relating to customers and subscribers of services using U.S. Licensed MESs, or customers and subscribers who are known to be domiciled or are holding themselves out as being domiciled in the United States, as well as billing records related to any Domestic Communication transmitted through a U.S. LES or routed through a U.S. POP, for so long as such records are kept, in the event that Inmarsat has or otherwise maintains any such billing records.

The phrase “on behalf of” as used in this Section does not include entities with which Inmarsat has contracted for peering, interconnection, roaming, long distance, resale, or distribution of BGAN Service.

2.5 Restriction on Storage Outside the U.S. Inmarsat shall ensure that the data and communications described in Section 2.4 of this Agreement are not stored outside of the United States unless:

- (a) such storage is based strictly on *bona fide* commercial reasons weighing against storage in the United States; and
- (b) the required notice has been given to the Government Parties pursuant to Section 5.9 of this Agreement.

2.6 Avoidance of Mandatory Destruction. Inmarsat shall ensure that the data and communications described in Section 2.4 of this Agreement are stored in a manner not subject to mandatory destruction under any foreign laws, if such data and communications are stored by or on behalf of Inmarsat for any reason.

2.7 Billing Records. To the extent that any billing records are generated or maintained by Inmarsat relating to customers and subscribers of services using U.S. Licensed MESs, Inmarsat shall store all such billing records for at least eighteen (18) months and shall make such records available in the United States.

2.8 Storage Pursuant to 18 U.S.C. § 2703(f). Upon a request made pursuant to 18 U.S.C. § 2703(f) by a Governmental Authority within the United States to preserve any information in the possession, custody, or control of Inmarsat, including any information that is listed in Section 2.4 above, Inmarsat shall store such preserved records or other evidence in the United States.

2.9 Compliance with U.S. Law. Nothing in this Agreement shall excuse Inmarsat from its obligation to comply with U.S. legal requirements, including those requiring the retention, preservation, or production of information, records, or data, those not to unlawfully intercept telecommunications or unlawfully access stored telecommunications, Chapters 119 and 121 of Title 18, United States Code, and the requirements of the Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001, *et seq.*

2.10 Customer Proprietary Network Information. With respect to Domestic Communications, Inmarsat shall comply with all applicable FCC rules and regulations governing access to and storage of Customer Proprietary Network Information (“CPNI”), as defined in 47 U.S.C. § 222(h)(1).

2.11 Storage of Protected Information. The storage of Classified and Sensitive Information by Inmarsat or its Affiliates shall be at an appropriately secure location in the United States or other secure location within the offices of a U.S. military facility, a U.S. Embassy or Consulate or other U.S. Government Authority.

### **ARTICLE 3: SECURITY**

3.1 Measures to Prevent Improper Use or Access. Inmarsat shall take all practicable measures to prevent the use of or access to Inmarsat’s equipment or facilities to conduct Electronic Surveillance of Domestic Communications, or to obtain or disclose Domestic Communications, Classified Information, or Sensitive Information, in violation of any U.S. federal, state, or local laws or the terms of this Agreement. These measures shall include creating and complying with any policies and procedures as required by 47 C.F.R. § 1.20003, as applicable, and other appropriate written technical, organizational, and personnel-related policies and procedures, implementation plans, and physical security measures.

3.2 Disclosure of, or Access to, Domestic Communications and Information by Foreign Individuals, Entities, or Governments. Inmarsat shall not, directly or indirectly, disclose, permit disclosure of, or provide access to Domestic Communications, or Call Associated Data, Transactional Data, or Subscriber Information related to Domestic Communications to any Foreign individual (other than Inmarsat employees with a need to know) or entity, or Foreign Governmental Authority, or to any person in response to the legal process or request by a Foreign individual or entity, or Foreign Governmental Authority, without first satisfying all applicable U.S. legal requirements, and obtaining the express written consent of the Government Parties or the authorization of a court of competent jurisdiction in the United States, provided that Inmarsat may

respond to legal process issued by Foreign Governmental Authority without obtaining such consent or court authorization after determining that such response would not be prohibited by applicable U.S. law, and making the notification to the Government Parties required herein. Any such requests or submission of legal process shall be reported to the Government Parties no later than five (5) business days after its is received by Inmarsat. Inmarsat shall take reasonable measures to ensure that it will promptly learn of all such requests or submission of legal process.

3.3 Disclosure of, or Access to, Certain Other Information by Foreign Individuals, Entities, or Governments. Inmarsat shall not, directly or indirectly, disclose or permit disclosure of, or provide access to:

- (a) Classified or Sensitive Information;
- (b) Subscriber Information, Transactional Data, Call Associated Data, or a copy of any Wire or Electronic Communications, intercepted or acquired pursuant to Lawful U.S. Process; or
- (c) the existence of Lawful U.S. Process that is not already a matter of public record;

to any Foreign individual (other than Inmarsat employees who are authorized and have a need to know) or entity, or Foreign Governmental Authority, or to any person in response to the legal process or request by a Foreign individual or entity, or Foreign Governmental Authority, without first satisfying all applicable U.S. legal requirements, and obtaining the express written consent of the Government Parties or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process shall be reported to the Government Parties no later than five (5) business days after its is received by Inmarsat. Inmarsat shall take reasonable measures to ensure that it will promptly learn of all such requests or submission of legal process.

3.4 Points of Contact. Within five (5) business days after the Effective Date, Inmarsat shall designate points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process. The points of contact shall be assigned to an office of Inmarsat or its Outsourcing Contractor in the U.S., shall be available twenty-four (24) hours per day, seven (7) days per week, and shall be responsible for accepting service for Inmarsat and for maintaining the security of Sensitive and Classified Information and any Lawful U.S. Process. Inmarsat shall immediately notify the Government Parties in writing of the points of contact, and thereafter shall promptly notify the Government Parties of any change in such designation. The points of contact shall be resident U.S. citizens who are reasonably believed by Inmarsat to be eligible for appropriate U.S. security clearances. Inmarsat and its Outsourcing Contractor as applicable shall cooperate with any request by a U.S. Governmental Authority that a background check and/or security clearance process be completed for a designated point of contact.

3.5 Security of Lawful U.S. Process, Classified and Sensitive Information. Inmarsat shall ensure that its Outsourcing Contractor protects the confidentiality and security of all Lawful U.S. Process, Classified and Sensitive Information in accordance with U.S. Federal and state law or regulation.



Inmarsat shall ensure that knowledge of the existence of any Lawful U.S. Process served upon Inmarsat's Outsourcing Contractor is limited to those individuals who are authorized to know and whose assistance is strictly necessary to ensure compliance. Inmarsat's Outsourcing Contractor shall maintain a list of the names, dates and places of birth, and current addresses of each such individual and the list shall include but not be limited to any technicians assisting in the implementation of Electronic Surveillance. Inmarsat's Outsourcing Contractor shall make the list available upon request to any law enforcement agency or officer seeking compliance with Lawful U.S. Process.

3.6 Information Security Plan. Inmarsat shall form and implement an Information Security Plan, which shall include provisions for the following:

- (a) Take appropriate measures to prevent unauthorized access to data or facilities that might contain Classified or Sensitive Information;
- (b) Assign U.S. citizens, who meet high standards of trustworthiness for maintaining the confidentiality of Sensitive Information, to positions that handle or regularly deal with information identifiable to such person as Sensitive Information;
- (c) Upon request from the Government Parties, provide the name and any other identifying information requested for each person who handles or regularly deals with Sensitive Information;
- (d) Require that personnel handling Classified Information, if any, shall have been granted appropriate U.S. security clearances; and
- (e) Provide that the points of contact described in Section 3.4 shall have sufficient authority over any of Inmarsat's employees who may handle Classified or Sensitive Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority and the terms of this Agreement;

3.7 Nondisclosure of Protected Data. Inmarsat shall not directly or indirectly disclose information concerning Lawful U.S. Process, Classified Information, or Sensitive Information to any third party, or officer, director, shareholder, employee, agent, or Contractor of Inmarsat (other than the Outsourcing Contractor when authorized and there is a need to know), including those who serve in a supervisory, managerial or officer role with respect to the employees working with the information, unless disclosure has been approved by prior written consent obtained from the Government Parties, or there is an official need for disclosure of the information in order to fulfill an obligation consistent with the purpose for which the information is collected or maintained and the disclosure has been approved by the entity that provided the information to Inmarsat. Any such disclosure shall be in strict compliance with Section 3.5 of this Agreement.

3.8 Written Notice of Obligations. By a written statement, Inmarsat shall instruct all appropriate officials, employees, contractors, and agents of Inmarsat as to the obligations of this Agreement, including the individuals' duty to report any violation of this Agreement and the reporting requirements in Sections 5.2, 5.5, and 5.8 of this Agreement, and shall issue periodic reminders to

them of such obligations. The written statement shall set forth in a clear and prominent manner the contact information for a senior manager to whom such information may be reported, and shall also state that Inmarsat will not discriminate against, or otherwise take adverse action against, anyone who reports such information to management or the United States government.

3.9 Access to Classified or Sensitive Information. Nothing contained in this Agreement shall limit or affect the authority of a U.S. Government Authority to deny, limit, or revoke whatever access Inmarsat might have to Classified or Sensitive Information under that Government Authority's jurisdiction.

#### **ARTICLE 4: DISPUTES**

4.1 Informal Resolution. The Parties shall use their best efforts to resolve any disagreements that may arise under this Agreement. Disagreements shall be addressed, in the first instance, at the staff level by the Parties' designated representatives. Any disagreement that has not been resolved at that level shall be submitted promptly to higher authorized officials, unless any of the Government Parties believes that important national interests can be protected, or Inmarsat believes that its paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 4.2. If, after meeting with higher authorized officials, any of the Parties determines that further negotiation would be fruitless, then that Party may resort to the remedies set forth in Section 4.2. If resolution of a disagreement requires access to Classified Information, the Parties shall designate a person or persons possessing the appropriate security clearances for the purpose of resolving that disagreement.

