NETWORK SECURITY AGREEMENT

This AGREEMENT is made as of the date of the last signature affixed hereto, by and among Telefonica Moviles, S.A. ("Moviles"), TEM Puerto Rico, Inc. ("TEM PR"), and NewComm Wireless Services, Inc. ("NewComm"), collectively or individually, a "Party," and the Federal Bureau of Investigation ("FBI"), the U.S. Department of Justice ("DOJ"), and the U.S. Department of Homeland Security ("DHS"), collectively or individually, a "Party," (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 Homeland Security Presidential Directive / Hspd-7, Critical Infrastructure Identification, Prioritization, and Protection);

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

WHEREAS, NewComm, doing business as MoviStar, holds the C block license for and operates a broadband Personal Communications Service ("PCS") system serving the San Juan, Puerto Rico Basic Trading Area ("BTA") and the Mayaguez, Puerto Rico BTA, along with 131 Fixed Microwave Services licenses and an authorization to provide international global resale and facilities-based telecommunications services (collectively, the "Puerto Rico License"), pursuant to Section 214 of the Communications Act of 1934, as amended (the "Act");

WHEREAS, NewComm, which is now majority owned and controlled by ClearComm, L.P. ("ClearComm"), a limited partnership organized under the laws of the state of Delaware, proposes to enter into a transaction (the "TEM PR Transaction") whereby a controlling 50.1% voting ownership interest in NewComm will be transferred to TEM PR, a corporation organized under the laws of the Commonwealth of Puerto Rico and wholly owned by Moviles, a publicly-traded Spanish corporation that, in turn, is

majority owned and controlled by Telefonica, S.A., a publicly-traded corporation organized under the laws of Spain;

WHEREAS, NewComm, ClearComm, and TEM PR have filed with the Federal Communications Commission ("FCC") certain Applications (WT Docket No. 02-366) under Sections 214 and 310(d) of the Act seeking FCC approval of the transfer of control of NewComm, as holder of the Puerto Rico Licenses and related authorizations, to TEM PR, together with a Petition for Declaratory Ruling that it is in the public interest for TEM PR to hold a greater than 25% interest in NewComm;

WHEREAS, the FCC's grant of the applications in FCC WT Docket No. 02-366 may be made subject to conditions relating to national security, law enforcement, and public safety;

WHEREAS, Moviles, TEM PR, and NewComm have agreed to enter into this Agreement with the FBI, DHS and DOJ to address issues raised by the FBI, DHS and DOJ, and to request that the FCC condition the authorizations and licenses granted by the FCC on their compliance with this Agreement;

WHEREAS, representatives of Moviles, TEM PR, and NewComm represent that they have no present plans, and are not aware of any present plans of any other entity, as a result of which NewComm will (a) provide, direct, control, supervise or manage Domestic Communications through facilities located outside the United States; or (b) route Domestic Communications outside the United States except as previously disclosed to the FBI, DOJ and DHS as indicated in a letter among the Parties dated April 28, 2004;

WHEREAS, the government of Spain has enacted Ley 5/1995 de Regimen Jurídico de Enajenación de Participaciones Públicas en Determinadas Empresas (Law 5/1995 of 23 March 1995 on the legal arrangements for disposal of public shareholdings in certain undertakings) (B.O.E. 1995, 7456), as amended ("Law"), and issued Real Decreto 8/1997 de 10 de enero, de applicación del régimen de autorización administrativa previa a Telefónica de España, Sociedad Anónima, y a otra sociedad de su grupo (Royal Decree 8/1997 of 10 January 1997 concerning the application of the rules governing advance administrative authorization to Telefonica S.A. and another company of its group) (B.O.E. 1997, 584), as amended ("Decree");

WHEREAS, the Law and Decree, which are in force for a term of ten (10) years from February 18, 1997, generally provide that certain company resolutions of Moviles and Telefonica, S.A are subject to rules governing advance administrative authorization from the government of Spain, including those resolutions that involve voluntary dissolution, spin-off, or merger; the substitution of company purpose; the sale or encumbrance, in any form and on any basis, of certain communications assets located in Spain; and the sale or encumbrance, in any form and on any basis, of shares or certificates representing capital that are owned by Moviles or Telefonica, S.A.; and

WHEREAS, representatives of Moviles, TEM PR, and NewComm represent that (a) the European Court of Justice has declared that the Law and Decree might constitute a violation of European law, and that the full application of the Law and Decree to Moviles and Telefonica, S.A. is uncertain; and (b) to the extent that the government of Spain has any rights with respect to Moviles and Telefonica, S.A. pursuant to the Law and Decree, the Law and Decree shall not impair the Parties' compliance with the terms of this Agreement;

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

ARTICLE 1: DEFINITION OF TERMS

As used in this Agreement:

1.1 "Affiliate" means any entity that NewComm, Moviles or TEM PR Controls.

1.2 "Call Associated Data" means any information related to a Domestic Communication or related to the sender or recipient of that Domestic Communication and 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 dialed digit extraction, in-band and out-of-band signaling, and party add, drop and hold.

1.3 "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.

1.4 "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 paragraphs (a) through (d) above; or

(f) the matters covered by this Agreement.

1.5 "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., Subtitle B, Chapter VII, Subchapter C.

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

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

1.8 "Domestic Communications Infrastructure" means (a) the transmission, switching, bridging and routing equipment (including software and upgrades) used by or on behalf of NewComm to provide, process, direct, control, supervise or manage Domestic Communications; (b) facilities and equipment used by or on behalf of NewComm that are physically located in the United States; and (c) facilities used by or on behalf of NewComm to control the equipment described in (a) and (b) above. Domestic Communications Infrastructure does not include equipment or facilities used by service providers other than NewComm or its Affiliates that are: (a) interconnecting communications providers; or (b) providers of services or content that are 1) accessible using the communications services of NewComm or its Affiliates, and 2) available in substantially similar form and on commercially reasonable terms through communications services of companies other than NewComm or its Affiliates. The phrase "on behalf of" as used in this Section does not include entities with which NewComm or any of its Affiliates has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree.

1.9 "Effective Date" means the date on which the TEM PR Transaction is consummated. NewComm will provide the FBI, DOJ and DHS with reasonable advance written notice of the Effective Date.

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

1.11 "Electronic Surveillance" means (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(4), (1), (2) 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) the acquisition of dialing, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law, as defined in 18 U.S.C. § 3121 *et seq.* and 50 U.S.C. § 1841 *et seq.*; (d) the acquisition of location-related information concerning a service subscriber or facility; (e) the preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (f) access to, or acquisition, interception or preservation of, wire, oral, or electronic communications or information as described in (a) through (e) above, and comparable state laws.

