AGREEMENT

This AGREEMENT is made as of the date of the last signature affixed hereto, by and between XO Communications, Inc. ("XO"), on the one hand, and the Federal Bureau of Investigation ("FBI") and the U.S. Department of Justice ("DOJ"), on the other (referred to individually as a "Party" and collectively as the "Parties").

RECITALS

WHEREAS, 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;

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

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

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

WHEREAS, XO has an obligation to protect from unauthorized disclosure the contents of wire and electronic communications;

WHEREAS, XO provides the following services: (1) Internet access services, including dedicated access services and DSL services; (2) private data networking services, including dedicated transmission capacity, virtual private network services, and Ethernet services; (3) hosting services, including web hosting, server collocation, and application hosting; (4) local and both domestic and international long distance voice services; (5) shared tenant services; (6) interactive voice response systems; and (7) integrated voice and data services;

WHEREAS, XO (or its affiliated entities) provides or facilitates electronic communication services, remote computing services, and interactive computing services in the United States, and certain of its customers (including, *inter alia*, Internet-related companies) are themselves providers of electronic communication services, remote computing services, and interactive computer services, all of which are subject to U.S. privacy and electronic surveillance laws;

WHEREAS, XO (or its affiliated entities) has direct physical or electronic access to certain customer facilities, including servers, storage media, network connections, bandwidth transport, and firewalls, and thereby has access to a variety of customer and end-user information that is subject to U.S. privacy and electronic surveillance laws;

WHEREAS, XO has entered into a Stock Purchase Agreement (the "Stock Purchase Agreement"), dated January 15, 2002, among XO, Forstmann Little & Co. Equity Partnership-VII, L.P. ("Forstmann Little Equity VII"), Forstmann Little & Co. Subordinated Debt and Equity Management Buyout Partnership-VIII, L.P. ("Forstmann Little MBO VIII") (Forstmann Little Equity VII and Forstmann Little MBO VIII, collectively "Forstmann Little"), and Teléfonos de México, S.A. de C.V. ("Telmex," and collectively with Forstmann Little, the "Investors");

WHEREAS, XO has filed with the Federal Communications Commission ("FCC") applications (in IB Docket No. 02-50) under Sections 214 and 310(d) of the Communications Act of 1934, as amended, seeking FCC approval of the transfer of control of XO, upon consummation of the transactions contemplated by and pursuant to the terms of the Stock Purchase Agreement, from Craig O. McCaw and the existing shareholders of XO to the new shareholders of XO, which will include, as 10 percent or greater shareholders, Teninver, S.A. de C.V. ("Teninver"), an indirect wholly-owned subsidiary of Telmex, and Forstmann Little;

WHEREAS, as disclosed to the FCC, Telmex is a publicly-traded Mexican corporation that (1) is controlled by Carso Global Telecom, S.A. de C.V., a Mexican holding company approximately 68 percent of the shares of which are held in trust for investment purposes for the benefit of Carlos Slim Helu and his family members, all of whom are Mexican citizens; and (2) has no foreign government ownership (direct or indirect) that is ten (10) percent or greater or of which XO is aware;

WHEREAS, following FCC grant of the applications in FCC IB Docket No. 02-50, and upon satisfaction of all other conditions set forth in, and consummation of the transactions contemplated by, the Stock Purchase Agreement, Telmex (through Teninver) proposes to acquire a non-controlling minority interest of approximately 40% of the stock of XO;

WHEREAS, following FCC grant of the applications in FCC IB Docket No. 02-50, and upon satisfaction of all other conditions set forth in, and consummation of the transactions contemplated by, the Stock Purchase Agreement, Forstmann Little proposes to acquire a non-controlling minority interest of approximately 40% of the stock of XO;

WHEREAS, the FCC's grant of the applications in FCC IB Docket No. 02-50 may be made subject to conditions relating to national security, law enforcement, and public safety, and whereas XO has agreed to enter into this Agreement with the FBI and the DOJ to address issues raised by the FBI and the DOJ, and to request that the FCC condition the authorizations and licenses granted by the FCC on their compliance with this Agreement;

WHEREAS, by Executive Order 12661, the President, pursuant to Section 721 of the Defense Production Act, as amended, authorized the Committee on Foreign Investment in the United States ("CFIUS") to review, for national security purposes, foreign acquisitions of U.S. companies;

WHEREAS, XO and Telmex may submit a voluntary notice with CFIUS regarding Telmex's proposed investment in XO, and XO has entered into this Agreement to resolve any

national security issues that the DOJ and the FBI might raise, including in the CFIUS review process;

WHEREAS, representatives of XO and the Investors have met with representatives of the FBI and the DOJ to discuss issues raised by the FBI and the DOJ. In these meetings, XO represented that: (a) XO has no present plans, or is not aware of present plans of any other entity that would result in a Domestic Communications Company providing Domestic Communications or Hosting Services through facilities located outside the United States (though the Parties recognize that XO may, for *bona fide* commercial reasons as provided in this Agreement, use such facilities); and (b) Telmex has advised that Telmex is an entity whose commercial operations are wholly separate from the Mexican Government and whose activities are overseen by independent regulatory authorities in Mexico. Further, XO represented that it operates in extremely competitive markets and, to XO's knowledge, controls less than one (1) percent of the total U.S. market for services, in terms of revenues.

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

ARTICLE 1: DEFINITION OF TERMS

As used in this Agreement:

1.1 "Call Associated Data" or "CAD" means any information related to a Domestic Communication or related to the sender or recipient of that Domestic Communication and, to the extent maintained by a Domestic Communications Company in the normal course of business, includes without limitation subscriber identification, called party number, calling party number, start time, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, post cut-through dial digit extraction, in-band and out-of-band signaling, and party add, drop and hold.

