

RELIANCE - YIPES

**AGREEMENT**

**THIS AGREEMENT** (the “**Agreement**”) is made as of the Effective Date, by and between the following:

Reliance Communications Limited (“**Reliance Communications**”), and its subsidiary

Reliance Gateway Net Limited (“**Reliance Gateway**”) (collectively “**Reliance**”),

FLAG Telecom Group Limited (“**FLAG Group**”), which is wholly owned by Reliance, and its subsidiary

FLAG Telecom Group Services (“**FLAG Services**”) (collectively “**FLAG**”),

(Reliance and FLAG, collectively, the “**Acquirer**”);

Yipes Holdings, Inc. (“**Yipes Holdings**”) and its subsidiary

Yipes Enterprise Services, Inc. (“**Yipes Services**”) (collectively “**Yipes**”),

(the Acquirer and Yipes, collectively, the “**Communications Service Providers**”), on behalf of themselves and all current and future affiliates and subsidiaries, and

the U.S. Department of Justice (“**DOJ**”), and

the U.S. Department of Homeland Security (“**DHS**”),

(the “**USG Parties**”)

(referred to individually as a “**Party**” and collectively as the “**Parties**”).

**RECITALS**

**WHEREAS**, the Parties undertake this Agreement based upon the following recitals:

(1) U.S. communication systems are essential to the ability of the U.S. Government to fulfill its responsibilities to the public to preserve the national security of the United States, to enforce the laws, and to maintain the safety of the public;

(2) the U.S. Government has an obligation to the public to ensure that U.S. communications and related information are secure in order to protect the privacy of U.S.

## RELIANCE - YIPES

persons, to enforce the laws, and to protect the national security of the United States;

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

(4) preventing the disruption and preserving the integrity of communications in the U.S. and preventing the unauthorized dissemination to Foreign Persons and Foreign Entities, including foreign governments, of certain information and technology is critical to preserving the national security of the United States;

(5) protection of Classified Information and Sensitive Information is also critical to U.S. national security;

(6) the Acquirer, a Foreign Entity, is a global provider of communications services;

(7) Yipes Services currently provides to the financial, legal, government (Federal state, and local), educational, and healthcare industries managed Ethernet and application delivery services, including common carrier transport services, via a network of more than 22,000 route kilometers of fiber and associated equipment across seventeen (17) major U.S. metropolitan markets;

(8) Yipes Services operates two (2) Network Operations Centers (NOCs) in the United States in Denver, Colorado, and San Francisco, California, and, in addition to its seventeen (17) domestic markets, has existing Points of Presence (POPs) in London, United Kingdom (U.K.), Tokyo, Japan, and Hong Kong, Peoples Republic of China, and is in the process of deploying additional POPs in Frankfurt, Germany, Toronto, Canada, and London, U.K.;

(9) Yipes Services has integrated its communications network with various global partners as well as major U.S. telecommunications common carriers and Internet service providers (ISPs);

(10) Yipes Services also has access to a certain customer and end-user information that is subject to U.S. privacy and electronic surveillance laws;

(11) Yipes Services has an obligation under U.S. law to protect from unauthorized disclosure the contents and Transactional Data of communications transiting its network as well as customer and end-user information;

## RELIANCE - YIPES

1.5 “**Classified Information**” shall have the meaning indicated in Executive Order 12958, as amended by Executive Order 13292, or any successor executive order, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act of 1954.

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

- (a) the sale, lease, mortgage, pledge, or other transfer of any or all of the principal assets of the entity, whether or not in the ordinary course of business;
- (b) the dissolution of the entity;
- (c) the closing and/or relocation of the production or research and development facilities of the entity;
- (d) the termination or nonfulfillment of contracts of the entity;
- (e) the amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in Section 1.6(a) through (d); or
- (f) the obligations of the Communications Service Providers under this Agreement.

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

1.8 “**Domestic Communications**” means: (a) Wire Communications or Electronic Communications (whether stored or not) from one U.S. location to another U.S. location; and (b) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States, in each case where such Wire Communications or Electronic Communications are transmitted (in whole or in part) via the Domestic Communications Infrastructure.

1.9 “**Domestic Communications Infrastructure**” means: (a) transmission, switching, bridging and routing equipment (including software and upgrades) used by or on behalf of Yipes to provide, process, direct, control, supervise or manage Domestic Communications; (b) facilities and equipment used by or on behalf of Yipes physically located in the United States; and (c) facilities to control the equipment described in (a) and (b) above, but does not include entities with which the Communications Service Providers have contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree, nor

## RELIANCE - YIPES

equipment or facilities used by service providers other than Yipes that are interconnecting communications providers.

1.10 “**Domestic Network Management Information**” means network management operations plans, processes and procedures; descriptions of the placement of NOC(s) and linkages (for service offload or administrative activities) to other domestic and international carriers, ISPs and other critical infrastructures; descriptions of networks and operations processes and procedures for management control and relation to the backbone infrastructure(s) including other service providers; description of any unique or proprietary control mechanisms as well as operating and administrative software; and network performance information.

