AGREEMENT

This AGREEMENT is made as of the date of the last signature affixed hereto by and between The Micronesian Telecommunications Corporation ("MTC") and Pacific Telecom, Inc. ("PTI"), on the one hand, and the Federal Bureau of Investigation ("FBI"), the U.S. Department of Justice ("DOJ"), the U.S. Department of Defense ("DOD"), and the U.S. Department of Homeland Security ("DHS"), on the other (referred to individually as a "Party" and collectively as the "Parties").

RECITALS

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

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

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

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

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

WHEREAS, MTC is the incumbent local exchange carrier in the Commonwealth of the Northern Mariana Islands ("CNMI"), and provides or will provide the following services in its own name or through its sole subsidiary, GTE Pacifica, Inc ("GTEP"), a CNMI corporation (and thereby either under GTEP's own name, GTEP's current trade name, Verizon Pacifica, or a successor trade name): (1) Internet access services, including dedicated access services and DSL services; (2) private data networking services, including dedicated transmission capacity, virtual private network services, and Ethernet services; (3) hosting services, including web hosting, server collocation, and application hosting; (4) local and both domestic and international long distance voice services; (5) interactive voice response systems; (6) integrated voice and data services; (7) cellular telephone and satellite uplink and downlink services; and (8) any other telecommunications service that MTC may offer in the future;

WHEREAS, MTC (or its affiliated entities) provides or facilitates electronic communication services, remote computing services, and interactive computing services in the

United States, and certain of its customers (including, inter alia, Internet-related companies) are themselves providers of electronic communication services, remote computing services, and interactive computer services, all of which are subject to U.S. privacy and electronic surveillance laws;

WHEREAS, MTC is the subject of the Purchase and Sale Agreement between Bell Atlantic New Zealand Holdings, Inc. and Citadel Holdings, Inc. and Tan Holdings Corporation dated as of November 23, 2001 ("PSA") and Amendment No. 1 to the PSA, which assigns and transfers all of Tan Holdings Corporation's right, title and interest in, to and under the PSA to Prospector Investment Holdings, Inc. as of February 27, 2003 (the "Purchase and Sale Agreement"), under the terms of which PTI will acquire all of the outstanding shares of MTC;

WHEREAS, MTC has filed with the Federal Communications Commission ("FCC") applications (in FCC IB Docket No. 03-115) under Sections 214 and 310(d) of the Communications Act of 1934, as amended (the " Communications Act"), 47 U.S.C. §§ 214 and 310(d), and the Act Relating to the Landing and Operation of Submarine Cables in the United States, as amended (the "Cable Landing License Act"), 47 U.S.C. §§ 34-39, seeking FCC approval of the transfer of control of MTC's FCC authorizations and licenses, upon consummation of the transactions contemplated by and pursuant to the terms of the Purchase and Sale Agreement, to PTI, and in connection therewith, MTC also has filed with the FCC a petition pursuant to Section 310(b)(4) of the Communications Act, for a declaratory ruling that the proposed foreign ownership by PTI is in the public interest;

WHEREAS, as disclosed to the FCC, PTI is a privately held corporation, organized and existing under the laws of the CNMI, that is a wholly-owned subsidiary of Prospector Investment Holdings, Inc. ("Prospector"), a Cayman Islands corporation, and Prospector is in turn indirectly affiliated through common ultimate ownership by Philippine citizens with Citadel Holdings, Inc., a diversified company organized under the laws of the Philippines;

WHEREAS, the FCC's grant of the applications in FCC IB Docket No. 03-115 may be made subject to conditions relating to national security, law enforcement, and public safety, and whereas MTC and PTI each have entered into this Agreement with the FBI, the DOJ, the DOD and the DHS to address issues raised by those departments and agencies, and to request that the FCC condition the transfer of control approved by the FCC on their compliance with this Agreement;

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

WHEREAS, MTC and PTI will submit a voluntary notice to CFIUS regarding PTI's proposed acquisition of MTC, and MTC and PTI have entered into this Agreement to resolve any national security issues that the DOJ, the FBI, the DOD and the DHS might raise, including in the CFIUS review process;

WHEREAS, representatives of MTC and PTI have met with representatives of the FBI, the DOJ, the DOD and the DHS to discuss issues raised by those departments and agencies. In these meetings, MTC and PTI represented that: (a) they have no present plans, and are not aware of present plans of any other entity, that would result in a Domestic Communications Company providing Domestic Communications or Hosting Services through facilities located outside the United States, and (b) none of PTI, Prospector or Citadel Holdings, Inc., are owned or controlled by any government; and

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

ARTICLE 1: DEFINITION OF TERMS

As used in this Agreement:

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

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

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

(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 nonfulfillment 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; or

(vi) MTC's obligations under this Agreement.

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

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

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

1.7. "DHS" means the U.S. Department of Homeland Security.

1.8. "DOD" means the U.S. Department of Defense.

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

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 Company" means all those subsidiaries, divisions, departments, branches and other components of MTC, and any other entity over which MTC 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 storage in connection with Hosting Services. If any subsidiary, division, department, branch or other component of MTC, or any other entity over which MTC has *de facto* or *de jure* control, provides Domestic Communications or engages in Hosting Services after the date that all the Parties execute this Agreement, then such entity shall be deemed to be a Domestic Communications Company. If any Domestic Communications Company enters into joint ventures under which a joint venture or another entity may provide Domestic Communications or engage in Hosting Services, and if a Domestic Communications Company has the power or authority to exercise *de facto* or *de jure* control over such entity, then MTC will ensure that that entity shall fully comply with the terms of this Agreement. The term "Domestic Communications Company" shall not include acquisitions by MTC in the U.S. after the date this Agreement is executed by all parties only if the DOJ or the FBI find that the terms of this Agreement are inadequate to address national security, law enforcement or public safety concerns presented by that acquisition and the necessary modifications to this Agreement cannot be reached pursuant to Section 8.7 below. Nothing in this definition shall exempt any Domestic Communications Company from its obligations under Section 5.3.