1.2 "Classified Information" means any information that has been determined pursuant to Executive Order 12958, or any predecessor or successor order, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act, to require protection against unauthorized disclosure.

1.3 "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 1.3(a) through (d); or

(f) XO's obligations under this Agreement.

1.4 "Controlled Unclassified Information" means unclassified information, the export of which is controlled by the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Chapter I, Subchapter M, or the Export Administration Regulations (EAR), 15 C.F.R., Chapter VII, Subchapter C.

1.5 "Data Centers" means (a) equipment (including firmware, software and upgrades), facilities, and premises used by (or on behalf of) one or more Domestic Communications Companies in connection with Hosting Services (including data storage and provisioning, control, maintenance, management, security, selling, billing, or monitoring of Hosting Services), and (b) equipment hosted by a Domestic Communications Company that is leased or owned by a Hosting Services customer.

1.6. "*De facto*" and "*de jure*" control have the meanings provided in 47 C.F.R. § 1.2110.

1.7. "DOJ" means the U.S. Department of Justice.

1.8 "Domestic Communications" means (i) Wire Communications or Electronic Communications (whether stored or not) from one U.S. location to another U.S. location and (ii) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States.

1.9 "Domestic Communications Company" means all those subsidiaries, divisions, departments, branches and other components of XO that (i) provide Domestic Communications, or (ii) engage in provisioning, control, maintenance, management, security, selling, billing, or monitoring of Hosting Services, or data storage in connection with Hosting Services. If any subsidiary, division, department, branch or other component of XO provides Domestic Communications or engages in Hosting Services after the date that all the Parties execute this Agreement, then such subsidiary, division, department, branch or other component of XO shall be deemed to be a Domestic Communications Company. If XO enters into joint ventures under which a joint venture or another entity may provide Domestic Communications or engage in Hosting Services, and if XO has the power or authority to exercise *de facto* or *de jure* control over such entity, then XO will ensure that that entity shall fully comply with the terms of this Agreement. The term "Domestic Communications Company" shall not include acquisitions by XO in the U.S. after the date this Agreement is executed by all parties only if the DOJ or the FBI find that the terms of this Agreement are inadequate to address national security, law enforcement or public safety concerns presented by that acquisition and the necessary modifications to this Agreement cannot be reached pursuant to Section 8.8 below.

1.10 "Domestic Communications Infrastructure" means (a) transmission and switching equipment (including software and upgrades) subject to control by a Domestic Communications Company and in use to provide, process, direct, control, supervise or manage Domestic

Communications, and (b) facilities and equipment in use by or on behalf of a Domestic Communications Company that are physically located in the United States; or (c) facilities in use by or on behalf of a Domestic Communications Company to control the equipment described in (a) and (b) above. Domestic Communications Infrastructure does not include equipment or facilities used by service providers that are not Domestic Communications Companies and that are:

(a) interconnecting communications providers; or

(b) providers of services or content that are

(i) accessible using the communications services of Domestic Communications Companies, and

(ii) available in substantially similar form and on commercially reasonable terms through communications services of companies other than Domestic Communications Companies.

1.11 "Effective Date" means the date on which the transactions contemplated by the Stock Purchase Agreement are consummated and Telmex acquires the stock of XO.

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

1.13 "Electronic Surveillance" means (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (b) access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 et seq.; (c) acquisition of dialing 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 or interception of, or preservation of communications or information as described in (a) through (e) above and comparable State laws.

1.14 "FBI" means the Federal Bureau of Investigation.

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

1.16 "Forstmann Little" means Forstmann Little & Co. Equity Partnership-VII, L.P. and Forstmann Little & Co. Subordinated Debt and Equity Management Buyout Partnership-VIII, L.P.

1.17 "Governmental Authority" or "Governmental 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.

1.18 "Hosting Services" means Web hosting (whether shared or dedicated, and including design, server management, maintenance and telecommunications services), Web site traffic management, electronic commerce, streamed media services, server collocation and management, application hosting, and all other similar services offered by XO or any of its subsidiaries, affiliates, divisions, departments, branches or other components.

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, Call Associated Data, or U.S. Hosting Data, including Transactional Data or Subscriber Information.

1.21 "Party" and "Parties" have the meanings given them in the Preamble.

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

1.23 "Sensitive Information" means information that is not Classified Information regarding (a) the persons or facilities that are the subjects of Lawful U.S. Process, (b) the identity of the government agency or agencies serving such Lawful U.S. Process, (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance pursuant to Lawful U.S. Process, (d) the means of carrying out Electronic Surveillance pursuant to Lawful U.S. Process, (e) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process, and (f) other information that is not Classified 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." Domestic Communications Companies may dispute pursuant to Article 4 whether information is Sensitive Information under this subparagraph. Such information shall be treated as Sensitive Information unless and until the dispute is resolved in the Domestic Communications Companies' favor.

1.24 "Sensitive Network Monitoring Position" means a position that involves access to Domestic Communications Infrastructure or Data Centers that enables a person to monitor the content of a subscriber's Wire or Electronic Communications (including those in electronic storage) other than (i) on occasion in the course of outside plant operations and maintenance functions or (ii) sales, marketing or customer care communications made by, or customer-oriented communications to, Domestic Communications Company personnel.

1.25 "Subscriber Information" means information relating to subscribers or customers of Domestic Communications Companies, including U.S. Hosting Services Customers (or the end-users of U.S. Hosting Services Customers), of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709. Such information shall also be considered Subscriber Information when it is sought pursuant to the provisions of other Lawful U.S. Process.