4.2 Enforcement of Agreement. Subject to Section 4.1 of this Agreement, if any Party believes that any other Party has breached or is about to breach this Agreement, that Party may bring an action against the other Party for appropriate judicial relief. Nothing in this Agreement shall limit or affect the right of a U.S. Government Authority to:

- (a) require that the Party or Parties believed to have breached, or about to breach, this Agreement cure such breach within thirty (30) days, or whatever shorter time period is appropriate under the circumstances, upon receiving written notice of such breach;
- (b) request that the FCC modify, condition, revoke, cancel, or render null and void any license, permit, or other authorization granted or given by the FCC to Inmarsat, request that the FCC take other action, or request that the FCC impose any other appropriate sanction, including but not limited to a forfeiture or other monetary penalty, against Inmarsat;
- (c) seek civil sanctions for any violation of any U.S. law or regulation or term of this Agreement; or
- (d) pursue criminal sanctions against Inmarsat or any of their respective directors, officers, employees, representatives or agents, or against any other person or entity, for violations of the criminal laws of the United States; or

- (e) seek suspension or debarment of Inmarsat from eligibility for contracting with the U.S. Government.

4.3 Irreparable Injury. Inmarsat agrees that the United States would suffer irreparable injury if for any reason Inmarsat failed to perform any of its obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, Inmarsat agrees that, in seeking to enforce this Agreement, the U.S. Parties shall be entitled, in addition to any other remedy available at law or equity, to specific performance and injunctive or other equitable relief.

4.4 Waiver. The availability of any civil remedy under this Agreement shall not prejudice the exercise of any other civil remedy under this Agreement or under any provision of law, nor shall any action taken by a Party in the exercise of any remedy be considered a waiver by that Party of any other rights or remedies. The failure of any Party to insist on strict performance of any of the provisions of this Agreement, or to exercise any right they grant, shall not be construed as a relinquishment or future waiver; rather, the provision or right shall continue in full force. No waiver by any Party of any provision or right shall be valid unless it is in writing and signed by the Party.

4.5 Waiver of Immunity. Inmarsat agrees that, to the extent that it or any of its property (including FCC licenses and authorizations and intangible property) is or becomes entitled at any time to any immunity on the ground of sovereignty or otherwise based upon a status as an agency or instrumentality of government from any legal action, suit, or proceeding or from setoff or counterclaim relating to this Agreement, from the jurisdiction of any competent court or the FCC, from service of process, from attachment prior to judgment, from attachment in aid of execution of a judgment, from execution pursuant to a judgment or arbitral award, or from any other legal process in any jurisdiction, it, for itself and its property expressly, irrevocably and unconditionally waives, and agrees not to plead or claim, any such immunity with respect to matters arising with respect to this Agreement or the obligations herein (including any obligation for the payment of money) in any proceeding brought by a U.S. federal, state or local Government Authority. Inmarsat agrees that the waiver in this provision is irrevocable and is not subject to withdrawal in any jurisdiction or under any statute, including the Foreign Sovereign Immunities Act, 28 U.S.C. § 1602 *et seq.* The foregoing waiver shall constitute a present waiver of immunity at any time any action is initiated by a U.S. federal, state or local Government Authority against Inmarsat with respect to compliance with this Agreement.

4.6 Forum Selection. Any civil action among the Parties for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement shall be brought, if at all, in the United States District Court for the District of Columbia.

4.7 Effectiveness of Article 4. This Article 4, and the obligations imposed and rights conferred herein, shall become effective upon the execution of this Agreement by all the Parties.

## **ARTICLE 5: REPORTING AND NOTICE**

5.1 Filings Concerning *de jure* or *de facto* control of Inmarsat. If Inmarsat makes any filing with the FCC or any other U.S. Government Authority relating to the *de jure* or *de facto* control of Inmarsat,

except for filings with the FCC for assignments or transfers of control that are *pro forma*, Inmarsat shall promptly provide to the Government Parties written notice and copies of such filing. This Section 5.1 shall become effective upon execution of this Agreement by all the Parties.

5.2 Change in Control. If any member of the management of Inmarsat (including officers and members of the Board of Directors) acquires any information that reasonably indicates that any single Foreign entity or individual, Foreign Governmental Authority, or Foreign Governmental Authority-controlled entity – other than those already identified to the Government Parties – has or will likely obtain an ownership interest (direct or indirect) in Inmarsat of more than 10 percent, as determined in accordance with 47 C.F.R. § 63.09, or if any Foreign entity or individual, Foreign Governmental Authority, or Foreign Governmental Authority-controlled entity singly or in combination with other Foreign entities or individuals, Foreign Governmental Authority(ies), or Foreign Governmental Authority-controlled entities has or will likely otherwise gain either (1) Control or (2) *de facto* or *de jure* control of Inmarsat, then such Director, officer or manager shall promptly cause Inmarsat to notify the Government Parties in writing within ten (10) calendar days. Notice under this Section 5.2 shall, at a minimum, if such information is known or reasonably available:

- (a) identify the Foreign entity or individual(s), Foreign Governmental Authority, or Foreign Governmental Authority-controlled entity (specifying the name, addresses and telephone numbers);
- (b) identify the beneficial owners of the increased or prospective increased interest in Inmarsat by the Foreign entity or individual(s), Foreign Governmental Authority, or Foreign Governmental Authority-controlled entity (specifying the name, addresses and telephone numbers of each beneficial owner); and
- (c) quantify the amount of ownership interest that the Foreign entity or individual(s), Foreign Governmental Authority, or Foreign Governmental Authority-controlled entity has or will likely obtain in Inmarsat and, if applicable, the basis for its prospective Control of Inmarsat.

5.3 Joint Ventures. In the event that Inmarsat enters into joint ventures or other arrangements under which the joint venture or another entity may provide Domestic Communications:

- (a) if Inmarsat has the power or authority to exercise *de facto* or *de jure* control over such joint venture or entity, then Inmarsat will require the entity to fully comply with the terms of this Agreement; or
- (b) if Inmarsat does not have *de facto* or *de jure* control over such joint venture or entity, the provisions of Section 5.4, Outsourcing Contracts, shall apply as if the joint venture or other arrangement was an Outsourcing Contract.

5.4 Outsourcing Contracts. Inmarsat shall ensure the following with regard to any Outsourcing Contracts, including any contracts for the resale or distribution of BGAN Service:

- (a) Inmarsat shall include written provisions in any Outsourcing Contract that require the contractor to comply with all applicable terms of this Agreement and the Implementation Plan, or shall take other reasonable, good-faith measures to ensure that the contractor is aware of, agrees to, and is bound to comply with all such terms.
- (b) Inmarsat shall not enter into any Outsourcing Contract that affords the contractor access to Sensitive Information, unless such access has been lawfully approved by the entity that provided the information.
- (c) Inmarsat shall not induce the contractor either to violate its obligations to Inmarsat related to this Agreement or the Implementation Plan, or to take any action that, if taken by Inmarsat, would violate this Agreement.
- (d) If Inmarsat receives any information that a contractor or any of its employees or agents has taken an action that, had it been taken by Inmarsat, would violate a provision of this Agreement or the Implementation Plan, or has violated its obligations to Inmarsat related to this Agreement or the Implementation Plan, Inmarsat (1) will notify the Government Parties promptly, and (2) in consultation and cooperation with them, will take all reasonable steps necessary to rectify promptly the situation, including terminating the Outsourcing Contract (with or without notice and opportunity for cure) or initiating and pursuing litigation or other remedies at law and equity.
- (e) Neither an Outsourcing Contract nor any provision of this Section 5.4 does nor shall it be construed to relieve Inmarsat of any of its obligations under this Agreement or the Implementation Plan.

5.5 Notice of Foreign Influence. If Inmarsat or its agents (including officers and members of the Board of Directors) acquires any information that reasonably indicates that any Foreign entity or individual, Foreign Governmental Authority, or Foreign Governmental Authority-controlled entity plans to participate or has participated in any aspect of the day-to-day management of Inmarsat or to exercise any Control of Inmarsat in such a way that (1) interferes with or impedes the performance by Inmarsat of its duties and obligations under the terms of this Agreement; (2) interferes with or impedes the exercise by Inmarsat of its rights under the Agreement; or (3) raises a concern with respect to the fulfillment by Inmarsat of its obligations under this Agreement, then such manager shall promptly notify the Government Parties in writing of the timing and the nature of the Foreign entity's or individual's, Foreign Governmental Authority's, or Foreign Governmental Authority-controlled entity's plans or actions.

5.6 Procedure and Process on Reporting. Within thirty (30) days of the Effective Date, Inmarsat shall adopt and distribute to all officers and directors, a written procedure or process for the reporting by officers and directors of noncompliance with this Agreement or the Implementation Plan, which shall incorporate the notice of reporting obligations by officials, employees, agents and contractors required under Section 3.8 of this Agreement. Any violation by Inmarsat of any material term of such corporate policy shall constitute a breach of this Agreement.

5.7 Non-retaliation. Within thirty (30) days of the Effective Date, Inmarsat shall, by duly authorized action of its Board of Directors, adopt and distribute to all officers and directors an official corporate policy that strictly prohibits Inmarsat from discriminating or taking any adverse action against any officer, director, employee, contractor, or agent because he or she has in good faith initiated or attempted to initiate a notice or report under Sections 5.2, 5.5, or 5.8 of this Agreement, or has notified or attempted to notify the management to report information that he or she believes in good faith is required to be reported to the Government Parties under either Sections 5.2, 5.5, or 5.8 of this Agreement or under Inmarsat's written notice to employees on the reporting of any such information. Any violation by Inmarsat of any material term of such corporate policy shall constitute a breach of this Agreement.

5.8 Reporting of Incidents. Inmarsat shall report to the Government Parties any information acquired by Inmarsat or any of its officers, directors, employees, contractors, or agents that reasonably indicates:

- (a) a breach of this Agreement;
- (b) access to or disclosure of Domestic Communications, or the conduct of Electronic Surveillance, in violation of federal, state or local law or regulation;
- (c) access to or disclosure of CPNI, Call-Associated Data, Transactional Data, or Subscriber Information, in violation of federal, state or local law or regulation; or
- (d) improper access to or disclosure of Classified or Sensitive Information.

This report shall be made in writing by the appropriate Inmarsat officer to the Government Parties no later than ten (10) calendar days after Inmarsat acquires information indicating a matter described in this Section. Inmarsat shall lawfully cooperate in investigating the matters described in this Section. Inmarsat need not report information where disclosure of such information would be in violation of an order of a court of competent jurisdiction in the United States.