1.11 “**Effective Date**” means the date this Agreement becomes effective, which is the date this Agreement is signed by the last Party to sign it (as indicated by the date stated opposite that Party’s signature).

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

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

1.14 “**FCC Application**” includes all information whether in oral or written form provided to the FCC or any agency of the U.S. Government in connection with that application.

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

1.16 “**Foreign Person**” means any Person who is not a U.S. Person as provided by 31 C.F.R. § 800.222.

1.17 “**Foreign Entity**” means any Foreign Person, any Entity established under the laws of a country other than the United States, or any government other than the U.S. Government or a U.S. state or local government.

## RELIANCE - YIPES

1.18 **“Government,” “Government Authority,” or “Government Authorities”** means any government, or any governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau or political subdivision and any court, tribunal, judicial or arbitral body.

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

1.20 **“Lawful U.S. Process”** means lawful U.S. federal, state, or local Electronic Surveillance or other court orders, processes, or authorizations issued under U.S. federal, state, or local law for physical search or seizure, production of tangible things, or Access to or disclosure of Domestic Communications, Transactional Data, or Subscriber Information.

1.21 **“Management of Yipes”** means its officers and members of the Board of Directors.

1.22 **“Network Operations Center” or “NOC”** means the facilities and equipment used to monitor, secure, maintain, configure, or operate communications, data, supervisory control and data acquisition (“SCADA”), or business management networks or equipment for Domestic Communications and the Domestic Communications Infrastructure.

1.23 **“NOC Services”** means 24x7 NOC or network management, network flow and/or monitoring services provided on behalf of the Communications Service Providers in support of Domestic Communications and the Domestic Communications Infrastructure.

1.24 **“NOC Services Personnel”** means all Personnel performing NOC Services wherever located.

1.25 **“Personnel”** means (i) employees, officers, directors, and agents and (ii) contract or temporary employees (part-time or full-time) who are under the direction or control of Yipes; provided, however, that “Personnel” does not include independent contractors, customers, customers’ agents, and vendors who are not employed by or operate under the direction or control of Yipes.

1.26 **“Screened Positions”** are those Personnel positions that

- (a) allow Access to the Domestic Communications Infrastructure and enables such persons in fact or potentially to monitor the content of Wire or Electronic Communications (including in electronic storage) and/or direct any form of such communications to an unauthorized recipient;
- (b) allow Access to Transactional Data;
- (c) allow Access to Sensitive Information;

## RELIANCE - YIPES

- (d) perform NOC Services; or
- (e) perform security services.

1.27 “**Security Officer**” means the Head of Security for Yipes, or a designee in a direct reporting relationship with the Head of Security, who serves as the Security Officer with the primary responsibility for ensuring compliance with the Communications Service Providers’ obligations under this Agreement.

1.28 “**Sensitive Information**” means information that is not Classified Information regarding: (a) the persons or facilities that are the subjects of Lawful U.S. Process; (b) the identity of the Government Authority or Government Authorities serving such Lawful U.S. Process; (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance; (d) the means of carrying out Electronic Surveillance; or (e) the type(s) of service, telephone number(s) or other similar identifiers, records, communications, or facilities subjected to Lawful U.S. Process; as well as all other information that is not Classified Information but is designated in writing by an authorized official of a federal, state, or local law enforcement agency or a U.S. intelligence agency as “Sensitive Information” of some type recognized by the agency involved. The designation “Sensitive” as used in this Section includes but is not limited to information marked or labeled “Official Use Only,” “Limited Official Use Only,” “Law Enforcement Sensitive,” “Sensitive Security Information,” “Sensitive but Unclassified,” “Controlled Unclassified Information,” or other similar designations.

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

1.30 “**Transactional Data**” includes the following when associated with a Domestic Communication but does not include the content of any communication:

- (a) “call identifying information,” as defined in 47 U.S.C. § 1001(2), including without limitation the telephone number or similar identifying designator;
- (b) any information related to the sender or recipient of that Domestic Communication, including, without limitation subscriber identification, called party number, calling party number, start time, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, post-cut-through dialed digit extraction, in-band and out-of-band signaling, and party add, drop and hold;

## RELIANCE - YIPES

- (c) any information relating specifically to the identity and physical address of a customer or subscriber, or account payer, or the end-user of such customer or subscriber, or account payer, or associated with such person relating to all telephone numbers, domain names, Internet Protocol (“IP”) addresses, Uniform Resource Locators (“URLs”), other identifying designators, types of services, length of service, fees, usage including billing records and connection logs, and the physical location of equipment, if known and if different from the location information provided under (e) below;
- (d) the time, date, size, or volume of data transfers, duration, domain names, Media Access Control (“MAC”) or IP addresses (including source and destination), URL’s, port numbers, packet sizes, protocols or services, special purpose flags, or other header information or identifying designators or characteristics, including electronic mail headers showing From: and To: addresses; and
- (e) as to any mode of transmission (including mobile transmissions), and to the extent permitted by U.S. laws, any information indicating as closely as possible the physical location to or from which a Domestic Communication is transmitted.