1.26 "Telmex" means Teléfonos de México, S.A. de C.V., a Mexican corporation, and includes its indirect wholly-owned subsidiary Teninver, S.A. de C.V.

1.27 "Transactional Data" means:

(a) "call identifying information," as defined in 47 U.S.C. § 1001(2), including without limitation the telephone number or similar identifying designator associated with a Domestic Communication;

(b) any information possessed by a Domestic Communications Company 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, 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 (c) below;

(c) the time, date, size or volume of data transfers, duration, domain names, MAC or IP addresses (including source and destination), URLs, port numbers, packet sizes, protocols or services, special purpose flags, or other header information or identifying designators or characteristics associated with any Domestic Communication, or other Wire or Electronic Communication within the definition of U.S. Hosting Data, including electronic mail headers showing From: and To: addresses; and

(d) as to any mode of transmission (including mobile transmissions), and to the extent permitted by U.S. laws, any information indicating as closely as possible the physical location to or from which a Domestic Communication, or other Wire or Electronic Communication within the definition of U.S. Hosting Data, is transmitted.

The term includes all records or other information of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c)(1) and (d) but does not include the content of any communication.

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

1.29 "U.S. Hosting Services Customer" is a customer or subscriber that receives Hosting Services from a Domestic Communications Company and that is U.S.-domiciled or holds itself out as being U.S.-domiciled. A customer or subscriber will be considered to be U.S.-domiciled if (i) it has its principal office(s) or place(s) of business in the United States, (ii) it is incorporated in the United States, (iii) it receives Hosting Services facilitated by a Data Center that is physically located in the United States, or (iv) other criteria tend to indicate that it is U.S.-domiciled.

1.30 "U.S. Hosting Data" means all data, records, documents, or information (including Domestic Communications, other Wire or Electronic Communications, Subscriber Information,

and Transactional Data) in any form (including paper, electronic, magnetic, mechanical, or photographic) transmitted, received, generated, maintained, processed, used by or stored in a Data Center for a U.S. Hosting Services Customer.

1.31 "XO" means XO Communications, Inc., a Delaware corporation.

1.32 "Wire Communication" has the meaning given it in 18 U.S.C. § 2510(1).

1.33 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 FBI and the DOJ in writing:

(a) In the absence of strictly *bona fide* commercial reasons, all Domestic Communications Infrastructure that is owned, operated or controlled by a Domestic Communications Company shall at all times be located in the United States and will be directed, controlled, supervised and managed by a Domestic Communications Company; and

(b) all Domestic Communications that are carried by or through, in whole or in part, the Domestic Communications Infrastructure shall pass through a facility under the control of a Domestic Communications Company and physically located in the United States, from which Electronic Surveillance can be conducted pursuant to Lawful U.S. Process. The Domestic Communications Company will provide technical or other assistance to facilitate such Electronic Surveillance.

2.2 Data Centers and Access to Communications. Except to the extent and under conditions concurred in by the FBI and the DOJ in writing:

(a) all Data Centers used to provide Hosting Services to U.S. Hosting Services Customers shall at all times be located in the United States, except strictly for a bona fide commercial reason; and

(b) a Domestic Communications Company shall, upon service of appropriate Lawful U.S. Process, ensure that Wire or Electronic Communications of a specified U.S. Hosting Services Customer that are transmitted to, from or through a Data Center shall be accessible from or pass through a facility under the control of a Domestic Communications Company and physically located in the United States, from which Electronic Surveillance can be conducted in a timely manner. The Domestic Communications Company will provide technical or other assistance to facilitate such Electronic Surveillance.

2.3 Compliance with Lawful U.S. Process. Domestic Communications Companies shall take all practicable steps to configure its Domestic Communications Infrastructure and Data Centers (except for equipment that is owned or controlled by a U.S. Hosting Services Customer and is collocated in XO-controlled space in a Data Center) to be capable of complying, and Domestic Communications Company 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 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. Domestic Communications Companies shall have the ability to provide in the United States the following:

(a) stored Domestic Communications, if such communications are stored by or on behalf of a Domestic Communications Company for any reason;

(b) any Wire Communications or Electronic Communications (including any other type of wire, voice or electronic communication not covered by the definitions of Wire Communication or Electronic Communication) received by, intended to be received by, or stored in the account of a customer or subscriber of a Domestic Communications Company, if such communications are stored by or on behalf of a Domestic Communications Company for any reason;

(c) Transactional Data and Call Associated Data relating to Domestic Communications, if such data are stored by or on behalf of a Domestic Communications Company for any reason;

(d) Subscriber Information, if such information is stored by or on behalf of a Domestic Communications Company for any reason, concerning customers who are U.S.-domiciled, customers who hold themselves out as being U.S.-domiciled, and customers who make a Domestic Communication; and

(e) billing records of customers who are U.S.-domiciled, customers who hold themselves out as being U.S.-domiciled, and customers who make a Domestic Communication, for so long as such records are kept and at a minimum for as long as such records are required to be kept pursuant to applicable U.S. law or this Agreement.

2.5 Mandatory Destruction. Domestic Communications Companies shall take all technically feasible steps to ensure that the data and communications described in Section 2.4(a)-(e) of this Agreement are stored in a manner not subject to mandatory destruction under any foreign laws, if

such data and communications are stored by or on behalf of a Domestic Communications Company for any reason. Domestic Communications Companies shall ensure that the data and communications described in Section 2.4(a)-(e) of this Agreement shall not be stored by or on behalf of a Domestic Communications Company outside of the United States unless such storage is strictly for *bona fide* commercial reasons weighing in favor of storage outside the United States.

