Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Telstra Incorporated	)	
	)	File No. SCL-LIC-20070621-00009
Application for Authority to Construct, Land and Operate a Private Fiber-Optic Cable System Linking Australia and the United States	)	

PETITION TO ADOPT CONDITIONS TO AUTHORIZATIONS AND LICENSES

The Department of Homeland Security ("DHS") and the Department of Justice ("DOJ") (collectively, the "Agencies"), submit this Petition to Adopt Conditions to Authorizations and Licenses ("Petition"), pursuant to Section 1.41 of the Federal Communications Commission ("Commission") rules.[1] Through this Petition, the Agencies advise the Commission that they have no objection to the Commission approving the authority sought in the above-referenced proceeding, provided that the Commission conditions its approval on the agreement of Telstra Incorporated to abide by the commitments and undertakings set forth in the April 16, 2008 agreement (the "Agreement"), which is attached hereto.

In the above-referenced proceeding, Telstra Incorporated petitioned the Commission for authority under the Cable Landing License Act of 1921[2] and Executive Order 10530[3] to

[1] 47 C.F.R. § 1.41.

[2] Pub. Law No. 8, 67th Congress, 42 Stat. 8 (1921); 47 U.S.C. §§ 34-39.

[3] Exec. Ord. No. 10530 § 5(a) (May 10, 1954), reprinted as amended in 3 U.S.C. § 301.

construct, land and operate a private fiber-optic submarine cable system linking Australia and the United States.

The Commission has long recognized that law enforcement, national security, and public safety concerns are part of its public interest analysis, and has accorded deference to the views of other U.S. government agencies with expertise in those areas. *See In the Matter of Comsat Corporation d/b/a Comsat Mobile Communications, etc.*, 16 FCC Rcd. 21661, 21707 ¶ 94 (2001).

After discussions with representatives of Telstra Incorporated in connection with the above-referenced proceeding, the Agencies have concluded that the additional commitments set forth in the Agreement will help ensure that the Agencies and other entities with responsibility for enforcing the law, protecting the national security, and preserving public safety can proceed appropriately to satisfy those responsibilities. Accordingly, the Agencies advise the Commission that they have no objection to the Commission granting the application in the above-referenced proceeding, provided that the Commission conditions its consent on compliance by Telstra Incorporated with the commitments set forth in the Agreement.

The Agencies are authorized to state that Telstra Incorporated does not object to the grant of this Petition.

Respectfully submitted,

/S/
Charles M. Steele
Chief of Staff
National Security Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

/S/
Stewart A. Baker
Assistant Secretary for Policy
U.S. Department of Homeland Security
3801 Nebraska Avenue, N.W.
Washington, DC 20528

April 16, 2008

AGREEMENT

THIS AGREEMENT (the "**Agreement**") is made as of the date of the last signature affixed hereto, by and between Telstra Incorporated ("**Telstra**") and the U.S. Department of Homeland Security ("**DHS**") (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 United States and its citizens to maintain the viability, integrity, and security of the communications systems of the United States (see e.g., Executive Order 13231, Critical Infrastructure Protection in the Information Age, and Homeland Security Presidential Directive / HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection);

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

WHEREAS, Telstra is a Delaware corporation that may provide business critical telecommunications services to enterprise companies and carriers including the U.S. Government;

WHEREAS, Telstra is a wholly-owned subsidiary of Telstra Holdings Pty Limited ("**Telstra Holdings**"), which in turn is a wholly-owned subsidiary of Telstra Corporation Limited ("**Telstra Corporation**"), an Australian company that owns operating subsidiaries that provide a range of communications services in Australia, the United States and select foreign countries;

WHEREAS, Telstra has an obligation to protect from unauthorized disclosure the contents of wire and electronic communications under U.S. law;

WHEREAS, Telstra provides electronic communication services including telephone services which are subject to U.S. privacy and electronic surveillance laws;

WHEREAS, Telstra has direct physical and electronic access to a variety of customer and end-user information that is subject to U.S. privacy and electronic surveillance laws;

WHEREAS, Telstra Corporation owns, operates, monitors and maintains extensive communications networks, with facilities in countries and cities throughout the Pacific region;

WHEREAS, Telstra has entered into an agreement with AT&T Corp. ("**ATTC**") to use ATTC's existing cable landing station in Keawaula, Hawaii, which is owned and operated by

ATTC, to interconnect a single point-to-point Cable System segment linking Australia and the United States, including with the mainland U.S. telecommunications network;

WHEREAS, on June 21, 2007, Telstra and ATTC applied to the Federal Communications Commission ("**FCC**") for a submarine cable landing license under the Cable Landing License Act of 1921[1] and Executive Order No. 10530[2], FCC File No SCL-LIC-20070621-00009 (the "**Application**");

WHEREAS, DHS will request that the FCC's grant of the pending Application be made subject to resolution of issues relating to national security, law enforcement, and public safety, and whereas Telstra has agreed to enter into this Agreement with DHS to address issues raised by DHS, and to petition that the FCC condition the requested authorization on compliance with this Agreement;

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

ARTICLE 1: DEFINITION OF TERMS

As used in this Agreement:

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

1.2 "**Affiliate**" means any entity in which Telstra has a greater than 50% ownership interest or over which Telstra exercises Control.

