

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

In the Matter of the Joint Application of)	
)	
Tofane Global SAS)	
<i>Transferee,</i>)	
)	IB File No. ITC-T/C-20180504-00082
KPN B.V.)	
<i>Transferor,</i>)	WC Docket No. 18-136
)	
and)	
)	
iBasis, Inc.)	
<i>Licensee</i>)	
)	
For Grant of Authority Pursuant to Section)	
214 of the Communications Act of 1934, as)	
amended, and Sections 63.04 and 63.24 of the)	
Commission’s Rules to Transfer Control of a)	
Company Holding Domestic and International)	
Section 214 Authorizations)	

**PETITION TO ADOPT CONDITIONS TO
AUTHORIZATIONS AND LICENSES**

The U.S. Department of Justice (“USDOJ”), to include its components, the National Security Division (“NSD”) and the Federal Bureau of Investigation (“FBI”), with the concurrence of the U.S. Department of Homeland Security (“DHS”) (collectively, the “Agencies”) submits this Petition to Adopt Conditions to Authorizations and Licenses (“Petition”) pursuant to Section 1.41 of the Federal Communications Commission (“Commission”) rules.¹ Through this Petition, the USDOJ advises the Commission that the

¹ 47 C.F.R. § 1.41 (2017).

Agencies have no objection to the Commission approving the authority sought in the above-referenced proceeding, provided that the Commission conditions its approval on the assurances of Tofane Global SAS (“Tofane”) and iBasis, Inc. (“iBasis”) to abide by the commitments and undertakings set forth in the December 14, 2018 Letter of Agreement (“LOA”), a copy of which is attached hereto.

The Commission has long recognized that law enforcement, national security, and public safety concerns are part of its public interest analysis and has accorded deference to the views of other U.S. government agencies with expertise in those areas. *See In the Matter of Comsat Corporation d/b/a Comsat Mobile Communications, etc.*, 16 FCC Rcd. 21661, 21707 ¶ 94 (2001).

After discussions with representatives of Tofane and iBasis in connection with the above-referenced proceeding, the Agencies have concluded that the additional commitments set forth in the LOA will help ensure that those agencies with responsibility for enforcing the law, protecting the national security, and preserving public safety can proceed appropriately to satisfy those responsibilities.

Accordingly, the USDOJ with the concurrence of DHS advises the Commission that it has no objection to the Commission granting the application in the above-referenced proceeding, provided that the Commission conditions its consent on compliance with the December 14, 2018 LOA.

December 14, 2018

Respectfully submitted,

LOYAAN A. EGAL
Deputy Chief
Foreign Investment Review Staff
National Security Division
United States Department of Justice

/s/ Siobhan E. Dupuy
SIOBHAN E. DUPUY
Attorney Advisor
Foreign Investment Review Staff
National Security Division
United States Department of Justice
Washington, DC 20530



10 Maguire Road
Lexington, MA 02421
Phone +1 781.430.7500
Fax +1 781.430.7300
iBasis.com

December 14, 2018

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

Subject: FCC IB File No. ITC-T/C-20180504-00082, WC Docket No. 18-136
Application by Tofane Global SAS, KPN B.V., and iBasis, Inc., for authority
pursuant to Section 214 of the Communications Act of 1934, as amended, to
transfer control of international Section 214 authorizations.

Dear Sir/Madam:

This Letter of Agreement (“LOA” or “Agreement”) sets forth the commitments made by iBasis, Inc. (“iBasis”) and Tofane Global SAS (“Tofane”) to the U.S. Department of Justice (“USDOJ”) in order to address national security, law enforcement, and public safety concerns arising from the joint application filed by Tofane, KPN B.V. (“KPN”) and iBasis with the Federal Communications Commission (“FCC”) requesting approval to transfer control of iBasis and its Section 214 authorizations to Tofane pursuant to Section 214 of the Communications Act, as amended (the “Act”), and the implementing regulations in Part 63 of Title 47 of the Code of Federal Regulations.