1.12. "Domestic Communications Infrastructure" means (a) transmission, switching, bridging and routing equipment (including software and upgrades) subject to control by a Domestic Communications Company and in use to provide, process, direct, control, supervise or manage Domestic Communications, and (b) facilities and equipment in use by or on behalf of a Domestic Communications Company that are physically located in the United States; or (c) facilities in use by or on behalf of a Domestic Communications Company to control the equipment described in (a) and (b) above. Domestic Communications Infrastructure does not include equipment or facilities used by service providers that are not Domestic Communications Companies and that are:

(i) interconnecting communications providers; or

(ii) providers of services or content that are

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

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

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.

1.13. "Effective Date" means the date on which the transactions contemplated by the Purchase and Sale Agreement are consummated.

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

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

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

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

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

1.19. "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 MTC or any of its subsidiaries, affiliates, divisions, departments, branches or other components.

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 Electronic Surveillance or other court orders, processes, or authorizations issued under U.S. Federal, state, or local law for physical search or seizure, production of tangible things, or access to or disclosure of Domestic Communications, Call Associated Data, or U.S. Hosting Data, including Transactional Data or Subscriber Information.

1.22. "MTC" means Micronesian Telecommunications Corporation.

1.23. "MTC Board" means the board of directors of MTC.

1.24. "Network Management Information" means network management operations plans, processes and procedures; the placement of Network Operating Center(s) and linkages (for service off load or administrative activities) to other domestic and international carriers, ISPs and other critical infrastructures; descriptions of IP 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.

1.25. "OPM" means the Office of Personnel Management of the U.S. Government.

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

1.27. "*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.

1.28. "PTI" means Pacific Telecom, Inc.

1.29. "Purchase and Sale Agreement" has the meaning given in the Recitals.

1.30. "Security Committee" means a committee of the MTC Board the mandate of which is to oversee security matters and implementation of this Agreement within MTC.

1.31. "Security Director" has the meaning given in Section 3.15.

1.32. "Security Officer" has the meaning given in Sections 3.10 and 3.13.

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

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

1.35. "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 a Domestic Communications Company relating specifically to the identity and physical address of a customer or subscriber, or account payer, or the end-user of such customer or subscriber, or account payer, or associated with such person relating to all telephone numbers, domain names, IP addresses, Uniform Resource Locators ("URLs"), other identifying designators, types of services, length of service, fees, usage including billing records and connection logs, and the physical location of equipment, if known and if different from the location information provided under (iii) below;

(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, including electronic mail headers showing From: and To: addresses; and

(iv) as to any mode of transmission (including mobile transmissions), and to the extent permitted by U.S. laws, any information indicating as closely as possible the

physical location to or from which a Domestic Communication, or other Wire or Electronic Communication within the definition of U.S. Hosting Data, is transmitted.

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

1.36. "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 the Northern Mariana Islands.

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

1.38. "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.

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

1.40. 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, DOD, and DHS in writing:

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

(ii) all Domestic Communications that are carried by or through, in whole or in part, the Domestic Communications Infrastructure shall pass through a facility under

the control of a Domestic Communications Company and physically located in the United States, from which Electronic Surveillance can be conducted pursuant to Lawful U.S. Process. The Domestic Communications Company will provide technical or other assistance to facilitate such Electronic Surveillance.

(iii) foreign connections to the domestic MTC network shall be on a gateway basis using industry best practices (i.e., both signaling and traffic shall be monitored for unauthorized access, network intrusions and other malicious activity). Such practices will be jointly determined by MTC and the FBI, DOJ, DOD and DHS.

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

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

2.3. Compliance with Lawful U.S. Process. Domestic Communications Companies shall take all practicable steps to configure their Domestic Communications Infrastructure and Data Centers (except for equipment that is owned or controlled by a U.S. Hosting Services Customer and is collocated in MTC-controlled space in a Data Center) to be capable of complying, and Domestic Communications Company employees in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with:

(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. Information Storage and Access. Domestic Communications Companies shall store exclusively in the United States the following:

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

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

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

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

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

(vi) Network Management Information.

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

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

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

2.8. Compliance with U.S. Law. Nothing in this Agreement shall excuse a Domestic Communications Company from any obligation it may have to comply with U.S. legal requirements for the retention, preservation, or production of such information or data.

Similarly, in any action to enforce Lawful U.S. Process, Domestic Communication Companies have not waived any legal right they might have to resist such process.

2.9. Routing of Domestic Communications and U.S. Hosting Data. 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 that are implemented pursuant to policies reviewed and approved by the third-party auditor selected pursuant to Section 5.8 of this Agreement, and (iv) as otherwise may be agreed in writing by the DOJ, the FBI, DOD and the DHS, Domestic Communications Companies shall not route Domestic Communications or U.S. Hosting Data outside the United States.

2.10. Interconnection arrangements with PTI, Prospector Investment Holdings and Subsidiaries. Interconnection arrangements between Domestic Communications Companies, on the one hand, and PTI, Prospector and Subsidiaries, on the other hand, shall be on an arm's length basis.

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

2.12. Storage of Protected Information. The storage of Classified, Controlled Unclassified, and Sensitive Information by a Domestic Communications Company or its contractors at any location outside of the United States is prohibited, unless the storage is at a U.S. military facility, a U.S. Embassy or Consulate or other location occupied by a U.S. government organization.

2.13. Network Topography. No later that 30 days after the Effective Date of this Agreement, MTC will provide to the FBI, DOJ, DHS and DOD a comprehensive description of the MTC domestic telecommunications network to include location of servers, routers, switches, operational systems software, and network security appliances and software.

ARTICLE 3: SECURITY

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

3.2. Visitation Policy. No later than ninety (90) days after the Effective Date, MTC shall adopt and implement a visitation policy for Domestic Communications Companies, for all visits to Domestic Communications Infrastructure. MTC will consult with DOJ, DHS and DOD on the design and implementation of its visitation policy. 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. The visitation policy shall require that:

(i) 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 MTC) by all non-U.S. persons, organizations and entities. The Security Officer shall approve or deny visit requests on the basis of their compliance with the visitation policy; the Security Officer may specifically deny any visit request on security or related grounds, which grounds will be described more fully in the visitation policy.

(ii) 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 within seven (7) days of the proposed visit because of an unforeseen exigency, the request may be communicated via 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 such proposed visit if the Security Officer determines that there is insufficient time to consider the request.

(iii) the exact purpose and justification for the visit must be set forth in detail sufficient to enable the Security Officer to make an informed decision concerning the appropriateness of the proposed visit, and 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.

(iv) the Security Officer evaluate the request as soon as practicable after receiving it. The Security Officer may approve or disapprove the 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.