2.6 U.S. Hosting Data Storage and Access. Domestic Communications Companies shall have the ability to provide in the United States stored U.S. Hosting Data (whether in "electronic storage" as defined in 18 U.S.C. § 2510(17) or stored in any other manner), except for stored U.S. Hosting Data located on equipment that is owned or controlled by a U.S. Hosting Services Customer and is collocated in XO-controlled space in a Data Center. Domestic Communications Companies shall ensure that such data shall not be stored outside of the United States unless such storage is strictly for bona fide commercial reasons weighing in favor of storage outside the United States. In any event, Domestic Communications Companies shall take all technically feasible steps to ensure that such data is stored in a manner not subject to mandatory destruction under any foreign laws.

2.7 Billing Records. Domestic Communications Companies shall store for at least 18 months all billing records described in Section 2.4(e) above and all billing records relating to U.S. Hosting Services Customers, and shall make such records available in the U.S. Nothing in this paragraph shall require a Domestic Communications Company to store such records for longer than 18 months.

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

2.9 Compliance with U.S. Law. Nothing in this Agreement shall excuse a Domestic Communications Company from any obligation it may have to comply with U.S. legal requirements for the retention, preservation, or production of such information or data. Similarly, in any action to enforce Lawful U.S. Process, Domestic Communication Companies have not waived any legal right they might have to resist such process.

2.10 Routing of Domestic Communications and U.S. Hosting Data. Except strictly for *bona fide* commercial reasons, Domestic Communications Companies shall not route Domestic Communications or U.S. Hosting Data outside the United States.

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

2.12 Storage of Protected Information. The storage of Classified, Controlled Unclassified, and Sensitive Information by a Domestic Communications Company or its contractors at any

location outside of the United States is prohibited, unless the storage is at a U.S. military facility, a U.S. Embassy or Consulate or other location occupied by a U.S. government organization.

ARTICLE 3: SECURITY

3.1 Measures to Prevent Improper Use or Access. Domestic Communications Companies shall take all reasonable measures to prevent the use of or access to the Domestic Communications Infrastructure or to Data Centers to conduct Electronic Surveillance, or to obtain or disclose Domestic Communications, U.S. Hosting Data, Classified Information, Sensitive Information, or Controlled Unclassified Information, in violation of any U.S. federal, state, or local laws or the terms of this Agreement. These measures shall include creating and complying with detailed technical, organizational, operational, and personnel controls, policies and written procedures, necessary implementation plans, and physical security measures.

3.2 Access by Foreign Government Authority. Domestic Communications Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide access to Domestic Communications, U.S. Hosting Data, Call Associated Data, Transactional Data, or Subscriber Information stored by Domestic Communications Companies in the United States to any person if the purpose of such access is to respond to the legal process or the request of or on behalf of a foreign government, identified representative, component or subdivision thereof without the express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process described in this Section 3.2 of this Agreement shall be reported to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received by and known to the security officer designated under Section 3.8 of this Agreement. Domestic Communications Companies shall take reasonable measures to ensure that the security officer designated under Section 3.8 of this Agreement will promptly learn of all such requests or submission of legal process described in this Section 3.2 of this Agreement.

3.3 Disclosure to Foreign Government Authorities. Domestic Communications Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide access to:

(a) Classified, Sensitive, or Controlled Unclassified Information; or

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

to any foreign government, identified representative, component or subdivision thereof without satisfying all applicable U.S. federal, state and local legal requirements pertinent thereto, and obtaining the express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States. Any requests or any legal process submitted by a foreign government, an identified representative, a component or subdivision thereof to Domestic Communications Companies for the communications, data or information identified in this

Section 3.3 of this Agreement that is maintained by Domestic Communications Companies shall be referred to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received by and known to the security officer designated under Section 3.8 of this Agreement 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. Domestic Communications Companies shall take reasonable measures to ensure that the security officer designated under Section 3.8 of this Agreement will promptly learn of all such requests or submission of legal process described in this Section 3.3.

3.4 Notification of Access or Disclosure Requests from Foreign Non-Governmental Entities. Within 90 days of receipt, Domestic Communications Companies shall notify DOJ in writing of legal process or requests by foreign nongovernmental entities to Domestic Communications Companies for access to or disclosure of (i) U.S. Hosting Data, or (ii) Domestic Communications carried by or through, in whole or in part, the Domestic Communications Infrastructure, unless the disclosure of the legal process or request would be in violation of an order of a court of competent jurisdiction within the United States.

3.5 Security of Lawful U.S. Process. Domestic Communications Companies shall protect the confidentiality and security of all Lawful U.S. Process served upon them and the confidentiality and security of Classified, Sensitive, and Controlled Unclassified Information in accordance with U.S. federal and state law or regulation and this Agreement. Information concerning Lawful U.S. Process, Classified Information, Sensitive Information, or Controlled Unclassified Information shall be under the custody and control of the security officer designated under Section 3.8 of this Agreement.

3.6 Points of Contact. Within fourteen (14) days after the Effective Date, Domestic Communications Companies shall designate points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process. The points of contact shall be assigned to Domestic Communications Companies' security office(s) 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 Classified, Sensitive, and Controlled Unclassified Information and any Lawful U.S. Process in accordance with the requirements of U.S. law and this Agreement. Promptly after designating such points of contact, Domestic Communications Companies shall notify the FBI and the DOJ in writing of the points of contact, and thereafter shall promptly notify the FBI and the DOJ of any change in such designation. The points of contact shall be resident U.S. citizens who are eligible for appropriate U.S. security clearances and shall serve as points of contact for new Domestic Communications Companies unless and until the FBI and the DOJ are notified of any change in designation. Domestic Communications Companies shall cooperate with any request by a Government Authority within the United States that a background check and/or security clearance process be completed for a designated point of contact.