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

1.32 **“Visitor”** means any Person who enters a Yipes facility other than Personnel.

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

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

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

2.1 **Domestic Communications Infrastructure.** Except to the extent and under conditions concurred in by the USG Parties in writing:

- (a) all Domestic Communications Infrastructure shall be directed, controlled, supervised and managed by Yipes exclusively from within the United States; and

## RELIANCE - YIPES

- (b) Yipes shall provide technical or other assistance upon lawful request to facilitate Electronic Surveillance pertaining to the Domestic Communications Infrastructure.

2.2 **NOCs.** With respect to NOCs on the Domestic Communications Infrastructure or otherwise having access to Domestic Communications, the Communications Service Providers agree as follows:

- (a) Yipes shall provide written notice to the USG Parties at least **thirty (30) days** prior to activating any new NOC on the Domestic Communications Infrastructure or decommissioning any NOC existing as of the Effective Date;
- (b) NOC Services Personnel located outside the United States shall not exercise control of U.S. network elements of the Domestic Communications Infrastructure, and if an event occurs that requires escalation or intervention, U.S.-based NOC Services Personnel shall address such event; provided, that NOC Services Personnel located outside the United States may address such event only with the oversight and direct authorization of U.S.-based NOC Services Personnel;
- (c) Yipes shall prevent unauthorized changes to any network flow or configuration of the Domestic Communications Infrastructure through NOC Services or other means.

2.3 **Compliance with Lawful U.S. Process.** The Communications Service Providers agree that Yipes shall take all practicable steps to configure the Domestic Communications Infrastructure to be capable of complying, and Yipes employees in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with:

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

2.4 **Information Storage and Access.** Unless otherwise agreed to by the Parties, Yipes shall store exclusively in the United States the following:



### RELIANCE - YIPES

- (a) Domestic Communications, if such communications are stored by or on behalf of Yipes for any reason;
- (b) Transactional Data, if such communications are stored by or on behalf of Yipes for any reason;
- (c) Subscriber Information, if such communications are stored by or on behalf of Yipes for any reason;
- (d) Billing Records of domestic customers or subscribers of Yipes, if such communications are stored by or on behalf of Yipes for any reason; and
- (e) Domestic Network Management Information, if such communications are stored by or on behalf of Yipes for any reason.

Notwithstanding the foregoing, nothing in this Section imposes any restriction on storage of Yipes account information, which shall include information relating to invoicing, collections and customer service used in the ordinary course of business. Furthermore, nothing in this Section is meant to exclude the use of Yipes Transactional Data for business or network management purposes in the normal course of business if said data is subject to security and access controls. The phrase "on behalf of" as used in this Section does not include entities with which Yipes contracts in the ordinary course of business for peering, interconnection, roaming, collocation, long distance, or other similar commercial arrangements.

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

**2.6 Compliance with U.S. Law.** Nothing in this Agreement shall excuse the Communications Service Providers from any obligation they may have to comply with U.S. legal requirements for the retention, preservation, or production of information, records or data as well as all applicable requirements of CALEA, as applicable by law.

### ARTICLE 3: SECURITY

**3.1 Security Officer.** Within **ten (10) business days** of the Effective Date, Yipes shall designate a Security Officer to act as the point of contact to the USG Parties regarding compliance with this Agreement and any national security issues.

- (a) The Security Officer shall

## RELIANCE - YIPES

- (i) be a resident U.S. citizen corporate officer of Yipes;
  - (ii) hold a U.S. security clearance or meet the criteria that would be considered in a security clearance process; and
  - (iii) possess the authority to enforce this Agreement.
- (b) The Communications Service Providers shall consult in advance of the designation of the Security Officer with the USG Parties and shall reasonably address any concerns raised by the USG Parties regarding the selection and identity of the Security Officer.
- (c) The Security Officer shall have access to all information necessary to perform his or her duties, including, without limitation, security-related and technical information and business information, including but not limited to information regarding the existing and emerging products and services of Yipes and business plans of the Communications Service Providers affecting Yipes' ability to perform its obligations under this Agreement.
- (d) If any action of the Security Officer to enforce compliance with this Agreement is blocked or denied or the relevant information under this Agreement is not provided for any reason, the Security Officer shall immediately (not to exceed **five (5) days** from acquiring actual notice) report that fact to the USG Parties.

3.2 **Continuation of Current Level of Security Standards.** Yipes shall take all reasonable measures to maintain its security standards and policies at no less than the level represented to the USG Parties as of the Effective Date.