1.3 "**Cable System**" means all equipment, facilities and services, including all network operations centers ("**NOCs**") pertaining to the single point-to-point cable system segment linking Australia and the United States at the ATTC cable landing station in Keawaula, Hawaii.

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

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

(a) the sale, lease, mortgage, pledge, or other transfer of any or all of the principal assets of the entity, whether or not in the ordinary course of business;

---

[1] Pub. Law No. 8, 67th Congress, 42 Stat. 8 (1921); U.S.C. §§ 34-39.

[2] Exec. Ord. No. 10530 § 5(a) (May 10, 1954), reprinted as amended in 3 U.S.C. § 301.

(b) the dissolution of the entity;

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

(d) the termination or nonfulfillment of contracts of the entity;

(e) the amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in Section 1.4(a) through (d); or

(f) Telstra's obligations under this Agreement.

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

1.7 "**Domestic**" where used in this Agreement, whether capitalized or lower case, means within the United States.

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

1.9 "**Domestic Communications Infrastructure**" means the portion of the Cable System used by or on behalf of Telstra that is located in the United States and is: (a) transmission, switching, bridging and routing equipment (including software and upgrades) to provide, process, direct, control, supervise or manage Domestic Communications; (b) facilities and equipment physically located in the United States; and (c) facilities to control the equipment described in (a) and (b) above, but does not include entities with which Telstra has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree, nor equipment or facilities used by service providers other than Telstra that are:

(1) interconnecting communications providers; or

(2) providers of services or content that are:

(A) accessible using the communications services of Telstra, and

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

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

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

1.12 "**Electronic Surveillance**," for the purposes of this Agreement, includes: (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (b)

Access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 *et seq.*; (c) acquisition of dialing, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 *et seq.* and 50 U.S.C. § 1841 *et seq.*; (d) acquisition of location-related information concerning a service subscriber or facility; (e) preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (f) Access to, or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (a) through (e) above and comparable state laws.

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

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

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

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

1.17 "**Lawful Australian Process**" means lawful Australian Commonwealth, State or Territory warrants or court orders, processes, or authorizations or requests issued under Australian Commonwealth, State or Territory law for physical search or seizure, production of tangible things, or access to or disclosure of telecommunications-related information, including Transactional Data or Australian subscriber information.

1.18 "**Management of Telstra**" means its officers and members of the Board of Directors.

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

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

1.21 "**Sensitive Information**" means information held by Telstra in the United States that is not Classified Information regarding:

(a) the persons or facilities that are the subjects of Lawful U.S. Process;

(b) the identity of the Government Authority or Government Authorities serving such Lawful U.S. Process;

(c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance in the United States;

(d) the means of carrying out Electronic Surveillance in the United States; or

(e) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process;

as well as all other information held by Telstra in the United States that is not Classified Information but is designated in writing by an authorized official of a federal, state, or local law enforcement agency or a U.S. intelligence agency as "Sensitive Information," provided that Telstra has been notified of such designation in writing pursuant to the terms of this Agreement. The designation "Sensitive" as used in this Section includes, but is not limited to, information marked or labeled "Official Use Only," "Limited Official Use Only," "Law Enforcement Sensitive," "Sensitive Security Information," "Sensitive but Unclassified," "Controlled Unclassified Information," or other similar designations.

1.22 "**Subscriber Information**" means all records or other information relating to domestic customers or subscribers of Telstra 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.

1.23 "**Transactional Data**" includes the following held by Telstra in the United States when associated with a Domestic Communication, but does not include the content of any communication:

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

(b) any information related to the sender or recipient of that Domestic Communication, including, without limitation subscriber identification, called party number, calling party number, start time, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, post-cut-through dialed digit extraction, in-band and out-of-band signaling, and party add, drop and hold;

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

(d) the time, date, size, or volume of data transfers, duration, domain names, Media Access Control ("MAC") or IP addresses (including source and destination), URL's, port numbers, packet sizes, protocols or services, special purpose flags, or other header information or identifying designators or characteristics, including electronic mail headers showing From: and To: addresses; and

(e) as to any mode of transmission (including mobile transmissions), and to the extent permitted by U.S. laws, any information indicating as closely as possible the physical location to or from which a Domestic Communication is transmitted in the United States.

