CONFIDENTIAL PURSUANT TO 50 APP. U.S.C. § 2170(c)
EXEMPT FROM DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT

SECURITY AGREEMENT

This SECURITY AGREEMENT ("Agreement") is made as of the Effective Date by and between América Móvil, S.A. de C.V., on behalf of itself and the subsidiaries through which it will hold its interest in TELPRI ("América Móvil"), and Telecomunicaciones de Puerto Rico, Inc. ("TELPRI"), (collectively, "the Companies"), on the one hand, and the U.S. Department of Justice ("DOJ"), and the U.S. Department of Homeland Security ("DHS"), on the other (collectively, "the USG Parties"), referred to individually by name or 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;

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

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

WHEREAS, TELPRI is the largest telecommunications service provider in Puerto Rico; through its wholly owned subsidiaries Puerto Rico Telephone Company, Inc. ("PRT") and PRT Larga Distancia, Inc. ("PRT LD"), TELPRI provides approximately 93% of wireline (domestic and long distance) and approximately 24% of the wireless telecommunications on the island; and additionally, TELPRI and its Puerto Rico-based companies provide on-island Internet access, private data services and virtual private network ("VPN");

WHEREAS, as disclosed to the Committee on Foreign Investment in the United States ("CFIUS"), TELPRI subsidiary PRT provides telecommunication services to federal government agencies and the Puerto Rico National Guard;

WHEREAS, according to a September 29, 2006 filing by the Companies and Verizon Communications Inc. ("Verizon") with CFIUS, Verizon and América Móvil have entered into an agreement whereby Verizon and other stockholders in TELPRI will sell the issued and outstanding shares of common stock of TELPRI to certain América Móvil subsidiaries, which will result in América Móvil's ultimate ownership and control of TELPRI (the "Transaction");

WHEREAS, by Executive Order 12661, the President, pursuant to Section 721 of the Defense Production Act, as amended, authorized CFIUS to review, for national security purposes, foreign acquisitions of U.S. companies;

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. "Access" or "Accessible" means the ability to physically or logically undertake any of the following actions: (i) read, divert, or otherwise obtain non-public information or technology from or about software, hardware, a system or a network; (ii) add, edit or alter information or technology stored on or by software, hardware, a system or a network; and (iii) alter the physical or logical state of software, hardware, a system or a network (e.g., turning it on or off, changing configuration, removing or adding components or connections).

1.2. "América Móvil" has the meaning given to it in the Preamble to this Agreement.

1.3. "Call Associated Data" means any information related to a Domestic Communication or related to the sender or recipient of Domestic Communication, to the extent the Domestic Companies maintain such information in the normal course of business. Call Associated Data 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.

1.4. "Classified Information" means information or technology that is classified according to 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.

1.5. "Closing Date" means the date on which the Transaction is consummated.

1.6. "Control" and "Controls" means the power, direct or indirect, whether exercised, exercisable or not exercised, through any means employable, to decide, direct or otherwise influence matters affecting an entity; in particular, but without limitation, to determine, direct, take, reach, or cause decisions regarding:

(i) 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;

(ii) the dissolution of the entity;

(iii) the closing and/or relocation of the production or research and development facilities of the entity;

(iv) the termination or non-fulfillment of contracts of the entity;

(v) the amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in subsections (i) through (iv) above; and

(vi) the Domestic Companies' obligations under this Agreement.

1.7. "Customer Information" means Identifying Information for any customer of TELPRI or PRT.

1.8. "Data Centers" means (a) equipment (including firmware, software and upgrades), facilities, and premises used by (or on behalf of) one or more Domestic 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 the Domestic Companies that is leased or owned by a Hosting Services customer.

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

1.10. "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.

1.11. "Domestic Communications Infrastructure" means (i) transmission, switching, bridging and routing equipment (including software and upgrades) in use to provide, process, direct, control, supervise or manage Domestic Communications; and (ii) facilities and equipment that are used to control the equipment described in (i). Domestic Communications Infrastructure does not include equipment dedicated to the termination of international undersea cables, provided that such equipment is utilized solely to effectuate the operation of undersea transport network(s) outside of the United States and in no manner controls land-based transport network(s) or their associated systems in the United States, nor does it include facilities and equipment intended and capable solely of performing billing, customer management, business management or marketing functions.

1.12. "Domestic Companies" means TELPRI and all existing and post-Agreement subsidiaries, divisions, departments, branches and other components of TELPRI, or any other entity over which TELPRI has *de facto* or *de jure* control, that (i) provide Domestic Communications, or (ii) engage in provisioning, control, maintenance, management, security, selling, billing, or monitoring of Hosting Services, or data.

1.13. "Effective Date" means the date of the last signature affixed to this Agreement by the Parties.

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

1.15. "FBI" means the Federal Bureau of Investigation.

1.16. "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.

1.17. "Foreign Person" means any Person who is not a U.S. Person as provided by 31 C.F.R. § 800.222.

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 the Domestic Companies.

1.19. "Identifying Information" means the name, address, telephone number, e-mail address, I.P. address, or any other information that is customarily used to identify a particular end user.

1.20. "Intercept" or "Intercepted" has the meaning defined in 18 U.S.C. § 2510(4).

1.21. "Lawful U.S. Process" means lawful U.S. federal, state, or local court orders, subpoenas, warrants, processes, or authorizations issued under U.S. federal, state, or local law for electronic surveillance, 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.

1.22. "Lawfully Authorized Electronic Surveillance" means:

(i) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(4), (1), (2), and (12), and electronic surveillance as defined in 50 U.S.C. § 1801(f);

(ii) access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 et seq.;

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

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

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

(vi) access to, or acquisition or interception of, or preservation of communications or information as described in (i) through (ii) above and comparable State laws.

1.23. "Network Management Information" means: network plans, processes and procedures; placement of Network Operating Center(s) and linkages to other domestic and international

carriers, ISPs or other critical infrastructures; descriptions of any IP networks and operations processes and procedures related to backbone infrastructure(s); description of any proprietary control mechanisms and operating and administrative software; and all network performance information.

