inmarsat
The mobile satellite company™

99 City Road
London EC1Y 1AX
United Kingdom
T +44 (0)20 7728 1000
F +44 (0)20 7728 1044
W inmarsat.com

September 13, 2019

Assistant Attorney General for National Security
United States Department of Justice
National Security Division
950 Pennsylvania Avenue NW
Washington, DC 20530

Subject: Inmarsat plc./Connect Bidco

IB Docket No. 19-216	ITC-T/C-20190603-00117
SES-T/C-20190603-00672	SES-T/C-20190603-00673
SES-T/C-20190603-00674	SES-T/C-20190603-00675
SES-T/C-20190603-00676	ISP-PDR-20190528-00003

Applications by Connect Bidco Limited (Connect Bidco) and Inmarsat plc. (Inmarsat) under sections 214 and 310(d) of the Communications Act of 1934, as amended, requesting approval to: (1) transfer control of licenses and authorizations held by Inmarsat's wholly owned U.S. subsidiaries from the public shareholders of Inmarsat to Connect Bidco, and (2) continue to have foreign investment in Inmarsat Group Holdings Inc. (IGHI) above the 25 percent benchmark.

Dear Sir/Madam:

This Letter of Agreement ("LOA") sets forth the commitments that Connect Bidco and Inmarsat plc's subsidiaries Inmarsat Group Holdings Inc., Inmarsat Solutions (US) Inc., Inmarsat Inc., and ISAT US Inc. (collectively "Inmarsat"); make to the U.S. Department of Justice ("USDOJ") to address national security, law enforcement, and public safety concerns arising from Inmarsat and Connect Bidco's applications to the Federal Communications Commission ("FCC"). Inmarsat and Connect Bidco have requested approval to transfer control of licenses and authorizations held by Inmarsat's wholly owned U.S. subsidiaries from the public shareholders of Inmarsat to Connect Bidco, pursuant to Section 214 of the Communications Act of 1934, as amended, 47 U.S.C. § 214, and the implementing regulations at 47 C.F.R. § 63.18(e)(1), (2). The Applicants also filed a petition for declaratory ruling to permit Inmarsat to continue to have foreign investment in IGHI above the 25 percent benchmark in pursuant to Section 310(b)(4) of the Act, as amended.

Inmarsat adopts as true and correct all statements Inmarsat or its representatives have made to USDOJ or other Team Telecom member agencies and the FCC in the course of the review of the above-referenced application and petition, and it hereby adopts those statements as the basis for this LOA.

Definitions

1. For purposes of this LOA, the following definitions apply:

a. "Access" means the ability to undertake physically or logically any of the following actions:

(i) To read, copy, divert, or otherwise obtain non-public information or technology from or about software, hardware, a database or other system, or a network;

(ii) To add, edit, delete, reconfigure, provision, or alter information or technology stored on or by software, hardware, a system or network; or

(iii) To alter the physical or logical state of software, hardware, a system or network.

b. "Call Detail Record" ("CDR") means the data records or call log records that contain information about each call made by a user and processed by switch, call manager, or call server.

c. "Customer Proprietary Network Information" ("CPNI") means as set forth in 47 U.S.C. § 222(h)(1).

d. "Date of this LOA" means the date on which Inmarsat executes this LOA.

e. "Days" means calendar days unless otherwise specified.

f. "Domestic Communications" ("DC") means:

(i) Wire Communications, or Electronic Communications (whether stored or not), from one location within the United States, including its territories, to another location within the United States; or

(ii) The U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates at a U.S.-Licensed Mobile Earth Station.

g. "Domestic Communications Infrastructure" ("DCI") means:

(i) Any Inmarsat system that physically is located in the United States, including its territories, including any transmission, switching,

bridging, and routing equipment, and any associated software (with the exception of commercial-off-the-shelf ("COTS") software used for common business functions, *e.g.*, Microsoft Office) used by, or on behalf of,[1] Inmarsat to provide, process, direct, control, supervise, or manage Domestic Communications; and

(ii) Network Operations Center ("NOC") facilities, as defined *infra*.

h. "Electronic Surveillance" means:

(i) The interception of wire, oral, or electronic communications as set forth in 18 U.S.C. § 2510(1), (2), (4) and (12), respectively, and electronic surveillance as set forth 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, 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 set forth in 18 U.S.C. § 3121 et seq. and 50 U.S.C. § 1841 et seq.*;*

(iv) Acquisition of location-related information concerning a subscriber or facility;

(v) Preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and

(vi) Access to or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (i) through (v) above and comparable state laws.

i. "Foreign" means non-United States, or its territories.

j. "Government" means any government, or governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau or political subdivision, and any court, tribunal, judicial or arbitral body.