3.7 Information Security Plan. Domestic Communications Companies shall develop, document, implement, and maintain an information security plan to:

(a) maintain appropriately secure facilities (*e.g.*, offices) within the United States for the handling and storage of any Classified, Sensitive or Controlled Unclassified Information;

(b) take appropriate measures to prevent unauthorized access to data or facilities that might contain Classified, Sensitive, or Controlled Unclassified Information;

(c) assign U.S. citizens, who meet high standards of trustworthiness for maintaining the confidentiality of Sensitive Information and Wire or Electronic Communications, to positions that handle or that regularly deal with information identifiable to such person as Sensitive Information or to Sensitive Network Monitoring Positions;

(d) upon request from the DOJ or FBI, provide the name, social security number and date of birth of each person who regularly handles or deals with Sensitive Information;

(e) require that personnel handling Classified Information shall have been granted appropriate security clearances;

(f) provide that the points of contact described in Section 3.6 of this Agreement shall have sufficient authority over any of Domestic Communications Companies' employees who may handle Classified, Sensitive, or Controlled Unclassified 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

(g) ensure that the disclosure of or access to Classified, Sensitive, or Controlled Unclassified Information is limited to those who have the appropriate security clearances and authority.

3.8 Security Officer Responsibilities and Duties. Within 14 calendar days after the Effective Date, XO shall designate, from among the points of contact selected pursuant to Section 3.6, a security officer within the United States with the primary responsibility for carrying out the Domestic Communications Companies' obligations under Sections 3.5, 3.6, and 3.7 of this Agreement.

3.9 Disclosure of Protected Data. In carrying out the responsibilities set forth in Section 3.8, the designated security officer shall not directly or indirectly disclose information concerning Lawful U.S. Process, Classified Information, Sensitive Information, or Controlled Unclassified Information to any XO or Domestic Communication Company's officer, director, shareholder, employee, agent, or contractor, including those who serve in a supervisory, managerial or officer role with respect to the security officer, unless disclosure has been approved by prior written consent obtained from the FBI or the DOJ 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.

3.10 Notice of Obligations. Domestic Communications Companies shall instruct appropriate officials, employees, contractors, and agents as to the security restrictions and safeguards imposed by this Agreement, including the reporting requirements in Sections 5.5, 5.6, and 5.7 of this Agreement, and shall issue periodic reminders to them of such obligations.

3.11 Access to Classified, Controlled Unclassified, or Sensitive Information. Nothing contained in this Agreement shall limit or affect the authority of a U.S. government agency to deny, limit or revoke Domestic Communications Companies' access to Classified, Controlled Unclassified, and Sensitive Information under that agency's jurisdiction.

ARTICLE 4: DISPUTES

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

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

(a) seek revocation by the FCC of any license, permit, or other authorization granted or given by the FCC to Domestic Communications Companies, or any other sanction by the FCC against Domestic Communications Companies;

(b) seek civil sanctions for any violation by XO or Domestic Communications Companies of any U.S. law or regulation or term of this Agreement; or

(c) pursue criminal sanctions against Domestic Communications Companies, or any director, officer, employee, representative, or agent of Domestic Communications Companies, or against any other person or entity, for violations of the criminal laws of the United States.

4.3 Irreparable Injury. XO agrees that the United States would suffer irreparable injury if for any reason a Domestic Communications Company failed to perform any of its significant obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, XO agrees that, in seeking to enforce this Agreement against Domestic Communications Companies, the FBI and the DOJ shall be entitled, in addition to any other

remedy available at law or equity, to specific performance and injunctive or other equitable relief.

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

4.5 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.

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

ARTICLE 5: AUDITING, REPORTING, NOTICE AND LIMITS

5.1 Filings re *de jure* or *de facto* control of a Domestic Communications Company. If any Domestic Communications Company makes any filing with the FCC or any other Governmental Authority relating to the *de facto* or *de jure* control of a Domestic Communications Company except for filings with the FCC for assignments or transfers of control to any Domestic Communications Company that are *pro forma*, XO shall promptly provide to the FBI and the DOJ written notice and copies of such filing. This Section 5.1 is effective upon execution of this Agreement by all the Parties.

5.2 Control of XO. If any member of the senior management of XO or a Domestic Communications Company (including the Chief Executive Officer, President, General Counsel, Chief Technical Officer, Chief Financial Officer or other senior officer) acquires any information that reasonably indicates that any single foreign entity or individual, other than Telmex, has or will likely obtain an ownership interest (direct or indirect) in XO above 25 percent, as determined in accordance with 47 C.F.R. § 63.09, or if any single foreign entity or individual has or will likely otherwise gain either (1) Control or (2) *de facto* or *de jure* control of XO, then such member shall promptly cause to be notified the security officer designated under Section 3.8 of this Agreement, who in turn, shall promptly notify the FBI and the DOJ in writing. 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 XO 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 in XO that has resulted in or will likely result in the entity or individual(s) increasing the ownership interest in or control of XO.

5.3 Notice of Decision to Store Information or Use Infrastructure Outside of the U.S. Domestic Communications Companies shall provide to the FBI and the DOJ thirty (30) days advance notice if a Domestic Communications Company plans to (i) store or have stored on its behalf a Domestic Communication, U.S. Hosting Data, Transactional Data, Call Associated Data, or Subscriber Information outside the United States; (ii) provide Domestic Communications from Domestic Communications Infrastructure that is located outside of the U.S.; or (iii) provide Hosting Services to a U.S. Hosting Services Customer using a Data Center located outside the U.S. Such notice shall, at a minimum, (a) include a description of the type of information or infrastructure to be stored or located outside the United States, (b) identify the custodian of the information if other than a Domestic Communications Company, (c) identify the location where the information or infrastructure is to be located, and (d) identify the factors considered in deciding to store or locate the information or infrastructure outside of the United States (see Sections 2.1(a), 2.2(a), 2.5, 2.6, and 2.10 of this Agreement). This Section 5.3 is effective upon execution of this Agreement by all the Parties.