(v) 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 MTC personnel involved, 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 third party auditor identified pursuant to Section 5.8 below, or the DOJ, FBI, DOD or DHS.

(vi) visitors 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.

The parties may agree in the visitation policy that certain visits of a routine and nonsensitive nature are exempt from one or more of the requirements above.

3.3. Records of Communications with Non-U.S. Citizens and Non-U.S. Entities. MTC shall maintain a full and complete record of every electronic or written communication by MTC directors, officers, employees and agents, with PTI directors, officers, employees and agents (including the names, business affiliations, and substance of the communications) that are related to interconnection agreements, Security Procedures and Policy, as well as major equipment purchases outlined in section 3.17, and Joint Venture provisions outlined in section 5.3, relating to Domestic Communications Companies. These records shall be maintained for a period of five (5) years by the Security Officer for provision at the request of the third party auditor identified pursuant to Section 5.8 below, or of the DOD, DOJ, FBI or DHS.

3.4. Access by Foreign Government Authority. Domestic Communications Companies shall not, directly or indirectly, disclose or permit disclosure of, or provide access to Domestic Communications, U.S. Hosting Data, Call Associated Data, Transactional Data, or Subscriber Information stored by Domestic Communications Companies to any person if the purpose of such access is to respond to the legal process or the request of or on behalf of a foreign government, identified representative, component or subdivision thereof without the express written consent of the DOJ or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process described in this Section 3.4 of this Agreement shall be reported to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received by and known to the Security Officer. Domestic Communications Companies 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 of this Agreement.

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

(i) Classified, Sensitive, or Controlled Unclassified 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 DOJ or the authorization of a court of competent jurisdiction in the United States. Any requests or any legal process submitted by a foreign government, an identified representative, a component or subdivision thereof to Domestic Communications Companies for the communications, data or information identified in this Section 3.5 of this Agreement that is maintained by Domestic Communications Companies shall be referred to the DOJ as soon as possible and in no event later than five (5) business days after such request or legal process is received by and known to the Security Officer unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. Domestic Communications Companies shall take reasonable measures to ensure that the Security Officer 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 ninety (90) days of receipt, Domestic Communications Companies shall notify DOJ in writing of legal process or requests by foreign nongovernmental entities to Domestic Communications Companies for access to or disclosure of (i) U.S. Hosting Data, or (ii) Domestic Communications carried by or through, in whole or in part, the Domestic Communications Infrastructure, unless the disclosure of the legal process or request would be in violation of an order of a court of competent jurisdiction within the United States.

3.7. Security of Lawful U.S. Process. Domestic Communications Companies shall protect the confidentiality and security of all Lawful U.S. Process served upon them and the confidentiality and security of Classified, Sensitive, and Controlled Unclassified Information in accordance with U.S. Federal and state law or regulation and this Agreement. Information concerning Lawful U.S. Process, Classified Information, Sensitive Information, or Controlled Unclassified Information shall be under the custody and control of the Security Officer. With respect to Controlled Unclassified Information, compliance with the ITAR and the EAR shall satisfy the requirements of this Section 3.7.

3.8. Points of Contact. Within fourteen (14) days after the Effective Date, Domestic Communications Companies shall designate in writing to the FBI, DOJ, DOD and DHS at least three nominees already holding U.S. security clearances, or who are eligible to receive such clearances and whose applications for such clearances have been submitted to DOD, to serve as a primary and two secondary points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process. The points of contact shall be assigned to Domestic Communications Companies' office(s) in the United States, shall be available twenty-four (24) hours per day, seven (7) days per week and shall be responsible for accepting service and maintaining the security of Classified, Sensitive, and Controlled Unclassified Information and any Lawful U.S. Process in accordance with the requirements of U.S. law and this Agreement. Promptly after designating such points of contact, Domestic Communications Companies shall notify the FBI, DOJ, DOD and DHS in writing of the points of contact, and thereafter shall promptly notify the FBI, DOJ, DOD and DHS of any change in such designation. The points of contact shall be resident U.S. citizens who hold U.S. security clearances (which may include interim security clearances), as outlined in Executive Order 12968, and shall serve as points of contact for new Domestic Communications Companies unless and until the FBI, DOJ, DOD and DHS are notified of any change in designation. Domestic Communications Companies shall cooperate with any request by a Government Authority within the United States that a background check and/or security clearance process be completed for a designated point of contact.

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

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

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

(iii) assign U.S. citizens to positions for which screening is contemplated pursuant to Section 3.12;

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

(v) require that personnel handling Classified Information shall have been granted appropriate security clearances pursuant to Executive Order 12968;

(vi) provide that the points of contact described in Section 3.8 of this Agreement shall have sufficient authority over any of Domestic Communications Companies' employees who may handle Classified, Sensitive, or Controlled Unclassified Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority and the terms of this Agreement;

(vii) 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;

(viii) 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

(ix) identify the types of positions that require screening pursuant to Section 3.12, the required rigor of such screening by type of position, and the criteria by which Domestic Communications Companies will accept or reject screened persons ("Screened Personnel").

3.10. Security Officer Responsibilities and Duties. The Head of Security of MTC, 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 Communications Companies' obligations under Article 3 and Sections 5.2, 5.5, 5.6, 5.7, 5.10, and 5.11 of this Agreement, and shall have the qualifications set forth in Section 3.13. Within thirty (30) days after the Effective Date, MTC shall notify the DOJ, FBI, DOD and DHS of the identity of the Security Officer.

3.11. Disclosure of Protected Data. In carrying out the responsibilities set forth in Section 3.10, the 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 to any officer, director, shareholder, employee, agent, or contractor of MTC or any Domestic Communications Company, including those who serve in a supervisory, managerial or officer role with respect to the Security Officer, except to a Security Director (i) consistent with the Security Officer's or the Security Committee's duties or (ii) to the extent required to comply with this Agreement, unless disclosure has been approved by prior written consent obtained from the FBI, DOJ, DOD or 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. With respect to Controlled Unclassified

Information, application for and receipt of an export authorization under the ITAR or the EAR, as appropriate, shall satisfy the requirements of this Section 3.11.