This LOA supersedes and replaces a previous letter dated August 22, 2006 from iBasis and KPN to DOJ, including the Federal Bureau of Investigation (“FBI”), and to the U.S. Department of Homeland Security, which included a number of commitments and served as a condition to the transfer of control of iBasis and its international Section 214 authorization, FCC IB File No. ITC-214-19971126-00741, to KPN (FCC IB File No. ITC-T/C-200607070-00337).

iBasis and Tofane (together, the “Parties”) adopt as true and correct any and all representations made by each party to USDOJ through the Team Telecom review process, whether such representations were made directly by Tofane or iBasis, or through each party’s counsel.

1. For purposes of this LOA, the following definitions apply:
 - a. “Tofane” means Tofane Global SAS or its successors-in-interest.

b. “Access” or “Accessible” means the ability to physically or logically undertake 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.

c. “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.

d. “Customer Proprietary Network Information” (“CPNI”) shall mean as defined in 47 U.S.C. § 222(h)(1).

e. “Date of this LOA” shall mean the date on which the LOA is executed by iBasis and Tofane.

f. “Domestic Communications” or “DC” means: (i) Wire Communications or Electronic Communications (whether stored or not) from one U.S. location to another U.S. location; or (ii) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States: (A) “Electronic Communication” has the meaning given it in 18 U.S.C. § 2510(12); (B) “Wire Communication” has the meaning given it in 18 U.S.C. § 2510(1).

g. “Domestic Communications Infrastructure” or “DCI” means: (i) the transmission and switching equipment (including hardware, software, and upgrades), routers, servers, security appliances, and fiber and copper cable and associated facilities owned (to include leased) and controlled by or on behalf of iBasis to provide, process, direct, control, supervise or manage Domestic Communications; (ii) facilities and equipment leased or owned by or on behalf of iBasis that are physically located in the United States; or (iii) the property, facilities and equipment leased or owned by or on behalf of iBasis to control the equipment or facilities described in (i) and (ii) above. The phrase “on behalf of,” as used in this paragraph, does not include entities with which iBasis has contracted for peering, interconnection, roaming, long distance, or other similar arrangements.

h. “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, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 et seq. and 50 U.S.C. § 1841 et seq.; (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.

j. “Geolocation Data” means any information collected by iBasis from its customers regarding a customer or the customer’s device location.

k. “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.

l. “Internet Protocol Detail Record” (“IPDR”) means a streaming data protocol used by Operations Support Systems (“OSS”) and Business Support Systems (“BSS”) to collect and record a user’s data traffic statistics on a network.

m. “Internet Search Information” includes any data collected by iBasis about its customer’s internet browsing or online purchasing activities through any mechanism permitted by the services offered by iBasis.

n. “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.

o. “Managed Network Service Provider” or (“MNSP”) means any third party that provides services to iBasis and its subsidiaries in support of its (a) telecom and/or Internet infrastructure, business, services, or operation including but not limited to: network operation; provisioning of Internet and telecom services; routine, corrective, and preventative maintenance, including switching, routing and testing; network and service monitoring; network performance, optimization, and reporting; network audits, provisioning, development, and the implementation of changes and upgrades; or (b) provision of DC or operation of DCI, including: customer support; OSS; BSS; NOCs; information technology; cloud operations/services; next generation, including 5G (SDN, NFV, Applications); and datacenter services/operations.

p. “Mercury Affiliates” means SFR ICS (formerly known as Mercury France), Meo ICS (formerly known as Mercury Portugal), and Altice Dominicana ICS (formerly known as Mercury Dominican Republic).

q. “Network Elements” means a facility, equipment, software, hardware or applications used in the provision of telecommunications services, including features,

functions and capabilities that are provided by means of such facility or equipment, including subscriber numbers, databases, signaling systems, and information sufficient for billing, receiving and/or aggregating customer data, and collection or used in the transmission, routing, or other provision of telecommunications services.

r. “Network Management Capabilities” means software or applications used to manage or monitor network operations.

s. “Network Operations Center” or “NOC” means any locations and facilities performing network management, monitoring, accumulation of accounting and usage data, maintenance, user support, or other operational functions for Domestic Communications.

t. “Non-U.S. Government” means any government, including an identified representative, agent, component or subdivision thereof, that is not a local, state, or federal government in the United States.