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

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

1.14 "Intercept" or "Intercepted" has the meaning given it in 18 U.S.C. § 2510(4).

1.15 "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, Transactional Data or Subscriber Information.

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

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

1.18 "*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 the FCC's Rules.

1.19 "Security Officer" has the meaning given in Section 3.10 of this Agreement.

1.20 "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; (d) the means of carrying out Electronic Surveillance; (e) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process; (f) information deemed to be Sensitive Information pursuant to Executive Order or Executive Decision; and (g) 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." NewComm 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 NewComm's favor.

1.21 "Subscriber Information" means information 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.

1.22 "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 NewComm, or an entity acting on behalf of NewComm, 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 (d) 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, 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 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. The phrase "on behalf of" as used in this Section does not include entities with which NewComm or any of its Affiliates has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree.

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

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

1.25 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, DOJ, and DHS in writing:

(a) all Domestic Communications Infrastructure shall at all times be located in the United States and will be directed, controlled, supervised and managed by NewComm; 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 NewComm and physically located in the United States, from which Electronic Surveillance can be conducted pursuant to Lawful U.S. Process. NewComm will provide technical or other assistance to facilitate such Electronic Surveillance.

2.2 Compliance with Lawful U.S. Process. NewComm shall ensure that at all times its Domestic Communications Infrastructure will be capable of complying, and NewComm's officials, agents and 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.*).

2.3 Information Storage and Access. NewComm, effective upon execution of this Agreement by all the Parties, shall store exclusively in the United States the following:

(a) stored Domestic Communications if such communications are stored by or on behalf of NewComm 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 NewComm customer or subscriber if such communications are stored by or on behalf of NewComm for any reason;

(c) Transactional Data and Call Associated Data relating to Domestic Communications if such information is stored by or on behalf of NewComm for any reason;

(d) Subscriber Information concerning NewComm customers or subscribers if such information is stored by or on behalf of NewComm for any reason;

(e) billing records relating to NewComm customers or subscribers, for so long as such records are kept and, at a minimum, for so long as such records are required to be kept pursuant to applicable U.S. law or this Agreement; and

(f) Network Management Information.

The phrase "on behalf of" as used in this Section does not include entities with which NewComm or any of its Affiliates has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree.

2.4 Reserved

2.5 Billing Records. NewComm shall store for at least two (2) years all billing records described in Section 2.3(e) above and shall make its billing records available in the United States. Nothing in this Section 2.5 shall require NewComm to store such records for longer than two years.

2.6 Storage Pursuant to 18 U.S.C. § 2703(f). Upon a request made pursuant to 18 U.S.C. § 2703(f) by a Government Authority in the United States to preserve any information in the possession, custody, or control of NewComm that is listed in Section 2.3 above, NewComm shall store such records in the United States.

2.7 Compliance with U.S. Law. Nothing in this Agreement shall excuse NewComm from any obligation it may have to comply with U.S. legal requirements for the retention, preservation, or production of information, records or data.

2.8 Routing of Domestic Communications. NewComm will not route Domestic Communications outside the United States.

2.9 CPNI. NewComm shall comply 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).

2.10 Storage of Protected Information. Neither NewComm nor its contractors shall store Classified, Controlled Unclassified, or Sensitive Information at any location outside the United States, unless the storage is at a U.S. military facility, a U.S. Embassy or Consulate or other location occupied or approved by a U.S. Government Authority. The issuance of a license under the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations shall satisfy this criterion with respect to Controlled Unclassified Information.

ARTICLE 3: SECURITY

3.1 Measures to Prevent Improper Use or Access. NewComm shall take all reasonable measures to prevent the use of or access to the Domestic Communications Infrastructure to conduct Electronic Surveillance, or to obtain or disclose Domestic Communications, 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 Visitation Policy. NewComm shall adopt and implement a visitation policy within ninety (90) days of the Effective Date. The policy shall apply to all visits by non-U.S. persons to Domestic Communications Infrastructure, except for Routine Business Visits, as defined in Section 3.3 below. NewComm shall consult with the DHS in the design and implementation of its visitation policy.

The visitation policy shall require that:

(a) The Security Officer shall review and approve or disapprove requests for visits to Domestic Communications Infrastructure (provided that, with respect to

carrier hotels and other shared facilities, this policy will apply solely to the portion of the facility controlled by NewComm) by non-U.S. persons, organizations or entities ("Visits"). The Security Officer shall approve or disapprove Visit requests on the basis of their consistency with the visitation policy. The Security Officer may specifically deny any Visit request on security or related grounds, which will be described more fully in the visitation policy.

(b) A written request for approval of a Visit must be submitted to the Security Officer no less than seven (7) days prior to the date of the proposed visit. If a written request cannot be provided seven (7) days before the proposed Visit because of an unforeseen exigency, the request may be communicated by telephone to the Security Officer and immediately confirmed in writing; however, the Security Officer may refuse to accept any request submitted less than seven (7) days prior to the date of a proposed Visit if the Security Officer determines there is insufficient time to consider the request.

(c) Each request shall set forth the exact purpose and justification for the Visit in sufficient detail to enable the Security Officer to make an informed decision concerning the appropriateness of the proposed Visit. The Security Officer may refuse to accept any request that he or she believes lacks sufficient information. Each proposed Visit and each individual visitor must be justified and a separate approval request must be submitted for each Visit, unless the Security Officer agrees to approve multiple Visits by the same person or persons for the same purpose, for a period not to exceed sixty (60) days.

(d) The Security Officer shall evaluate the request, as soon as practicable after receiving it. The Security Officer may approve or disapprove a request pending submittal of additional information by the requester. When practicable, the Security Officer's decision shall be communicated to the requester by any means at least one (1) day prior to the date of the proposed Visit, and, in all cases, the decision shall be confirmed in writing as promptly as possible.

(e) A record of all 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 NewComm personnel involved, shall be maintained by the Security Officer. In addition, a chronological file of all documentation associated with such Visits, together with records of approvals and disapprovals, shall be maintained for two (2) years by the Security Officer for provision at the request of the FBI, DOJ, or DHS.

(f) Visitors shall be escorted at all times by an employee, and within conditions, including appropriate restrictions on access, set forth by the Security Officer that are commensurate with the place and purpose of the Visit.