3.12. Screening of Personnel. Each Domestic Communications Company shall implement a thorough screening process through a reputable third-party to ensure that all personnel 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) or to have access to Transactional Data, Call Associated Data or Subscriber Information, persons who have access to Sensitive Information, and security personnel meet personnel screening requirements agreed to by MTC, DOJ, the FBI, DOD and DHS. 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, an additional criminal record check, and a review of at least three references. Newly hired personnel will also be required to sign a non-disclosure agreement approved in advance by DOJ, FBI, DOD and DHS.

(i) MTC shall consult with DOJ, FBI, DOD and DHS on the screening procedures utilized by the reputable third party and shall provide to DOJ, FBI, DOD and DHS a list of the positions subject to screening. MTC shall utilize the criteria identified pursuant to Section 3.9 (ix) to screen personnel, shall report the results of such screening on a regular basis to the Security Committee, and shall, upon request, provide to the investigations services of the DOJ, the FBI, DOD and DHS or, in the alternative, to the investigations service of OPM, 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) If the DOJ, the FBI, DOD or DHS so desires, it may on its own, or through OPM's investigations service, conduct further background checks for Screened Personnel. MTC will cooperate with any U.S. government agency undertaking any such further background checks.

(iii) Individuals who are rejected by the DOJ, the FBI, DOD or DHS for the screening requirements agreed to pursuant to this Section 3.12 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. MTC will notify the DOJ, the FBI, DOD and DHS of the transfer, departure, or job modification of any individual rejected as a result of the screening conducted pursuant to this Section 3.12 of this Agreement within seven (7) days of such transfer or departure, and shall provide the DOJ, the FBI, DOD and DHS with the name, date of birth and social security number of such individual.

(iv) MTC 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. MTC shall monitor on a regular basis the status of Screened Personnel, and shall remove personnel who no longer meet the Screened Personnel requirements.

(v) MTC shall maintain records relating to the status of Screened Personnel, and shall provide these records, upon request, to the DOJ, FBI, DOD or DHS or any third party auditor appointed under the terms of Section 5.8 below.

3.13. Qualification of Principal Network and Security Officers. MTC shall employ a Head of Network Operations and a Head of Security for Domestic Communications Companies. Within thirty (30) days after the Effective Date, MTC shall notify the DOJ, FBI, DOD and DHS of the identities of the Head of Network Operations and the Head of Security. The Head of Network Operations and the Head of Security, and any designee of the Head of Security who serves as the Security Officer under Section 3.10, shall be resident citizens of the United States who, if not already in possession of U.S. security clearances, shall apply for U.S. security clearances pursuant to Executive Order 12968 immediately upon their appointment; who are subject to the screening requirements of Section 3.12 of this Agreement; and whose appointment to the position is not objected to by the DOJ, FBI, DOD and DHS within ten (10) days of receiving notice thereof. If the Head of Network Operations, the Head of Security, or any designee of the Head of Security who serves as the Security Officer under Section 3.10, does not already possess a U.S. security clearance, he or she may nevertheless serve in that position, subject to DOJ, FBI, DOD and DHS approval, pursuant to an interim security clearance. MTC shall have the right to remove the Head of Network Operations or the Head of Security at any time and to appoint a replacement, subject to the terms of this Section. MTC shall promptly appoint a person who meets the qualifications of this Section to fill any such vacancy, and shall promptly notify the DOJ, FBI, DOD, and DHS in writing of such appointment. In no event shall a vacancy for the position of Head of Network Operations or Head of Security exist for a period of more than ninety (90) days before MTC appoints a qualified candidate to fill such vacancy.

3.14. Qualification of General Counsel and Head of Human Resources. Within thirty (30) days after the Effective Date, MTC shall notify DOJ, FBI, DHS and DOD of the identities of the Human Resources executive responsible for hiring and screening and the General Counsel. The Human Resources executive responsible for hiring and screening and the General Counsel shall be resident citizens of the United States who, if not already in possession of U.S. security clearances, shall apply for U.S. security clearances pursuant to Executive Order 12968 immediately upon their appointment; who are subject to the screening requirements of Section 3.12 of this Agreement; and whose appointment to the position is not objected to by the DOJ, the FBI, DOD or DHS within ten (10) days of receiving notice thereof. If the Human Resources executive responsible for hiring and screening or the General Counsel does not already possess a U.S. security clearance, he or she may nevertheless serve in that position, subject to DOJ, FBI, DOD and DHS approval, pursuant to an interim security clearance. MTC shall have the right to remove the Human Resources executive responsible for hiring and screening and the General Counsel at any time and to appoint a replacement, subject to the terms of this Section. MTC shall promptly appoint a person who meets the qualifications of this Section to fill any such vacancy, and shall promptly notify the DOJ, FBI, DOD, and DHS in writing of such appointment. In no event shall a vacancy for the position of Human Resources executive

responsible for hiring and screening or General Counsel exist for a period of more than ninety (90) days before MTC appoints a qualified candidate to fill such vacancy.

3.15. Establishment of Security Committee of MTC Board. The MTC Board shall establish a Security Committee to oversee security matters within Domestic Communications Companies. 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, shall apply for U.S. security clearances pursuant to Executive Order 12968 immediately upon their appointment to the Security Committee; 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 DOJ, FBI, DOD and DHS approval, pursuant to an interim security clearance. The Security Committee shall supervise and report to the full MTC Board on all matters related to security, including implementation of 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 Head of Security on MTC's compliance with this Agreement, and also shall receive a summary of any report issued pursuant to this Agreement, including reports made in connection with audits conducted pursuant to Section 5.8 of this Agreement and the annual report on compliance issued pursuant to Section 5.11 of this Agreement. The Security Committee shall, in turn, provide general reporting to the full MTC Board on MTC's compliance with this Agreement.

3.16. Number and Notice of Appointment of Security Directors. Subject to Section 3.20 below, fifty (50) percent of the members of the MTC Board nominated by PTI and elected to the MTC Board shall be Security Directors. Notice of the proposed appointment of a Security Director shall be provided in writing to the DOJ, FBI, DOD and DHS by MTC. The DOJ, FBI, DOD and DHS shall have the opportunity to review and disapprove the appointment of a Security Director within thirty (30) days of receiving notice of the proposed appointment. If the DOJ, FBI, DOD or DHS objects to the appointment of an individual as Security Director within the 30-day timeframe, the appointment of that individual shall be rescinded and a different candidate shall be appointed.