[1] The phrase "on behalf of," as used in this paragraph, does not include entities with which Inmarsat has contracted for peering, interconnection, roaming, long distance, wholesale network access, or other similar arrangements.

k. "Lawful U.S. Process" means U.S. federal, state, or local court orders, subpoenas, warrants, processes, directives, certificates or authorizations, and other orders, legal process, statutory authorizations and certifications for Electronic Surveillance, physical search and seizure, production of tangible things or Access to or disclosure of Domestic Communications, call-associated data, transactional data, Subscriber Information, or associated records.

l. "Managed Network Service Provider" ("MNSP") means any third party that has Access to Principal Equipment for the purpose of:

(i) Network operation; provisioning of Internet and telecommunications services; routine, corrective, and preventative maintenance, including switching, routing, and testing; network and service monitoring; network performance, optimization, and reporting; network audits, provisioning, creation and implementation of modifications or upgrades; or

(ii) Provision of DC or operation of DCI, including: customer support; OSS; BSS; Network Operations Centers ("NOCs"); information technology; cloud operations/services; 5G (SDN, NFV, Applications); and datacenter services and operations.

m. "Mobile Earth Station" ("MES") means a mobile earth terminal or "MET" (*i.e.*, a hand-held portable, or other mobile terminal capable of receiving and/or transmitting Domestic Communications by satellite), and includes a mobile earth terminal capable of receiving and/or transmitting Inmarsat services.

n. "Non U.S.-Licensed MES" means an Inmarsat MES other than a U.S.-Licensed MES.

o. "Network Operations Center" ("NOC") means any locations and facilities performing network management, monitoring, accumulating accounting and usage data, maintenance, or user support.

p. "Network Security Plan" ("NSP") means a network systems security plan that addresses information security, including need to know access rights; remote access, physical security; cybersecurity; third-party contractors (managed service providers); Outsourcing, maintenance and retention of system logs, protection of Lawful U.S. Process, protection of U.S. Records obtained by Inmarsat from customers or through provision of services, and data breach notifications.

q. "NIST-Compliant Cybersecurity Plan" means a cybersecurity plan that is consistent with the most recently published version of the National Institute of

Standards and Technology (NIST) Cybersecurity Framework, available at https://www.nist.gov/cyberframework.

r. "Outsource" means performing the obligations of this LOA or supporting the services and operational needs of Inmarsat at issue in this LOA using personnel that are not employees of Inmarsat.

s. "Person" means any natural person or legal entity.

t. "Personally Identifiable Information" or PII means any information that uniquely identifies and correlates to a natural person or can be used to distinguish or trace a natural person's identity, alone, including his or her name, social security number, or biometric records, or when combined with other personal or identifying information that is linked or linkable to a specific individual, including date and place of birth, or parent's surname, including any "personal identifier information" as set forth in 31 C.F.R. § 800.402(c)(6)(vi)(B).

u. "Principal Equipment" means all major system components of the primary telecommunications and information DCI that supports core telecommunications or information services (e.g., voice, data, text, MMS, FAX, video, Internet, OTT, Apps), functions (e.g., network/element management, maintenance, provisioning, NOC, etc.), and operations (e.g., OSS/BSS, customer support, billing, backups, cloud services, etc.), which, as of the date of this LOA, are Inmarsat's (i) radio access network (RAN); (ii) radio frequency systems (RFS); (iii) core network, including Inmarsat's NOCs; (iv) operations support system and business support system (OSS/BSS); and (v) telemetry, tracking, and command (TT&C) system. Principal Equipment includes, but is not limited to, routers, servers, circuit switches or soft-switches, PBXs, call processors, databases, storage devices, load balancers, radios, smart antennas, transmission equipment (RF/Microwave/Wi-Fi/Fiber Optic/Satellite Transponders and Power equipment/solar arrays/Thrusters/stabilizers/ sensors), RAN, SDR, equalizers/ amplifiers, MDF, digital/optical cross-connects, PFE, multiplexers, HLR/VLR, gateway routers, signaling, Network Function Virtualizations, hypervisors, EPC, BSC, BT, or eNodeB.