u. “Offshoring” means performing obligations of this Agreement through the use of entities and personnel outside of the territorial limits of the United States, whether those entities or personnel are employees of iBasis or its subsidiaries, or third parties.

v. “Outsource” or “Outsourcing” means, with respect to Domestic Communications, supporting the services and operational needs of iBasis at issue in this LOA through the use of contractors or third parties.

w. “Personal Identifiable Information” (“PII”) means the name and aliases, social security number, date of birth, place of birth, citizenship status, contact information, and current address of an individual.

x. “Principal Equipment” means all primary telecommunications and information network (e.g., wireline, wireless, subsea, satellite, LAN, WAN, WLAN, SAN, MAN, IP, MPLS, FR, Wi-Fi, 3G/4G/LTE, 5G, etc.), equipment (e.g., hardware, software, platforms, OS, applications, protocols), that supports core telecommunication/information services (e.g., voice, data, text, MMS, FAX, video, Internet, OTT, Apps), functions (e.g., network/element management, maintenance, provisioning, NOC, etc.), operations (e.g., OSS/BSS, customer support, billing, backups, cloud services, etc.) including but not limited to routers, servers, circuit switches/softswitches, PBXs, call processors, databases, storage devices, load balancers, radios, smart antennas, transmission equipment (RF/Microwave/Wi-Fi/Fiber Optic), RAN, SDR, equalizers/amplifiers, MDF, digital/optical cross-connects, PFE, multiplexers, HLR/VLR, gateway routers, signaling, Network Function Virtualizations, hypervisors, EPC, BSC, BT, eNodeB, etc.

y. “Security Incident” means (i) any known breach or suspected breach of the Agreement, including a violation of any Network and Systems Security Plan

(“NSSP”) or use of Outsourced or Offshore service providers or network equipment except in compliance with the terms of this Agreement; (ii) any known exploitation or suspected exploitation of a security vulnerability; (iii) any unauthorized Access to, or disclosure of PII; (iv) any unauthorized Access to, or disclosure of, information obtained from or relating to U.S. federal, state or local government entities; or (v) any one or more of the following that affect the company’s computer network(s) or associated information systems: (A) unplanned disruptions to a service or denial of a service; (B) unauthorized processing or storage of data; (C) unauthorized changes 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 Agreement.

z. “Sensitive Information” means 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; or
- vi. other 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.”

aa. “Subscriber Information” means information of the type referred to and accessible subject to the procedures specified in 18 U.S.C. § 2703(c)(2) or 18 U.S.C. § 2709, as amended or superseded.

bb. “Transactional Data” means:

- i. any “call-identifying information,” as defined in 47 U.S.C. § 1001(2), as amended or superseded, including, without limitation, the telephone number or similar identifying designator associated with a communication;
- ii. Internet address or similar identifying designator associated with a communication;
- iii. the time, date, size, and duration of a communication;
- iv. any information relating specifically to the identity and physical/logical address of a subscriber, user, or account payer of iBasis;

- v. to the extent associated with a subscriber, user, or account payer of iBasis, any information relating to telephone numbers, Internet addresses, e-mail accounts, text messages, Instant Messages (“IMs”) or similar identifying designators, to include the physical location of equipment, if known and if different from the location information otherwise provided and the types of service, length of service, fees, and usage, including CDRs, CPNI, and any other billing records; and
- vi. any information indicating, as closely as possible, the physical location to or from which a communication is transmitted.

cc. “U.S. Records” means iBasis’ customer billing records, Subscriber Information, text, Internet Search Information, online purchasing information, or Geolocation Data, CPNI, and any other related information used, processed, or maintained in the ordinary course of business relating to the services offered by iBasis in the United States, including information subject to disclosure to a U.S. federal or state governmental entity under the procedures specified in 18 U.S.C. § 2703(c) and (d) and 18 U.S.C. § 2709.

2. iBasis confirms that it will comply with all applicable lawful interception statutes, regulations, and requirements, including the Communications Assistance for Law Enforcement Act (“CALEA”), 47 U.S.C. 1001 *et seq.*, and its implementing regulations, as well as comply with all court orders and other Lawful U.S. Process for lawfully authorized Electronic Surveillance.