3.3 Routine Business Visits. Notwithstanding Section 3.2, Routine Business Visits, as defined below, 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 NewComm; (b) do not involve the transfer or receipt of any information regarding the security of such facilities; and (c) pertain only to the commercial aspects of NewComm's business. These may include:

(a) 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;

(b) 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

(c) Visits concerning fiscal, financial, or legal matters involving NewComm.

The visitation policy established under Section 3.2 may elaborate on the types of visits that qualify as Routine Business Visits.

3.4 Access by Foreign Government Authority. NewComm shall not, directly or indirectly, disclose or permit disclosure of, or provide access to Domestic Communications, Call Associated Data, Transactional Data, or Subscriber Information stored by or on behalf of NewComm 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, or 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 3.4 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. NewComm shall take reasonable measures to ensure that the Security Officer will promptly learn of all such requests or submission of legal process described in this Section 3.4.

3.5 Disclosure to Foreign Government Authorities. NewComm 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 a copy of any Wire Communication 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, and obtaining the express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States, provided that the provision of Controlled Unclassified Information shall be permitted in accordance with the terms of a license received under the ITAR or EAR, as applicable. Any requests or any legal process submitted by a foreign government, or an identified representative, a component or subdivision thereof, to NewComm for the communications, data or information identified in this Section 3.5 that is maintained by NewComm 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, 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. NewComm shall take reasonable measures to ensure that the Security Officer will promptly learn of all such requests or submission of legal process described in this Section 3.5.

3.6 Notification of Access or Disclosure Requests from Foreign Non-Governmental Entities. Within three (3) months after receiving legal process or requests from foreign non-governmental entities for access to or disclosure of Domestic Communications, NewComm shall notify the DOJ in writing of such legal process or requests, unless the disclosure of such legal process or requests would be in violation of an order of a court of competent jurisdiction within the United States.

3.7 Points of Contact. Within five (5) business days after execution of this Agreement, NewComm shall designate in writing to the FBI, DOJ, and DHS, one or more nominees already holding U.S. security clearances or which NewComm has a reasonable basis to believe is eligible to receive U.S. security clearances to serve as points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process on behalf of NewComm. NewComm shall provide in writing, in accordance with Section 5.15 of this Agreement, to the FBI, DOJ, and DHS the name and contact information for each point of contact. The points of contact shall be assigned to NewComm's 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. The points of contact shall undergo the screening process defined in Section 3.15 of this Agreement. If there is any change in the designated points of contact, NewComm shall notify the FBI, DOJ and DHS immediately in writing, providing updated identity and contact information. Persons serving as points of contact shall be resident U.S. citizens who hold or are eligible to receive U.S. security clearances (which may include interim clearances),

as outlined in Executive Order 12968. NewComm shall comply with any request by a Government Authority in the United States that a background check and/or security clearance process be completed for a designated point of contact.

3.8 Security of Lawful U.S. Process. NewComm shall protect the confidentiality and security of all Lawful U.S. Process served upon it 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 Controlled Unclassified Information, Lawful U.S. Process, Classified Information or Sensitive Information shall be under the custody and control of the Security Officer.

3.9 Information Security Plan. NewComm shall develop, document, implement, and maintain an information security plan to:

(a) 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;

(b) take appropriate measures to prevent unauthorized access to data or to the section(s), if any, of the facilities that might contain Classified, Sensitive, or Controlled Unclassified Information;

(c) assign U.S. citizens to positions for which screening is contemplated pursuant to Section 3.15;

(d) upon written request from the FBI, DOJ or DHS, 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 pursuant to Executive Order 12968;

(f) provide that the points of contact described in Section 3.7 shall have sufficient authority over any of NewComm's 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 authorities and the terms of this Agreement;

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

(h) establish a formal incident response capability with reference to OMB Circular A-130 and NIST Special Publications 800-3, 800-18 and 800-47; and

(i) identify the types of positions that require screening pursuant to Section 3.15, the required rigor of such screening by type of position, and the criteria by which NewComm will accept or reject screened persons ("Screened Personnel").

3.10 Security Officer Responsibilities and Duties. Immediately upon execution of this Agreement, NewComm shall designate, from among the points of contact selected pursuant to Section 3.7, a Security Officer within the United States with the primary responsibility for carrying out NewComm's obligations under Articles 2, 3 and 5 of this Agreement. The Security Officer shall stand in a direct reporting relationship with the Director of Network.

3.11 Qualifications and Responsibilities of Director of Network. Immediately upon execution of this Agreement, NewComm shall notify the FBI, DOJ, and DHS of the identity of the Director of Network. The Director of Network shall be subject to all of the requirements of the points of contact in Section 3.7, including the screening requirements of Section 3.15 of this Agreement. The Director of Network shall have direct management oversight of the Domestic Communications Infrastructure. If the holder of the position of Director of Network changes, NewComm shall notify the FBI, DOJ, and DHS immediately in writing, providing updated identity and contact information. In no event shall a vacancy for the position of Director of Network exist for a period of more than ninety (90) days before NewComm appoints a qualified candidate to fill such vacancy.

3.12 Nondisclosure of Protected Data. 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 third party, or officer, director, shareholder, employee, agent, or contractor of NewComm, Moviles, or TEM PR, 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, DOJ, and DHS, 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, provided that the disclosure of Controlled Unclassified Information not related to the subject matter of this Agreement need only be consistent with the ITAR or EAR, as applicable.

3.13 Notice of Obligations. NewComm shall instruct appropriate officials, employees, contractors, and agents as to NewComm's obligations under this Agreement, including the individuals' duty to report any violation of this Agreement and the reporting requirements in Sections 5.2, 5.6, and 5.9 of this Agreement, and shall issue periodic reminders to them of such obligations.

3.14 Access to Classified, Controlled Unclassified, or Sensitive Information. Nothing contained in this Agreement shall limit or affect the authority of a U.S. Government

Authority to deny, limit or revoke NewComm's access to Classified, Controlled Unclassified, and Sensitive Information under that Government Authority's jurisdiction.

3.15 Screening of Personnel. NewComm shall implement a thorough screening process through the Security Officer or a reputable third party to ensure that all personnel whose positions involve access to the Domestic Communications Infrastructure that enables those persons to monitor the content of Wire or Electronic Communications (including in electronic storage) or to have access to Network Management Information, Transactional Data, Call Associated Data, or Subscriber Information, persons who have access to Sensitive Information, and security personnel meet personnel screening requirements commensurate with the risk posed to national security by their access to facilities, equipment, or information subject to this Agreement.