3.3 **Measures to Prevent Improper Use or Access.** Yipes shall take all reasonable measures to prevent the use of or Access to the Domestic Communications Infrastructure to conduct Electronic Surveillance, or to Access, obtain or disclose Domestic Communications, Transactional Data, Subscriber Information, Sensitive Information, in violation of any U.S. federal, state, or local laws or the terms of this Agreement. These measures shall include maintaining and/or creating and complying with written policies and procedures related to a comprehensive security strategy for Domestic Communications and the Domestic Communications Infrastructure, including all related activities of the Communications Services Providers. Upon written request of the USG Parties (or any of them), these policies and procedures shall be made available to the requesting Party or Parties. Furthermore, Yipes agrees to meet and confer with the USG Parties and reasonably address any concerns they may raise as part of the procedure described herein.

## RELIANCE - YIPES

3.4 **Access by Foreign Government Authorities.** Notwithstanding the provisions of Article 2.4 above, the Communications Service Providers shall not, directly or indirectly, disclose or permit disclosure of, or provide Access to Domestic Communications, Transactional Data, or Subscriber Information, stored by or on behalf of Yipes to any person if the purpose of such Access is to respond to legal process or the request of or on behalf of a Foreign Government, identified representative, component or subdivision thereof, without the express written consent of the USG Parties or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process shall be reported to the USG Parties as soon as possible and in no event later than **ten (10) business days** after such request or legal process is received by or known to Yipes. Yipes shall take reasonable measures to ensure that they will promptly learn of all such requests or submission of legal process.

3.5 **Disclosure to Foreign Government Authorities.** Yipes shall not, directly or indirectly, disclose or permit disclosure of, or provide Access to:

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

to any Foreign Government, identified representative, component or subdivision thereof, without satisfying all applicable U.S. federal, state and local legal requirements, and without obtaining either the express written consent of the USG Parties or the authorization of a court of competent jurisdiction in the United States. Any requests or any legal process submitted by a Foreign Government, an identified representative, a component or subdivision thereof to Yipes for the communications, data or information identified that is maintained by Yipes shall be referred to the USG Parties as soon as possible and in no event later than **ten (10) business days** after such request or legal process is received by or known to Yipes, 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. Yipes shall take reasonable measures to ensure that it will promptly learn of all such requests or submission of legal process.

3.6 **Notification of Access or Disclosure Requests from Foreign Non-Governmental Entities.** Within **ten (10) business days** after receiving legal process or requests from Foreign non-governmental entities for Access to or disclosure of Domestic Communications, Yipes shall notify the USG Parties in writing of such legal process or requests, unless such disclosure would be in violation of an order of a court of competent jurisdiction within the United States.

3.7 **Security of Lawful U.S. Process.** Yipes shall protect the confidentiality and security of all Lawful U.S. Process served upon it and the confidentiality and security of Sensitive

## RELIANCE - YIPES

Information in accordance with U.S. Federal and state law or regulation and this Agreement. Information concerning Lawful U.S. Process, or Sensitive Information shall be under the custody and control of the Security Officer.

**3.8 Restrictions Relating to Electronic Surveillance and Lawful U.S. Process.** Yipes shall control all activities related to implementation of Lawful U.S. Process, including activation of any CALEA or other lawfully authorized Electronic Surveillance capability, exclusively from within the United States. The Security Officer will limit access to any information related to lawfully authorized Electronic Surveillance activities or equipment or to Lawful U.S. Process, including but not limited to all related intercepts, orders data and equipment. Specifically, unless otherwise agreed by the USG Parties or the agent of the USG who supplied the information, the Security Officer will ensure that only U.S. citizens with a need to know have access to such information and will control access to documents and systems in order to ensure the requisite limitations. The Security Officer will promptly report to the USG Parties any attempt to access the information above or interfere with any lawfully authorized Electronic Surveillance activities, in a manner that is inconsistent with the requirements of this Agreement. The Security Officer will maintain a list of the identities of individuals to whom he or she has provided access to any lawfully authorized Electronic Surveillance activities or equipment or to Lawful U.S. Process, and will produce such list upon request by a USG Party or its designee.

**3.9 Points of Contact.** Within **ten (10) business days** of the Effective Date, Yipes shall designate points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process relating to Domestic Communications carried by or through, in whole or in part, the Domestic Communications Infrastructure, or relating to its customers or subscribers. The points of contact shall be in the United States, shall be available **twenty-four (24) hours per day, seven (7) days per week** and shall be responsible for accepting service and maintaining the security of Sensitive Information and any Lawful U.S. Process relating to Domestic Communications carried by or through, in whole or in part, the Domestic Communications Infrastructure, or relating to customers or subscribers of Yipes. Within **five (5) business days** of designating such points of contact, Yipes shall notify the USG Parties in writing of the points of contact, and thereafter shall notify the USG Parties of any change in such designation within **five (5) business days** of such change. The points of contact shall be resident U.S. citizens who, based on the information in Yipes possession, are eligible for appropriate U.S. security clearances. Yipes shall cooperate with any request by a Government Authority within the United States that a background check, security clearance process or both be completed for a designated point of contact.