v. "Security Incident" means:

(i) Any known or suspected breach of this LOA, including a violation of any approved policy or procedure under this LOA;

(ii) Any unauthorized Access to, or disclosure of, PII of U.S. customers;

(iii) Any unauthorized Access to, or disclosure of, information obtained from or relating to U.S. Government entities; or

(iv) Any one or more of the following which compromise the storage or processing of U.S. Records or Domestic Communications by the company's computer network(s) or associated information systems:

A. Unplanned disruptions, including those caused by a denial of service attack;
B. Unauthorized processing or storage of data;
C. Unauthorized modifications to system hardware, firmware, or software; or
D. Attempts from unauthorized sources to Access systems or data if these attempts to Access systems or data may materially affect company's ability to comply with the terms of this LOA.

x. "Subscriber Information" means any information of the type referred to and accessible subject to the procedures set forth in 18 U.S.C. § 2703(c)(2) or 18 U.S.C. § 2709, as amended or superseded.

y. "Team Telecom" or "Team Telecom Agencies" means USDOJ, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Department of Defense (DoD).

aa. "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.

bb. "U.S. Records" means Inmarsat's customer billing records, Subscriber Information, PII, CDRs, and CPNI, and any other information related to U.S. citizens used, processed, or maintained in the ordinary course of business related to the services offered by Inmarsat within the United States, including information subject to disclosure to a U.S. federal or state governmental entity under the procedures set forth in 18 U.S.C. § 2703(c), (d) and 18 U.S.C. § 2709.

Lawful U.S. Process

2. Inmarsat agrees to comply with all Lawful U.S. Process, including process relating to Electronic Surveillance.

3. Inmarsat agrees to 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 Network Security Plan.

4. Upon receipt of any Lawful U.S. Process, Inmarsat agrees to make available any and all information responsive to the Lawful U.S. Process within the territorial boundaries of the United States and otherwise provide to the requesting officials, in a manner and time consistent with the Lawful U.S. Process

5. Inmarsat agrees not to provide, or otherwise allow the disclosure of, or Access to, U.S. Records or Domestic Communications, to any Foreign Government, or Foreign Person (other than (a) an Inmarsat employee who has been screened pursuant to Paragraph 14 herein, (b) an Inmarsat affiliate, and (c) an employee of an Outsourced service provider, which provider was approved by USDOJ pursuant to Paragraphs 28 or 29, in each case, with a need to know), without prior written consent of USDOJ, or a court of competent jurisdiction in the United States.

6. Inmarsat agrees not to disclose the receipt of Lawful U.S. Process, or compliance with Lawful U.S. Process, to any Foreign Government, or any Person (other than (a) an Inmarsat employee who has been screened pursuant to Paragraph 14 herein, (b) an Inmarsat affiliate, and (c) an employee of an Outsourced service provider, which provider was approved by USDOJ pursuant to Paragraphs 28 or 29, in each case, with a need to know) not authorized under the Lawful U.S. Process, without prior written consent of USDOJ, or a court of competent jurisdiction in the United States.

7. Inmarsat agrees to refer any requests for U.S. Records from a Foreign Person (other than (a) an Inmarsat employee, (b) Inmarsat affiliate, and (c) an employee of an Outsourced service provider, which provider was approved by USDOJ pursuant to Paragraphs 28 or 29, with a need to know), or a Foreign Government, including any legal process from a Foreign Government, to USDOJ as soon as possible, but in no event later than five (5) days after such a request, or legal process, is received by, or made known to, Inmarsat, unless disclosure of the request, or legal process, would be in violation of U.S. law, or in violation of an order of a court of competent jurisdiction in the United States.

8. Inmarsat agrees not to comply with such requests from Foreign Governments and Persons without written approval from USDOJ, or an order of a court of competent jurisdiction in the United States.

9. Inmarsat agrees to ensure that U.S. Records are not subject to mandatory destruction under any Foreign laws.

Personnel

10. Inmarsat agrees to designate and maintain a U.S. law enforcement point of contact ("LEPOC") in the United States who will be subject to prior approval by USDOJ, including the FBI. The LEPOC shall be a U.S. citizen residing in the United States or its territories, and the LEPOC must be approved by the FBI to receive service of Lawful U.S. Process for U.S. Records and, where possible, to assist and support lawful requests for surveillance or production of U.S. Records by U.S. federal, state, and local law enforcement agencies.