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

1.25. "Personnel" means an entity's (i) employees, officers, directors, and agents, and (ii) contract or temporary employees (part-time or full-time) who are under the direction and control of the entity and have Access to its products or services.

1.26 "Routine Business Visits" has the meaning given it in Section 3.6 of this Agreement.

1.27. "Security Incident" means any of the following incidents with respect to the Domestic Companies' products and services, when such incidents materially harm the national security interests of the United States: (i) the insertion of malicious code; insertion and/or transmittal of viruses or worms; denial of service attacks; use of botnets; phishing; identity theft; and unauthorized redirection or misdirection of Internet page requests (for purposes of the foregoing list an incident that is within the reporting guidelines of the United States Computer Emergency Readiness Team shall be considered a Security Incident); (ii) unauthorized addition, alteration, deletion, acquisition, theft, transfer, diversion of or Access to Classified Information, Sensitive Information, USG Customer Information and Customer Information; (iii) establishment of unauthorized communications channels to any foreign government or other unauthorized recipient; (iv) other unauthorized addition, alteration, deletion, acquisition, theft, transfer, diversion of or Access to information or technology as identified in collaboration with the USG Parties in the Security Policy required under Section 3.2 of this Agreement; or (v) any other similar use of the Domestic Companies' Products or Services.

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 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 Lawfully Authorized Electronic Surveillance pursuant to Lawful U.S. Process, (d) the means of carrying out Lawfully Authorized 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 any other U.S. Government information that is designated in writing by an authorized official as "Sensitive Information," "Official Use Only," "Limited Official Use Only," "Law Enforcement Sensitive," "Sensitive Security Information," "Not For Distribution to Foreigners," "NOFORN," or other similar categories.

1.29. "Subscriber Information" means information relating to subscribers or customers of Domestic 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.

1.30. "Stock Purchase Agreement" means the Stock Purchase Agreement, dated April 2, 2006, by and between GTE Holdings (Puerto Rico) LLC and Sercotel, S.A. de C.V., which is a subsidiary of América Móvil.

1.31. "TELPRI" has the meaning given to it in the Preamble.

1.32. "Transaction" means the purchase of TELPRI by América Móvil pursuant to the terms of the Stock Purchase Agreement.

1.33. "Transactional Data" means:

(i) "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;

(ii) any information possessed by the Domestic Companies relating to the identity or location of any customer, subscriber, account payer, or any end-user relating to all telephone numbers, domain names, IP addresses, Uniform Resource Locators ("URLs");

(iii) 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;

(iv) any information related to any mode of transmission (including mobile transmissions); and

(v) any information indicating 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, which 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).

1.34. "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, and specifically includes the Commonwealth of Puerto Rico.

1.35. "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 but not limited to 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.

1.36. "U.S. Hosting Services Customer" means any customer or subscriber that receives Hosting Services from the Domestic Companies that are U.S.-domiciled or holds itself out as being U.S.-domiciled.

1.37. "USG Customer Information" means any Identifying Information for any customer of the Domestic Companies that qualifies as or constitutes the U.S. Government as well as any other records or information pertaining to telecommunications equipment needs and/or purchases by the U.S. Government.

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

1.39. Other Definitional Provisions. Other capitalized terms used in this Agreement, including in the Preamble, 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:

(i) all Domestic Communications Infrastructure owned, operated or controlled by the Domestic Companies shall at all times be located in the United States and directed, controlled, supervised and managed by the Domestic Companies;

(ii) all Domestic Communications that are carried by or through the Domestic Communications Infrastructure shall pass through facilities under the control of the Domestic Companies that are physically located in the United States, and from which Lawfully Authorized Electronic Surveillance can be conducted pursuant to Lawful U.S. Process. Domestic Companies will provide technical or other assistance to facilitate such Lawfully Authorized Electronic Surveillance; and

(iii) all foreign connections traffic for circuit-switched communications and, to the extent technically feasible, Internet communications shall be monitored using industry best-practices, by the Domestic Companies for unauthorized access, unauthorized network intrusions and any other malicious activity.

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

(i) all Data Centers used to provide Hosting Services to U.S. Hosting Services Customers shall at all times be located in the United States; and

(ii) the Domestic Companies shall ensure that Wire or Electronic Communications of any specified U.S. Hosting Services Customer that are transmitted to, from or

through a Data Center shall be accessible from, or pass through a U.S.-based facility that is under the control of the Domestic Companies, and from which Lawfully Authorized Electronic Surveillance can be conducted.

2.3. Domestic Infrastructure and Data Center Compliance with Lawful U.S. Process. The Domestic Companies shall take all steps necessary to configure Domestic Communications Infrastructure and Data Centers to comply with:

(i) Lawful U.S. Process;

(ii) 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

(iii) 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. Domestic Employee Compliance with Lawful U.S. Process. The Domestic Companies shall take all steps necessary to ensure that its employees in the United States have unconstrained authority to comply with:

(i) Lawful U.S. Process;

(ii) 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

(iii) 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.

2.5. Information Storage. The Domestic Companies shall store exclusively in the United States the following:

(i) stored Domestic Communications;

(ii) Wire Communications or Electronic Communications received by, intended to be received by, or stored in the account of a customer or subscriber of the Domestic Companies.

(iii) Transactional Data and Call Associated Data relating to Domestic Communications;

(iv) Subscriber Information concerning customers who are U.S.-domiciled, customers who hold themselves out as being U.S.-domiciled, and customers who make any Domestic Communication;

(v) billing records of customers who are U.S.-domiciled, customers who hold themselves out as being U.S.-domiciled, and customers who make any Domestic Communication; and

(vi) Network Management Information, provided, however, that duplicate copies of such Network Management Information may be maintained at América Móvil's headquarters in Mexico City, Mexico.

2.6. U.S. Hosting Data Storage and Access. The Domestic Companies shall be able to provide to the USG Parties any stored U.S. Hosting Data. The Domestic Companies shall not store U.S. Hosting Data outside of the United States without written authorization from the USG Parties. Additionally, the Domestic Companies shall take all steps necessary to ensure that U.S. Hosting Data is stored in a manner not subject to mandatory destruction under any foreign laws.