**3.10 Information Security.** Yipes shall:

- (a) take appropriate measures to prevent unauthorized Access to data or facilities that might contain Sensitive Information;

## RELIANCE - YIPES

- (b) upon request from the USG Parties, provide the name, date of birth, and other relevant requested identifier information of each person who regularly handles or deals with Sensitive Information;
- (c) provide that the points of contact described in this Agreement shall have sufficient authority over any of Yipes employees who may handle 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
- (d) maintain appropriately secure facilities (e.g., offices) for the handling and storage of any Sensitive Information.

3.11 **Nondisclosure of Protected Data.** Yipes shall not directly or indirectly disclose information concerning Lawful U.S. Process, or Sensitive Information to any third party, or to any officer, director, shareholder, employee, agent, or contractor of the Communications Service Providers, including those who serve in a supervisory, managerial or executive role with respect to the employees working with the information, unless disclosure has been approved by prior written consent obtained from the USG 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.

3.12 **Notice of Obligations.** The Communications Services Providers shall instruct appropriate officials, employees, contractors, and agents as to their obligations under this Agreement, including the individuals' duty to report any violation of this Agreement and the reporting requirements of this Agreement, and shall issue periodic reminders to them of such obligations.

3.13 **Personnel Screening Process.** Yipes shall implement a thorough Personnel Screening Process within 60 days after the Effective Date of this Agreement. Yipes shall employ a reputable third party to screen any Personnel hired after the Effective Date who will occupy Screened Positions. These procedures must outline all screening requirements and investigative techniques to be used by the private party as well as how derogatory information will be handled and criteria for rejecting employees or applicants for screened positions. Yipes shall submit these procedures for review by the USG Parties within 30 days of the Effective Date of this Agreement. If the USG Parties do not object in writing within 30 days of receipt, Yipes can begin implementation. The USG Parties must be notified of any material change to the Personnel Screening Process. Yipes must immediately address reasonable concerns raised by the USG Parties regarding those changes.

The Personnel Screening Process must address the reliability and trustworthiness of Personnel in all Screened Positions. The process should include the following elements:

## RELIANCE - YIPES

- (1) At a minimum the Personnel Screening Process must require that the private party doing the actual investigative work conduct a background and credit check, in addition to a 5-year public criminal records check.
- (2) To the extent permitted by law, Yipes must maintain records regarding all Personnel candidates for Screened Positions who were not hired solely because of screening conducted under the Personnel Screening Process, including identifying information and a summary of the reason(s) for rejection.
- (3) Yipes must maintain records relating to the security screening status of all current and former Personnel in Screened Positions for a minimum of 3 years and must provide those records upon lawful request to the USG Parties or any third-party auditor designated by a USG Party.
- (4) Yipes shall provide annual instruction to Personnel in Screened Positions as to their obligations under the Agreement and the maintenance of their trustworthiness determination or requirements otherwise agreed. Yipes shall monitor the status of Personnel in Screened Positions, and shall remove Personnel who no longer meet the Screened Positions requirements.

3.14 **Visitor Access Control Plan.** Yipes must maintain procedures for controlling access to its facilities by Visitors. Any persons present at Yipes facilities who are not Personnel must be designated as Visitors and shall be subject to the Visitor Access Control Plan. This Visitor Access Control Plan shall include escort policies, access controls, and identification mechanisms consistent with this Agreement. It must be forwarded to the USG Parties for consultations. The USG Parties' objections, if any, must be reasonably addressed. It shall be implemented within 30 days of the Effective Date or such later date as agreed to the by the Parties during the consultations.

## **ARTICLE 4: REPORTING AND NOTICE**

4.1 **Filings Concerning de jure or de facto Control of Yipes.** If the Communications Service Providers make any filing with the FCC or any other Government Authority relating to the *de facto* or *de jure* control of Yipes or the Domestic Communications Infrastructure except for filings with the FCC for assignments or transfers of control that are *pro forma*, the Communications Service Providers shall promptly provide to the USG Parties written notice and copies of such filing.

4.2 **Change in Control.** If any member of the Management of Yipes acquires any information that reasonably indicates that any single foreign entity or individual, other than those already identified in connection with the pending FCC Application identified in this Agreement, has or will likely obtain an ownership interest (direct or indirect) in Yipes or the Domestic

## RELIANCE - YIPES

Communications Infrastructure above ten (10) percent, as determined in accordance with 47 C.F.R. § 63.09, or if any foreign entity or individual, singly or in combination with other foreign entities or individuals, has or will likely otherwise gain either: (i) Control; or (ii) *de facto* or *de jure* control of Yipes or the Domestic Communications Infrastructure, then such officer or director shall promptly cause Yipes to notify the USG Parties in writing within **ten (10) business days**. Notice under this Section shall, at a minimum:

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

**4.3 Notice of Foreign Influence.** If any member of the Management of Yipes acquires any information that reasonably indicates that any Foreign Government, any Foreign Government-controlled entity, or any Foreign Entity plans to participate or has participated in any aspect of the day-to-day management of Yipes or the Domestic Communications Infrastructure in such a way that:

- (a) interferes with or impedes the performance by Yipes of its duties and obligations under the terms of this Agreement;
- (b) interferes with or impedes the exercise by Yipes of its rights under the Agreement; or
- (c) raises a concern with respect to the fulfillment by the Communications Service Providers of their obligations under this Agreement;

then such officer or director shall within **ten (10) business days** notify the USG Parties in writing of the timing and the nature of the Foreign Government's or entity's plans or actions.