5.4 Joint Ventures. A Domestic Communications Company may have entered into or may enter into joint ventures under which the joint venture or entity may provide Domestic Communications. To the extent that such Domestic Communications Company does not have *de facto* or *de jure* control over a joint venture or entity, such Domestic Communications Company shall in good faith (a) notify such entity of this Agreement and its purposes, (b) endeavor to have such entity comply with this Agreement as if it were a Domestic Communications Company, and (c) consult with the FBI or the DOJ about the activities of such entity. Nothing in this Section 5.4 does nor shall it be construed to relieve Domestic Communications Companies of obligations under Article 2 of this Agreement. The obligations of Domestic Communications Companies under this Section 5.4 shall not be considered "significant obligations" for purposes of Section 4.3 of this Agreement.

5.5 Outsourcing Third Parties. If a Domestic Communications Company outsources functions covered by this Agreement to a third party that is not a Domestic Communications Company, that Domestic Communications Company shall take reasonable steps to ensure that the third party complies with the applicable terms of this Agreement. Such steps shall include the following:

(a) the Domestic Communications Company shall include in its contracts with any such third parties written provisions requiring that such third parties comply with all applicable terms of this Agreement (or take other reasonable, good-faith measures to ensure that such third parties are aware of, agree to, and are bound to comply with the applicable obligations of this Agreement);

(b) if the Domestic Communications Company learns that the outsourcing third party or the outsourcing third party's employee has violated an applicable provision of this Agreement, the Domestic Communications Company will notify the DOJ and the FBI promptly; and

(c) with consultation and, as appropriate, cooperation with the DOJ and the FBI, the Domestic Communications Company will take reasonable steps necessary to rectify promptly the situation, which steps may (among others) include terminating the arrangement with the outsourcing third party, including after notice and opportunity for cure, and/or initiating and pursuing litigation or other remedies at law and equity.

5.6 Notice of Foreign Influence. If any member of the senior management of XO or a Domestic Communications Company (including the Chief Executive Officer, President, General Counsel, Chief Technical Officer, Chief Financial Officer or other senior officer) acquires any information that reasonably indicates that any foreign government, any foreign government-controlled entity, or any foreign entity:

(a) plans to participate or has participated in any aspect of the day-to-day management of XO or a Domestic Communications Company in such a way that interferes with or impedes the performance by XO or a Domestic Communications Company of its duties and obligations under the terms of this Agreement, or interferes with or impedes the exercise by XO or a Domestic Communications Company of its rights under the Agreement, or

(b) plans to exercise or has exercised, as a direct or indirect shareholder of XO or a Domestic Communications Company or their subsidiaries, any Control of XO or a Domestic Communications Company in such a way that interferes with or impedes the performance by XO or a Domestic Communications Company of its duties and obligations under the terms of this Agreement, or interferes with or impedes the exercise by XO or a Domestic Communications Company of its rights under the terms of this Agreement, or in such a way that foreseeably concerns XO's or a Domestic Communications Company's obligations under this Agreement,

then such member shall promptly cause to be notified the security officer designated under Section 3.8 of this Agreement, who in turn, shall promptly notify the FBI and the DOJ in writing of the timing and the nature of the foreign government's or entity 's plans and/or actions.

5.7 Reporting of Incidents. XO and Domestic Communications Companies shall take practicable steps to ensure that, if any XO or Domestic Communications Companies officer, director, employee, contractor or agent acquires any information that reasonably indicates: (a) a breach of this Agreement; (b) access to or disclosure of U.S. Hosting Data or Domestic Communications, or the conduct of Electronic Surveillance, in violation of federal, state or local law or regulation; (c) access to or disclosure of CPNI or Subscriber Information in violation of federal, state or local law or regulation (except for violations of FCC regulations relating to improper use of CPNI); or (d) improper access to or disclosure of Classified, Sensitive, or Controlled Unclassified Information, then the individual will notify the security officer designated in Section 3.8 of this Agreement, who will in turn notify the FBI and the DOJ in the same manner as specified in Section 5.6. This report shall be made promptly and in any event no later than 10 calendar days after XO or the Domestic Communications Company acquires information indicating a matter described in Section 5.7(a)-(d) of this Agreement. XO and the Domestic Communications Companies shall lawfully cooperate in investigating the matters described in this section of this Agreement. XO or the Domestic Communications Company

need not report information where disclosure of such information would be in violation of an order of a court of competent jurisdiction in the United States.

5.8 Access to Information. In response to reasonable requests made by the FBI or the DOJ, Domestic Communications Companies shall provide access to information concerning technical, physical, management, or other security measures and other reasonably available information needed by the DOJ or the FBI to assess compliance with the then-effective terms of this Agreement.

5.9 Visits and Inspections. The FBI and the DOJ may visit and inspect any part of Domestic Communications Companies' Domestic Communications Infrastructure, Data Centers, and security offices for the purpose of verifying compliance with the terms of this Agreement. Such inspections shall be reasonable in number and be conducted during normal business hours upon reasonable notice, which shall ordinarily be no less than 24 hours in advance of the visit. Domestic Communications Companies may have appropriate Domestic Communications Companies employees accompany U.S. government representatives throughout any such inspection.