3.17. Approval of Acquisition. Acquiring or upgrading network hardware (*e.g.*, routers, switches, servers and network transmission capability) and network operating systems software requires prior approval of a Security Director, unless subject to other procedures pursuant to a policy to be negotiated with DHS. That policy may provide for simplified procedures for non-sensitive acquisitions and upgrades *(e.g.*, vetting by the Head of Network Operations).

3.18. Participation of Security Directors in Committees of the Board of MTC. A quorum for a meeting of the MTC Board or any committee of the MTC Board shall require at least one Security Director, unless the issues addressed at such meeting in no respect address or affect the obligations of MTC under this Agreement. In the event that the MTC Board or any committee of the MTC Board must address at a meeting, for reasons of exigent circumstances, an issue related to or affecting the obligations of MTC 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 formation of a quorum provided that the Security Officer of MTC attends the meeting.

3.19. Attendance of Security Directors at Board Meetings of Domestic Communications Companies. A meeting of the board of a Domestic Communications Company or of a board committee of a Domestic Commications 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 Communications Company under this Agreement. In the event that the board of a Domestic Communications Company or a board committee of a Domestic Communications Company must address at a meeting, for reasons of exigent circumstances, an issue related to or affecting the obligations of the Domestic Communications 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 of MTC attends the meeting.

3.20. Removal of Security Directors. Any Security Director may be removed for any reason permitted by the provisions of applicable law or under the charter of MTC, provided that:

(i) the removal of a Security Director shall not become effective until that Security Director, DOJ, the FBI, DOD and DHS have received written notification, a successor who is qualified to become a Security Director within the terms of this Agreement is selected, DOJ, the FBI, DOD and DHS receive written notice of such selection under the terms of this Agreement, and DOJ, the FBI, DOD or DHS do not object to the proposed Security Director within thirty (30) days of such notice; and

(ii) notification to DOJ, the FBI, DOD and DHS of the removal of a Security Director shall be the responsibility of the General Counsel of MTC.

Notwithstanding the foregoing, however, if immediate removal of any Security Director is deemed necessary to prevent actual or possible violation of any statute or regulation or actual or possible damage to MTC, the Security Director may be temporarily suspended, pending written notification to the FBI, DOJ, DOD and DHS, and removed upon the approval of the removal by the FBI, DOJ, DOD and DHS. The written notification to DOJ, FBI, DOD and DHS shall set forth the reasons for the removal if such reasons are related to the performance of this Agreement In the event of any vacancy in the position of Security Director, however occurring, MTC will give prompt written notice of such vacancy to DOJ, the FBI, DOD and DHS through the General Counsel of MTC, or if that position is vacant, through the Chief Operating Officer of MTC. MTC shall promptly nominate a person who meets the qualifications in Section 3.15 to fill such vacancy, and shall promptly notify DOJ, the FBI, DOD and DHS in writing of such nomination. In no event shall a vacancy for the position of Security Director exist for a period of more than ninety (90) days before MTC nominates a qualified candidate to fill such vacancy.

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

3.22. Operational Control of MTC Network. Except to the extent and under conditions concurred in by the FBI, DOJ, DOD and DHS in writing, operational control of the Domestic Communications Infrastructure will be restricted to MTC facilities located in the United States.

3.23. Security Standards and Practices, and Consultations with U.S. Government. Domestic Communications Companies will maintain or exceed security standards and practices utilized within the U.S. telecommunications industry and will consult with the DOJ and other appropriate U.S. government agencies on steps to maintain or exceed such standards and practices.

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

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

ARTICLE 4: DISPUTES

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

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

(i) require that the Party or Parties believed to have breached, or about to breach, this Agreement cure such breach within thirty (30) days upon receiving written notice of such breach;

(ii) 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 Domestic Communications Companies, or request that the FCC impose any other

appropriate sanction, including but not limited to a forfeiture or other monetary penalty, against Domestic Communications Companies;

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

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

(v) seek suspension or debarment of MTC or Domestic Communications Companies from eligibility for contracting with the U.S. government.

4.3. Irreparable Injury. PTI and MTC agree that the United States would suffer irreparable injury if for any reason a Domestic Communications Company failed to perform any of its material obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, PTI and MTC agree that, in seeking to enforce this Agreement against Domestic Communications Companies, the FBI, DOJ, DOD and DHS shall be entitled, in addition to any other remedy available at law or equity, to specific performance and immediate injunctive or other equitable relief. The obligations in Section 5.5 or 5.6 are material for the purpose of this Section. (Listing these sections does not imply that obligations in other sections are not material).

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 among the Parties that a civil action among the Parties for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement shall be brought, if at all, in the United States District Court for the District of Columbia.

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

ARTICLE 5: AUDITING, REPORTING, NOTICE AND LIMITS

5.1. Filings re *de jure* or *de facto* control of a Domestic Communications Company. If any Domestic Communications Company makes any filing with the FCC or any other Governmental Authority relating to the *de facto* or *de jure* control of a Domestic Communications Company except for filings with the FCC for assignments or transfers of control to any Domestic Communications Company that are *pro forma*, MTC shall promptly provide to the FBI, the DOJ,

DOD and DHS written notice and copies of such filing. This Section 5.1 is effective upon execution of this Agreement by all the Parties.

5.2. Control of MTC. If any member of the Security Committee or of the senior management of MTC or a Domestic Communications Company (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 senior officer) acquires any information that reasonably indicates that any single foreign entity or individual, other than PTI has obtained or will likely obtain an ownership interest (direct or indirect) in MTC or a Domestic Communications Company above ten (10) percent, as determined in accordance with 47 C.F.R. § 63.09, or if any single foreign entity or individual has gained or will likely otherwise gain either (1) Control or (2) *de facto* or *de jure* control of MTC or a Domestic Communications Company, then such member shall promptly cause to be notified the Security Officer or a Security Director, who in turn, shall promptly notify the DOJ, FBI, DOD and DHS in writing. Notice under this section shall, at a minimum:

(i) Identify the entity or individual(s) (specifying the name, addresses and telephone numbers of the entity);

(ii) Identify the beneficial owners of the increased or prospective increased interest in MTC or a Domestic Communications Company by the entity or individual(s) (specifying the name, addresses and telephone numbers of each beneficial owner); and

(iii) Quantify the amount of ownership interest in MTC or a Domestic Communications Company that has resulted in or will likely result in the entity or individual(s) increasing the ownership interest in or control of MTC or a Domestic Communications Company.