**4.4 Procedure and Process on Reporting.** Within **forty-five (45) days** of the Effective Date, Yipes shall adopt and distribute to the Management of Yipes, a written procedure or process for the reporting by the Management of Yipes of noncompliance with this Agreement. This written procedure or process shall also provide for the reporting by employees, agents and contractors to the Management of Yipes of information that must be reported to the USG Parties

## RELIANCE - YIPES

under this Agreement. Any violation by Yipes of any material term of such corporate policy shall constitute a breach of this Agreement. By a written statement, Yipes shall notify all employees, contractors and agents that the general categories of information identified in this Agreement should be disclosed to the Management of Yipes and shall set forth in a clear and prominent manner the contact information for a senior manager to whom such information may be reported. The written statement informing employees, contractors, and agents of the need to report this information shall also state that Yipes shall not discriminate against, or otherwise take adverse action against, anyone who reports such information to the Management of Yipes or the United States Government.

4.5 **Non-retaliation.** Within **forty-five (45) days** after the Effective Date, Yipes shall, by duly authorized action of its Board of Directors, adopt and distribute to the Management of Yipes an official corporate policy that strictly prohibits the Communications Service Providers 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 this Agreement, or has notified or attempted to notify the Management of Yipes to report information that he or she believes in good faith is required to be reported to USG Parties under either this Agreement or under Yipes written notice to employees on the reporting of any such information. Any violation by the Communications Service Providers of any material term of such corporate policy shall constitute a breach of this Agreement.

4.6 **Reporting of Incidents.** Yipes shall report to the USG Parties any information acquired by Yipes 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 Transactional Data in violation of federal, state, or local law or regulation (except for violations of FCC regulations relating to improper commercial use of Transactional Data); or
- (d) improper Access to or disclosure of Sensitive Information.

This report shall be made in writing by an appropriate officer of Yipes to the USG Parties no later than **ten (10) business days** after Yipes acquires information indicating a matter described in this Section. Yipes shall lawfully cooperate in investigating the matters described in this Section. Yipes 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.



## RELIANCE - YIPES

4.7 **Access to Information and Facilities.** The USG Parties may visit, at any time, any part of the Domestic Communications Infrastructure and Yipes security offices to conduct on-site reviews concerning the implementation of the terms of this Agreement and may at any time require unimpeded Access to information concerning technical, physical, management, or other security measures needed by the USG Parties to verify compliance with the terms of this Agreement.

4.8 **Access to Personnel.** Upon reasonable notice from the USG Parties, the Communications Services Providers shall make available for interview any Personnel of Yipes who is in a position to provide information to verify compliance with the terms of this Agreement.

4.9 **Annual Report.** On or before the last day of January of each year, the Security Officer of Yipes shall submit to the USG Parties a report assessing the Communications Service Providers' compliance with the terms of this Agreement for the preceding calendar year. 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 Yipes knowledge, will or reasonably could affect the effectiveness of or its compliance with this Agreement.

4.10 **CALEA Capabilities.** On or before the last day of February of each year, an appropriate technically competent officer of Yipes shall submit to the USG Parties a report assessing the CALEA Capabilities of the Domestic Communications Infrastructure and on an on-going basis said officer shall provide written notice to the USG Parties not less than **thirty (30) days** prior to any change to the Domestic Communications Infrastructure which would alter the CALEA Capabilities as previously reported.

4.11 **Emerging Products and Services.** On or before the last day of March of each year, Yipes shall provide to the USG Parties a description of any products and/or services, other than those identified as of the Effective Date, which Yipes has offered to any U.S.-based customer during the previous year.

RELIANCE - YIPES

4.12 **Notices.** Following the Effective Date, 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, or to such other representatives at such addresses as the Parties may designate in accordance with this Section:

Department of Justice  
Assistant Attorney General for National Security  
National Security Division  
950 Pennsylvania Avenue, NW  
Washington, DC 20530  
ttelecom@usdoj.gov

Department of Homeland Security  
Assistant Secretary for Policy  
Washington, DC 20528  
ip-fcc@dhs.gov

For Reliance Communications and Reliance Gateway:

Hasit Shukla  
Company Secretary  
Reliance Communications Limited  
'H' Block, 1st Floor  
Dhirubhai Ambani Knowledge City  
Navi Mumbai – 400 710  
Maharashtra State, India  
Hasit.Shukla@relianceada.com

With a copy to:

Tara K. Giunta, Esq.  
Paul Hastings Janofsky & Walker LLP  
875 15th Street, NW  
Washington, DC 20005  
U.S.A.  
taragiunta@paulhastings.com

RELIANCE - YIPES

For FLAG Group and FLAG Services:

Prakash Shenoy  
FLAG Telecom Ltd.  
Sovereign Court  
635 Simpson Road  
West Drayton  
Middlesex – UB7 OJE  
United Kingdom  
pshenoy@flagtelecom.com

With a copy to:

Tara K. Giunta, Esq.  
Paul Hastings Janofsky & Walker LLP  
875 15th Street, NW  
Washington, DC 20005  
U.S.A.  
taragiunta@paulhastings.com

For Yipes Holdings and Yipes Services:

Howard Warner  
General Counsel  
114 Sansome Street  
11th Floor  
San Francisco, CA 94104  
U.S.A.  
hwarner@yipes.com

With a copy to:

Mark Hornor  
Associate General Counsel  
114 Sansome Street  
11th Floor  
San Francisco, CA 94104  
U.S.A.  
mhornor@yipes.com

## RELIANCE - YIPES

### ARTICLE 5: FREEDOM OF INFORMATION ACT

5.1 **Protection from Disclosure.** The USG Parties shall take all reasonable measures to protect from public disclosure all information submitted by the Communications Service Providers (or other entities in accordance with the terms of this Agreement) to the USG Parties in connection with this Agreement and clearly marked with the legend "Business Confidential; subject to protection under 5 U.S.C. § 553(b); not to be released without notice to the filing party" or similar designation. Such markings shall signify that it is the Communications Service Providers 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, the USG Parties, as appropriate, shall notify the Communications Service Providers of the intended disclosure as provided by Executive Order 12600, 52 Fed. Reg. 23781 (June 25, 1987). If the Communications Service Providers object to the intended disclosure and their objections are not sustained, the USG Parties, as appropriate, shall notify the Communications Service Providers of its intention to release (as provided by Section 5 of E.O. 12600) not later than **five (5) business days** prior to disclosure of the challenged information.

5.2 **Use of Information for U.S. Government Purposes.** Nothing in this Agreement shall prevent the USG Parties from lawfully disseminating information as appropriate to seek enforcement of this Agreement, or from lawfully sharing information as appropriate with other federal, state, or local Government Authorities to protect public safety, law enforcement, or national security interests, provided that the USG Parties take all reasonable measures to protect the information from public disclosure. Further, nothing in this Agreement shall limit the ability of the USG Parties to disclose this Agreement or any information related to this Agreement to enforce or comply with any federal law or regulation.

### ARTICLE 6: FCC CONDITION

6.1 **FCC Approval.** Upon the execution of this Agreement by all the Parties, the USG Parties shall, on their own motion at an appropriate time or at the request of the Communications Service Providers, notify the FCC that, provided the FCC adopts a condition substantially the same as set forth in Exhibit A attached hereto (the "**Condition to FCC Authorization**"), the USG Parties have no objection to the FCC's grant of the pending Application described in the

## RELIANCE - YIPES

Recitals of this Agreement. This Section is effective upon the Effective Date, provided however that in the case of a material modification or withdrawal of the Application after the execution of this Agreement the effectiveness of this Section may be suspended by the USG Parties, and any such FCC filing is subject to the right to object.

### ARTICLE 7: DISPUTES

7.1 **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 the Assistant Secretary Policy of DHS, the Assistant Attorney General for the National Security Division of DOJ, and the General Counsel of Yipes Holdings and Yipes Services, or their respective designees, unless the USG Parties believe that important national interests can be protected, or Yipes believes that paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 7.2. 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 7.2.

7.2 **Enforcement of Agreement.** Subject to Section 7.1 of this Agreement, if any of the Parties 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 Yipes, 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 Yipes;
- (c) seek civil sanctions for any violation by the Communications Service Providers of any U.S. law or regulation or term of this Agreement;
- (d) pursue criminal sanctions against the Communications Service Providers, or any officer, director, employee, contractor, or agent of the Communications Service

## RELIANCE - YIPES

Providers, or against any other person or entity, for violations of the criminal laws of the United States; or

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

7.3 **Irreparable Injury**. The Communications Service Providers agree that the United States would suffer irreparable injury if for any reason the Communications Service Providers (or any of them) failed to perform any of its obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, the Communications Service Providers agree that, in seeking to enforce this Agreement, the USG Parties shall be entitled, in addition to any other remedy available at law or equity, to specific performance and injunctive or other equitable relief.

7.4 **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.

7.5 **Waiver of Immunity**. The Communications Service Providers agree that, to the extent that they or any of their 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. The Communications Service Providers agree 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 the Communications Service Providers (or any of them) with respect to compliance with this Agreement.

## RELIANCE - YIPES

7.6 **Forum Selection.** It is agreed by and between the Parties that a 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.

## ARTICLE 8: OTHER

8.1 **Right to Make and Perform Agreement.** The Communications Service Providers represent that they have 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 the Communications Service Providers 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 obligation imposed by any U.S. federal, state, or local laws on the Communications Service Providers; (b) any enforcement authority available under any U.S. or state laws; (c) the sovereign immunity of the United States; or (d) any authority the U.S. Government may possess over the activities or facilities of the Communications Service Providers 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 shall include any future amendments to such statutory provisions.

