

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) Innarsat 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) Innarsat 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) Innarsat shall not induce the contractor either to violate its obligations to Innarsat related to this Agreement or the Implementation Plan, or to take any action that, if taken by Innarsat, would violate this Agreement.
- (d) If Innarsat receives any information that a contractor or any of its employees or agents has taken an action that, had it been taken by Innarsat, would violate a provision of this Agreement or the Implementation Plan, or has violated its obligations to Innarsat related to this Agreement or the Implementation Plan, Innarsat (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 Innarsat of any of its obligations under this Agreement or the Implementation Plan.

5.5 **Notice of Foreign Influence.** If Innarsat 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 Innarsat or to exercise any Control of Innarsat in such a way that (1) interferes with or impedes the performance by Innarsat of its duties and obligations under the terms of this Agreement; (2) interferes with or impedes the exercise by Innarsat of its rights under the Agreement; or (3) raises a concern with respect to the fulfillment by Innarsat 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, Innarsat 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 Innarsat 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.** Innarsat agrees that in any application or petition by Innarsat, 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 Innarsat system, or to offer, distribute, or resell Domestic Communications in the United States for communications utilizing the Innarsat system, Innarsat 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 Innarsat 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.** Innarsat 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 Innarsat 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 Innarsat, (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 of Innarsat 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 Innarsat signed by all of

*then, waive any provision of this Agreement intended for their benefit unless such waiver is objected to by Innarsat. The Government Parties agree to consider promptly and in good faith possible modifications to this Agreement if Innarsat 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 Innarsat. The Government Parties agree to negotiate in good faith and promptly with respect to any request by Innarsat for relief from application of specific provisions of this Agreement if those provisions become unduly burdensome or have an adverse affect on Innarsat'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 Innarsat 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 Innarsat, and on all Affiliates of Innarsat.

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 Innarsat, nor any transferee or assignee of the FCC licenses or authorizations held by Innarsat, 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: [Signature]  
 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 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-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, 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 Allant, 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 TII Aeronautical Corp. ("TIIA") and 9 percent owned by IDB Mobile Communications, Inc., which is in turn 100 percent owned by TIIA. TIIA 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.