5.9 Notice of Decision to Store Information Outside of the United States. Inmarsat shall provide to the Government Parties thirty (30) days advanced notice if it plans to store or have stored on its behalf outside the United States any of the information specified in Section 2.4 herein. Such notice shall, at a minimum:

- (a) include a description of the type of information to be stored outside the United States;
- (b) identify the custodian of the information, if other than Inmarsat;
- (c) identify the location where the information is to be located; and
- (d) identify the factors considered, pursuant to Section 2.5 of this Agreement, in deciding to store the information outside of the United States.

5.10 Access to Information and Facilities.

(a) The Government Parties or their designees may visit any part of Inmarsat's Domestic Communications Infrastructure to conduct on-site reviews concerning the implementation of the terms of this Agreement, and Inmarsat will provide unimpeded access for such on-site reviews.

(b) Inmarsat will voluntarily provide prompt and unimpeded access to and disclosure of all records and information concerning technical, physical, management, or other security measures, as needed by the Government Parties or their designees to verify compliance with the terms of this Agreement including the Implementation Plan.

5.11 Access to Personnel. Upon reasonable notice from the Government Parties or their designees, Inmarsat shall make available for interview any officers or employees of Inmarsat and any contractors located in the United States, who are in a position to provide information to verify compliance with the terms of this Agreement.

5.12 Annual Report. On or before the last day of January of each year, a designated senior corporate officer of Inmarsat shall submit to the Government Parties a report assessing Inmarsat's compliance with the terms of this Agreement for the preceding calendar year (or since the Effective Date in the case of the first such report). The report shall include:

- (a) a copy of the then-current policies and procedures adopted to comply with this Agreement;
- (b) a summary of the changes, if any, to the policies or procedures, and the reasons for those changes;
- (c) a summary of any known acts of noncompliance with the terms of this Agreement, whether inadvertent or intentional, with a discussion of what steps have been or will be taken to prevent such acts from occurring in the future; and
- (d) identification of any other issues that, to Inmarsat's knowledge, will or reasonably could affect the effectiveness of or its compliance with this Agreement.

5.13 Notices. Effective upon execution of this Agreement by all the Parties, all notices and other communications relating to this Agreement, such as a proposed modification, shall be in writing and shall be deemed given as of the date of receipt and shall be sent by electronic mail (if an email is specified below or in a subsequent notice) and one of the following methods:

(a) delivered personally, (b) sent by facsimile, (c) sent by documented overnight courier service, or (d) sent by registered or certified mail, postage prepaid, addressed to the Parties' designated representatives at the addresses shown below, unless provided otherwise in this Agreement; provided, however, that upon written notification to the Parties, a Party may unilaterally amend or modify its designated representative information, notwithstanding any provision to the contrary in Section 8.6 of this Agreement:

Department of Justice  
Assistant Attorney General for National Security  
National Security Division

950 Pennsylvania Avenue, NW  
Washington, DC 20530

Department of Homeland Security  
Assistant Secretary for Policy  
3801 Nebraska Avenue, N.W.  
Washington, D.C. 20528

Note: All notices and other communications shall, in addition to the foregoing methods of delivery, be sent by email to [ip-fcc@dhs.gov](mailto:ip-fcc@dhs.gov) and/or such other email account as DHS may designate in the future.

Diane Cornell  
Vice President, Government Affairs  
Inmarsat  
1101 Connecticut Avenue, N.W.  
Suite 1200  
Washington, D.C.20036

## **ARTICLE 6: CONFIDENTIALITY; USE OF INFORMATION**

6.1 Confidentiality. The Government Parties shall take all measures required by law to protect from public disclosure all information submitted by Inmarsat (or other entities in accordance with the terms of this Agreement including the Implementation Plan) to them in connection with this Agreement and clearly marked with the legend “Business Confidential; subject to protection under 5 U.S.C. § 553(b)” or similar designation. Such markings shall signify that it is the company’s position that the information so marked constitutes “trade secrets” and/or “commercial or financial information obtained from a person and privileged or confidential,” or otherwise warrants protection within the meaning of 5 U.S.C. § 552(b)(4). For the purposes of 5 U.S.C. § 552(b)(4), the Parties agree that information so marked is voluntarily submitted. If a request is made under 5 U.S.C. §552(a)(3) for information so marked, and disclosure of any information (including disclosure in redacted form) is contemplated, Inmarsat shall be provided with the notices and procedures required by law, including those specified in Executive Order 12600, 52 Fed. Reg. 23781 (June 25, 1987)).

6.2 Use of Information by U.S. Government for Any Lawful Purpose. Nothing in this Agreement shall prevent the Government Parties or any other U.S. Governmental Authority from lawfully disseminating this Agreement or using any information produced under or otherwise related to this Agreement to seek enforcement of this Agreement, or for any other lawful purpose.

## **ARTICLE 7: FCC CONDITION**

7.1 FCC Approval. Upon the execution of this Agreement, including the Implementation Plan, by all of the Parties, Inmarsat shall request that the FCC adopt a condition to Inmarsat’s existing



or pending FCC authorizations, substantially the same as set forth in Exhibit A attached hereto (the “Condition to FCC Authorization”).

7.2 Right to Object to Future FCC Filings. Inmarsat agrees that in any application or petition by Inmarsat, filed with or granted by the FCC after the execution of this Agreement by all the Parties, for a license or other authority under Titles II and III of the Communications Act of 1934, as amended, to provide service to or operate MESs in the United States for communications utilizing the Inmarsat system, or to offer, distribute, or resell Domestic Communications in the United States for communications utilizing the Inmarsat system, Inmarsat shall request that the FCC condition the grant of such licensing or other authority on compliance with the terms of this Agreement, as amended if necessary. Notwithstanding Section 8.9, nothing in this Agreement shall preclude the Government Parties or any other U.S. Governmental Authority from opposing, formally or informally, any FCC application or petition by Inmarsat for other authority, or to transfer its license(s) to a third party (except with respect to *pro forma* assignments or *pro forma* transfers of control), and to seek additional or different terms that would, consistent with the public interest, address any concerns regarding the ability of the United States to enforce the laws, preserve the national security, and protect the public safety, raised by the services and transactions underlying any such application or petition.

## ARTICLE 8: OTHER

8.1 Right to Make and Perform Agreement. Inmarsat represents that it has and shall continue to have throughout the term of this Agreement the full right to enter into this Agreement and perform its obligations hereunder and that this Agreement is a legal, valid, and binding obligation of Inmarsat enforceable in accordance with its terms.

8.2 Headings. The article and section headings and numbering in this Agreement are inserted for convenience only and shall not affect the meaning or interpretation of the terms of this Agreement.

8.3 Other Laws. Nothing in this Agreement is intended to limit or constitute a waiver of (a) any obligations imposed by any U.S. federal, state, or local law or regulation on Inmarsat, (b) any enforcement authority available under any U.S. federal, state, or local law or regulation, (c) the sovereign immunity of the United States, or (d) any authority the U.S. Government may possess over the activities or facilities if Inmarsat located within or outside the United States (including authority pursuant to the International Emergency Economic Powers Act). Nothing in this Agreement is intended to or is to be interpreted to require the Parties to violate any applicable U.S. law.

8.4 Statutory References. All references in this Agreement to statutory provisions and executive orders shall include any future amendments to such statutory provisions and executive orders.

8.5 Non-Parties. Nothing in this Agreement is intended to confer or does confer any rights on any person other than the Parties and any Government Authorities entitled to effect Electronic Surveillance pursuant to Lawful U.S. Process.

8.6 Modification. This Agreement may only be modified by written agreement signed by all of the Parties, provided that the Government Parties may, by a written notice to Inmarsat signed by all of

them, waive any provision of this Agreement intended for their benefit unless such waiver is objected to by Inmarsat. The Government Parties agree to consider promptly and in good faith possible modifications to this Agreement if Inmarsat believes that the obligations imposed on it under this Agreement are substantially more restrictive than those imposed on other U.S. and foreign licensed service providers in like circumstances in order to protect U.S. national security, law enforcement, and public safety concerns. Any substantial modification to this Agreement shall be reported to the FCC within thirty (30) days after approval in writing by the Parties.

8.7 Severability. The provisions of this Agreement shall be severable and if any provision thereof or the application of such provision under any circumstances is held invalid by a court of competent jurisdiction, it shall not affect any other provision of this Agreement or the application of any provision thereof.

8.8 Changes in Circumstances for Inmarsat. The Government Parties agree to negotiate in good faith and promptly with respect to any request by Inmarsat for relief from application of specific provisions of this Agreement if those provisions become unduly burdensome or have an adverse affect on Inmarsat's competitive position.

8.9 Changes in Circumstances for the Government Parties. If after the date that all the Parties have executed this Agreement, the Government Parties find that the terms of this Agreement are inadequate to address national security, law enforcement, or public safety concerns, then Inmarsat will negotiate in good faith to modify this Agreement to address those concerns.

8.10 Counterparts. This Agreement may be executed in one or more counterparts, including by facsimile, each of which shall together constitute one and the same instrument.

8.11 Successors and Assigns: This Agreement shall inure to the benefit of, and shall be binding upon, the Parties, and their respective successors and assigns. This Agreement shall also be binding on all subsidiaries, divisions, departments, branches, and other components or agents of Inmarsat, and on all Affiliates of Inmarsat.

8.12 Effectiveness of Article 8. This Article 8, and the obligations imposed and rights conferred herein, shall be effective upon execution of this Agreement by all the Parties.

8.13 Effectiveness of Agreement. Except as otherwise specifically provided elsewhere in this Agreement, the obligations imposed and rights conferred by this Agreement shall take effect upon the Effective Date.

8.14 [NOT USED]

8.15 Suspension of Agreement and Obligations Hereunder. This Agreement shall be suspended upon thirty (30) days notice to the Government Parties that neither Inmarsat, nor any transferee or assignee of the FCC licenses or authorizations held by Inmarsat, provides or facilitates Domestic Communications in the United States, unless any of the Government Parties, within that 30-day period, seeks additional information or objects to the suspension.