5.3. Joint Ventures. A Domestic Communications Company may have entered into or may enter into joint ventures under which the joint venture or entity may provide Domestic Communications.

(i) To the extent that such Domestic Communications Company does not have *de facto* or *de jure* control over a joint venture or entity, such Domestic Communications Company shall in good faith (a) notify such entity of this Agreement and its purposes, (b) endeavor to have such entity comply with this Agreement as if it were a Domestic Communications Company, and (c) consult with the DOJ, FBI, DOD or DHS about the activities of such entity. Nothing in this Section 5.3 shall be construed to relieve Domestic Communications Companies of obligations under Article 2 of this Agreement.

(ii) If a Domestic Communications Company enters into joint venture under which the joint venture or entity may provide Domestic Communications or transmission, switching, bridging, routing equipment (including software and upgrades), facilities used to provide, process, direct, control, supervise or manage Domestic Communications, the Domestic Communications Company must

provide DHS with notice no later than 30 days before the joint venture offers Domestic Communications service. DHS will have 30 days from receipt of the notice to review and provide the Domestic Communications Company 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.

5.4. Outsourcing. A Domestic Communications Company shall not outsource functions covered by this Agreement to an entity that is not a Domestic Communications Company, except pursuant to an outsourcing policy to be negotiated with DHS. Such policy shall include prior notice of the proposed outsourcing and the right of DHS to object within thirty (30) days to the proposed outsourcing; the parties may agree in the outsourcing policy to exclude classes of outsourcing contracts of a routine and nonsensitive nature from this notice and approval requirement. Further:

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

(ii) the Domestic Communications Company 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) the Domestic Communications Company shall notify the DOJ, FBI, DOD and DHS within thirty (30) days of contracting out operation of the Domestic Communications Infrastructure to an entity that is not a Domestic Communications Company, which notice shall identify the name of the entity and the nature of the contract;

(iv) if the Domestic Communications Company learns that the entity or the entity's employee has violated an applicable provision of this Agreement, the Domestic Communications Company will notify the DOJ, FBI, DOD and DHS promptly; and

(v) with consultation and, as appropriate, cooperation with DOJ, FBI, DOD and DHS, the Domestic Communications Company will take reasonable steps necessary to rectify promptly the situation, which steps may (among others) include terminating the arrangement with the 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.

5.5. Notice of Foreign Influence. If any member of the Security Committee or of the senior management of PTI, MTC or a Domestic Communications Company (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 senior officer) acquires any information that reasonably indicates that any foreign government, any foreign government-controlled entity, or any foreign entity:

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

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

then such member shall promptly cause to be notified the Security Officer or a Security Director, who in turn, shall promptly notify the FBI, DOJ, DOD and DHS in writing of the timing and the nature of the foreign government's or entity's plans and/or actions.

5.6. Reporting of Incidents. MTC and Domestic Communications Companies shall take practicable steps to ensure that, if any MTC or Domestic Communications Company officer, director, employee, contractor or agent acquires any information that reasonably indicates: (a) a breach of this Agreement; (b) access to or disclosure of U.S. Hosting Data or Domestic Communications, or the conduct of Electronic Surveillance, in violation of Federal, state or local law or regulation; (c) access to or disclosure of CPNI or Subscriber Information in violation of Federal, state or local law or regulation (except for violations of FCC regulations relating to improper commercial use of CPNI); or (d) improper access to or disclosure of Classified, Sensitive, or Controlled Unclassified Information, then the individual will notify the Security Officer or a Security Director, who will in turn notify the FBI and the DOJ in the same manner as specified in Section 5.5. This report shall be made promptly and in any event no later than ten (10) calendar days after MTC or the Domestic Communications Company acquires information indicating a matter described in this Section 5.6(a)-(d) of this Agreement. MTC and the Domestic Communications Companies shall lawfully cooperate in investigating the matters described in this section of this Agreement. MTC or the Domestic Communications Company need not report information where disclosure of such information would be in violation of an order of a court of competent jurisdiction in the United States.

5.7. Non-Retaliation. MTC and each Domestic Communications Company shall, by duly authorized action of its respective Board of Directors, adopt and distribute an official corporate policy that strictly prohibits MTC or a Domestic Communications Company 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, 5.5 or 5.6 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 FBI, DOJ, DOD and DHS by the Security Officer or a Security Director under Sections 5.2, 5.5 or 5.6 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 MTC or a Domestic Communications Company of any material term of such corporate policy shall constitute a breach of this Agreement.

5.8. Third Party Audits. MTC shall retain and pay for a neutral third party to audit objectively on an annual basis its compliance with agreed elements of this Agreement. MTC shall provide notice of its selected auditor to the DOJ, FBI, DOD and DHS, and the DOJ, FBI, DOD and DHS shall be able to review and approve or disapprove the selected auditor and terms of reference for that auditor within thirty (30) days of receiving notice. In addition, MTC shall provide to the DOJ, FBI, DOD and DHS a copy of its contract with the third party auditor, which shall include terms defining the scope and purpose of the audits. The DOJ, FBI, DOD and DHS 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, MTC shall ensure that all reports generated by the auditor are provided promptly to the DOJ, FBI, DOD and DHS. Domestic Communications Companies also will provide the DOJ, FBI, DOD and DHS with access to facilities, information, and personnel consistent with Sections 5.9 and 5.10 below in the event that the DOJ, FBI, DOD or DHS wishes to conduct its own audit of a Domestic Communication Company. 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 will be subject to review and approval by the DOJ, the FBI, DOD and the DHS;

(ii) Authority for the auditor to review and analyze MTC policies and procedures designed to implement this Agreement;

(iii) Authority for the auditor to review and analyze relevant information related to the configuration of the MTC network;

(iv) The Head of Network Operations will report periodically on technical advancements that enhance compliance with this Agreement;

(v) Authority for the auditor to review and analyze minutes of MTC Board and other Board Committee meetings held in accordance with the terms of this Agreement;

(vi) Authority for the auditor to review and analyze Security Director and Security Officer logs and records including, but not limited to, records relating to facility

visits, employee screening data and any reports submitted in accordance with Section 5.6 of this Agreement;

(vii) Authority for the auditor to conduct a reasonable number of unannounced inspections of MTC key facilities each year.