2.7. Billing Records. The Domestic Companies shall store for at least five years all billing records described in Section 2.5(v) above.

2.8. Routing of Domestic Communications and U.S. Hosting Data. To the extent that routing of Domestic Communications and U.S. Hosting Data is controlled by the Companies or their affiliates, and except for routing of traffic (i) from or to U.S. states, territories and possessions outside the Continental United States, (ii) to avoid network disruptions, (iii) consistent with least-cost routing practices implemented pursuant to agreement between the Domestic Companies and the USG Parties, and (iv) only as agreed to in writing by the USG Parties, the Domestic Companies shall not route Domestic Communications or U.S. Hosting Data outside the United States. To the extent that routing of Domestic Communications and U.S. Hosting Data is controlled by the Companies or their affiliates, notwithstanding the foregoing and except for traffic bound to or from Mexico, Domestic Companies shall not route Domestic Communications or U.S. Hosting Data through Mexico. USG Parties recognize that the Domestic Companies' subscribers may choose alternative providers for their long distance service and that the Domestic Companies do not control interstate or international routing of calls for such subscribers.

2.9. Storage of Protected Information. The storage of Classified and Sensitive Information by the Domestic Companies or its contractors at any location outside of the United States is prohibited. Classified and Sensitive Information stored or maintained by the Domestic Companies in electronic form shall be encrypted.

2.10. Network Topology. Before the Closing Date, the Domestic Companies will provide to the USG Parties a comprehensive description of their domestic telecommunications network topology, including the location of servers, routers, switches, operational systems software, and network security appliances and software, and shall provide updates to such description upon request of any of the USG Parties.

2.11. Interconnection arrangements with América Móvil. Interconnection arrangements between Domestic Companies, on the one hand, and América Móvil, on the other hand, shall be made only through arms-length agreements based on commercial terms.

2.12. CPNI. Domestic Companies shall comply, with respect to Domestic Communications, with all applicable Federal Communications Commission ("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).

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

ARTICLE 3: SECURITY

3.1. Security Policies and Procedures. The Domestic Companies shall take reasonable steps and adopt an internal compliance process designed to prevent Security Incidents by the Companies, their Personnel, and any third party person or entity, including any foreign government, with respect to any of the Domestic Companies' products or services; such process shall include training and annual certification procedures. In the absence of prior approval by the USG Parties, the Companies shall not authorize any person or entity to take any action that, in the absence of such authorization, would constitute a Security Incident unless such authorization is consistent with this Agreement and with the normal course of the Companies' business. The Domestic Companies also will maintain or exceed security standards and best practices utilized within the U.S. telecommunications industry and will consult with the USG Parties and other appropriate U.S. Government agencies on steps to maintain or exceed such standards and practices. The Domestic Companies shall take measures consistent with such practices to prevent the use of or access to the Domestic Communications Infrastructure or to Data Centers to conduct Lawfully Authorized Electronic Surveillance, or to obtain or disclose Domestic Communications, U.S. Hosting Data, Classified Information, or Sensitive Information, in violation of any U.S. federal, state, or local laws, or the terms of this Agreement. These measures shall include maintenance of all existing Domestic Companies' security policies and procedures, and shall include provisions consistent with industry best practices for: maintenance of password systems, non-destructive access logs, including in particular, logs regarding any access to a capability to conduct electronic surveillance, and non-destructive audit logs; periodic internal network security audits; periodic switch audits to discover unauthorized "Free Line Service" accounts; physical security for access to Domestic Communications Infrastructure; and ensuring the placement of firewalls and associated security levels.

3.2. Maintenance of Existing Security Policies and Procedures. Consistent with Section 3.1 above, the Domestic Companies will maintain all existing security policies and procedures (attached hereto as Appendix A). The Domestic Companies will make all relevant information concerning these policies and procedures available to the USG Parties before the Closing Date of this Agreement and within thirty days of receipt of a written request made by the USG Parties during the life of this Agreement. Upon receipt of a written notice at least forty-eight hours in

advance from the USG Parties, the Companies will meet and confer with the USG Parties or their designees to address any concern. The Companies will provide at least thirty days advance written notice to the USG Parties of any proposed change to existing security policies. The Companies agree that if a Senate-confirmed official of any USG Party determines in writing that the proposed change would result in undue national security risk, the Companies will forgo the proposed change.

3.3. Security of Pre-Existing Lawfully Authorized Electronic Surveillance, Lawful U.S. Process and Protected Information. Prior to the Closing Date, the Domestic Companies' Security Officer(s) will secure all existing electronic surveillance equipment or processes, pursuant to procedures negotiated with the USG Parties, and will certify compliance with the requirements of Sections 2.9 and 3.1 of this Agreement with regard to any pre-existing Lawful U.S. Process, Classified, and Sensitive Information, including but not limited to: any order to intercept communications, order for a pen register or a trap and trace device, subpoena, or other lawful demand by a U.S. Government agency for U.S. records, including all Title III and FISA related intercepts and related orders data. América Móvil will not interfere with that securing of pre-existing electronic surveillance activities, Lawful U.S. Process or other information pursuant to this Section. Additionally, América Móvil and the Domestic Companies will not allow any person other than the Domestic Companies' Security Officer(s) to access any such information without first obtaining written authorization for such access from the USG Parties or from the agent of the USG who originally supplied the information to the Domestic Companies.

3.4. Security Officer Appointment, Responsibilities and Duties. The Head of Security of the Domestic Companies, or a designee in a direct reporting relationship with the Head of Security, shall serve as the Security Officer with the primary responsibility for ensuring compliance with the Domestic Companies' obligations under this Agreement, and shall be a resident citizen of the United States with an active security clearance or eligibility to apply for a security clearance as outlined in Executive Order 12968. The Domestic Companies will ensure that the Security Officer cooperates with any request by a USG Party for clearance or further background checks. Within thirty days after the Closing Date, the Domestic Companies shall notify the USG Parties of the identity of the Security Officer.