3. Upon receipt of any Lawful U.S. Process, iBasis shall place within the territorial boundaries of the United States any and all information requested by the Lawful U.S. Process within the period of time for response specified in the Lawful U.S. Process, or as required by law, and shall thereafter comply with the Lawful U.S. Process.

4. iBasis agrees to notify USDOJ, at least 30 calendar days in advance, of any change to (a) its current services portfolio or (b) any peering relationships or joint ventures with Foreign companies providing data aggregation or reselling services.

5. iBasis agrees that it will not, directly or indirectly, disclose or permit disclosure of or Access to U.S. Records or Domestic Communications or any information (including call content and call data) pertaining to a wiretap order, pen/trap and trace order, subpoena, or any other Lawful U.S. Process demand if the purpose of such disclosure or access is to respond to the legal process or request on behalf of a non-U.S. Government entity without first satisfying all pertinent requirements of U.S. law and obtaining the express written consent of USDOJ, or the authorization of a court of competent jurisdiction in the United States. Any such requests for legal process submitted by a non-U.S. Government entity to iBasis shall be referred to USDOJ as soon as possible, but in no event later than five (5) business days after such request or legal process is received by or made known to iBasis, unless disclosure of the request or legal process

would be in violation of U.S. law or an order of a court of competent jurisdiction in the United States.

6. Measures to Prevent Improper Use or Access: iBasis shall take all practicable measures to (a) prevent the use of or Access to the equipment or facilities supporting those portions of iBasis' DCI's necessary for conducting Electronic Surveillance where such use or Access would violate any U.S. law or the terms of this Agreement or any implementation plans; (b) prevent sharing of any captured data packets with any Mercury Affiliate; and (c) prevent any Mercury Affiliates from having operational Access to iBasis' infrastructure, DCI, customer records, or electronic interfaces that allow control and monitoring of the iBasis infrastructure or data content. These measures shall include technical, organizational, personnel-related policies and written procedures, as well as necessary implementation plans and physical security measures.

7. With regard to Foreign production of virtual mobile profiles of mobile network operators, iBasis agrees that:

- i) the Foreign production of such profiles used in devices in the United States shall be limited solely to the initial profile, to include initial profiles produced by Giesecke+Devrient ("G&D). Unless specifically approved in writing by the USDOJ, no follow on remote access to phone/eSIM cards, such as customization, updating or other provisioning of that profile, is permitted from Foreign locations; and
- ii. eSIM cards with virtual mobile profiles produced outside the United States will be subject to statistically relevant integrity tests (e.g., Byte counts) to ensure the integrity of the initial eSIM profile.

8. iBasis agrees to draft and submit: (a) a NIST-Compliant Cyber Security Plan; and (b) a NSSP, which will be forwarded to USDOJ within 60 calendar days of the Date of this LOA for objection or non-objection. The NSSP shall address, but not be limited to, information security, remote access, physical security, cyber-security, third party contractors, Outsourcing and Offshoring, system logs, protection of Lawful U.S. Process and protection of U.S. Records obtained by iBasis from its customers or through the provision of services.

9. iBasis agrees to require any MNSP to disclose any data breach of any U.S. Records, or any loss of U.S. Records, whether from a data breach or other cause, within 48 hours of the third party discovering the breach or loss. To the extent that iBasis has current agreements with any third party providers of services with Access to U.S. Records, iBasis agrees to amend those agreements to require those third parties to make disclosure of breaches or loss of U.S. Records consistent with this paragraph, and shall forward copies of those amended agreements to USDOJ points of contacts listed herein within five (5) business days of executing those amendments.

10. iBasis agrees to notify the FBI and U.S. Secret Service within seven (7) business days upon having knowledge that a person or entity without authorization, or in exceeding their

or its authorization, has intentionally gained Access to, used, or disclosed any of its customer's CPNI or that of a third party used by iBasis, and shall report the matter to the central reporting facility through the following portal:

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

11. iBasis agrees to designate a Security Officer within 30 calendar days from the Date of this LOA. The Security Officer will have appropriate senior-level corporate authority within iBasis, and the necessary resources and skills, to maintain iBasis' security policies and procedures and oversee iBasis' compliance with this LOA. The Security Officer will be a U.S. citizen residing in the United States, and, if not already in possession of a U.S. security clearance, shall be eligible to hold such security clearance immediately upon appointment. The Security Officer will be subject to USDOJ's review and non-objection and may be subject to a background check at the sole discretion of USDOJ. If USDOJ objects to the Security Officer nominee, such objection must be made within 30 calendar days of receiving notice of the nominee. The Security Officer will serve as the primary point of contact for USDOJ regarding any national security, law enforcement, or public safety concerns that USDOJ may raise. The Security Officer shall be responsible for receiving and promptly effectuating any requests for information pursuant to this LOA and for otherwise ensuring compliance with obligations set forth in this LOA. iBasis shall notify USDOJ of any proposed change to the Security Officer at least 10 calendar days in advance of such change, (except in the case of the unexpected firing, resignation or death of the Security Officer in which case such written notice must be provided within five (5) calendar days of such event). Any subsequently proposed Security Officer shall be subject to USDOJ's review and non-objection and may be subject to a background check at the sole discretion of USDOJ. As applicable, the Security Officer will instruct and train iBasis officers, employees, contractors and agents on the requirements of this LOA.

12. iBasis agrees to maintain a U.S. law enforcement point of contact ("LEPOC") in the United States. The LEPOC shall be a U.S. citizen residing in the United States unless USDOJ agrees in writing otherwise, and the LEPOC must be approved by the FBI to receive service 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. This LEPOC and his/her contact information will be provided to USDOJ within 15 business days from the date iBasis receives the FCC's approval of the transfer. In addition, iBasis will give USDOJ, including the FBI, at least 30 calendar days' prior written notice of any change to its LEPOC (except in the case of the unexpected firing, resignation or death of the LEPOC in which case such written notice must be provided within five (5) calendar days of such event), and iBasis' nominated replacement shall be subject to USDOJ, including the FBI, review and approval. iBasis also agrees that the 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) calendar days after receiving such Lawful U.S. Process unless granted an extension by USDOJ.

13. iBasis agrees to provide USDOJ within 30 calendar days from the date that the FCC approves the transfer of control:

- 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.

14. iBasis agrees to meet and confer with USDOJ and to consider any concerns USDOJ may raise about the Principal Equipment List submitted pursuant to this LOA and will work with USDOJ if there are any concerns related to such Principal Equipment List.

15. iBasis agrees to provide USDOJ notice at least 10 business days in advance to performing any maintenance, repair, or replacement that would result in any material modification to existing Principal Equipment or systems or software used with or supporting the Principal Equipment, including the names of providers, suppliers, and entities that will perform any maintenance, repair, or replacement. USDOJ shall object or non-object to such new Principal Equipment or change/modification to the Principal Equipment within 30 calendar days of receipt of notice. iBasis need not comply with the advance notice requirement for any maintenance, repair, or replacement that is undertaken in response to an unforeseen or uncontrollable event and that is necessary to ensure the continued operability of the iBasis' network. However, in such circumstances, iBasis shall provide advance notice to USDOJ of the material modification, if practicable, and, if impracticable, iBasis shall provide notice within 10 business days after the material modification of the Principal Equipment commences. iBasis agrees to meet and confer with USDOJ and to consider any concerns USDOJ may raise about materials submitted pursuant to this provision.

16. iBasis agrees to provide notice at least 30 calendar days in advance to making any modifications to the list of vendors, contractors, or subcontractors involved in providing, installing, operating, managing, or maintaining the Principal Equipment. In addition, iBasis shall provide notice at least 30 calendar days in advance to changing the service offerings or support from a previously-listed vendor, contractor, subcontractor (i.e., where a previously-listed provider will be offering support in a previously unidentified way). iBasis agrees to negotiate in good-faith to resolve any national security, law enforcement, or public safety concerns USDOJ may raise with respect to materials submitted pursuant to this provision.

17. iBasis agrees to take all reasonable measures to prevent unauthorized Access to the DCI and to prevent any unlawful use or disclosure of information carried on the same. Such measures shall include a NIST-compliant cyber-security plan, security procedures for any remote virtual private network ("VPN") access to the DCI, contractual safeguards and screening procedures for personnel with administrative Access to the DCI; and procedures for applying security patches to systems and applications. iBasis will submit policies regarding logical (access) security measures for the DCI to USDOJ within 60 calendar days from the Date of this

LOA. iBasis agrees to meet and confer with USDOJ, including the FBI, regarding such policies upon request.