11. Inmarsat agrees to provide the LEPOC's PII to USDOJ within fifteen (15) days from the date Inmarsat receives the FCC's approval of the application.

12. Inmarsat agrees to notify USDOJ, including the FBI, in writing at least thirty (30) days prior to modifying its LEPOC for USDOJ and FBI objection or non-objection.

13. Inmarsat agrees that the designated LEPOC will have Access to all U.S. Records, and, in response to Lawful U.S. Process, will make such records available promptly and, in any event, no later than five (5) days after receiving such Lawful U.S. Process unless USDOJ grants an extension.

14. To the extent permitted by applicable local law, Inmarsat agrees to implement, either directly or through a vendor or service provider, a process to screen existing or newly hired Inmarsat personnel or any personnel performing under an agreement pursuant to which such personnel have Access to U.S. Records, Domestic Communications, or DCI through Inmarsat. The personnel screening process shall include background investigations, public criminal records checks, or other analogous means to ascertain a Person's trustworthiness. To satisfy its obligation under this Paragraph with respect to the employees of Outsourced service providers, Inmarsat shall contractually commit such Outsourced service providers to comply with the personnel screening process set forth in this Paragraph.

Unauthorized Access and Security Incidents

15. Inmarsat agrees to take all practicable measures to prevent unauthorized Access to, to prevent any unlawful use of, or disclosure of information relating to U.S. Records, DC, and the DCI.

16. To this end, Inmarsat agrees to notify USDOJ of any non-U.S. citizen (other than (a) Inmarsat employees who have been screened pursuant to Paragraph 14 herein and (b) an employee of an Outsourced service provider, which provider was approved by USDOJ pursuant to Paragraphs 28 or 29) that will be granted Access to U.S. Records, Domestic Communications, or the DCI for USDOJ objection or non-objection no less than thirty (30)

days before such Access is granted. Inmarsat agrees to provide PII and any other information USDOJ, in its sole discretion, determines is necessary to complete its review.

17. Inmarsat agrees to draft: (1) a NIST-Compliant Cybersecurity Plan; (2) an updated version of the NSP; (3) an Access Control Policy; and (4) Information Security Policy which Inmarsat will provide to USDOJ within sixty (60) days of the Date of this LOA. Such policies shall be subject to USDOJ objection or non-objection within thirty (30) days of submission.

18. Inmarsat agrees that the NSP will address, but not be limited to, information security including the use of encryption on Inmarsat networks; remote access; physical security; cybersecurity; third-party contractors; Outsourcing; maintenance and retention of system logs; protection of Lawful U.S. Process; protection of U.S. Records obtained by Inmarsat in the ordinary course of business, and Inmarsat's specific plan regarding new contracts or any amendments to any existing contracts with third-party providers of services to require those third parties to notify Inmarsat in the event of a breach or loss of U.S. Records within a specified time period after discovery, not to exceed five (5) days from the date of discovery.

19. Inmarsat agrees to notify USDOJ at least thirty (30) days prior to changing the location(s) for storing U.S. Records (a) from a location within the United States or its territories to a location outside of the United States or it its territories or (b) from a location outside of the United States or its territories to another location outside of the United States or its territories for USDOJ objection or non-objection. Such notice shall include:

a. The new location(s) where the information is to be stored;
b. A description of the type of information that will be stored in the new location;
c. The reason for changing the storage location; and
d. The custodian of the information (even if such custodian is Inmarsat).

20. Inmarsat agrees to notify USDOJ at least seven (7) days prior to changing the location(s) for storing U.S. Records from a location outside of the United States to a location within the United States or its territories. Such notice will include all of the requisite information required for notification under Paragraph 19(a-d) of this LOA.

Reporting Incidents and Breaches

21. Except as otherwise required by law or this LOA to report sooner, Inmarsat agrees to report to USDOJ promptly, but no later than fifteen (15) calendar days, if it learns of information that reasonably indicates:

a. A Security Incident;

b. Unauthorized Access to, or disclosure of, any information relating to services provided by Inmarsat, or referring or relating in any way to Inmarsat's customers in the United States or its territories;
c. Any unauthorized Access to, or disclosure of, DC in violation of federal, state, or local law; or
d. Any material breach of the commitments made in this LOA.