(a) NewComm shall consult with the DOJ, FBI, and DHS on the screening procedures required under this Section. The DOJ, FBI, and DHS shall take into consideration NewComm's current and proposed screening procedures in its determination of such screening procedures, which shall be consistent with the guidance to U.S. government agencies under Executive Order 10450, and agrees to provide a list of positions subject to screening under this Section to the DOJ, FBI, and DHS. The parties shall categorize the positions according to the risk posed to national security by the level of access to facilities, equipment, and information subject to this Agreement and shall agree upon the level of screening necessary to satisfy this Section for each access level. Upon request, NewComm shall provide to the investigation services of the DOJ, FBI, and DHS, or, in the alternative, to the investigation service of the United States Office of Personnel Management ("OPM"), all the information it collects in its screening process of each candidate. Candidates for these positions shall be informed, and shall consent, that the information collected during the screening process may be provided to the U.S. government. Current and newly hired personnel subject to screening will be required to sign a non-disclosure agreement approved in advance by the DOJ, FBI, and DHS.

(b) If the DOJ, FBI, or DHS so desires, it may on its own, or through OPM's investigations service, conduct further background checks on screened personnel. NewComm will cooperate with any U.S. government agency undertaking any such further background checks.

(c) Individuals who are rejected by NewComm or by the DOJ, FBI, or DHS under the screening requirements of this Section 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. Any rejection by the DOJ, FBI, or DHS shall be provided in writing to NewComm within a reasonable time, no longer than thirty days after receipt of said rejection,

in accordance with Section 5.15. NewComm will notify the DOJ, FBI, and DHS of the transfer, departure, or job modification of any individual rejected as a result of the screening conducted pursuant to this Section within seven (7) days of such transfer or departure, and shall provide the DOJ, FBI, and DHS with the name, date of birth and social security number of such individual.

(d) NewComm 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 upon. NewComm shall monitor on a regular basis the status of screened personnel, and shall remove screened personnel who no longer meet the screened personnel requirements.

(e) NewComm shall maintain records relating to the status of screened personnel, and shall provide these records, upon request, to the DOJ, FBI, or DHS.

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 Maria Dolores Pizarro Figueroa of NewComm, the General Counsel of the FBI, the Deputy Attorney General of the DOJ, the General Counsel of the DHS, or their respective designees, unless the FBI, DOJ or DHS believes that important national interests can be protected, or NewComm believes that 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 Party believes that any other Party has breached or is about to breach this Agreement, that Party may bring an action against the other Party for appropriate judicial relief. Subject to Article 7 of this Agreement, nothing in this Agreement shall limit or affect the right of a U.S. government agency to:

(a) require that the Party or Parties believed to have breached, or about to breach, this Agreement cure such breach within thirty (30) days, or whatever shorter time period is appropriate under the circumstances, upon receiving written notice of such breach;

(b) request that the FCC modify, condition, revoke, cancel, or render null and void any license, permit, or other authorization granted or given by the FCC to NewComm, or request that the FCC impose any other appropriate sanction, including but not limited to a forfeiture or other monetary penalty, against NewComm;

(c) seek civil sanctions for any violation by NewComm or an Affiliate of any U.S. law or regulation or term of this Agreement;

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

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

4.3 Irreparable Injury. NewComm agrees that the United States would suffer irreparable injury if for any reason NewComm were to fail to perform any of its obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, NewComm agrees that, in seeking to enforce this Agreement, the FBI, DOJ, and DHS 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 become effective upon 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 NewComm. If NewComm makes any filing with the FCC or any other Government Authority relating to a change in the *de*

facto or *de jure* control of NewComm except for filings with the FCC for assignments or transfers of control that are *pro forma*, NewComm shall promptly provide to the FBI, DOJ and DHS written notice and copies of such filing. This Section 5.1 shall become effective upon execution of this Agreement by all the Parties.

5.2 Control of NewComm. If any member of the senior management of NewComm (including the Chief Executive Officer, President, General Counsel, Chief Technical Officer, Chief Financial Officer, Director of Network, or other senior officer) acquires any information that reasonably indicates that any single foreign entity or individual, other than Moviles, has or will likely obtain an ownership interest (direct or indirect) in NewComm above 10 percent, as determined in accordance with 47 C.F.R. § 63.09, or if any foreign entity or individual, singly or in combination with other foreign entities or individuals, has or will likely otherwise gain either (1) Control or (2) *de facto* or *de jure* control of NewComm, then such senior manager shall cause NewComm through its Security Officer to notify the FBI, DOJ and DHS in writing within ten (10) calendar days. Notice under this Section shall, at a minimum:

(a) Identify the entity or individual(s) (specifying the name, address(es) and telephone number(s) of the entity);

(b) Identify the beneficial owner(s) of the increased or prospective increased interest in NewComm by the entity or individual(s) (specifying the name, address(es) and telephone number(s) of each beneficial owner); and

(c) Quantify the amount of ownership interest in NewComm that the entity or individual(s) has or will likely obtain by increasing its ownership interest in or Control of NewComm.

5.3 Joint Ventures. NewComm may enter into joint ventures or other arrangements under which the joint venture or another entity may provide Domestic Communications.

(a) If NewComm has the power or authority to exercise *de facto* or *de jure* control over such entity, then NewComm will require the entity to fully comply with the terms of this Agreement.

(b) To the extent NewComm does not have *de facto* or *de jure* control over such joint venture or entity, NewComm shall in good faith notify such entity of this Agreement and its purposes, endeavor to have such entity fully comply with this Agreement, and consult with the FBI, DOJ, or DHS about the activities of such entity. Nothing in this Section 5.3 shall be construed to relieve NewComm of its obligations under Article 2 of this Agreement.

(c) If NewComm enters into a joint venture under which the joint venture or entity may provide Domestic Communications, or transmission, switching, bridging, or routing equipment (including software and upgrades), or facilities

used to provide, process, direct, control, supervise or manage Domestic Communications, NewComm must provide the DHS with notice no later than thirty (30) days before the joint venture offers Domestic Communications service, equipment or facilities. The DHS will have thirty (30) days from receipt of the notice to review and provide NewComm with any objection to the joint venture. Any objection shall be based on national security, law enforcement, or public safety grounds. If the DHS objects, the joint venture shall not offer Domestic Communications service, equipment or facilities.