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

(ix) Authority for the auditor to conduct a reasonable number of confidential interviews of MTC employees concerning compliance with this Agreement.

5.9. Access to Information and Facilities. FBI, DOJ, DOD and DHS may visit with thirty (30) minutes notice any part of Domestic Communications Companies' 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 FBI, DOJ, DOD or DHS to verify compliance with the then-effective terms of this Agreement. Within sixty (60) days of the Effective Date, the parties will develop procedures for implementation of this Section 5.8.

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

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

(i) a copy of all audit reports compiled by the third party auditor conducted pursuant to Section 5.8 of this Agreement;

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

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

(iv) 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

(v) identification of any other issues that, to Domestic Communications Companies' knowledge, will or reasonably could affect the effectiveness of or compliance with this Agreement.

MTC and all Domestic Communications Companies shall make available to the Security Officer, in a timely fashion, all information necessary to complete the report required by this Section.

5.12. Information and Reports Concerning Network Architecture. MTC shall provide to the DOJ, FBI, DHS and DOD, on a quarterly basis, the following information regarding the interconnections and control of the Domestic Communications Infrastructure:

(i) 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.

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

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

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

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

MTC shall promptly report any material changes, upgrades and/or modifications to the items described in (i) - (v) 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 (i) - (v) 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.

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

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

Federal Bureau of Investigation
General Counsel
935 Pennsylvania Avenue, N.W.
Washington, DC 20535

Department of Defense
Office of General Counsel
Attn: Deputy General Counsel
for Acquisition and Logistics
The Pentagon, Room 3D973
1600 Defense Pentagon
Washington, DC 20301-1600

Department of Homeland Security
Washington, D.C. 20528
Attn: General Counsel, Office of the General Counsel
Telephone: 202-692-4237
Fax: 202-282-8415
(By Personal Delivery or E-mail Only)

Micronesian Telecommunications Corp.
[Contact Information and Address]

Pacific Telecom, Inc.
[Contact Information and Address]

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

ARTICLE 6: FREEDOM OF INFORMATION ACT

6.1. Protection from Disclosure. The DOJ, FBI, DOD and DHS shall take all reasonable measures to protect from public disclosure all information submitted by a Domestic Communications Company or other entities in accordance with the terms of this Agreement to the DOJ, FBI, DOD or DHS in connection with this Agreement and clearly marked with the legend "Business Confidential; subject to protection under 5 U.S.C. § 552(b); not to be released without notice to the filing party" or similar designation. Such markings shall signify that it is

the company's position that the information so marked constitutes "trade secrets" and/or "commercial or financial information obtained from a person and privileged or confidential," or otherwise warrants protection within the meaning of 5 U.S.C. § 552(b)(4). For the purposes of 5 U.S.C. § 552(b)(4), the Parties agree that information so marked is voluntarily submitted. If a request is made under 5 U.S.C. § 552(a)(3) for information so marked, and disclosure of any information (including disclosure in redacted form) is contemplated, the DOJ, FBI, DOD or DHS, as appropriate, shall notify the company of the intended disclosure as provided by Executive Order 12600, 52 Fed. Reg. 23781 (June 1987). If the Domestic Communications Company objects to the intended disclosure and its objections are not sustained, the DOJ, FBI, DOD or DHS, as appropriate, shall notify the company of its intention to release (as provided by Section 5 of Executive Order 12600) not later than five business days prior to disclosure of the challenged information. The Parties note that information submitted by a Domestic Communications Company or other entities in accordance with the terms of this Agreement may be protected from disclosure under the Critical Information Infrastructure Act of 2002.

6.2. Use of Information for U.S. Government Purposes. Nothing in this Agreement shall prevent the FBI, DOJ, DOD or DHS from lawfully disseminating information as appropriate to seek enforcement of this Agreement, or from lawfully sharing information as appropriate with other Federal, state, or local government agencies to protect public safety, law enforcement, or national security interests, provided that the FBI, DOJ, DOD or DHS take all reasonable measures to protect from public disclosure the information marked as described in Section 6.1.

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

ARTICLE 7: FCC CONDITION AND CFIUS

7.1. FCC Approval. Upon the execution of this Agreement by all the Parties, the DOJ, FBI, DOD 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 DOJ, FBI, DOD and DHS have no objection to the FCC's grant of the applications filed with the FCC in FCC IB Docket No. 03-115. This Section 7.1 is effective upon execution of this Agreement by all the Parties.

7.2. Future Applications. MTC agrees that, in any application or petition by any Domestic Communications Company to the FCC for licensing or other authority filed with or granted by the FCC after the Effective Date, except with respect to *pro forma* assignments or *pro forma* transfers of control, the Domestic Communications Company shall request that the FCC condition the grant of such licensing or other authority on compliance with the terms of this Agreement. Notwithstanding Section 8.9, the FBI, DOJ, DOD and DHS reserve the right to object, formally or informally, to the grant of any other FCC application or petition of MTC or a Domestic Communications Company for a license or other authorization under Titles II or III of the Communications Act of 1934, as amended, and to seek additional or different terms that would, consistent with the public interest, address any threat to their ability to enforce the laws,

preserve the national security, and protect the public safety raised by the transactions underlying such applications or petitions.

7.3. CFIUS. Provided that the FCC adopts the Condition to FCC Authorization, the Attorney General, the Secretary of Defense and the Secretary of Homeland Security shall not make any objection to the CFIUS or to the President concerning PTI's acquisition of MTC or grant of the applications filed with the FCC in FCC IB Docket No. 03-115. This commitment, however, does not extend to any objection the Attorney General, the Secretary of Defense or the Secretary of Homeland Security may wish to raise with the CFIUS or the President in the event that (a) PTI, MTC or any Domestic Communications Company fails to comply with the terms of this Agreement, (b) the Attorney General, the Secretary of Defense or the Secretary of Homeland Security learns that the representations of MTC made to the DOJ, the FBI, the DOD, the DHS or the FCC above are materially untrue or incomplete, (c) there is a material increase in the authority of a foreign entity to exercise Control of MTC or a Domestic Communications Company, or (d) there is any other material change in the circumstances associated with the transactions at issue.

ARTICLE 8: OTHER

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

8.2. Right to Make and Perform Agreement. PTI and MTC each represent that each 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 PTI and MTC enforceable in accordance with its terms.