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 that utilize Lawful U.S. Process.

8.6 **Entire Agreement; Modifications.** This Agreement constitutes the entire agreement between the Parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations, and discussions, whether oral or written, of the Parties with respect to the subject matter. This Agreement may only be modified by written agreement signed by all of the Parties. The USG Parties agree to consider promptly and in good faith possible modifications to this Agreement if the Communications Service Providers believe that the obligations imposed on them 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

## RELIANCE - YIPES

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 Yipes**. The USG Parties agree to negotiate in good faith and promptly with respect to any request by the Communications Service Providers for relief from application of specific provisions of this Agreement if there is a change in circumstances such that those provisions become unduly burdensome or have a demonstrably adverse effect on Yipes competitive position.

8.9 **Changes in Circumstances for the USG Parties**. If after the date that all the Parties have executed this Agreement, the USG Parties find that the terms of this Agreement are inadequate to address national security, law enforcement, or public safety concerns, then the Communications Service Providers shall 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 the Communications Service Providers, and on all Affiliates of the Communications Service Providers.

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

8.13 **Notice of Additional Services**. The Communications Service Providers shall provide a minimum of **thirty (30) days** advanced notice to the USG Parties in the event that the Communications Service Providers or any Affiliate changes or intends to change the technical or operation plans set forth in the Recitals to this Agreement such that the material representations made therein are no longer fully accurate, true and complete.



**RELIANCE - YIPES**

8.14 **Non-Circumvention.** The Communications Service Providers shall not take any action outside the United States, through the use of a contractor, or through the use of any other agent which violates this Agreement.


*[Signature Pages Follow]*

RELIANCE - YIPES

This Agreement is executed on behalf of the Parties:

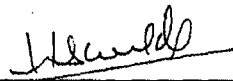
Date: 16<sup>th</sup> November 2007

Reliance Communications Limited

By:   
Printed Name: Hasit Shukla  
Title: Company Secretary

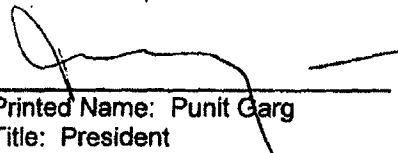
Date: 16<sup>th</sup> November 2007

Reliance Gateway Net Limited

By:   
Printed Name: Hasit Shukla  
Title: Authorised Signatory

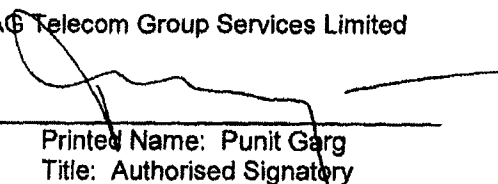
Date: 16<sup>th</sup> November 2007

FLAG Telecom Group Limited

By:   
Printed Name: Punit Garg  
Title: President

Date: 16<sup>th</sup> November 2007

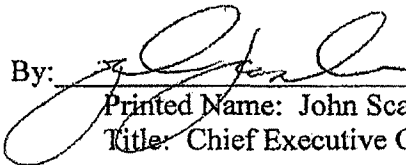
FLAG Telecom Group Services Limited

By:   
Printed Name: Punit Garg  
Title: Authorised Signatory

RELIANCE - YIPES

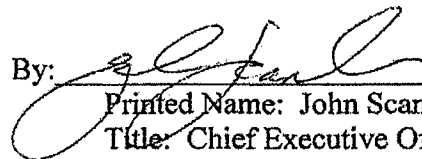
Yipes Holdings, Inc.

Date: 16 November 2007

By:   
Printed Name: John Scanlon  
Title: Chief Executive Officer


Yipes Enterprise Services, Inc.

Date: 16 November 2007

By:   
Printed Name: John Scanlon  
Title: Chief Executive Officer

**United States Department of Homeland Security**

Date: NOV 30 2007

By:   
Stewart A. Baker  
Assistant Secretary for Policy

**United States Department of Justice**

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

By: \_\_\_\_\_  
Kenneth L. Wainstein  
Assistant Attorney General for National  
Security

RELIANCE - YIPES

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

**IT IS FURTHER ORDERED**, that this authorization and any licenses granted thereunder are subject to compliance with the provisions of the agreement (the "**Agreement**") between Reliance Communications Limited, Reliance Gateway Net Limited, FLAG Telecom Group Limited, FLAG Telecom Group Services, Yipes Holdings, Inc., Yipes Enterprise Services, Inc., on behalf of themselves and all current and future affiliates and subsidiaries, and the U.S. Department of Justice ("**DOJ**"), and the U.S. Department of Homeland Security ("**DHS**"), dated October \_\_, 2007, which Agreement is designed to address national security, law enforcement, and public safety concerns of DOJ and DHS regarding the authority granted herein. Nothing in the Agreement is intended to limit any obligation imposed by federal law or regulation including, but not limited to, 47 U.S.C. § 222(a) and (c)(1) and the FCC's implementing regulations.