5.4 Reserved

5.5 Outsourcing. If NewComm contracts for functions covered by this Agreement to a third party, NewComm shall take reasonable steps to ensure that the third party complies with the applicable terms of this Agreement with respect to functions covered by this Agreement. Such steps shall include, at a minimum:

(a) NewComm shall disclose this Agreement in its entirety and shall discuss with the third party those specific obligations of NewComm under the Agreement that relate to the contracted-for services;

(b) NewComm shall promptly thereafter provide a concise report, in writing, to the DHS, DOJ and FBI setting forth, as to each such specific obligation of NewComm under the Agreement, the commitments of the third party that will ensure NewComm's compliance with each of its obligations;

(c) NewComm shall notify the DHS no later than thirty (30) days before contracting out any function covered by this Agreement to a third party that is identified, after reasonable inquiry by NewComm, as either Controlled by one or more foreign persons or combination of foreign persons under common Control, or ten (10) percent or more of whose voting equity is held, directly or indirectly, by one or more foreign persons or combination of foreign persons under common Control, which notice shall identify the name of the entity, state the functions covered by this Agreement to be performed under the contract, and include the report required under Section 5.5(b) above. The DHS will have thirty (30) days from receipt of the notice to review and provide NewComm with any objection to the contract. Any objection shall be based on national security, law enforcement, or public safety grounds. If the DHS objects in accordance with this Section, NewComm shall not proceed with execution or performance of the contract;

(d) NewComm shall include, in all contracts to perform functions covered by this Agreement with third parties that are either Controlled by, or have ten (10) percent or more of their voting equity held, directly or indirectly, by one or more foreign persons or combination of foreign persons under common Control, written provisions requiring the following:

(i) The third party shall execute a nondisclosure agreement in a form approved by the DOJ, FBI and DHS which will include provisions barring disclosure of information obtained pursuant to the contract to any other person without the prior written permission of NewComm, and holding the third party liable for disclosure violations committed by any of its agents including directors, officers, employees, representatives or contractors;

(ii) To the extent that the third party or any employee or agent of such third party has security responsibilities, or has access to the Domestic Communications Infrastructure that enables those persons to monitor the content of Wire or Electronic Communications (including in electronic storage) or to obtain Network Management Information, such persons shall be subject to personnel screening, consistent with the level of screening required under Section 3.15 of this Agreement for NewComm personnel with similar access;

(iii) To the extent that the third party or any employee or agent of such third party has access to Transactional Data, Call Associated Data or Subscriber Information, such persons shall be specifically identified to NewComm, including each individual's name, date of birth, nationality, passport number (if applicable), and social security number (or equivalent), and NewComm shall retain the right to receive and review such identifying information, to provide it to the DOJ, FBI or DHS upon their written request, and to exclude individuals from having access to its Transactional Data, Call Associated Data or Subscriber Information;

(iv) Performance of the contract may not be assigned, delegated, or transferred to any other person or entity;

(v) Such contracts shall be subject to U.S. law and the third party shall consent to the jurisdiction of the U.S. federal courts in the District of Columbia for enforcement of the contract;

(e) if NewComm receives information that reasonably indicates that the third party or any employee or agent has taken an action that, had it been committed by NewComm, would violate an applicable provision of this Agreement, or has violated its obligations to NewComm related to this Agreement, NewComm will notify the DOJ, FBI and DHS promptly, and with consultation and, as appropriate, cooperation with the DOJ, FBI and DHS, NewComm will take reasonable steps necessary to rectify the situation promptly, which steps may include (among others) terminating the outsourcing arrangement with the third party, including after notice and opportunity for cure, or initiating and pursuing litigation or other remedies at law and equity;

provided, however, that NewComm shall not contract for functions covered by this Agreement to any entity where, as a result of such contract, the entity would gain access to Sensitive Information.

Peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree shall not constitute outsourced functions for purposes of this Section.

For preexisting contracts that were in force on January 13, 2004, NewComm shall use its commercially reasonable best efforts to obtain the third party's commitments to comply with all applicable undertakings set forth in this Section 5.5, and shall promptly thereafter provide to the DHS, DOJ and FBI the report required under Section 5.5(b) above. The applicable provisions of this Section 5.5 shall apply in full to proposed contracts that were not signed as of January 13, 2004, and also to preexisting contracts that are subject to termination, renewal, or renegotiation of material terms after January 13, 2004.

5.6 Notice of Foreign Influence. If any member of the NewComm Board of Directors or senior management of NewComm (including the Chief Executive Officer, President, General Counsel, Chief Technical Officer, Chief Financial Officer, Director of Network, 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 NewComm in such a way that interferes with or impedes NewComm's performance of its duties and obligations under the terms of this Agreement, interferes with or impedes NewComm's exercise of its rights under the Agreement, or foreseeably concerns NewComm's obligations under this Agreement; or

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

then such member shall promptly notify the Security Officer who, in turn, shall promptly notify the FBI, DOJ and DHS in writing of the timing and the nature of the foreign government's or entity's plans and actions.

5.7 Non-Retaliation. NewComm shall, by duly authorized action of its General Manager, ratified by its Board of Directors, adopt and distribute an official corporate policy that strictly prohibits NewComm 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, 5.6 or 5.9 of this Agreement, or has notified or attempted to notify directly the Security Officer to convey information that he or she believes in good faith would be required to be reported to the FBI, DOJ, and DHS by the Security Officer under Sections 5.2, 5.6, or 5.9 of this Agreement. Such corporate policy shall set forth in a clear and prominent manner the contact information for the Security Officer 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 NewComm of any material term of such corporate policy shall constitute a breach of this Agreement.

5.8 Security Audit. NewComm shall conduct audits on an annual basis to assess its compliance with the terms of this Agreement, and shall furnish to the DOJ, FBI, and DHS a report in accordance with Section 5.12. NewComm shall provide DOJ, FBI, and DHS with a description of the scope and purpose of the audits at least three (3) months in advance of commencing an audit, and DOJ, FBI, and DHS shall have the right to review and approve the terms defining the scope and purpose of the audits. NewComm shall ensure that the auditor has full and unimpeded corporate authority to conduct the audits without restriction or limitation by any officer, director, employee, contractor or agent of NewComm. The terms defining the scope and purposes of the audits shall include, at a minimum, authority for the auditor (a) to review and analyze NewComm policies and procedures designed to implement this Agreement, all relevant information related to the configuration of the NewComm network, all minutes of meetings held or actions taken by the NewComm Board of Directors or Committees of the Board in accordance with this Agreement, all Security Officer logs and records including records related to facility visits, personnel screening data, and any reports submitted in accordance with Section 5.9 of this Agreement; and (b) to conduct a reasonable number of unannounced inspections of NewComm facilities each year, a reasonable volume of random testing of network firewalls, access points and other systems for potential vulnerabilities, and a reasonable number of confidential interviews of NewComm officers, directors, employees, contractors or agents concerning compliance with this Agreement. Upon request, NewComm shall provide the DOJ, FBI, or DHS with access to facilities, information, and personnel consistent with Sections 5.10 and 5.11 below in the event that the DOJ, FBI, or DHS wishes to conduct its own annual audit of NewComm's compliance with this Agreement.