18. iBasis agrees to provide USDOJ within 30 calendar days from the Date of this LOA with a list of:

- a. All persons who have Access to Sensitive Information;
- b. All persons who have Access to Domestic Communications Infrastructure to monitor the content of Domestic Communications;
- c. All persons who have the ability to monitor personnel with Access to Domestic Communications under this subsection;
- d. All persons who have Access to Transactional Data, Subscriber Information, CPNI, CDRs, IPDRs, or PII for customers and network users of iBasis;
- e. All persons who have limited access to Domestic Communications Infrastructure;
- f. All persons who provision Network Elements either onsite or remotely;
- g. All vendors, contractors, or subcontractors, including billing vendors and managed service providers, involved in Accessing, managing, or maintaining CDR, Classified Information, CPNI, IPDR, PII, Sensitive Information, Subscriber Information or Transactional Data; and
- h. All vendors, contractors, or subcontractors, including managed service providers, involved in providing network or software services, to include network security and cloud solutions.

19. USDOJ shall approve or disapprove any person included on the list required pursuant to Paragraph 18 within 30 calendar days of receipt unless extended or otherwise delayed by awaiting responses to inquiries for further information from iBasis, in which event USDOJ shall be afforded additional time to approve or disapprove the listed person. USDOJ's additional time to approve or disapprove shall be the original 30-day window extended by the number of days USDOJ awaited a response from iBasis. Failure by USDOJ to respond within the required timeframe shall not be deemed to constitute a non-objection to the listed person.

20. iBasis shall provide USDOJ notice at least 30 calendar days in advance to making any modifications or additions to the list of vendors, contractors, or subcontractors provided pursuant to Paragraph 18. In addition, iBasis shall provide notice at least 30 calendar days in advance to changing in any material respects the service offerings or support from a previously listed vendor, contractor, subcontractor provided pursuant to Paragraph 18 (i.e., where a previously listed provider will be offering support in a previously unidentified way). USDOJ

shall approve or disapprove any additions, modification or change proposed pursuant to this Paragraph within 30 calendar days of receipt unless extended or otherwise delayed by awaiting responses to inquiries for further information from iBasis. Notwithstanding the foregoing, in the event of exigent circumstances, USDOJ may extend the time for its approval or disapproval of any notice provided by iBasis under this Paragraph by a maximum of 30 additional calendar days by giving written notice of such extension to iBasis within 30 calendar days of the initial receipt of the notice. USDOJ agrees that it will make good-faith efforts to respond to each notice within the initial 30-day period (subject to any automatic extensions provided for above) and will not routinely request extensions under this Paragraph.

21. iBasis agrees to promptly notify USDOJ, including the points of contact (“POCs”) listed herein, of any breaches of this agreement, as well as any other Security Incidents such as, but not limited to cyber-security incidents, intrusions or breaches of the DCI or Network Elements. The notification shall take place no later than 15 calendar days after iBasis or any third party providing Outsource or Offshore services to iBasis discovers the incident, intrusion or breach takes place, or sooner when required by statute or regulations.

22. iBasis agrees to instruct and train appropriate officials, employees, contractors, and agents as to iBasis’ obligations under this LOA, including the individuals’ duty to report any violation, and shall issue periodic reminders of such obligations. iBasis shall issue these instructions in writing within 60 calendar days of the Date of this LOA. iBasis will submit a copy to USDOJ at the same time. Upon request, iBasis agrees to provide USDOJ a list of individuals who have completed LOA training.

23. iBasis agrees not to monitor, collect, market, or sell data from any U.S. Government customers in any way, including for any commercial purpose. This is not intended to conflict with any law enforcement provision of this LOA or other legal requirements.

24. iBasis agrees to permit USDOJ requests for site visits and approve all requests to conduct on-site interviews of iBasis employees.