8.16 Termination of Agreement. This Agreement shall be terminated in its entirety upon the written determination of the Government Parties that Inmarsat has provided notice and reasonably satisfactory documentation that no foreign entity or combination of foreign entities (including one or more persons under common Control) either Controls Inmarsat or holds, directly or indirectly, a ten (10) percent or greater interest in Inmarsat, and that this Agreement is no longer necessary to in order to protect U.S. national security, law enforcement, or public safety concerns. It is expressly acknowledged that this Agreement shall not be terminated with respect to Inmarsat during such time as BGAN Service is provided or facilitated within the United States by Inmarsat via any facilities or equipment, including but not limited to any land earth station, located outside of the U.S. If this Agreement is not terminated pursuant to this provision, the Government Parties agree to consider promptly and in good faith possible modifications to this Agreement.

8.17 Notice of Additional Services. Inmarsat shall provide a minimum of thirty (30) days advanced notice to the Government Parties in the event that Inmarsat or any Affiliate changes or intends to change its present services with respect to Domestic Communications, as set forth in the Recitals to this Agreement, such that the material representations made therein are no longer fully accurate, true and complete. In no event will such notice relieve any Party to this Agreement of obligations under this Agreement or be construed as a waiver of any Party's rights under this Agreement.

This Agreement is executed on behalf of the Parties:

**Inmarsat**

Date: 9/23/08

By: Diane Cornell  
Printed Name: Diane Cornell  
Title: Vice President, Government Affairs

**United States Department of Justice**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Printed Name: J. Patrick Rowan  
Title: Acting Assistant Attorney General for National Security

**Department of Homeland Security**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Printed Name: Stewart A. Baker  
Title: Assistant Secretary for Policy

8.16 Termination of Agreement. This Agreement shall be terminated in its entirety upon the written determination of the Government Parties that Inmarsat has provided notice and reasonably satisfactory documentation that no foreign entity or combination of foreign entities (including one or more persons under common Control) either Controls Inmarsat or holds, directly or indirectly, a ten (10) percent or greater interest in Inmarsat, and that this Agreement is no longer necessary to in order to protect U.S. national security, law enforcement, or public safety concerns. It is expressly acknowledged that this Agreement shall not be terminated with respect to Inmarsat during such time as BGAN Service is provided or facilitated within the United States by Inmarsat via any facilities or equipment, including but not limited to any land earth station, located outside of the U.S. If this Agreement is not terminated pursuant to this provision, the Government Parties agree to consider promptly and in good faith possible modifications to this Agreement.

8.17 Notice of Additional Services. Inmarsat shall provide a minimum of thirty (30) days advanced notice to the Government Parties in the event that Inmarsat or any Affiliate changes or intends to change its present services with respect to Domestic Communications, as set forth in the Recitals to this Agreement, such that the material representations made therein are no longer fully accurate, true and complete. In no event will such notice relieve any Party to this Agreement of obligations under this Agreement or be construed as a waiver of any Party's rights under this Agreement.

This Agreement is executed on behalf of the Parties:

**Inmarsat**

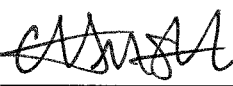
Date: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name: Diane Cornell  
Title: Vice President, Government Affairs

**United States Department of Justice**

Date: 9-17-08

By:  / c. Steele for JPR

Printed Name: J. Patrick Rowan  
Title: Acting Assistant Attorney General for National Security

**Department of Homeland Security**

Date: \_\_\_\_\_

By: \_\_\_\_\_

Printed Name: Stewart A. Baker  
Title: Assistant Secretary for Policy

8.16 Termination of Agreement. This Agreement shall be terminated in its entirety upon the written determination of the Government Parties that Inmarsat has provided notice and reasonably satisfactory documentation that no foreign entity or combination of foreign entities (including one or more persons under common Control) either Controls Inmarsat or holds, directly or indirectly, a ten (10) percent or greater interest in Inmarsat, and that this Agreement is no longer necessary to in order to protect U.S. national security, law enforcement, or public safety concerns. It is expressly acknowledged that this Agreement shall not be terminated with respect to Inmarsat during such time as BGAN Service is provided or facilitated within the United States by Inmarsat via any facilities or equipment, including but not limited to any land earth station, located outside of the U.S. If this Agreement is not terminated pursuant to this provision, the Government Parties agree to consider promptly and in good faith possible modifications to this Agreement.

8.17 Notice of Additional Services. Inmarsat shall provide a minimum of thirty (30) days advanced notice to the Government Parties in the event that Inmarsat or any Affiliate changes or intends to change its present services with respect to Domestic Communications, as set forth in the Recitals to this Agreement, such that the material representations made therein are no longer fully accurate, true and complete. In no event will such notice relieve any Party to this Agreement of obligations under this Agreement or be construed as a waiver of any Party's rights under this Agreement.

This Agreement is executed on behalf of the Parties:

**Inmarsat**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Printed Name: Diane Cornell  
Title: Vice President, Government Affairs


**United States Department of Justice**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Printed Name: J. Patrick Rowan  
Title: Acting Assistant Attorney General for National Security

**Department of Homeland Security**

Date: \_\_\_\_\_

By:  \_\_\_\_\_  
Printed Name: Stewart A. Baker  
Title: Assistant Secretary for Policy

**EXHIBIT A**  
**CONDITION TO FCC AUTHORIZATION**

IT IS FURTHER ORDERED, that this authorization and any licenses related thereto are subject to compliance with the provisions of the Agreement attached hereto between Inmarsat, on the one hand, and the Department of Justice (“DOJ”) and the Department of Homeland Security (“DHS”), on the other hand, dated \_\_\_\_\_, 2008, which Agreement is intended to enhance the protection of U.S. national security, law enforcement, and public safety. Nothing in this Agreement is intended to limit any obligation imposed by Federal law or regulation.

## **EXHIBIT B**

This Agreement is made this 7<sup>th</sup> day of August, 2001 by and between: MarineSat Communications Network, Inc. and Stratos Mobile Networks (USA) LLC (collectively, "Stratos"), and the U.S. Department of Justice ("DOJ") and the Federal Bureau of Investigation ("FBI") (collectively with all other parties hereto, "the Parties"). This Agreement is effective as of the date of last signature affixed hereto.

## RECITALS

WHEREAS, the U.S. telecommunications system is essential to the U.S. economy and to U.S. national security, law enforcement, and public safety;

WHEREAS, the U.S. government considers it critical to maintain the viability, integrity and security of the U.S. telecommunications system (*see, e.g.*, Presidential Decision Directive 63 on Critical Infrastructure Protection);

WHEREAS, the U.S. government considers it critical to ensure the confidentiality of its lawfully authorized surveillance and related activities, and to ensure the confidentiality of Classified, Controlled Unclassified, and Sensitive Information;

WHEREAS, Stratos currently provides service to Inmarsat mobile earth terminals ("METs") outside of the United States, and has filed with the Federal Communications Commission ("FCC") license applications under Sections 214 and 310(b) of the Communications Act of 1934, as amended, to provide service to METs inside the United States (*see Application Pursuant to Section 214 for Authority to Provide Domestic Land Mobile Services Using the Inmarsat Ltd. Satellite System*, File No. SES-MS-C-20010220-00349, *Applications for Blanket Licenses to Operate Mobile Earth Terminals with Non-U.S. Licensed Satellites*, File Nos. SES-LIC-20010221-00360; SES-LIC-20010221-00361; SES-LIC-20010221-00362; SES-LIC-20010221-00363, *Application for Section 214 Authority to Provide Inmarsat M4 Services*, File No. SES-MS-C-20000426-00861, and *Application for Blanket Authority to Operate Mobile Earth Terminals*, File No. SES-LIC-20000426-00630);

WHEREAS, MarineSat Communications Network, Inc. d/b/a Stratos Communications is 100 percent owned by Stratos Holdings, Inc., a Delaware holding corporation, which is in turn 100 percent owned by Stratos Global Corp., which has its principal place of business in Toronto, Ontario, Canada and is 65 percent indirectly owned by Aliant, Inc., a Canadian holding company with its principal place of business in Saint John, New Brunswick, Canada;

WHEREAS, Stratos Mobile Networks (USA) LLC is a Delaware-registered limited liability corporation 91 percent owned by TH Aeronautical Corp. ("THA") and 9 percent owned by IDB Mobile Communications, Inc., which is in turn 100 percent owned by THA. THA is 100 percent owned by Stratos Wireless, Inc., which has its principal place of business in Saint John's, Newfoundland, Canada and is in turn 100 percent owned by Stratos Global Corp., which has its principal place of business in Toronto, Ontario, Canada;



WHEREAS, Stratos has met with the FBI and DOJ to discuss the proposed services and the government's responsibilities concerning national security, law enforcement and public safety. In these meetings, Stratos advised: (a) that some of the Domestic Communications Infrastructure Stratos would employ (e.g., satellite gateway earth stations) to route Domestic Communications are located outside the United States; (b) that the Domestic Communications Infrastructure that is located outside the United States is located for *bona fide* commercial reasons; (c) that Stratos plans to route all Domestic Communications through a Point of Presence physically located in the United States, from which the government can conduct Electronic Surveillance pursuant to U.S. Lawful Process; and (d) that Stratos' Domestic Communications Infrastructure within the United States currently consists of the Nortel MMCS switch (and related trunking equipment) located in the Stratos facility at 5 Teleport Drive, Staten Island, New York, which is also Stratos' current Point of Presence within the United States;

NOW THEREFORE, the Parties are entering into this Agreement to address national security, law enforcement, and public safety concerns.

#### ARTICLE I: INFORMATION STORAGE AND ACCESS

- 1.1 Point of Presence: Pursuant to the Stratos Implementation Plan, Domestic Communications shall be routed through a Point of Presence, which is a network switch under the control of Stratos and is physically located in the United States, from which Electronic Surveillance can be conducted pursuant to Lawful U.S. Process. Stratos will provide technical or other assistance to facilitate such Electronic Surveillance.
- 1.2 Stratos Implementation Plan: Certain of the rights and obligations of the Parties are set forth in further detail in an Implementation Plan dated August 7, 2001, which is consistent with this Agreement. Stratos shall comply with the Implementation Plan, which may be amended from time to time pursuant to Section 7.7.
- 1.3 CPNI: Stratos shall comply with all applicable FCC rules and regulations governing access to and storage of Customer Proprietary Network Information ("CPNI"), as defined in 47 U.S.C. § 222(f)(1).
- 1.4 Compliance with Lawful U.S. Process: Stratos shall take all practicable steps to configure its Domestic Communications Infrastructure such that Stratos is capable of complying, and Stratos employees in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with Lawful U.S. Process, the orders of the President in the exercise of his/her authority under § 706 of the Communications Act of 1934, as amended (47 U.S.C. § 606), and under § 302(e) of the Aviation Act of 1958 (49 U.S.C. § 40107(b)) and Executive Order 11161 (as amended by Executive Order 11382), and National Security and Emergency Preparedness rules, regulations and orders issued pursuant to the Communications Act of 1934, as amended (47 U.S.C. § 151 *et seq.*).