3.5. Visitation Policy. No later than ninety days after the Closing Date, the Domestic Companies shall adopt and implement a visitation policy for all visits by Foreign Persons to Domestic Communications Infrastructure. The visitation policy shall differentiate between categories of visits based on the sensitivity of the information, equipment and personnel to which the visitors will have access, and shall include a Routine Business Visit exception, as defined below. Under the policy, a written request for approval of a visit must be submitted to the Security Officer no less than seven days prior to the date of the proposed visit. For all visits to Domestic Communications Infrastructure covered by the policy, the Security Officer shall review and approve or disapprove the requests. A record of all such visit requests, including the decision to approve or disapprove, and information regarding consummated visits, such as date and place, as well as the names, business affiliation and dates of birth of the visitors, and the Domestic Companies' personnel involved, shall be maintained by the Security Officer for 2 years. During all such visits, visitors will be escorted at all times by an employee, and within conditions set forth by the Security Officer.

3.6 Routine Business Visits. Notwithstanding Section 3.5, Routine Business Visits may occur without prior approval by the Security Officer. A record of Routine Business Visits, including a log that contains the names of the visitors, their business affiliations, and the purpose of their visits, shall be maintained by the Security Officer for a period of at least two (2) years from the date of the visit itself. "Routine Business Visits" are those that: (a) are made in connection with the regular day-to-day business operations of the Domestic Companies; (b) do not involve Access to Call Associated Data, Classified Information, Customer Information, Domestic Communications, Domestic Communications Infrastructure, Sensitive Information, Subscriber Information, Transactional Data, U.S. Hosting Data, or USG Customer Information; and (c) pertain only to the commercial aspects of the Domestic Companies' business. These may include, but not limited to:

(i) visits for the purpose of discussing or reviewing such commercial subjects as company performance versus plans or budgets; inventory, accounts receivable, accounting and financial controls; and business plans and implementation of business plans;

(ii) visits of the kind made by customers or commercial suppliers in general regarding the solicitation of orders, the quotation of prices, or the provision of products and services on a commercial basis; and

(iii) visits concerning fiscal, financial, or legal matters involving a Domestic Company.

3.7. Restrictions on Access to Lawfully Authorized Electronic Surveillance Information and Equipment, Lawful U.S. Process. 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 Title III and FISA related intercepts, orders data and equipment. Specifically, unless otherwise agreed by the USG Parties or the agent of the USG who supplied the information to the Domestic Companies, 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 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.

3.8. Access by Foreign Government Authority. The Domestic 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 Companies 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 USG Parties or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process described in this Agreement shall be reported to the USG Parties as

soon as possible and in no event later than five business days after such request or legal process is received by and known to the Security Officer. Domestic Companies shall take reasonable measures to ensure that the Security Officer will promptly learn of all such requests or submission of legal process.

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

(i) Classified or Sensitive Information; or

(ii) Subscriber Information, Transactional Data, Call Associated Data, or 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 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 Domestic Companies for the communications, data or information identified in this Agreement that is maintained by Domestic Companies shall be referred to the USG Parties as soon as possible and in no event later than five business days after such request or legal process is received by and known to the Security Officer, 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. The Domestic Companies shall take reasonable measures to ensure that the Security Officer will promptly learn of all such requests or submission of legal process.

3.10. Notification of Access or Disclosure Requests from Foreign Non-Governmental Entities. Within thirty days of receipt, the Domestic Companies shall notify the USG Parties in writing of legal process or requests by foreign nongovernmental entities to Domestic 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.

3.11. Security of Lawful U.S. Process. The Domestic Companies shall protect the confidentiality and security of all Lawful U.S. Process served upon them and the confidentiality and security of Classified and Sensitive Information in accordance with U.S. Federal and state law or regulation and this Agreement. Information concerning Lawful U.S. Process, Classified Information, or Sensitive Information shall be under the custody and control of the Security Officer.

3.12. Disclosure of Protected Data. The Security Officer shall not directly or indirectly disclose information concerning Lawful U.S. Process, Classified Information or Sensitive Information to any third party, or to any officer, director, shareholder, employee, agent, or contractor of América Móvil, including those who serve in a supervisory, managerial or officer

role with respect to the Security Officer, except to the extent required to comply with this Agreement, unless disclosure has been approved by prior written consent obtained from the USG Parties.

3.13. Removal of Security Director or Security Officer. Any Security Officer may be removed for any reason permitted by the provisions of applicable law or under the charter of the Domestic Companies, provided that:

(i) the removal of a Security Director or Security Officer shall not become effective until the USG Parties have received written notification of removal; a successor who is qualified within the terms of this Agreement is selected; the USG Parties receive written notice of the proposed replacement; and the USG Parties do not object to the proposed replacement within ten days of receipt of such notice; and

(ii) notwithstanding the foregoing, however, if immediate removal of any Security Director or Security Officer is deemed necessary to prevent actual or possible violation of any statute or regulation or actual or possible damage to the Domestic Companies, the individual may be temporarily suspended, pending written notification to the USG Parties, and removed upon the approval by the USG Parties.

(iii) In no event shall a vacancy for the position of Security Director or Security Officer exist for a period of more than thirty days before Domestic Companies nominate a qualified candidate to fill such vacancy.

3.14. Point of Contact. Within fourteen days after the Closing Date, the Domestic Companies shall designate in writing to the USG Parties at least one nominee already holding a U.S. security clearance, or reasonably believed to be eligible for such a clearance, to serve as a primary point of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process. The point of contact shall be assigned to the Domestic Companies' office(s) in the United States, shall be available twenty-four hours per day, seven days per week and shall be responsible for accepting service and maintaining the security of Classified and Sensitive Information and any Lawful U.S. Process in accordance with the requirements of U.S. law and this Agreement. The Domestic Companies shall promptly notify the USG Parties of any change in such designation. The Domestic Companies shall cooperate with any request by a U.S. federal, state or local government entity within the United States that a further background check or further security clearance process be completed for a designated point of contact.