25. iBasis further agrees that it will provide USDOJ notice at least 30 calendar days in advance of all Outsourced or Offshore service providers, including but not limited to services provided in relation to:

- Network Operation Center(s);
- Network maintenance services;
- Customer support services;
- Any operation/service that could potentially expose U.S. DCI and U.S. Records, including but not limited to customer data and records, CDR, or CPNI; and
- Any Network Management Capabilities that are provided by a person or entity owned, managed, manufactured or controlled by one or more foreign governmental or non-public entities.

USDOJ shall object or non-object to Outsourced or Offshore service providers, within 30 calendar days of receipt of notice.

26. iBasis agrees to provide USDOJ with notice of any material changes to its business, including but not limited to corporate structure changes, ownership changes, corporate name changes, business model changes, corporate headquarter location changes, or business operation location changes within 30 calendar days in advance of such change.

27. The Parties agree to provide an annual report to USDOJ regarding iBasis' compliance with this Agreement, to include:

- a. Certifications that there were no changes (where no changes were reported to USDOJ/FBI during the preceding year);
- b. Certification that iBasis has been in CALEA compliance;
- c. Notice(s) regarding iBasis' 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 list of individuals with access to U.S. CDRs of iBasis;
- d. Recertification on any changes in the services that iBasis provides or confirmation that no additional services are being offered;
- e. Notification(s) of any relationships with foreign-owned telecommunications partners, including any peer relationships;
- f. Updated list of iBasis's Principal Equipment, vendors and suppliers;
- g. Updated NSSPs and Procedures;
- h. Updated NIST-Compliant Cyber Security Plan;
- i. Notification(s) of the installation and/or purchase or lease of any foreign-manufactured telecommunication equipment (including, but not limited to, switches, routers, software, and hardware);
- j. Report(s) of any occurrences of cyber-security incidences, network and enterprise breaches, and unauthorized Access to customer data and information;
- k. A re-identification of the name of and contact information of the Security Officer and the LEPOC; and
- l. Notifications regarding any other matter of interest to this LOA.

The annual report will be due every 31st day of January of each calendar year, beginning on January 31, 2020, and will be addressed to:

Assistant Attorney General for National Security
U.S. Department of Justice
National Security Division
Three Constitution Square, 175 N Street NE,
Washington, DC 20002

Attention: FIRS/Team Telecom Staff

Courtesy electronic copies of all notices and communications will also be sent to the following or individuals identified in the future to the Parties by USDOJ: Bermel Paz, USDOJ (at Bermel.Paz@usdoj.gov); Siobhan Dupuy, USDOJ (at Siobhan.Dupuy@usdoj.gov); David Jividen, USDOJ (at David.Jividen@usdoj.gov); Loyaan Egal, USDOJ (at Loyaan.Egal@usdoj.gov) and FIRS Team (at FIRS-TT@usdoj.gov).

28. Tofane agrees to ensure that iBasis complies with the obligations of iBasis under this LOA.

29. The Parties agree that in the event that the commitments set forth in this letter are breached, USDOJ may request that the FCC modify, condition, revoke, cancel, or render null and void any relevant license, permit, or other authorization granted by the FCC to iBasis or its successors-in-interest, in addition to any other remedy available by law or equity. Nothing herein shall be construed to be a waiver by the Parties of, or limitation on, their right to oppose or comment on any such request.

31. The Parties understand that, upon execution of this LOA by an authorized representative or attorney, or shortly thereafter, USDOJ shall notify the FCC that it has no objection to the FCC's consent to the applications.

32. This LOA may be executed in one or more counterparts, including by facsimile and portable document format, each of which shall together constitute one and the same instrument.

[SIGNATURE PAGES FOLLOW]

Assistant Attorney General for National Security
December 14, 2018
Page 14

Sincerely,




Alexandre Pébureau
President
Tofane Global SAS
December 14, 2018

Name:
Title:
iBasis, Inc.
December 14, 2018

Assistant Attorney General for National Security
December 14, 2018
Page 14

Sincerely,

Alexandre Pébereau
President
Tofane Global SAS
December 14, 2018

A handwritten signature in black ink, appearing to read 'Feddo Hazewind', written over a horizontal line.

Name: Feddo Hazewind
Title: CEO
iBasis, Inc.
December 14, 2018