- 1.5 Information Storage and Access: Stratos shall make available in the United States:
- (i) stored Domestic Communications, if such communications are stored by or on behalf of Stratos for any reason;
  - (ii) any Wire Communications or Electronic Communications (including any other type of wire, voice or electronic communication not covered by the definitions of Wire Communication or Electronic Communication) received by, intended to be received by, or stored in the account of a Stratos U.S.-Licensed MET, or routed to Stratos' Point of Presence in the United States and stored by or on behalf of Stratos for any reason;
  - (iii) Transactional Data and Call Associated Data relating to Domestic Communications, if such information is stored by or on behalf of Stratos for any reason (although all Parties recognize that Stratos currently does not store such information except as part of billing records);
  - (iv) billing records relating to Stratos customers or subscribers for its U.S. Licensed METs, Stratos customers and subscribers domiciled in the United States, or Stratos customers and subscribers who hold themselves out as being domiciled in the United States, as well as billing records related to any call routed through Stratos' Point of Presence in the United States, if such information is stored by or on behalf of Stratos for any reason, for so long as such records are kept pursuant to applicable U.S. law or this Agreement; and
  - (v) Subscriber Information concerning Stratos customers or subscribers for its U.S.-Licensed METs, Stratos customers or subscribers domiciled in the United States, or Stratos customers or subscribers who hold themselves out as being domiciled in the United States, as well as Subscriber Information related to any call routed through Stratos' Point of Presence in the United States, if such information is stored by or on behalf of Stratos for any reason.
- 1.6 Storage Pursuant to 18 U.S.C. § 2703(f): Upon a request made pursuant to 18 U.S.C. § 2703(f) by a governmental entity within the United States to preserve any of the information enumerated in Section 1.5, Stratos shall store such preserved records or other evidence in the United States.
- 1.7 Mandatory Destruction: Stratos shall take all practicable steps to store the data and communications described in Section 1.5 in a manner not subject to mandatory destruction under any foreign laws, if such data and communications are stored by or on behalf of Stratos for any reason. Except for strictly *bona fide* commercial reasons, such data and communications shall be stored in the United States.
- 1.8 Billing Records: Stratos shall store for at least eighteen (18) months all billing records maintained for a U.S.-Licensed MET.

- 1.9 Communications of a U.S.-Licensed MET: No communications of a U.S.-Licensed MET shall be routed outside the United States except for strictly *bona fide* commercial reasons.
- 1.10 Communications of a Non-U.S.-Licensed MET: Electronic Surveillance pursuant to Lawful U.S. Process of a Non-U.S.-Licensed MET shall be conducted pursuant to the Stratos Implementation Plan.
- 1.11 Domestic Communications Infrastructure: Except for strictly *bona fide* commercial reasons, Domestic Communications Infrastructure shall be located in the United States and shall be directed, controlled, supervised and managed by Stratos.
- 1.12 Compliance with U.S. Law: Nothing in this Agreement shall excuse Stratos from any obligation it may have to comply with U.S. legal requirements for the retention, preservation, or production of such information or data. Similarly, in any action to enforce Lawful U.S. Process, Stratos has not waived any legal right it might have to resist such process.

## ARTICLE II: NON-OBJECTION BY DOJ AND FBI TO GRANT OF LICENSES TO STRATOS

- 2.1 Non-Objection to Current Application: Upon the execution of this Agreement by all the Parties, the FBI and DOJ shall promptly notify the FCC that, provided the FCC adopts a condition substantially the same as set forth in Exhibit A attached hereto, the FBI and DOJ have no objection to the FCC's grant or approval of Stratos' applications (*Application Pursuant to Section 214 for Authority to Provide Domestic Land Mobile Services Using the Inmarsat Ltd. Satellite System*, File No. SES-MS-20010220-00349, *Applications for Blanket Licenses to Operate Mobile Earth Terminals with Non-U.S. Licensed Satellites*, File Nos. SES-LIC-20010221-00360; SES-LIC-20010221-00361; SES-LIC-20010221-00362; SES-LIC-20010221-00363, *Application for Section 214 Authority to Provide Inmarsat M4 Services*, File No. SES-MS-20000426-00861, *Application for Blanket Authority to Operate Mobile Earth Terminals*, File No. SES-LIC-20000426-00630, and *Application Pursuant to Section 214 for Authority to Provide Domestic Aeronautical Mobile Satellite Services via the Inmarsat System*, File No. ITC-214-19981214-00859).
- 2.2 Non-Objection to Future Applications: The FBI and DOJ agree not to object, formally or informally, to the grant of any other FCC application of Stratos for a license under Titles II and III of the Communications Act of 1934, as amended, to provide service to and operate METs in the United States for communications via the Inmarsat Space Segment, provided that such application makes clear that the terms and conditions of this Agreement and the Implementation Plan shall apply to any license issued pursuant to that application. Nothing in this Agreement shall preclude the DOJ or the FBI from opposing,

formally or informally, a FCC application by Stratos to transfer its license(s) to a third party.

### ARTICLE III: SECURITY OFFICE

- 3.1 Location of Security Office: Stratos shall maintain within the United States a security office. Stratos shall within the security office:
- (i) take appropriate measures to prevent unauthorized access to data or facilities that might contain Classified Information or Sensitive Information;
  - (ii) assign U.S. citizens, who meet high standards of trustworthiness for maintaining the confidentiality of Sensitive Information, to positions that handle or that regularly deal with information identifiable to such person as Sensitive Information;
  - (iii) upon request from the DOJ or FBI, provide the name, social security number, and date of birth of each person who regularly handles or deals with Sensitive Information;
  - (iv) require that personnel handling Classified Information shall have been granted appropriate security clearances;
  - (v) provide that the points of contact described in Section 3.6 shall have sufficient authority over any of Stratos' employees who may handle Classified Information or Sensitive Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority and the terms of this Agreement; and
  - (vi) maintain appropriately secure facilities (e.g., offices) for the handling and storage of any Classified Information and Sensitive Information.
- 3.2 Measures to Prevent Improper Use or Access: Stratos shall take reasonable measures to prevent the use of or access to Stratos' equipment or facilities to conduct Electronic Surveillance in violation of any U.S. federal, state, or local law or the terms of this Agreement. These measures shall take the form of technical, organizational, personnel-related policies and written procedures, necessary implementation plans, and physical security measures.
- 3.3 Access by Foreign Government Authorities: Stratos shall not provide access to Domestic Communications, Call Associated Data, Transactional Data, or Subscriber Information stored in the United States to any person, if the purpose of such access is to respond to the legal process or the request of or on behalf of a foreign government, identified representative, or a component or subdivision thereof, without the express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United

States. Any requests or submission of legal process described in this Section shall be reported to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received by Stratos, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. Stratos shall take reasonable measures to ensure that it will learn of all such requests or submission of legal process described in this Section.

3.4 Disclosure to Foreign Government Authorities: Stratos shall not, directly or indirectly, disclose or permit disclosure of, or provide access to:

(i) Classified or Sensitive Information, or

(ii) Subscriber Information, Transactional Data, Call Associated Data, or a copy of any Wire Communication or Electronic Communication intercepted or acquired pursuant to Lawful U.S. Process

to any foreign government or a component or subdivision thereof without satisfying all applicable U.S. federal, state and local legal requirements pertinent thereto, and obtaining the express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States. Stratos shall notify the DOJ of any requests or any legal process submitted to Stratos by a foreign government or a component or subdivision thereof for communications, data or information identified in this paragraph. Stratos shall provide such notice to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received by Stratos, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. Stratos shall take reasonable measures to ensure that it will learn of all such requests or submission of legal process described in this Section.

3.5 Notification of Access or Disclosure Requests: Stratos shall notify DOJ in writing of legal process or requests by foreign non-governmental entities for access to or disclosure of Domestic Communications unless the disclosure of the legal process or requests would be in violation of an order of a court of competent jurisdiction within the United States. Stratos shall provide such notice to the DOJ no later than ninety (90) days after such request or legal process is received by Stratos, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States.

3.6 Points of Contact: Within sixty (60) days after execution of this Agreement by all parties, Stratos shall designate points of contact within the United States with the authority and responsibility for accepting and overseeing compliance with Lawful U.S. Process. The points of contact will be available 24 hours per day, 7 days per week and shall be responsible for accepting service and maintaining the security of Classified Information and any Lawful U.S. Process for Electronic Surveillance in accordance with the requirements of U.S. law. Stratos will immediately notify in writing the DOJ and the

FBI of such designation, and thereafter shall promptly notify the FBI and DOJ of any change in that designation. The points of contact shall be resident U.S. citizens who are eligible for appropriate U.S. security clearances. If necessary to receive or handle Sensitive or Classified Information, Stratos shall cooperate with any request by a government entity within the United States that a background check and/or security clearance process be completed for a designated point of contact.