5.9 Reporting of Incidents. NewComm shall report to the FBI, DOJ and DHS any information acquired by NewComm, or by any NewComm officer, director, employee, contractor or agent, that reasonably indicates:

(a) a violation of this Agreement;

(b) access to or disclosure of Domestic Communications, or the conduct of Electronic Surveillance, in violation of Federal, state or local law or regulation;

(c) access to or disclosure of 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, Sensitive, or Controlled Unclassified Information.

This report shall be made in writing by the Security Officer to the DOJ, FBI and DHS no later than ten (10) calendar days after NewComm acquires information that reasonably indicates a matter described in this Section 5.9. NewComm shall lawfully cooperate in investigating the matters described in this Section. NewComm 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.

5.10 Access to Information and Facilities. The FBI, DOJ and DHS may visit any part of NewComm's Domestic Communications Infrastructure and security offices to conduct on-site reviews concerning the implementation of the terms of this Agreement and may at any time require unimpeded access to information concerning technical, physical, management, or other security measures needed by the DOJ, FBI or DHS to verify compliance with the terms of this Agreement.

5.11 Access to Personnel. Upon reasonable notice from the FBI, the DOJ, or DHS, NewComm shall make available for interview any officers or employees of NewComm, 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 terms of this Agreement; provided that the Parties shall, in good faith, take into consideration the actual availability of the necessary individuals.

5.12 Annual Report. On or before the last business day of January of each year after the Effective Date, the Chief Executive Officer or a designated senior corporate officer of NewComm shall submit to the FBI, DOJ and DHS a report assessing NewComm's compliance with the terms of this Agreement for the preceding calendar year. The report shall include:

(a) a copy of all security audit reports compiled following an audit conducted pursuant to Section 5.8;

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

(c) a summary of the changes, if any, to the policies or procedures, and the reasons for those changes;

(d) a summary of any known acts of noncompliance with the terms of this Agreement, whether inadvertent or intentional, with a discussion of what steps have been or will be taken to prevent such acts from occurring in the future; and

(e) identification of any other issues that will or could affect the effectiveness of or compliance with this Agreement.

NewComm shall make available to the Security Officer in a timely fashion all information necessary to prepare the report required by this Section.

5.13 Information and Reports Concerning Network Architecture. If requested by the DOJ, FBI, or DHS, NewComm shall provide to the DOJ, FBI, and DHS, the following information regarding the interconnections and control of the Domestic Communications Infrastructure:

(a) A description of the plans, processes and/or procedures, relating to network management operations, that prevent the Domestic Communications Infrastructure from being accessed or controlled from outside the United States.

(b) A description of the placement of the Network Operations Center and interconnection (for service offload or administrative activities) to other domestic and international carriers, ISPs and critical U.S. financial, energy, and transportation infrastructures.

(c) A description of NewComm's networks and operations processes, procedures for management control and relation to the backbone infrastructures of other service providers.

(d) A description of any unique or proprietary control mechanisms of NewComm as well as of NewComm's operating and administrative software.

(e) A report of Network Management Information that includes an assurance that network performance satisfies FCC rules and reporting requirements.

Once a report has been made under this Section 5.13, NewComm shall promptly report any material changes, upgrades and/or modifications to the items described in (a) - (e) above, including the installation of critical equipment and software. For the purposes of this Section, critical equipment and software shall include: routers, switches, gateways, network security appliances, network management/test equipment, operating systems and network and security software (including new versions, patches, upgrades, and replacement software), and other hardware, software, or systems performing similar functions. Monitors, desktop computers, desktop computer applications, disk drives, power supplies, printers, racks and the like are not "critical equipment or software" unless they perform functions similar to those of the items described in (a) - (e) above. Similarly, "material" shall refer to those changes, modifications and upgrades that alter

network operating characteristics or architecture--it does not apply to spare parts replacement, the one-for-one swapping of identical equipment or the related re-loading of system software or backups; provided, however, that network security configuration and capabilities remain unchanged.

5.14 Compliance Assurance. Moviles and TEM PR will take all steps necessary to ensure that NewComm complies with the terms of this Agreement.

5.15 Notices. Effective upon execution of this Agreement by all the Parties, all notices and other communications relating to this Agreement, such as a proposed modification, shall be in writing and shall be deemed given as of the date of receipt and shall be: (a) delivered personally; or (b) sent by facsimile; or (except as noted below) (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 5.15.

NewComm Wireless Services, Inc.
Valencia Park
Edificio 17 Calle Numero 2
Suite 600
Guaynabo, Puerto Rico 00968
Telephone: 787.749.5800
Fax: 787.749.5880

Telefonica Moviles, S.A.
Juan Ramon Balcells Olivero
Goya #24
28001 Madrid, Spain
Telephone: 34 91 423 3910
Fax: 34 91 423 4294

TEM Puerto Rico, Inc.
Maria Dolores Pizarro Figueroa
Valencia Park
Edificio 17 Calle Numero 2
Suite 600
Guaynabo, Puerto Rico 00968
Telephone: 787.273.5629
Fax: 787.749.5880

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

Department of Homeland Security
Washington, DC 20528
Attn: Assistant Secretary for Infrastructure Protection

With a copy to:

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

ARTICLE 6: FREEDOM OF INFORMATION ACT

6.1 Protection from Disclosure. The DOJ, FBI and DHS shall take all reasonable measures to protect from public disclosure all information submitted by NewComm to the FBI, DOJ and DHS in connection with this Agreement and clearly marked with the legend "Confidential; Subject to Protection Under 5 U.S.C. Section 553(b); Not to be Released Without Notice to NewComm" or similar designation. Such markings shall signify that it is NewComm'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 FBI, DOJ or DHS, as appropriate, shall notify NewComm of the intended disclosure as provided by Executive Order 12600, 52 Fed. Reg. 23781 (1987). If NewComm objects to the intended disclosure and its objections are not sustained, the FBI, DOJ or DHS, as appropriate, shall notify NewComm of its intention to release (as provided by Section 5 of Executive Order 12600) not later than five (5) 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, DOJ, or DHS from lawfully disseminating information as appropriate to seek enforcement of this Agreement, or from lawfully sharing information as appropriate with other Government Authorities to protect public safety, law enforcement, or national security interests, provided that the FBI, DOJ and DHS take all reasonable measures to protect from public disclosure the information marked as described in Section 6.1.