22. Inmarsat agrees to require any third-party service provider with Access to U.S. Records to disclose to Inmarsat any data breach of any U.S. Records, or any loss of U.S. Records, whether from a data breach, or other cause, within five (5) days of the third party discovering the breach or loss. Consistent with the standard set forth in the agreements that Inmarsat already has with any third-party service providers with Access to U.S. Records, Inmarsat agrees to notify those third parties that they must disclose any breaches, or loss of U.S. Records consistent with this paragraph.

23. Inmarsat agrees to notify USDOJ, including the points of contact (POC) listed in Paragraph 31, in writing of any of the Security Incidents or breaches described in Paragraphs 21 or 22 of this LOA. The notification shall take place no later than fifteen (15) days after Inmarsat or any third party providing Outsourced services to Inmarsat discovers the incident, intrusion, or breach has taken or taking place, or sooner when required by statute or regulations.

24. Inmarsat agrees to notify the FBI and U.S. Secret Service within seven (7) business days upon learning that a Person without authorization, or in exceeding their authorization, has gained Access to, used, or disclosed any of Inmarsat's U.S. customers' information, including CPNI, or CPNI of a third party maintained by Inmarsat, and shall report the matter to the central reporting facility through the following portal:

https://www.cpnireporting.gov/cpni/content/disclaimer.seam

Principal Equipment

25. Inmarsat agrees to provide USDOJ within ninety (90) days from the date Inmarsat receives the FCC's approval, a Principal Equipment List for USDOJ objection or non-objection. At Inmarsat's request, USDOJ will grant extensions of the foregoing deadline provided that Inmarsat demonstrates that it was unable to satisfy the then-current deadline despite using commercially reasonable and diligent efforts. The Principal Equipment List shall include the following:

a. A complete and current list of all Principal Equipment, including:

(i) a description of each item and the functions supported;
(ii) each item's manufacturer; and

(iii) the model and/or version number of any hardware or software; and

b. Any vendors, contractors, or subcontractors involved in providing, installing, operating, managing, or maintaining the Principal Equipment.

26. Inmarsat agrees to notify USDOJ in writing within at least thirty (30) days of introducing any new and Principal Equipment or modifying any of its Principal Equipment for USDOJ objection or non-objection. For purposes of the prior sentence and Paragraph 27, (a) the patch, update, or version upgrade of any software that qualifies as Principal Equipment and (b) the repair, replacement, maintenance, and version upgrade of any hardware that qualifies as Principal Equipment, shall not, in either case, qualify as a modification of such software or hardware provided that the foregoing does not result in the addition of any new Principal Equipment into Inmarsat's networks of a type that has not previously been noticed to and approved by USDOJ. Inmarsat agrees not to introduce any new Principal Equipment or modify any of its Principal Equipment in a manner that is in violation of U.S. law.

27. Inmarsat agrees to provide USDOJ with the names of providers, suppliers, and entities that will perform any maintenance, repair, or replacement that may result in any material modification to its Principal Equipment or systems or software used with or supporting the Principal Equipment. USDOJ will object or non-object to such new Principal Equipment or modification to the Principal Equipment within thirty (30) days of receipt of notice.

Outsourced Services

28. Inmarsat agrees to provide USDOJ within ninety (90) days from the date Inmarsat receives the FCC's approval, a list of all Outsourced service providers for any of the following operations or services to the extent that they are involved in the DCI or the storage or processing of U.S. Records or Domestic Communications for USDOJ objection or non-objection:

a. MNSP services;

b. Network Operations Center(s);

c. Network maintenance services;

d. Billing or customer support services;

e. Any operation or service that could potentially expose the DCI, U.S. Records, or Domestic Communications and

f. Deploying any network elements, hardware, software, core network equipment, and network management capabilities that are owned, managed, manufactured or controlled by a Foreign Government.

29. Inmarsat agrees to notify USDOJ in writing within thirty (30) days of using of any new Outsourced service providers that provide the operations or services set forth in Paragraph 28. USDOJ agrees to object or non-object to any new Outsourced service providers, within thirty (30) days of receiving notice.

Network Operations Centers

30. Inmarsat agrees to notify USDOJ in writing at least sixty (60) days prior to changing the location of its Network Operations Centers for USDOJ objection or non-objection.