3.15. Screening of Additional Personnel. The Domestic Companies shall implement a thorough screening process through a reputable third party to ensure compliance with all personnel screening requirements agreed to by the Domestic Companies and the USG Parties, which includes screening for any existing or newly hired personnel (such personnel, upon completion of screening procedures, to be considered "Screened Personnel"):

(i) whose position involves access to the Domestic Communications Infrastructure that enables those persons to monitor the content of Wire or Electronic Communications (including in electronic storage);

(ii) whose position allows access to Transactional Data, Call Associated Data or Subscriber Information; and

(iii) all persons who have access to Sensitive Information or USG Facilities or premises; and

(iv) all security personnel.

3.16. Screening Process Requirements. The screening process undertaken pursuant to this Section shall follow the guidance to U.S. Government agencies for screening civilian Federal employees in Executive Order 10450, and shall specifically include a background and financial investigation, in addition to a criminal records check.

(i) The Domestic Companies shall consult with the USG Parties on the screening procedures utilized by the reputable third party and shall provide to the USG Parties a list of the positions subject to screening within sixty days of the Closing Date. The Domestic Companies shall utilize the criteria identified pursuant to Section 3.15 of this Agreement to screen personnel, shall report the results of such screening on a regular basis to the Security Officer, and shall, upon request, provide to the USG Parties all the information it collects in its screening process of each candidate. Candidates for these positions shall be informed that the information collected during the screening process may be provided to the U.S. Government, and the candidates shall consent to the sharing of this information with the U.S. Government.

(ii) The Domestic Companies will cooperate with a request by the USG Parties or any U.S. Government agency desiring to conduct any further background checks.

(iii) Individuals who are rejected pursuant to such further background checks by the USG Parties for the screening requirements of this Agreement will not be hired or, if they have begun their employment, will be immediately removed from their positions or otherwise have their duties immediately modified so that they are no longer performing a function that would require screening under this Section. The Domestic Companies will notify the USG Parties of the transfer, departure, or job modification of any individual rejected because of the screening conducted pursuant to this Agreement within seven days of such transfer or departure, and shall provide the USG Parties with the name, date of birth and social security number of such individual.

(iv) The Domestic Companies shall provide training programs to instruct Screened Personnel as to their obligations under the Agreement and the maintenance of their trustworthiness determination or requirements otherwise agreed. The Domestic Companies shall monitor on a regular basis the status of Screened

Personnel, and shall remove personnel who no longer meet the Screened Personnel requirements.

(v) The Domestic Companies shall maintain records relating to the status of Screened Personnel, and shall provide these records, upon request, to any or all of the USG Parties.

3.17. Notification of Changes to Corporate Leadership. Except as set out below, the Companies will provide at least thirty days advance written notice to the USG Parties of any proposed replacement with a Foreign Person of a member of the Board of Directors or senior management at the Vice President level or above of any of the companies incorporated in the United States. In exigent circumstances, such as the acquisition of TELPRI to be consummated on the Closing Date, the Companies agree to provide written notice to the USG Parties of the replacement of any members of the Board or senior management with a Foreign Person as soon as practicable, and in no case less than 10 business days after the replacement is effectuated. This notice shall include sufficient information to confirm the identity of the proposed Foreign Person. If, within 30 days of notice, the USG Parties object to the proposed replacement with a Foreign Person of a member of the Board of Directors or of senior management the Domestic Companies, the Companies will not appoint that candidate to the position, or will remove that individual from the position.

3.18. Operational Control of the Domestic Companies' Network. Except to the extent and under conditions concurred in by the USG Parties in writing, operational control of the Domestic Communications Infrastructure, including network administration, maintenance and provisioning, will be restricted to the Domestic Companies' facilities located in the United States, and the Domestic Companies shall prohibit remote access from outside the United States, to network elements, any capabilities to conduct electronic surveillance, and operational support systems.

3.19. Notice of Obligations. The Domestic Companies shall instruct appropriate officials, employees, contractors, and agents as to the security restrictions and safeguards imposed by this Agreement.

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

3.21. Security Meetings with the U.S. Government. Upon request by any or all of the USG Parties, the Companies shall meet with the requesting USG Parties and any other U.S. Government entity designated by the USG Parties, to discuss matters concerning the Companies' compliance with and enforcement of this Agreement and any other issue that could affect U.S. national security. The USG Parties shall coordinate such meetings and take reasonable steps so as not to place an undue economic burden on the Companies.

3.22. U.S. Government Access to Facilities, Records and Personnel. Upon forty-eight hours prior written request from the USG Parties, the Domestic Companies shall provide access to all records requested and/or physical access to facilities and personnel requested. The Companies

may request a meeting to discuss the scope of the U.S. Government agency's request or other reasonable concerns, and the U.S. Government agency shall meet with the Companies as soon as possible, but the meeting request shall not excuse the Domestic Companies' obligation to comply within the forty-eight hours.

3.23. Establishment of Security Committee of TELPRI Board. The TELPRI board of directors shall establish a Security Committee to oversee the Domestic Companies' implementation of and compliance with this Agreement. The Security Committee shall be comprised solely of directors ("Security Directors") who are U.S. citizens; who, if not already in possession of U.S. security clearances, are reasonably believed to be eligible to apply for security clearances pursuant to Executive Order 12968; and who satisfy the independent director requirements of the New York Stock Exchange. If a Security Director does not already possess a U.S. security clearance, he or she may nevertheless serve as Security Director, subject to approval by the USG Parties. The Security Committee shall supervise and report to the full TELPRI board of directors on the Domestic Companies' implementation of and compliance with this Agreement, consistent with their obligation to keep such information confidential. To perform its function, the Security Committee shall, among other things, receive reports from the Security Officer on TELPRI's compliance with this Agreement, and also shall receive a summary of any report issued pursuant to this Agreement, including the annual report on compliance issued pursuant to Section 5.5 of this Agreement. The Security Committee shall, in turn, provide general reporting to the full TELPRI Board on TELPRI's compliance with this Agreement. Not fewer than two TELPRI directors shall serve at any time as the Security Committee of the TELPRI Board.