5.10 Access to Personnel. Upon reasonable notice from the FBI or the DOJ, Domestic Communications Companies will make reasonably available for interview officers or employees of Domestic Communications Companies, and will seek to require contractors to make available appropriate personnel located in the United States who are in a position to provide information to verify compliance with the then-effective terms of this Agreement.

5.11 Annual Report. On or before the last day of January of each year, a designated senior corporate officer of Domestic Communications Companies shall submit to the FBI and the DOJ a report assessing Domestic Communications Companies' compliance with the terms of this Agreement for the preceding calendar year. The report shall include:

(a) a copy of the 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 material 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 Domestic Communications Companies' knowledge, will or reasonably could affect the effectiveness of or compliance with this Agreement.

5.12 Notices. Effective upon execution of this Agreement by all the Parties, all notices and other communications given or made relating to this Agreement, such as a proposed modification, shall be in writing and shall be deemed to have been duly given or made as of the date of receipt and shall be (a) delivered personally, or (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 others addresses as the Parties may designate in accordance with this Section:

Department of Justice
Assistant Attorney General
Criminal Division
Main Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Federal Bureau of Investigation
General Counsel
935 Pennsylvania Avenue, NW
Washington, DC 20535

Cathleen A. Massey
Vice President – External Affairs/Asst. General Counsel
XO COMMUNICATIONS, INC.
1730 Rhode Island Ave. NW, Suite 1000
Washington, DC 20036
Telephone: (202) 721-0983
Fax: (202) 721-0995

XO COMMUNICATIONS, INC.
11111 Sunset Hills Road
Reston, VA 20190
Attention: General Counsel
Telephone: (703) 547-2000
Fax: (703) 547-2025

With a copy to:

Federal Bureau of Investigation
The Assistant Director
National Security Division
935 Pennsylvania Avenue, NW
Washington, DC 20535

Kelley Drye & Warren L.L.P.
1200 Nineteenth Street, N.W.
Washington, D.C. 20036-2423
Attention: Brad E. Mutschelknaus

ARTICLE 6: FREEDOM OF INFORMATION ACT

6.1 Protection from Disclosure. The DOJ and FBI shall take all reasonable measures to protect from public disclosure all information submitted by a Domestic Communications Company or other entities in accordance with the terms of this Agreement to the DOJ or FBI 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 company's position that the information so marked constitutes "trade secrets" and/or "commercial or financial information obtained from a person and privileged or confidential," or otherwise warrants protection within the meaning of 5 U.S.C. 552(b)(4). For the purposes of 5 U.S.C. 552(b)(4), the Parties agree that information so marked is voluntarily submitted. If a request is made under 5 U.S.C. 552(a)(3) for information so marked, and disclosure of any information (including disclosure in redacted form) is contemplated, the DOJ or FBI, as appropriate, shall notify the company of the intended disclosure as provided by Executive Order 12600, 52 Fed. Reg. 23781 (June 25, 1987). If the Domestic Communications Company objects to the intended disclosure and its objections are not sustained, the DOJ or FBI, as appropriate, shall notify the company of its intention to release (as provided by Section 5 of E.O. 12600) not later than five business days prior to disclosure of the challenged information.

6.2 Use of Information for U.S. Government Purposes. Nothing in this Agreement shall prevent the FBI or the DOJ 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 agencies to protect public safety, law enforcement, or national security interests, provided that the FBI and the DOJ take all reasonable measures to protect from public disclosure the information marked as described in Section 6.1.

6.3 Unlawful Disclosure of Information. The DOJ and FBI acknowledge that officers and employees of the United States and of any department or agency thereof are subject to liability under 18 U.S.C. § 1905 for unlawful disclosure of information provided to them by other Parties to this Agreement.

ARTICLE 7: FCC CONDITION AND CFIUS

7.1 FCC Approval. Upon the execution of this Agreement by all the Parties, the FBI and the DOJ shall promptly notify the FCC that, provided the FCC adopts a condition substantially the same as set forth in Exhibit A attached hereto (the "Condition to FCC Authorization"), the FBI and the DOJ have no objection to the FCC's grant of the applications filed with the FCC in FCC IB Docket No. 02-50. This Section 7.1 is effective upon execution of this Agreement by all the Parties.

7.2 Future Applications. XO agrees that in any application or petition by any Domestic Communications Company to the FCC for licensing or other authority filed with or granted by the FCC after the Effective Date, except with respect to *pro forma* assignments or *pro forma* transfers of control, the Domestic Communications Company shall request that the FCC condition the grant of such licensing or other authority on compliance with the terms of this Agreement. Notwithstanding Section 8.8, the FBI and the DOJ reserve the right to object, formally or informally, to the grant of any other FCC application or petition of XO or a Domestic Communications Company for a license or other authorization under Titles II and III of the

Communications Act of 1934, as amended, and to seek additional or different terms that would, consistent with the public interest, address any threat to their ability to enforce the laws, preserve the national security and protect the public safety raised by the transactions underlying such applications or petitions.

7.3 CFIUS. Provided that the FCC adopts the Condition to FCC Authorization, the Attorney General shall not make any objection to the CFIUS or the President concerning Telmex's investment in XO or grant of the applications filed with the FCC in FCC IB Docket No. 02-50. This commitment, however, does not extend to any objection the Attorney General may wish to raise with the CFIUS or the President in the event that (a) XO fails to comply with the terms of this Agreement, (b) the Attorney General learns that the representations of XO made to the DOJ, the FBI, or the FCC above are materially untrue or incomplete, (c) there is a material increase in the authority of a foreign entity to exercise Control of XO or a Domestic Communications Company, or (d) there is any other material change in the circumstances associated with the transactions at issue.