Annual Report

31. Inmarsat agrees to provide an annual report to USDOJ regarding its compliance with this LOA, to include:

a. Certification that there were no changes (where no changes were reported to USDOJ during the preceding year);
b. The company's handling of U.S. Records, Domestic Communications, and Lawful U.S. Process (*i.e.,* whether handled properly and in accordance with the assurances contained herein) including a list of individuals with Access to U.S. Records;
c. Notification(s) of the installation and/or purchase or lease of any Foreign-manufactured Principal Equipment (including, but not limited to, switches, routers, software, hardware) as well as a list of all Outsourced service suppliers covered under Paragraphs 28 and 29;
d. Notification(s) of any relationships with Foreign-owned telecommunications partners, including any network peering (traffic exchange) relationships;
e. Updated list of all terrestrial network partners that interconnect to Inmarsat's Satellite Access Stations and network points of presence.
f. Updated network diagrams showing all network points of presence, NOCs, Meet Me Places, and Earth Stations;
g. Updated NIST-Compliant Cybersecurity Plan, NSP, Access Control Policy, and Information Security Policy;
h. Report(s) of any occurrences of Security Incidents including but not limited to cybersecurity incidences, network and enterprise breaches, and unauthorized Access to U.S. Records;
i. Recertification of the services that Inmarsat provides or confirmation that no additional services are being offered;
j. Recertification that Connect Bidco has no employees;
k. Recertification that Inmarsat Government and its subsidiaries remain subject to the DCSA proxy agreement;
l. A re-identification of the name of and contact information of the LEPOC; and

m. Notifications regarding any other matter of interest to this LOA.

The annual report will be due each calendar year beginning one (1) year from the Date of this LOA, and shall be addressed to:

Assistant Attorney General for National Security
U.S. Department of Justice
National Security Division
950 Pennsylvania Avenue NW
Washington, DC 20530
Attention: Foreign Investment Review Section / Team Telecom

With a second copy to:

Foreign Investment Review Section / Team Telecom
U.S. Department of Justice
National Security Division
3 Constitution Square, 175 N Street NE
Washington, DC 20002

Inmarsat agrees to send courtesy electronic copies of all notices and communications to the following individuals or any other individuals that DOJ identifies to Inmarsat in the future: Lee Licata, USDOJ (at Lee.Licata@usdoj.gov); Eric Johnson (at Eric.S.Johnson@usdoj.gov); Loyaan Egal, USDOJ (at Loyaan.Egal@usdoj.gov) and FIRS Team (at FIRS-TT@usdoj.gov).

Miscellaneous

32. Inmarsat agrees to permit USDOJ's requests for visits to sites controlled by Inmarsat or to which Inmarsat otherwise has authority to permit such site visits and approve all requests to conduct on-site interviews of Inmarsat employees.

33. Inmarsat agree to negotiate in good faith and promptly with USDOJ if USDOJ finds that the terms of this LOA are inadequate to resolve any national security, law enforcement, or public safety concerns.

34. Inmarsat agrees that in the event that it fails to comply with a material commitment set forth in this LOA, USDOJ may, after providing notice to Inmarsat detailing the alleged noncompliance and a reasonable period of not less than fifteen (15) calendar days to cure the noncompliance consistent with previous agreements and as appropriate given the severity of the noncompliance, request the FCC modify, condition, revoke, cancel, terminate or render null and void any relevant license, permit, or other authorization granted by the FCC to Inmarsat or its successors-in-interest in addition to pursuing any other remedy available at law or equity.

35. Inmarsat agrees that this agreement supersedes the following agreements, all of which shall terminate and be of no further effect following the Date of this LOA:

a. The September 17, 2008 Agreement between Inmarsat Global Ltd., its affiliates, and subsidiaries on one hand, and USDOJ and DHS on the other hand.
b. The August 7, 2001 Agreement between MarineSat Communications Network, Inc. and Stratos Mobile Networks (US), LLC on one hand and USDOJ and FBI on the other hand.
c. The 2007 Amendment to the agreement referenced in Paragraph 35(b) between Robert M. Franklin, CIP Canada Investment Inc., Stratos Mobile Networks Inc, and DHS.

Confidentiality

36. Inmarsat agrees to the obligations set forth herein based on USDOJ's commitment to 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 LOA) to them in connection with this LOA 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), Inmarsat and USDOJ 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)).

37. Inmarsat understands that, upon execution of this LOA by an authorized representative or attorney, or shortly thereafter, USDOJ agrees to notify the FCC that it does not object to the FCC's consent to Inmarsat's application.

Sincerely,

Inmarsat plc

By:  Date: September 13, 2019

Alison Horrocks
Chief Corporate Affairs Officer