3.23. Attendance of Security Directors at Board Meetings of Domestic Companies. A meeting of the board of a Domestic Company or of a board committee of a Domestic Company shall not occur without a Security Director in attendance, whether as a member or as an observer, unless the issues addressed at such meeting in no respect address or affect the obligations of the Domestic Company under this Agreement. In the event that the board of a Domestic Company or a board committee of a Domestic Company must address at a meeting, for reasons of exigent circumstances, an issue related to or affecting the obligations of the Domestic Company under this Agreement, and all Security Director positions are vacant at the time of such a meeting, the absence of the Security Director will not prevent the meeting provided that the Security Officer attends the meeting.

ARTICLE 4: DISPUTES AND REMEDIES

4.1. Informal Resolution. The Parties shall use their best efforts to resolve any disagreements or incidents that may arise under this Agreement. Disagreements or incidents 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 policy-level officials of the USG Parties, unless those higher authorized officials believe that important national interests can be protected, or the Companies believe that their paramount commercial interests can be resolved, only by resorting to the measures set forth in 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 this Agreement.

4.2. Enforcement of 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 injunctive or other judicial relief. Nothing in this Agreement shall limit or affect the right of any Party to exercise any rights it may have under law or regulation or this Agreement. In the case of the USG Parties, this includes, but is not limited to, any or all of the following:

(i) require that the Party or Parties believed to have breached, or about to breach, this Agreement cure such breach within thirty days upon receiving written notice of such breach;

(ii) require that the Companies pay monetary damages and reasonable costs associated with compensating the USG Parties for actual and direct expenses associated with an incident of breach; provided, however, that nothing in this provision shall require the Companies to compensate the USG Parties for any indirect or consequential damages;

(iii) seek civil remedies for any violation by the Companies of any U.S. law or regulation or term of this Agreement;

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

(v) seek suspension or debarment of the Companies from eligibility for contracting with the U.S. Government.

4.3. Security Incidents. Notwithstanding any provision of this Agreement to the contrary, the Parties agree that if any Personnel of the Companies knowingly uses or participates in the use of the Domestic Companies' Services or Products in any Security Incident, this shall constitute a breach of this Agreement.

4.4. Indemnification of Security Directors, and Security Officer. The Companies shall indemnify and hold harmless the Security Directors and the Security Officer of the Domestic Companies from any and all claims arising from, or in any way connected to, his or her performance as a Security Director or Security Officer under this Agreement except for his or her own individual gross negligence or willful misconduct. The Companies shall advance fees and costs incurred in connection with the defense of such claim. The Companies may purchase insurance to cover this indemnification.

4.5. Non-Waiver of Third Party Claims. Nothing contained in this Article 13 shall be deemed a waiver of any claims or remedies the Companies may have against third parties related to this Agreement.

4.6. Irreparable Injury. The Companies agree that the United States would suffer irreparable injury if for any reason they failed to perform any of their material obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, the Companies 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 immediate injunctive or other equitable relief.

ARTICLE 5: REPORTING, NOTICE AND LIMITS

5.1. Outsourcing. The Domestic Companies shall not outsource functions covered by this Agreement, except pursuant to an outsourcing policy to be negotiated with the USG Parties. Such policy shall include prior notice of the proposed outsourcing and the right of the USG Parties to object within thirty days of receipt of notice to the proposed outsourcing. The parties agree to exclude from this notice and approval requirement outsourcing contracts that do not provide Access to Call Associated Data, Classified Information, Customer Information, Domestic Communications, Domestic Communications Infrastructure, Sensitive Information, Subscriber Information, Transactional Data, U.S. Hosting Data, or USG Customer Information. Further:

(i) the Domestic Companies shall ensure that the entity complies with the applicable terms of this Agreement;

(ii) the Domestic Companies shall include in its contracts with any such entities written provisions requiring that such entities comply with all applicable terms of this Agreement (and otherwise ensure that such entities are aware of, agree to, and are bound to comply with the applicable obligations of this Agreement);

(iii) if the Domestic Companies are reasonably uncertain as to whether an outsourcing contract is covered by the outsourcing policy, they shall include in the contract a provision that such contract may be terminated should the USG Parties object to the contract, shall notify the USG Parties within thirty days of executing the contract, which notice shall identify the name of the entity and the nature of the contract, and the USG Parties shall have 30 days from notice in which to object to the outsourcing contract;

(iv) if the Domestic Companies learn that the entity or the entity's employee has violated an applicable provision of this Agreement, the Domestic Companies will notify the USG Parties promptly; and

(v) with consultation and, as appropriate, cooperation with the USG Parties, the Domestic Companies will take reasonable steps necessary to rectify promptly the situation, which steps may (among others) include terminating the arrangement with the entity, including after notice and opportunity for cure, and/or initiating and pursuing litigation or other remedies at law and equity. Peering, interconnection and purchase of local access service shall not constitute outsourced functions for purposes of this Agreement.

5.2. Notice of Foreign Influence. If any member of the senior management of América Móvil or the Domestic Companies (including the Chief Executive Officer, President, General Counsel, Chief Technical Officer, Chief Financial Officer, Head of Network Operations, Head of Security, Security Officer, or other such senior officer) acquires any information that reasonably indicates that any Foreign Person has acted or plans to act in any way that interferes with or impedes the

performance by the Domestic Companies of their duties and obligations under the terms of this Agreement, or the exercise by the Domestic Companies of their rights under this Agreement, then such member shall promptly cause to be notified the Security Officer, who in turn shall promptly notify the USG Parties in writing of the timing and the nature of the foreign government's or entity's plans and/or actions.

5.3. Reporting of Incidents. The Domestic Companies shall take practicable steps to ensure that, if any of their officers, directors, employees, contractors or agents acquire 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 Lawfully Authorized 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 commercial use of CPNI); or (d) improper access to or disclosure of Classified or Sensitive Information, then the individual will notify the Security Officer or a Security Director, who will in turn notify the USG Parties in the same manner as specified in Section 5.2. This report shall be made promptly and in any event no later than ten calendar days after the Domestic Companies acquire information indicating a matter described in this Section 5.3(a)-(d) of this Agreement. The Domestic Companies shall lawfully cooperate in investigating the matters described in this Section of this Agreement. The Domestic Companies 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.