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 Exhibit A attached hereto (the "Condition to FCC Authorization"), the FBI, DOJ and DHS have no objection to the grant of NewComm's Petition for Declaratory Ruling and the Applications filed with the FCC in WT Docket No. 02-366. This Section 7.1 is effective upon execution of this Agreement by all the Parties.

7.2 CFIUS Process. Provided that the FCC adopts the Condition to the FCC Authorization, the Attorney General or the Secretary of Homeland Security shall not object to or oppose the TEM PR Transaction within the process conducted by the Committee on Foreign Investment in the United Status ("CFIUS") or in any other forum or process examining the national security effects of the TEM PR Transaction. This commitment, however, does not extend to any objection the Attorney General or the Secretary of Homeland Security may wish to raise with CFIUS or the President in the event that (a) NewComm fails to comply with the terms of this Agreement; (b) the representations of NewComm made to the DOJ, FBI, DHS, or FCC above are materially untrue or incomplete; (c) there is a material increase in the authority of a foreign entity to exercise Control of NewComm; or (d) there is any other material change in the circumstances associated with the transaction at issue. The DOJ, FBI or DHS shall not register an objection or challenge or otherwise prevent or impede CFIUS's approval before the date the FCC adopts the Condition to the FCC Authorization, unless (a), (b), (c) or (d) occurs. This Section 7.2 shall become effective upon execution of this Agreement by all the Parties.

7.3 Future Applications. NewComm, Moviles, and TEM PR agree that in any application or petition by any of them or their Affiliates 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, such Party or its Affiliate shall request that the FCC condition the grant of such licensing or other authority on compliance with the terms of this Agreement. Notwithstanding Section 8.9, the FBI, DOJ and DHS reserve the right to object, formally or informally, to the grant of any FCC application or petition of such Party or its Affiliate for a license or other authorization under 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.

ARTICLE 8: OTHER

8.1 Right to Make and Perform Agreement. NewComm 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 NewComm enforceable in accordance with its terms.

8.2 Headings. The headings, including article and section headings, and numbering in this Agreement are inserted for convenience only and shall not affect the meaning or interpretation of the terms of this Agreement.

8.3 Other Laws. Nothing in this Agreement is intended to limit or constitute a waiver of (a) any obligation imposed by any U.S., state or local laws on NewComm; (b) any enforcement authority available under any U.S. or state laws; (c) the sovereign immunity of the United States; or (d) any authority over NewComm's activities or facilities located within or outside the United States that the U.S. Government may possess (including without limitation authority pursuant to the International Emergency Economic Powers Act). Nothing in this Agreement is intended to cause or is to be interpreted to require the Parties to violate any applicable U.S. law.

8.4 Statutory References. All references in this Agreement to statutory provisions shall include any future amendments to such statutory provisions.

8.5 Non-Parties. Nothing in this Agreement is intended to confer or does confer any rights on any person other than the Parties and any Government Authorities in the United States entitled to effect Electronic Surveillance pursuant to Lawful U.S. Process.

8.6 Modifications. This Agreement may be modified only by written agreement signed by all of the Parties. The DOJ, FBI, and DHS agree to consider promptly and in good faith possible modifications to this Agreement if NewComm believes that the obligations imposed on it under this Agreement are substantially more restrictive than those imposed on other U.S. or 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 Severability. The provisions of this Agreement shall be severable and if any provision thereof or the application of such provision under any circumstances is held invalid by a court of competent jurisdiction, it shall not affect any other provision of this Agreement or the application of any provision thereof.

8.8 Changes in Circumstances for NewComm. The DOJ, FBI, and DHS agree to negotiate in good faith and promptly with respect to any request by NewComm for relief from application of specific provisions of this Agreement to future NewComm activities or services if those provisions become unduly burdensome or adversely affect NewComm's competitive position.

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

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

8.11 Successors and Assigns. This Agreement shall inure to the benefit of, and shall be binding upon, the Parties, and their respective successors and assigns. This Agreement shall also be binding on all subsidiaries, divisions, departments, branches, and other components or agents of NewComm, and on all Affiliates of NewComm.

8.12 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.

8.13 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.

8.14 Suspension of Agreement / Foreign Ownership.

(a) This Agreement shall be suspended in its entirety with respect to Moviles or TEM PR and any subsidiaries, divisions, departments, branches, and other components or agents or Affiliates of Moviles or TEM PR thirty (30) days after receipt from NewComm of notice and documentation reasonably satisfactory to the FBI, DOJ and DHS that neither TEM PR nor Moviles nor any subsidiaries, divisions, departments, branches, and other components or agents or Affiliates of Moviles or TEM PR either Controls NewComm or holds, directly or indirectly, a ten (10) percent or greater interest in NewComm. Said suspension shall remain in place unless and until Moviles or TEM PR and any subsidiaries, divisions, departments, branches, and other components or agents or Affiliates of Moviles or TEM PR either Controls or holds, directly or indirectly, a ten (10) percent or greater interest in NewComm.

(b) This Agreement shall be suspended in its entirety with respect to NewComm and any subsidiaries, divisions, departments, branches, and other components or agents or Affiliates of NewComm thirty (30) days after receipt from NewComm of notice and documentation reasonably satisfactory to the FBI, DOJ and DHS that no foreign entity or combination of foreign entities (including one or more foreign persons under common Control) either Controls NewComm or holds, directly or indirectly, a ten (10) percent or greater interest in NewComm. Said suspension shall remain in place with respect to NewComm and any subsidiaries, divisions, departments, branches, and other components or agents or Affiliates of NewComm unless and until a foreign entity or combination of foreign entities (including one or more foreign persons under common Control) either Controls NewComm or holds, directly or indirectly, a ten (10) percent or greater interest in NewComm.