- 3.7 Security of Lawful Process: Stratos shall protect the confidentiality and security of all Lawful U.S. Process served upon it and the confidentiality and security of Classified Information and Sensitive Information in accordance with U.S. federal and state law or regulations.
- 3.8 Notice of Obligations: Stratos shall instruct appropriate officials, employees, contractors and agents as to their obligations under this Agreement and issue periodic reminders to them of such obligations.
- 3.9 Access to Classified or Sensitive Information: Nothing contained in this Agreement shall limit or affect the authority of a U.S. government agency to deny, limit or revoke Stratos' access to Classified and Sensitive Information under that agency's jurisdiction.
- 3.10 Reporting of Incidents: Stratos shall take practicable steps to ensure that, if any Stratos official, employee, contractor or agent acquires any information that reasonably indicates: (i) a breach of this Agreement; (ii) Electronic Surveillance conducted in violation of U.S. federal, state or local law or regulation; (iii) access to or disclosure of CPNI or Subscriber Information in violation of U.S. federal, state or local law or regulation (except for violations of FCC regulations relating to improper use of CPNI); or (iv) improper access to or disclosure of Classified Information or Sensitive Information, then Stratos shall notify the FBI and DOJ. This report shall be made promptly and in any event no later than ten (10) calendar days after Stratos acquires such information. Stratos shall lawfully cooperate in investigating the matters described in this Section. Stratos need not report information where disclosure of such information would be in violation of an order of a court of competent jurisdiction within the United States. This Section is effective thirty (30) calendar days after execution of this Agreement by all Parties.
- 3.11 Notice of Decision to Store Information Outside the United States: Stratos shall provide to the FBI and DOJ thirty (30) calendar days advance notice if Stratos (or any entity with which Stratos has contracted or made other arrangements for data or communications processing or storage) plans to store outside of the United States Domestic Communications, Transactional Data, Call Associated Data, or Subscriber Information that was previously stored within the United States. Such notice shall, at a minimum, (a) include a description of the type of information to be stored outside the United States, (b) identify the custodian of the information if other than Stratos, (c) identify the location where the information is to be stored, and (d) identify the factors considered in deciding to store the information outside of the United States (see Section 1.7). This section is effective thirty (30) calendar days after execution of this Agreement by all Parties.

- 3.12 Joint Ventures: Stratos may enter into joint ventures under which the joint venture or entity may provide Domestic Communications. To the extent Stratos does not have *de facto* or *de jure* control over such joint venture or entity, Stratos shall in good faith endeavor to have such entity comply with this Agreement as if it were a subsidiary of Stratos and shall consult with the FBI or the DOJ about the activities of such entity. This Section is effective upon execution of this Agreement by all the Parties. Nothing in this Section relieves, nor shall it be construed to relieve, Stratos of its obligations under Sections 1.5 and 1.7.
- 3.13 Outsourcing Third Parties: If Stratos outsources functions covered by this Agreement to a third party, Stratos shall take reasonable steps to ensure that those third parties comply with the applicable terms of this Agreement.
- 3.14 Access to Information: In response to reasonable requests made by the FBI or the DOJ, Stratos shall provide access to information concerning technical, physical, management, or other security measures and other reasonably available information needed by the DOJ or the FBI to assess compliance with the terms of this Agreement.
- 3.15 Visits and Inspections: Upon reasonable notice and during reasonable hours, the FBI and the DOJ may visit and inspect any part of Stratos' Domestic Communications Infrastructure and security office for the purpose of verifying compliance with the terms of this Agreement. Stratos may have appropriate Stratos employees accompany U.S. government representatives throughout any such inspection.
- 3.16 Access to Personnel: Upon reasonable notice from the FBI or the DOJ, Stratos will make available for interview officers or employees of Stratos, and will seek to require contractors to make available appropriate personnel located in the United States who are in a position to provide information to verify compliance with this Agreement.
- 3.17 Annual Report: On or before the last day of January of each year, a designated senior corporate officer of Stratos shall submit to the FBI and the DOJ a report assessing Stratos' compliance with the terms of this Agreement for the preceding calendar year. The report shall include:
- (i) a copy of the policies and procedures adopted to comply with this Agreement;
  - (ii) a summary of the changes, if any, to the policies and procedures, and the reasons for those changes;
  - (iii) a summary of any known acts of noncompliance with the terms of this Agreement, whether inadvertent or intentional, with a discussion of what steps have been or will be taken to prevent such acts from occurring in the future; and
  - (iv) identification of any other issues that, to Stratos' knowledge, will or reasonably could affect the effectiveness of or compliance with this Agreement.

## ARTICLE IV: DEFINITIONS

As used in this Agreement:

- 4.1 “Call Associated Data” means any information possessed by Stratos relating to a Domestic Communication or relating to the sender or recipient of that Domestic Communication and may include without limitation subscriber identification, called party number, calling party number, start time, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, dual tone multifrequency (dialed digit extraction), inband and outofband signaling, and party add, drop, and hold.
- 4.2 “Classified Information” means any information that has been determined pursuant to Executive Order 12958, or any predecessor or successor Executive Order, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act, to require protection against unauthorized disclosure.
- 4.3 “De facto” and “de jure” control have the meaning provided in 47 C.F.R. § 1.2110.
- 4.4 “Domestic Communications” means (i) Wire Communications or Electronic Communications (whether stored or not) between a U.S.-Licensed MET and another U.S. location, and (ii) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates from or terminates to a U.S.-Licensed MET.
- 4.5 “Domestic Communications Infrastructure” means the facilities and equipment of Stratos used to provide, process, direct, control, supervise or manage Domestic Communications. Domestic Communications Infrastructure may be located, for *bona fide* commercial reasons, outside the United States.
- 4.6 “Electronic Communication” has the meaning given it in 18 U.S.C. § 2510(12).
- 4.7 “Electronic Surveillance” means (i) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (ii) access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 *et seq.*; (iii) acquisition of dialing or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 *et seq.* and 50 U.S.C. § 1841 *et seq.*; (iv) acquisition of location-related information concerning a telecommunications service subscriber; (v) preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (vi) including access to, or acquisition or interpretation of, communications or information as described in (i) through (v) above and comparable State laws.
- 4.8 “Foreign” where used in this Agreement, whether capitalized or lower case, means non-U.S.



- 4.9 “Intercept” or “Intercepted” has the meaning defined in 18 U.S.C. § 2510(4).
- 4.10 “Lawful U.S. Process” means lawful requests by U.S. federal, state or local law enforcement agencies or U.S. intelligence agencies, certifications, and court orders regarding Electronic Surveillance and the acquisition of Subscriber Information.
- 4.11 “Non-U.S.-Licensed MET” means an Inmarsat MET that is not covered by a Stratos license or authorization to provide service to METs inside the United States.
- 4.12 “Parties” has the meaning given it in the Preamble.
- 4.13 “Pro forma assignments” or “pro forma transfers of control” are transfers or assignments that do not “involve a substantial change in ownership or control” of the licenses as provided in 47 U.S.C. § 309(c)(2)(B).
- 4.14 “Sensitive Information” means unclassified information regarding (i) the persons or facilities that are the subjects of Lawful U.S. Process, (ii) the identity of the government agency or agencies serving such Lawful U.S. Process, (iii) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance, (iv) the means of carrying out Electronic Surveillance, (v) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process, and (vi) other unclassified information designated in writing by an authorized official of a federal, state or local law enforcement agency or a U.S. intelligence agency as “Sensitive Information.”
- 4.15 “Subscriber Information” means information of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709. Such information shall also be considered Subscriber Information when it is sought pursuant to the provisions of other Lawful U.S. Process.
- 4.16 “Transactional Data” means:
- a) any “call identifying information,” as defined in 47 U.S.C. § 1001(2), possessed by Stratos, including without limitation the telephone number or similar identifying designator associated with a Domestic Communication;
  - b) Internet address or similar identifying designator associated with a Domestic Communication;
  - c) the time, date, size and duration of a Domestic Communication;
  - d) any information possessed by Stratos relating specifically to the identity and physical address of a Stratos U.S. subscriber, user, or account payer;

- e) to the extent associated with such a U.S. subscriber, user or account payer, any information possessed by Stratos relating to telephone numbers, Internet addresses, or similar identifying designators; the physical location of equipment if known and if different from the location information provided under (f) below; types of service; length of service; fees; and usage, including billing records; and
- f) to the extent permitted by U.S. laws, any information possessed by Stratos indicating as closely as possible the physical location to or from which a Domestic Communication is transmitted.
- 4.17 "United States" or "U.S." means the United States of America including all of its States, districts, territories, possessions, commonwealths, and the territorial and special maritime jurisdiction of the United States.
- 4.18 "U.S.-Licensed MET" means a MET covered by Stratos' *Applications for Blanket Licenses to Operate Mobile Earth Terminals with Non-U.S. Licensed Satellites*, File Nos. SES-LIC-20010221-00360; SES-LIC-20010221-00361; SES-LIC-20010221-00362; SES-LIC-20010221-00363, *Application for Blanket Authority to Operate Mobile Earth Terminals*, File No. SES-LIC-20000426-00630, or by any future Stratos Title III license granted to provide service to METs inside the United States.
- 4.19 "Wire Communication" has the meaning given it in 18 U.S.C. § 2510(1).
- 4.20 Other Definitional Provisions: Other capitalized terms used in this Agreement and not defined in this Article IV shall have the meanings assigned them elsewhere in this Agreement. The definitions in this Agreement are applicable to the singular as well as the plural forms of such terms and to the masculine as well as the feminine and neuter genders of such term. Whenever the words "include," "includes," or "including" are used in this Agreement, they shall be deemed to be followed by the words "without limitation."

## ARTICLE V: FREEDOM OF INFORMATION ACT

- 5.1 Protection from Disclosure: The DOJ and FBI shall take all reasonable measures to protect from public disclosure all information submitted by Stratos to the DOJ or FBI in connection with this Agreement and clearly marked with the legend "Confidential" or similar designation. Such markings shall signify that it is Stratos' position that the information so marked constitutes "trade secrets" and/or "commercial or financial information obtained from a person and privileged or confidential," or otherwise warrants protection within the meaning of 5 U.S.C. § 552(b)(4). If a request is made under 5 U.S.C. § 552(a)(3) for information so marked, and disclosure of any information (including disclosure in redacted form) is contemplated, the DOJ or FBI, as appropriate, shall notify Stratos of the intended disclosure as provided by Executive Order 12600, 52 Fed. Reg. 23781 (June 25, 1987). If Stratos objects to the intended disclosure and its

objections are not sustained, the DOJ or FBI, as appropriate, shall notify Stratos of its intention to release (as provided by Section 5 of Executive Order 12600) not later than five (5) business days prior to disclosure of the challenged information.

- 5.2 Use of Information for U.S. Government Purposes: Nothing in this Agreement shall prevent the DOJ or the FBI from lawfully disseminating information as appropriate to seek enforcement of this Agreement, provided that the DOJ and FBI take all reasonable measures to protect from public disclosure the information marked as described in Section 5.1.