5.4. Non-Retaliation. The Domestic Companies shall, by duly authorized action of their respective boards of directors, adopt and distribute an official corporate policy that strictly prohibits any of the Domestic Companies from discriminating or taking any adverse action against any officer, director, employee, contractor or agent because he or she has in good faith initiated or attempted to initiate a notice or report under Sections 5.2 and 5.3 of this Agreement, or has notified or attempted to notify directly the Security Officer or a Security Director named in the policy to convey information that he or she believes in good faith would be required to be reported to the USG Parties by the Security Officer or a Security Director under Sections 5.2, and 5.5 of this Agreement. Such corporate policy shall set forth in a clear and prominent manner the contact information for the Security Officer or one or more Security Directors to whom such contacts may be made directly by any officer, director, employee, contractor or agent for the purpose of such report or notification. Any violation by the Domestic Companies of any material term of such corporate policy shall constitute a breach of this Agreement.

5.5. Annual Report. On or before the last day of January of each year, the Security Officer shall submit to the USG Parties a report assessing Domestic Companies' compliance with the terms of this Agreement for the preceding calendar year. The report shall include:

(i) a certification of compliance with this agreement, signed by the Security Officer;

(ii) a copy of the policies and procedures adopted to comply with this Agreement;

(iii) 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

(iv) identification of any other issues that, to Domestic Companies' knowledge, will or reasonably could affect the effectiveness of or compliance with this Agreement. The Domestic Companies shall make available to the Security Officer, in a timely fashion, all information necessary to complete the report required by this Section.

5.6. Third Party Network Security Audits. The Domestic Companies shall retain and pay for a neutral third party telecommunications engineer to audit its operations objectively on an annual basis. The Domestic Companies shall provide notice of its selected auditor to the USG Parties, and the USG Parties shall be able to review and approve or disapprove the selected auditor and terms of reference for that auditor within thirty days of receiving notice. In addition, the Domestic Companies shall provide to the USG Parties a copy of its contract with the third party auditor, which shall include terms defining the scope and purpose of the audits. The USG Parties shall have the right to review and approve the terms defining the scope and purpose of the audits. Through its contract with the third party auditor, the Domestic Companies shall ensure that all reports generated by the auditor are provided promptly to the USG Parties. The Domestic Companies also will provide the USG Parties with access to facilities, information, and personnel consistent with Sections 3.22 in the event that the USG Parties wish to conduct their own audit of the Domestic Companies. The terms defining the scope and purpose of the audits shall include, at a minimum, the following:

(i) Development of an initial vulnerability and risk assessment based on this Agreement, and a detailed audit work plan based on such assessment, which work plan may, at the discretion of the USG Parties, be subject to review and approval by the USG Parties;

(ii) Authority for the auditor to review and analyze the Domestic Companies' security policies and procedures related to network security;

(iii) Authority to audit the integrity of password systems, review access logs, review logs regarding any access to a capability to conduct electronic surveillance, conduct switch audits to discover "Free Line Service" accounts;

(iv) Authority for the auditor to review and analyze relevant information related to the configuration of the Domestic Companies' network;

(v) Authority for the auditor to conduct a reasonable number of unannounced inspections of the Domestic Companies facilities;

(vii) Authority for the auditor to conduct a reasonable volume of random testing of network firewalls, access points and other systems for potential vulnerabilities;

(viii) Other authorities related to network security as agreed by the parties after consultation with the USG Parties.

ARTICLE 6: FREEDOM OF INFORMATION ACT

6.1. Protection of Information. The USG Parties shall fully comply with any and all applicable U.S. laws and regulations relating to the confidentiality and protection of information

supplied to the USG Parties by the Companies pursuant to the terms of this Agreement, including obligations under 50 App. U.S.C. § 2170(c), 31 C.F.R. § 800.702, and 18 U.S.C. § 1905.

6.2. Use of Information for U.S. Government Purposes. The USG Parties shall use information supplied to the USG Parties by the Companies pursuant to this Agreement only for the purposes set forth in this Agreement. Nothing in this Agreement shall prevent 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 USG Parties take all reasonable measures to protect from public disclosure the information marked as described in Section 6.3.

6.3 FOIA Confidentiality. To the extent so marked by the Companies, all information supplied to the USG Parties by the Companies pursuant to the terms of this Agreement contains proprietary, trade secret, commercial, or financial information, and shall be deemed voluntarily provided pursuant to a request for confidentiality, and is exempt from disclosure under the Freedom of Information Act (5 U.S.C. § 552) under Exemption (b)(4).

ARTICLE 7: FCC CONDITION AND CFIUS PROCESS

7.1 FCC Approval. Upon execution of this Agreement by all the Parties, the FBI, DOJ and DHS shall promptly notify the FCC that, provided the FCC adopts a condition substantially the same as set forth in Appendix B to this Agreement, the FBI, DOJ and DHS have no objection to the grant of América Móvil's Petition for Declaratory Ruling and applications filed with the FCC as reflected in WT Docket No. 06-113. This Section 7.1 is effective upon the Effective Date.

7.2. CFIUS. In consideration for the execution of this Agreement, the USG Parties will not make any objection to CFIUS or the President concerning the Transaction.

ARTICLE 8: MISCELLANEOUS PROVISIONS

8.1. Obligations of América Móvil. América Móvil shall cause the Domestic Companies to comply with this Agreement and, where appropriate, shall act through their subsidiaries to discharge their obligations under this Agreement.