ARTICLE 8: OTHER

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

8.2 Headings. The Article 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 XO or any Domestic Communications Company, (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 of XO or any Domestic Communications Company located within or outside the United States. 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 Governmental Authorities entitled to effect Electronic Surveillance pursuant to Lawful U.S. Process.

8.6 Modifications. This Agreement may only be modified by written agreement signed by all of the Parties. The FBI and the DOJ agree to consider in good faith and promptly possible modifications to this Agreement if XO believes that the obligations imposed on XO or the Domestic Communications Companies under this Agreement are substantially more restrictive than those imposed on other U.S. and foreign licensed service providers in like circumstances in order to protect U.S. national security, law enforcement, and public safety concerns. Any

substantial modification to this Agreement shall be reported to the FCC within thirty (30) days after approval in writing by the Parties.

8.7 Changes in Circumstances for XO or Domestic Communications Companies. The DOJ and the FBI agree to negotiate in good faith and promptly with respect to any request by XO or a Domestic Communications Company for relief from application of specific provisions of this Agreement: (a) if a Domestic Communications Company provides Domestic Communications solely through the resale of transmission or switching facilities owned by third parties, or (b) as regards future Domestic Communications Company activities or services, if those provisions become unduly burdensome or adversely affect XO's or a Domestic Communications Company's competitive position.

8.8 Changes in Circumstances for DOJ or FBI. If after the date that all the Parties have executed this Agreement the DOJ or the FBI finds that the terms of this Agreement are inadequate to address national security, law enforcement, or public safety concerns presented, or if a foreign government acquires an ownership interest in Telmex, then XO will negotiate in good faith to modify this Agreement to address those concerns.

8.9 Partial Invalidity. If any portion of this Agreement is declared invalid by a U.S. court of competent jurisdiction, this Agreement shall be construed as if such portion had never existed, unless such construction would constitute a substantial deviation from the Parties' intent as reflected in this Agreement.

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.

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 Termination of Agreement. This Agreement shall terminate upon fifteen (15) days notice to the FBI and the DOJ if no covered XO entity is a Domestic Communications Company.

8.14 Suspension of Agreement With Respect to a Domestic Communications Company. This Agreement shall be suspended upon thirty (30) days notice to the FBI and DOJ with respect to any covered XO entity if said entity is no longer a Domestic Communications Company.

8.15 Suspension of Agreement If No Foreign Ownership. This Agreement shall be suspended in its entirety with respect to XO and all Domestic Communications Companies thirty (30) days after receipt from XO of notice and documentation reasonably satisfactory to the DOJ and FBI that neither Telmex nor any other foreign entity neither Controls XO or a Domestic Communications Company nor holds, directly or indirectly, a ten (10) percent or greater interest in XO or a Domestic Communications Company, unless the DOJ and FBI notify XO within said thirty (30) day period that this Agreement shall not be suspended in order to protect U.S. national

security, law enforcement, and public safety concerns. If this Agreement is not suspended pursuant to this provision, the DOJ and the FBI agree to consider promptly and in good faith possible modifications to this Agreement. Notwithstanding anything to the contrary in this Section 8.15, this Agreement shall remain in effect with respect to XO and the Domestic Communications Companies for so long as (and the obligations of XO and the Domestic Communications Companies shall not be suspended and any suspension of the obligations of XO and the Domestic Communications Companies shall terminate if) Telmex or any other foreign entity shall either Control or hold, at any time does hold, or is a party to an agreement to hold, directly or indirectly, a ten (10) percent or greater ownership interest in XO or any Domestic Communications Company or any transferee or assignee of the FCC licenses or authorizations held by XO or a Domestic Communications Company.

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

This Agreement is executed on behalf of the Parties:

XO Communications, Inc.

Date: September 5, 2002

By: _____

Printed Name: R. Gerald Salemme

Title: Senior Vice President, External Affairs

Federal Bureau of Investigation

Date: _____

By: _____

Printed Name: Kenneth L. Wainstein

Title: General Counsel

United States Department of Justice

Date: _____

By: _____

Printed Name:

Title: Deputy Attorney General

This Agreement is executed on behalf of the Parties:

XO Communications, Inc.

Date:_____

By:_____
Printed Name: R. Gerald Salemme
Title: Senior Vice President, External Affairs

Federal Bureau of Investigation

Date:_____

By:_____
Printed Name: Kenneth L. Wainstein
Title: General Counsel

United States Department of Justice

Date: 9-16-02

By: John C Keeney, acting AAG, Criminal
Printed Name:
Title: Deputy Attorney General pursuant to delegated authority

This Agreement is executed on behalf of the Parties:

XO Communications, Inc.

Date:_____

By:_____
Printed Name:
Title:

Federal Bureau of Investigation

Date: September 10, 2002

By: /Kenneth L. Wainstein/
Printed Name: Kenneth L. Wainstein
Title: General Counsel

United States Department of Justice

Date:_____

By:_____
Printed Name: John G. Malcolm
Title: Deputy Assistant Attorney General

EXHIBIT A

CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that the authorization and any licenses transferred thereunder are subject to compliance with the provisions of the Agreement attached hereto between XO on the one hand, and the Department of Justice (the "DOJ") and the Federal Bureau of Investigation (the "FBI") on the other, dated SEPTEMBER 16, 2002, which Agreement is designed to address national security, law enforcement, and public safety issues of the FBI and the DOJ regarding the authority granted herein. Nothing in this Agreement is intended to limit any obligation imposed by Federal law or regulation including, but not limited to, 47 U.S.C. § 222(a) and (c)(1) and the FCC's implementing regulations.