## ARTICLE VI: DISPUTES

- 6.1 Informal Resolution: The Parties shall use their best efforts to resolve any disagreements that may arise under this Agreement. Disagreements shall be addressed, in the first instance, at the staff level by the Parties' designated representatives. Any disagreement that has not been resolved at that level shall be submitted promptly to higher authorized officials, unless the DOJ or the FBI believe that important national interests can be protected, or Stratos believes that paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 6.2 below. If, after meeting with higher authorized officials, either party determines that further negotiations would be fruitless, then either party may resort to the remedies set forth in Section 6.2 below. If resolution of a disagreement requires access to Classified Information, the Parties shall designate a person possessing the appropriate security clearances.
- 6.2 Enforcement of Agreement: Subject to Section 6.1 of this Agreement, if any Party believes that any other Party has breached or is about to breach this Agreement, that Party may bring an action against the other Party for appropriate judicial relief. Nothing in this Agreement shall limit or affect the right of a U.S. Government agency to:
- (i) seek revocation by the FCC of any license, permit, or other authorization granted or given by the FCC to Stratos, or seek any other action by the FCC regarding Stratos; or
  - (ii) seek civil sanctions for any violation by Stratos of any U.S. law or regulation or term of this Agreement; or
  - (iii) pursue criminal sanctions against Stratos, or any director, officer, employee, representative, or agent of Stratos, or against any other person or entity, for violations of the criminal laws of the United States.
- 6.3 Forum Selection: It is agreed by and between the Parties that a civil action for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement shall be brought, if at all, in the United States District Court for the District of Columbia.

- 6.4 Irreparable Injury: Stratos agrees that the United States would suffer irreparable injury if for any reason Stratos failed to perform any of its significant obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, Stratos agrees that, in seeking to enforce this Agreement against Stratos, the FBI and DOJ shall be entitled, in addition to any other remedy available at law or equity, to specific performance and injunctive or other equitable relief.

## ARTICLE VII: OTHER

- 7.1 Right to Make and Perform Agreement: The Parties represent that, to the best of their knowledge, they have and shall continue to have throughout the term of this Agreement the full right to enter into this Agreement and perform their obligations hereunder and that this Agreement is a legal, valid and binding obligation enforceable in accordance with its terms.
- 7.2 Waiver: The availability of any civil remedy under this Agreement shall not prejudice the exercise of any other civil remedy under this Agreement or under any provision of law, nor shall any action taken by a Party in the exercise of any remedy be considered a waiver by that Party of any other rights or remedies. The failure of any Party to insist on strict performance of any of the provisions of this Agreement, or to exercise any right they grant, shall not be construed as a relinquishment or future waiver, rather, the provision or right shall continue in full force. No waiver by any Party of any provision or right shall be valid unless it is in writing and signed by the Party.
- 7.3 Headings: The article and section headings and numbering in this Agreement are inserted for convenience only and shall not affect the meaning or interpretation of this Agreement.
- 7.4 Other Laws: Nothing in this Agreement is intended to limit or constitute a waiver of (i) any obligation imposed by any U.S. laws on the Parties or by U.S. state or local laws on Stratos, (ii) any enforcement authority available under any U.S. or state laws, (iii) the sovereign immunity of the United States, or (iv) any authority over Stratos' activities or facilities located outside the United States that the U.S. Government may possess. Nothing in this Agreement is intended to, or is to be interpreted to, require the Parties to violate any applicable U.S. law.
- 7.5 Statutory References: All references in this Agreement to statutory provisions shall include any future amendments to such statutory provisions.
- 7.6 Non-Parties: Nothing in this Agreement is intended to confer or does confer any rights or obligations on any Person other than the Parties and any other U.S. Governmental Authorities entitled to effect Electronic Surveillance pursuant to Lawful U.S. Process.

- 7.7 Modification: This Agreement and the Implementation Plan may only be modified by written agreement signed by all of the Parties. The DOJ and FBI agree to consider in good faith possible modifications to this Agreement if Stratos believes that the obligations imposed on it under this Agreement are substantially more restrictive than those imposed on other U.S. and foreign licensed service providers in like circumstances in order to protect U.S. national security, law enforcement, and public safety concerns. Any substantial modification to this Agreement shall be reported to the FCC within thirty (30) days after approval in writing by the Parties.
- 7.8 Partial Invalidity: If any portion of this Agreement is declared invalid by a U.S. court of competent jurisdiction, this Agreement shall be construed as if such portion had never existed, unless such construction would constitute a substantial deviation from the Parties' intent as reflected in this Agreement.
- 7.9 Good Faith Negotiations: The DOJ and the FBI agree to negotiate in good faith and promptly with respect to any request by Stratos for relief from application of specific provisions of this Agreement to future Stratos activities or services if those provisions become unduly burdensome to Stratos or adversely affect Stratos' competitive position. If the DOJ or the FBI find that the terms of this Agreement are inadequate to address national security concerns presented by an acquisition by Stratos in the United States after the date that all the Parties have executed this Agreement, Stratos shall negotiate in good faith to modify this Agreement to address those concerns.
- 7.10 Successors and Assigns: This Agreement shall inure to the benefit of, and shall be binding upon, the Parties and their respective successors and assigns.
- 7.11 Control of Stratos: If Stratos makes any filing with the FCC or any other governmental agency relating to the *de jure* or *de facto* control of Stratos, except for filing with the FCC for assignments or transfers of control to any U.S. subsidiary of Stratos that are *pro forma*, Stratos shall promptly provide to the FBI and DOJ written notice and copies of such filing.
- 7.12 Notices: All written communications or other written notices relating to this Agreement, such as a proposed modification, shall be deemed given: (i) when delivered personally; (ii) if by facsimile, upon transmission with confirmation of receipt by the receiving Party's facsimile terminal; (iii) if sent by documented overnight courier service, on the date delivered; or (iv) if sent by mail, five (5) business days after being mailed by registered or certified U.S. mail, postage prepaid, addressed to the Parties' designated representatives at the addresses shown below, or to such other representatives at such other addresses as the Parties may designate in accordance with this Section:

Department of Justice  
Assistant Attorney General  
Criminal Division  
950 Pennsylvania Ave., N.W.  
Washington, D.C. 20530

Federal Bureau of Investigation  
Assistant Director  
National Security Division  
935 Pennsylvania Ave., N.W.  
Washington, D.C. 20535

Federal Bureau of Investigation  
Office of General Counsel  
935 Pennsylvania Ave., N.W.  
Washington, D.C. 20535

Stratos Mobile Networks (USA) LLC  
Facilities Manager  
5 Teleport Drive  
Staten Island, NY 10311

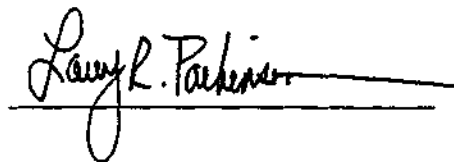
with copy to:  
Alfred M. Mamlet  
Steptoe & Johnson, LLP  
1330 Connecticut Ave., N.W.  
Washington, D.C. 20036

This Agreement is executed on behalf of the Parties:

Federal Bureau of Investigation

Date: August 9, 2001  
Printed Name: Larry R. Parkinson  
Title: General Counsel

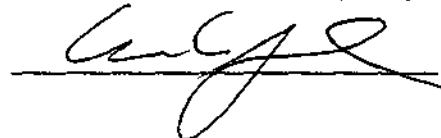
By:



MarineSat Communications Network, Inc. and Stratos Mobile Networks (USA) LLC

Date: August 7, 2001  
Printed Name: Carmen Lloyd  
Title: President

By:



**United States Department of Justice**

Date: 8/13/01

By: Mary Ellen Warlow

Printed Name: Mary Ellen Warlow

Title: Acting Deputy Assistant Attorney General

## Exhibit A

### CONDITION TO FCC LICENSES

IT IS FURTHER ORDERED, that the authorizations and licenses related thereto are subject to compliance with the provisions of the Agreement attached hereto between MarineSat Communications Network, Inc. and Stratos Mobile Networks (USA) LLC on the one hand, and the U.S. Department of Justice (the "DOJ") and the Federal Bureau of Investigation (the "FBI") on the other, dated August 7, 2001, which Agreement is designed to address national security, law enforcement and public safety issues of the DOJ and the FBI regarding the authority and licenses granted herein. Nothing in this Agreement is intended to limit any obligation imposed by Federal law or regulation including, but not limited to, 47 U.S.C. § 222(a) and (c)(1) and the FCC's implementing regulations.



## **EXHIBIT C**

## **Amendment No. 1**

THIS AMENDMENT NO. 1 (hereinafter "Amendment") to the Agreement dated August 7, 2001 ("Agreement"), by and between Stratos Communications, Inc. (previously MarineSat Communications Network, Inc.), and Stratos Mobile Networks (USA) LLC (collectively, "Stratos Parties") and the Department of Justice ("DOJ") and the Federal Bureau of Investigation ("FBI") (collectively with the Stratos Parties, "the 2001 Signatories"), a copy of which is attached as Exhibit A, is hereby agreed by and between the 2001 Signatories, Robert M. Franklin ("Trustee"), CIP Canada Investment Inc. ("CIP Canada"), Stratos Mobile Networks, Inc. and the Department of Homeland Security ("DHS") (collectively "the 2007 Signatories"). This Amendment is effective as of the date of the last signature hereto ("Effective Date").

WHEREAS the 2001 Signatories desire to enter into this Amendment to add parties to the Agreement, to add commitments by the Trustee and CIP Canada in connection with a proposed transaction to be effective if such transaction is consummated, and to clarify the obligations of all signatories under the Agreement, as of the Effective Date;

WHEREAS CIP UK Holdings Limited ("CIP UK"), its subsidiary CIP Canada, and Stratos Global Corporation ("Stratos Global") have entered into a Plan of Arrangement effective March 19, 2007, which provides that upon receipt of regulatory approvals including by the FCC, all of the issued and outstanding shares of Stratos Global will be transferred to a Canadian trust created by CIP Canada;

WHEREAS CIP Canada and the Trustee have entered into a Trust Agreement effective April 2, 2007, which provides for an irrevocable trust ("Trust") giving the Trustee legal title to the Stratos Global shares, until either the dissolution of the Trust, or the removal of the Trustee and replacement by a successor at the election of CIP Canada following (i) a finding by an independent party that the Trustee has engaged in malfeasance, criminal conduct, or wanton or willful neglect, or (ii) a judgment of incompetence by a court of competent jurisdiction, either of which would require regulatory approval;

WHEREAS the Trust Agreement also provides that the Trustee has a fiduciary duty to manage the Stratos Global shares for the benefit of CIP Canada, that the Trustee does not have authority to sell, transfer, assign, or otherwise dispose of the Stratos Global shares during the trust period, that CIP Canada will have no legal control over, or operational responsibility for, Stratos Global prior to the dissolution of the Trust, and whereas the Stratos Global Board of Directors and Stratos management retain operational responsibility for Stratos Global notwithstanding the Trust Agreement and the Plan of Arrangement; and

WHEREAS, the Trust Agreement provides that, subject to receipt of regulatory approval, the Trust will dissolve on or before April 14, 2009 and the Trustee will transfer legal title to the Stratos shares to CIP Canada, or to a third party in the event Inmarsat Finance does not exercise its call option to acquire CIP UK.