8.2. Corporate Structure. As soon as possible prior to the Closing Date, the Companies shall provide to the USG Parties a description of the contemplated corporate structure of the Companies as it relates to América Móvil's ownership and control of the Domestic Companies (the "Corporate Structure"), including the placement of the subsidiaries within the Corporate Structure that will be in effect as of the Closing Date, which description shall be included as Appendix C to this Agreement. The description shall identify the parent company or companies of each of the Companies and the subsidiaries in the Corporate Structure. Following the Closing Date, the Companies shall notify the USG Parties prior to any modification of the Companies' Corporate Structure and shall provide an updated description, which shall be incorporated into Appendix C; provided that if a modification to the Corporate Structure does not change the entity that Controls the Companies, then the Companies shall notify the USG Parties of the change within 30 days after consummation of the change, which shall be incorporated into Appendix C.

8.3. Right to Make and Perform Agreement. The Parties represent that they have and shall continue to have throughout the term of this Agreement the authority and full right to enter into this Agreement and perform the obligations hereunder, and that this Agreement is a legal, valid, and binding obligation of the Parties and is enforceable in accordance with its terms.

8.4. 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.

8.5. Other Laws. Nothing in this Agreement is intended to limit or alter or constitute a waiver of (a) any obligation imposed on the Companies, their Personnel, or their agents by any U.S. federal, state or local laws, (b) any enforcement authority available under any U.S. federal, state, or local laws, (c) the sovereign immunity of the United States, (d) any authority or jurisdiction the U.S. Government may possess over the activities of the Companies, their Personnel, or their agents located within or outside the United States, or (e) any rights of the Companies, their Personnel, or their agents under the U.S. Constitution, any state constitution, or any U.S. federal, state, or local laws. Nothing in this Agreement is intended to or is to be interpreted to require the Companies, their Personnel, or the USG Parties to violate any applicable U.S. law. Likewise, nothing in this Agreement limits the right of the U.S. Government to pursue criminal or civil sanctions or charges against the Companies or their Personnel in an appropriate case, and nothing in this Agreement provides the Companies, their Personnel, or their agents with any relief from civil liability in an appropriate case.

8.6. Choice of Law. This Agreement shall be governed by and interpreted according to the laws of the District of Columbia.

8.7. Forum Selection. Any civil action among the Companies and the USG 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 or the United States Court of Federal Claims.

8.8. Integrated Agreement. This Agreement and all appendices hereto is a fully integrated agreement.

8.9. Statutory and Regulatory References. All references in this Agreement to statutory and regulatory provisions shall include any future amendments or revisions to such provisions.

8.10. 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 Closing Date.

8.11. Modifications. This Agreement may only be modified by written agreement signed by all of the Parties.

8.12. Non-Parties. Nothing in this Agreement is intended to confer or does confer any rights on any person other than the Parties.

8.13. Changes in Circumstances for USG Parties. If, after the Closing Date, the USG Parties find that the terms of this Agreement are inadequate to address their national security concerns, then the Companies will negotiate in good faith to modify this Agreement to address those concerns. In the event that improvements in technology may enhance the efficacy of this Agreement to protect the national security, the Parties will negotiate promptly and in good faith to amend the Agreement to implement such advances.

8.14. Termination. After the Closing Date, this Agreement may be terminated at any time by a written agreement signed by the Parties.

8.15. Termination of Stock Purchase Agreement. If the Stock Purchase Agreement is terminated prior to the Closing Date, the Companies shall promptly provide written notification of such termination to the USG Parties, and upon receipt of such written notice, this Agreement shall automatically terminate.

8.16. 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.

8.17. Counterparts. This Agreement may be executed in one or more counterparts, including by facsimile, each of which shall together constitute the same instrument.

8.18. Successors and Assigns. This Agreement shall inure to the benefit of and shall be binding upon the Parties and their respective successors and assigns; for purposes of this Agreement, successors and assigns under this Section shall include any corporate name changes.

8.19. Notices. As of the Closing Date, 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 sent by electronic mail and by one of the following means: (a) delivered personally, (b) sent by facsimile, (c) sent by documented overnight courier service, or (d) sent by registered or certified mail, postage prepaid, addressed to the Parties' designated representatives at the addresses shown below, unless provided otherwise in this Agreement; provided, however, that upon written notification to the Parties, any party to this Agreement may unilaterally amend or modify its designated representative information, notwithstanding any provision to the contrary in this Agreement:

For América Móvil and TELPRI:
América Móvil, S.A. de C.V.:
Alejandro Cantú Jiménez
Lago Alberto 366
Torre 1, Piso 2
Colonia Anáhuac
11320 Mexico, D.F.
011-52-525-703-3990
acantu@americamovil.com

For the U.S. Department of Justice:
Christopher P. Simkins
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 2311
Washington, D.C. 20530
(202) 305-8761 (phone)
(202) 305-8565 (fax)
christopher.simkins@usdoj.gov

For the U.S. Department of Homeland Security:
Sanchitha Jayaram
Office of the Assistant Secretary for Policy
U.S. Department of Homeland Security
NAC, Building 17-134
Anacostia Naval Annex, Bldg 410
245 Murray Lane, SW
Washington, D.C. 20528
(202) 447-3817 (phone)
(202) 282-8503 (fax)
IP-CFIUS@DHS.GOV

This Agreement is executed on behalf of the Parties:

América Móvil, S.A. de C.V.

Date: By:_____
Name:
Title:

Telecomunicaciones de Puerto Rico, Inc.

Date: By:_____
Name:
Title:

United States Department of Justice

Date: By:_____
Name:
Title:

United States Department of Homeland Security

Date: By:_____
Name:
Title:

APPENDIX A

TELPRI SECURITY POLICIES AND PROCEDURES

APPENDIX B

CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that this authorization and any licenses related thereto are subject to compliance with the provisions of the Agreement attached hereto between América Móvil, S.A. de C.V., on behalf of itself and its subsidiaries through which it will hold its interest in TELPRI ("América Móvil), and Telecomunicaciones de Puerto Rico, Inc. ("TELPRI"), (collectively, "the Companies"), on the one hand, and the U.S. Department of Justice ("DOJ"), and the U.S. Department of Homeland Security ("DHS"), on the other (collectively, "the USG Parties"), dated _____, 2006, which Agreement is intended to enhance the protection of U.S. national security, law enforcement, and public safety. Nothing in this Agreement is intended to limit any obligation imposed by Federal law or regulation.