(c) This Agreement shall remain in effect with respect to NewComm for so long as (and the obligations of NewComm shall not be suspended and any suspension of the obligations of NewComm shall terminate if) either TEM PR or any foreign entity (including one or more foreign persons under common Control) shall Control NewComm or any transferee or assignee of the FCC licenses or authorizations held by NewComm, or hold, directly or indirectly, a ten (10) percent or greater interest in NewComm or any transferee or assignee of the FCC licenses or authorizations held by NewComm.

(d) Notwithstanding the foregoing or Section 7.3 of this Agreement, the acquisition of Control of NewComm, or any transferee or assignee of the FCC licenses or authorizations held by NewComm, by a U.S. entity in which a foreign entity (including one or more foreign persons under common Control) holds, directly or indirectly, a ten (10) percent or greater minority ownership interest (but does not Control the U.S. entity) shall not continue or revive provisions of this Agreement, provided that such U.S. entity is already subject to a Network Security Agreement, and provided further that NewComm and the acquirer will modify such Network Security Agreement if the DOJ, FBI or DHS finds that its terms are inadequate to address national security, law enforcement, or public safety concerns arising from the acquisition. For purposes of this provision, Network Security Agreement means an agreement (other than a letter agreement) entered into between a provider of Domestic Communications and the DOJ and/or FBI which is expressly intended to address national security, law enforcement and public safety concerns arising from foreign investment in such Domestic Communications provider.

This Agreement is executed on behalf of the Parties:

NewComm Wireless Services, Inc.

Date: April 29, 2004

By: _____
Printed Name: Javier O. Lamoso
Title: Chairman and Chief Executive Officer

TEM Puerto Rico, Inc.

Date: _____

By: _____
Printed Name:
Title:

Telefonica Moviles, S.A.

Date: _____

By: _____
Printed Name:
Title:

Federal Bureau of Investigation

Date: _____

By: _____
Printed Name: Patrick W. Kelley
Title: Deputy General Counsel

United States Department of Justice

Date: _____

By: _____
Printed Name:
Title:

United States Department of Homeland Security

Date: _____

By: _____
Printed Name: Robert P. Liscouski
Title: Assistant Secretary, Infrastructure Protection

This Agreement is executed on behalf of the Parties:

NewComm Wireless Services, Inc.

Date:_____

By:_____
Printed Name:
Title: Chairman and Chief Executive Officer

TEM Puerto Rico, Inc.

Date: April 29, 2004

By:_____
Printed Name: Makia D. Pizarro-Figueroa
Title: General counsel

Telefonica Moviles, S.A.

Date:_____

By:_____
Printed Name:
Title:

Federal Bureau of Investigation

Date:_____

By:_____
Printed Name: Patrick W. Kelley
Title: Deputy General Counsel

United States Department of Justice

Date:_____

By:_____
Printed Name:
Title:

United States Department of Homeland Security

Date:_____

By:_____
Printed Name: Robert P. Liscouski
Title: Assistant Secretary, Infrastructure Protection

This Agreement is executed on behalf of the Parties:

NewComm Wireless Services, Inc.

Date:_____

By:_____
Printed Name:
Title: Chairman and Chief Executive Officer

TEM Puerto Rico, Inc.

Date:_____

By:_____
Printed Name:
Title:

Telefonica Moviles, S.A.

Date: April 29, 2004

By:_____
Printed Name: Antonio Hornedo Muguiro
Title: General Counsel

Date: April 29, 2004

And By:_____
Printed Name: Ernesto Lopez Mozo
Title: Chief Executive Officer

Federal Bureau of Investigation

Date:_____

By:_____
Printed Name: Patrick W. Kelley
Title: Deputy General Counsel

United States Department of Justice

Date:_____

By:_____
Printed Name:
Title:

United States Department of Homeland Security

Date:_____

By:_____
Printed Name: Robert P. Liscouski
Title: Assistant Secretary, Infrastructure Protection

This Agreement is executed on behalf of the Parties:

NewComm Wireless Services, Inc.

Date:_____

By:_____
Printed Name:
Title: Chairman and Chief Executive Officer

TEM Puerto Rico, Inc.

Date:_____

By:_____
Printed Name:
Title:

Telefonica Moviles, S.A.

Date:_____

By:_____
Printed Name:
Title:

Federal Bureau of Investigation

Date: 05/14/2004

By: Patrick W. Kelley
Printed Name: Patrick W. Kelley
Title: Deputy General Counsel

United States Department of Justice

Date:_____

By:_____
Printed Name:
Title:

United States Department of Homeland Security

Date:_____

By:_____
Printed Name: Robert P. Liscouski
Title: Assistant Secretary, Infrastructure Protection

This Agreement is executed on behalf of the Parties:

NewComm Wireless Services, Inc.

Date:_____ By:_____
Printed Name:
Title: Chairman and Chief Executive Officer

TEM Puerto Rico, Inc.

Date:_____ By:_____
Printed Name:
Title:

Telefonica Moviles, S.A.

Date:_____ By:_____
Printed Name:
Title:

Federal Bureau of Investigation

Date:_____ By:_____
Printed Name: Patrick W. Kelley
Title: Deputy General Counsel

United States Department of Justice

Date: 5/11/04 By: Laura H. Parsky
Printed Name: Laura H. Parsky
Title: Deputy Assistant Attorney General

United States Department of Homeland Security

Date:_____ By:_____
Printed Name: Robert P. Liscouski
Title: Assistant Secretary, Infrastructure Protection

This Agreement is executed on behalf of the Parties:

NewComm Wireless Services, Inc.

Date:_____

By:_____
Printed Name:
Title: Chairman and Chief Executive Officer

TEM Puerto Rico, Inc.

Date:_____

By:_____
Printed Name:
Title:

Telefonica Moviles, S.A.

Date:_____

By:_____
Printed Name:
Title:

Federal Bureau of Investigation

Date:_____

By:_____
Printed Name: Patrick W. Kelley
Title: Deputy General Counsel

United States Department of Justice

Date:_____

By:_____
Printed Name:
Title:

United States Department of Homeland Security

Date: 5/11/04

By: Lina W. Gabbrielli
Printed Name: Robert P. Liscouski
Title: Assistant Secretary, Infrastructure Protection

EXHIBIT A
CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that the authorizations and the licenses related thereto are subject to compliance with the provisions of the Agreement attached hereto between Telefonica Moviles, S.A., TEM Puerto Rico, Inc., and NewComm Wireless Services, Inc. on the one hand, and the FBI, DOJ and DHS, on the other, dated May 14, 2004, which Agreement is designed to address national security, law enforcement, and public safety concerns of the FBI, DOJ and DHS regarding the authority and licenses 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.