8.3. 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.

8.4. Other Laws. Nothing in this Agreement is intended to limit or constitute a waiver of (a) any obligation imposed by any U.S. Federal, state or local laws on PTI, MTC or any Domestic Communications Company, (b) any enforcement authority available under any U.S. or state laws, (c) the sovereign immunity of the United States, or (d) any authority the U.S. government may possess (including without limitation authority pursuant to International Emergency Economic Powers Act) over the activities of PTI, MTC or any Domestic Communications Company located within or outside the United States. Nothing in this Agreement is intended to or is to be interpreted to require the Parties to violate any applicable U.S. law.

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

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

8.7. Modifications. This Agreement may only be modified by written agreement signed by all of the Parties. The DOJ, FBI, DOD and DHS agree to consider in good faith and promptly possible modifications to this Agreement if PTI or MTC believes that the obligations imposed on PTI, MTC or the Domestic Communications Companies under this Agreement are substantially more restrictive than those imposed on other U.S. and foreign licensed service providers in like circumstances in order to protect U.S. national security, law enforcement, and public safety concerns. Any substantial modification to this Agreement shall be reported to the FCC within thirty (30) days after approval in writing by the Parties.

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

8.9. Changes in Circumstances for the DOJ, FBI, DHS or the DOD. If after the date that all the Parties have executed this Agreement, the DOJ, FBI, DOD or DHS finds that the terms of this Agreement are inadequate to address national security, law enforcement, or public safety concerns presented, then the other Parties 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, enforce the laws or protect the safety of the public, the parties will work promptly to amend the agreement to implement such advances.

8.10. Periodic Review. To ensure that this Agreement and the policies implemented in furtherance of this Agreement continue to adequtely preserve the national security, law enforcement and public safety objectives, the terms of this Agreement and those policies shall be reviewed by the parties at least every 18 months from the Execution Date.

8.11. 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.

8.12. 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.

8.13. Successors and Assigns. This Agreement shall inure to the benefit of, and shall be binding upon, the Parties, and their respective successors and assigns.

8.14. 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.

8.15. Termination of Agreement. If the Purchase and Sale Agreement is terminated prior to the Effective Date, MTC shall promptly provide written notification of such termination to the FBI, DOJ, DHS and DOD, and upon receipt of such written notice, this Agreement shall automatically terminate. After the Effective Date, this Agreement shall terminate upon thirty (30) days prior written notice from MTC to the FBI, DOJ, DHS and DOD, provided that at such time there is no Domestic Communications Company.

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

8.17. Suspension of Agreement If No Significant Foreign Ownership. This Agreement shall be suspended in its entirety with respect to PTI, MTC and all Domestic Communications Companies thirty (30) days after receipt from PTI and MTC of notice and documentation reasonably satisfactory to the DOJ, FBI, DOD, and DHS that neither PTI nor any other foreign entity either Controls MTC or a Domestic Communications Company or holds, directly or indirectly, a ten (10) percent or greater interest in MTC or a Domestic Communications Company, unless the DOJ, FBI, DOD and DHS notify PTI and MTC within said thirty (30) day period that this Agreement shall not be suspended in order to protect U.S. national security, law enforcement, and public safety concerns. If this Agreement is not suspended pursuant to this provision, the DOJ, FBI, DOD and DHS agree to consider promptly and in good faith possible modifications to this Agreement. Notwithstanding anything to the contrary in this Section 8.16, this Agreement shall remain in effect with respect to PTI, MTC and the Domestic Communications Companies for so long as (and the obligations of PTI, MTC and the Domestic Communications Companies shall not be suspended and any suspension of the obligations of PTI, MTC and the Domestic Communications Companies shall terminate if) PTI or any other foreign entity shall either Control or hold, at any time does hold, or is a party to an agreement to hold, directly or indirectly, a ten (10) percent or greater ownership interest, as determined in accordance with 47 C.F.R. § 63.09, in MTC or any Domestic Communications Company or any transferee or assignee of the FCC licenses or authorizations held by MTC or a Domestic Communications Company.

8.18. Pledging of Stock or Assets of Domestic Communications Companies. Nothing in this Agreement shall be interpreted to prevent MTC from pledging the stock or assets of any Domestic Communications Company in connection with the borrowing of funds and similar financial activities by MTC, nor shall such pledging of stock or assets excuse performance of the obligations in this Agreement by MTC or any Domestic Communications Company.

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

This Agreement is executed on behalf of the Parties:

Micronesian Telecommunications Corp.

Date: 09/29/2003

By: /s/ JOHN DOHERTY
Printed Name: John Doherty
Title: President

Pacific Telecom, Inc.

Date: 09/16/2003

By: /s/ JOSE RICARDO DELGADO
Printed Name: Jose Ricardo Delgado
Title: President

Federal Bureau of Investigation

Date: 10/01/2003

By: /s/ PATRICK W. KELLEY
Printed Name: Patrick W. Kelley
Title: Deputy General Counsel

United States Department of Justice

Date: 10/01/2003

By: /s/ JOHN A. MALCOLM
Printed Name: John A. Malcolm
Title: Deputy Asst. Attorney General

United States Department of Defense

Date: 10/06/2003

By: /s/ JOHN P. STENBIT
Printed Name: John B. Stenbit
Title: ASD NII (CIO)

United States Department of Homeland Security

Date: 09/21/2003

By: /s/ ROBERT P. LISCOWSKI
Printed Name: Robert P. Liscowski
Title: Asst. Secretary for Infrastructure Protection

EXHIBIT A

CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that consent to the transfer of control of MTC and grant of a declaratory ruling pursuant to 47 U.S.C. § 310(b)(4) are subject to compliance with the provisions of the Agreement attached hereto among MTC and PTI on the one hand, and the United States Department of Justice ("DOJ"), the Federal Bureau of Investigation ("FBI"), the United States Department of Defense ("DOD"), and the United States Department of Homeland Security ("DHS"), on the other, dated 10/06/2003, which Agreement is designed to address national security, law enforcement, and public safety issues of the DOJ, the FBI, the DOD and the DHS regarding the authority granted herein. Nothing in this Agreement is intended to limit any obligation imposed by Federal law or regulation including, but not limited to, 47 U.S.C. § 222(a) and (c)(1) and the FCC's implementing regulations.