NOW, THEREFORE, in consideration of the promises, terms and conditions of this

Amendment, and for other consideration, receipt of which is hereby acknowledged, the 2007 Signatories hereby agree as follows:

SECTION 1. This Amendment is entered into pursuant to Section 7.7 of the Agreement.

SECTION 2. The Agreement shall be amended as of the Effective Date such that Stratos Mobile Networks, Inc. is hereby added as a signatory and party to the Agreement with all of the full rights, benefits and obligations of the Stratos Parties.

SECTION 3. The Agreement shall be amended as of the Effective Date such that DHS is hereby added as a signatory and party to the Agreement with all the rights, benefits and obligations of DOJ and FBI.

SECTION 4. During the period between the Effective Date and either the dissolution of the Trust or the resignation or removal of Trustee, Trustee undertakes the obligation not to interfere with or impede the ability of the Stratos Parties or Stratos Mobile Networks, Inc. to discharge their obligations under the Agreement.

SECTION 5. During the period between the Effective Date and the purchase of the issued and outstanding shares of Stratos Global by a third party, pursuant to regulatory approval, CIP Canada undertakes the obligation not to interfere with or impede the ability of the Stratos Parties or Stratos Mobile Networks, Inc. to discharge their obligations under the Agreement.

SECTION 6. The Agreement shall be amended as of the Effective Date, to modify Section 7.12 by adding the following addresses:

Department of Homeland Security  
Assistant Secretary for Policy  
Email: [ip-fcc@dhs.gov](mailto:ip-fcc@dhs.gov)

Robert M. Franklin, Trustee  
34 Plymbridge Crescent  
Willowdale, Ontario  
M2P 1P5 Canada

CIP Canada Investment Inc.  
Suite 600, 570 Queen Street  
Fredericton, New Brunswick  
E3B 6Z6 Canada

with copies to:

James D. Scarlett  
Torys LLP

Suite 3000  
79 Wellington Street West  
Box 270, TD Centre  
Toronto, Ontario  
M5K 1N2 Canada  
*Counsel for Robert M. Franklin, Trustee*

Patricia J. Paoletta  
Harris, Wiltshire & Grannis LLP  
1200 18th Street, N.W., Suite 1200  
Washington, D.C. 20036-2516  
*Counsel for CIP Canada Investment Inc.*

and

Laura Fraedrich  
Kirkland & Ellis LLP  
655 15th Street, N.W.  
Washington, D.C. 20005-5793  
*Counsel for CIP Canada Investment Inc.*

In addition, the following address is hereby substituted for the Stratos Mobile Networks (USA) LLC address in Section 7.12:

Stratos Communications, Inc.  
Stratos Mobile Networks (USA), LLC  
Stratos Mobile Networks, Inc.  
6901 Rockledge Drive, Suite 900  
Bethesda, MD 20817

SECTION 7. Except as provided in this Amendment, all terms of the Agreement remain in full force and effect. This Amendment may be signed in any number of counterparts, each of which shall constitute an original and all of which shall constitute one and the same agreement.

SECTION 8. The Stratos Parties, Stratos Mobile Networks, Inc., DOJ, FBI, and DHS further agree pursuant to Section 1.2 and 7.7 of the Agreement to an Amended Implementation Plan dated \_\_\_\_\_, 2007, a copy of which is attached hereto as Exhibit B. For clarification, the Amended Implementation Plan is confidential and will not be attached to any public filing of this Amendment.

*[Remainder of this Page Intentionally Left Blank; Signature Pages follow]*

This Amendment is Executed on behalf of the 2007 Signatories:

**Department of Justice**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Sigal Mandelker  
Deputy Assistant Attorney General  
Criminal Division

**Department of Homeland Security**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Stewart A. Baker  
Assistant Secretary for Policy


**Federal Bureau of Investigation**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Elaine N. Lammert  
Deputy General Counsel

**Stratos Communications, Inc.  
Stratos Mobile Networks (USA) LLC  
Stratos Mobile Networks, Inc.**

Date: \_\_\_\_\_

By:   
James J. Parrin  
Chief Executive Officer

**Robert M. Franklin, Trustee**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Robert M. Franklin  
Trustee

**CIP Canada Investment Inc.**


Date: \_\_\_\_\_

By: \_\_\_\_\_  
Johannes Jacobus (Hans) Lipman  
Chairman and Director

This Amendment is Executed on behalf of the 2007 Signatories:

**Department of Justice**

Date: 8/8/2007

By:   
Sigal Mandelker  
Deputy Assistant Attorney General  
Criminal Division

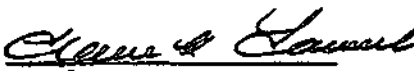
**Department of Homeland Security**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Stewart A. Baker  
Assistant Secretary for Policy


**Federal Bureau of Investigation**

Date: 8/14/2007

By:   
Elaine N. Lammert  
Deputy General Counsel

**Stratos Communications, Inc.  
Stratos Mobile Networks (USA) LLC  
Stratos Mobile Networks, Inc.**

Date: \_\_\_\_\_

By:   
James J. Parr  
Chief Executive Officer

**Robert M. Franklin, Trustee**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Robert M. Franklin  
Trustee

This Amendment is Executed on behalf of the 2007 Signatories:

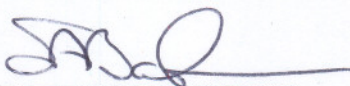
**Department of Justice**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Sigal Mandelker  
Deputy Assistant Attorney General  
Criminal Division

**Department of Homeland Security**

Date: 10 Aug 07

By:   
Stewart A. Baker  
Assistant Secretary for Policy

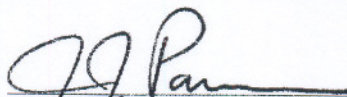
**Federal Bureau of Investigation**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Elaine N. Lammert  
Deputy General Counsel

**Stratos Communications, Inc.  
Stratos Mobile Networks (USA) LLC  
Stratos Mobile Networks, Inc.**

Date: \_\_\_\_\_

By:   
James J. Parrin  
Chief Executive Officer

**Robert M. Franklin, Trustee**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Robert M. Franklin  
Trustee



This Amendment is Executed on behalf of the 2007 Signatories:

**Department of Justice**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Sigal Mandelker  
Deputy Assistant Attorney General  
Criminal Division

**Department of Homeland Security**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Stewart A. Baker  
Assistant Secretary for Policy

**Federal Bureau of Investigation**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
Elaine N. Lammert  
Deputy General Counsel

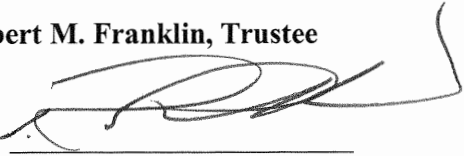
**Stratos Communications, Inc.  
Stratos Mobile Networks, Inc.**

Date: \_\_\_\_\_

By: \_\_\_\_\_  
James J. Parm  
Chief Executive Officer

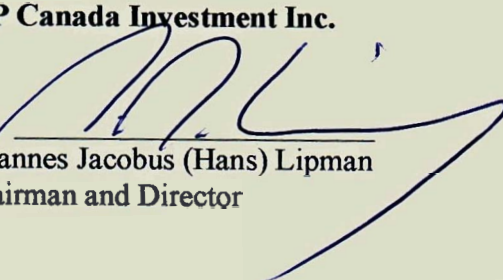
**Robert M. Franklin, Trustee**

Date: July 18, 2007

By:   
\_\_\_\_\_  
Robert M. Franklin  
Trustee

**CIP Canada Investment Inc.**

Date: 23/7/2007

By:   
Johannes Jacobus (Hans) Lipman  
Chairman and Director

## CERTIFICATE OF SERVICE

I hereby certify that on this 9<sup>th</sup> day of January, 2009, I caused a true and correct copy of the foregoing PETITION TO ADOPT CONDITIONS TO AUTHORIZATIONS AND LICENSES to be served via electronic mail delivery to each of the following parties:

Helen Domenici, Chief  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

John Giusti, Deputy Bureau Chief  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Roderick Porter, Deputy Bureau Chief  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Arthur Lechtman, Legal Advisor  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Steven Spaeth, Legal Advisor  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

James Ball, Chief  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Howard Griboff, Deputy Division Chief  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

George Li, Deputy Division Chief  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Francis Gutierrez, Associate Division Chief  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

David Krech, Associate Division Chief  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

JoAnn Sutton, Assistant Division Chief  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Paul Locke, Assistant Chief of Engineering  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Susan O'Connell  
Policy Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Robert Nelson, Chief  
Satellite Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Cassandra Thomas, Deputy Division Chief  
Satellite Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Fern Jarmulnek, Deputy Division Chief  
Satellite Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Karl Kensinger, Associate Division Chief  
Satellite Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Kathryn Medley, Branch Chief  
Engineering Branch  
Satellite Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Andrea Kelly, Branch Chief  
Policy Branch  
Satellite Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Scott Kotler, Branch Chief  
System Analysis Branch  
Satellite Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Stephen Duall  
Policy Branch  
Satellite Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Jeanette Spriggs  
Policy Branch  
Satellite Division  
International Bureau  
Federal Communications Commission  
445 12th Street, SW  
Washington, DC 20554

Diane J. Cornell  
Chris Murphy  
Inmarsat, Inc.  
1101 Connecticut Avenue, NW Suite 1200  
Washington D.C. 20036

/s/ Valerie M. Barrish

---

Valerie M. Barrish