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

1.25 **"Telstra"** means Telstra Incorporated and its subsidiaries.

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

1.27 **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 **Compliance with Lawful U.S. Process.** Telstra shall configure its Domestic Communications Infrastructure to be capable of complying, and Telstra employees in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with:

(a) Lawful U.S. Process;

(b) the orders of the President of the United States in the exercise of his/her authority under § 706 of the Communications Act of 1934, as amended, (47 U.S.C. § 606), and under § 302(e) of the Aviation Act of 1958 (49 U.S.C. § 40107(b)) and Executive Order 11161 (as amended by Executive Order 11382); and

(c) National Security and Emergency Preparedness rules, regulations and orders issued pursuant to the Communications Act of 1934, as amended (47 U.S.C. § 151 *et seq.*).

2.2 **Information Storage and Access.** Unless otherwise agreed to by the Parties, Telstra shall make the following available in the United States:

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

(b) any Wire Communications or Electronic Communications received by, intended to be received by, or stored in the account of a domestic customer or subscriber of Telstra, if such communications are stored by or on behalf of Telstra for any reason;

(c) Transactional Data, if such data are stored by or on behalf of Telstra for any reason;

(d) Subscriber Information, if such information is stored by or on behalf of Telstra for any reason;

(e) billing records of domestic customers or subscribers, if such information is stored by or on behalf of Telstra for any reason; and

(f) Network Management Information.

Nothing in this Section is meant to exclude the use of Transactional Data for operational business or network management purposes in the normal course of business if said data is subject to security and Access controls. The phrase "on behalf of" as used in this Section does not include entities with which Telstra has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree.

2.3 **Storage Pursuant to 18 U.S.C. § 2703(f)**. Upon a request made pursuant to 18 U.S.C. § 2703(f) by a Government Authority within the United States to preserve any information in the possession, custody, or control of Telstra, including any information that is listed in Section 3.3 below, Telstra shall store such preserved records or other evidence in the United States.

2.4 **Compliance with Applicable Law**. Nothing in this Agreement shall excuse Telstra from any obligation they may have to comply with applicable legal requirements for the retention, preservation, or production of information, records or data as well as all applicable requirements of the Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001, et seq.

2.5 **Storage of Protected Information**. Telstra shall store all Classified Information and Sensitive Information in the United States.

ARTICLE 3: SECURITY

3.1 **Measures to Prevent Improper Use or Access**. Telstra shall take all reasonable measures to prevent the use of or Access to the Domestic Communications Infrastructure to conduct Electronic Surveillance, or to Access, obtain or disclose Domestic Communications, Transactional Data, Subscriber Information, Classified Information or Sensitive Information, in violation of any U.S. federal, state, or local laws or the terms of this Agreement. Telstra shall submit the policies and procedures regarding these measures to DHS within **ninety (90) calendar** days of the effective date for review. Telstra agrees to meet and confer with DHS and reasonably address any concerns DHS may raise about the policies or the procedures described therein.

3.2 **Access by Foreign Government Authorities**. Telstra shall not, directly or indirectly, disclose or permit disclosure of, or provide Access to Domestic Communications, Transactional

Data, or Subscriber Information, stored by or on behalf of Telstra 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 DHS or the authorization of a court of competent jurisdiction. Any such requests or submission of legal process shall be reported to DHS as soon as possible and in no event later than **ten (10) business days** after such request or legal process is received by or known to Telstra. Telstra shall take reasonable measures to ensure that it will promptly learn of all such requests or submission of legal process.

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

(a) Classified or Sensitive Information;

(b) Transactional Data, Subscriber Information, or a copy of any Domestic Communications, intercepted or acquired pursuant to Lawful U.S. Process; or

(c) the existence of Lawful U.S. Process that is not already a matter of public record,

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

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

3.5 **Security of Lawful U.S. Process**. Telstra shall protect the confidentiality and security of all Lawful U.S. Process served upon it and the confidentiality and security of Classified and Sensitive Information in accordance with U.S. federal and state law or regulation and this Agreement.

3.6 **Points of Contact**. Within **ten (10) business days** after the Effective Date, Telstra shall designate points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful U.S. Process relating to Domestic Communications carried by or through, in whole or in part, the Domestic Communications Infrastructure, or relating to its customers or subscribers. The points of contact shall be in the United States, shall be available **twenty-four (24) hours per day, seven (7) days per week** and shall be responsible for accepting service and maintaining the security of Classified Information, Sensitive Information and any Lawful U.S. Process relating to Domestic Communications

carried by or through, in whole or in part, the Domestic Communications Infrastructure, or relating to Telstra's customers or subscribers. Within **ten (10) business days** after designating such points of contact, Telstra shall notify DHS in writing of the points of contact, and thereafter shall notify DHS within **ten (10) business days** of any change in such designation. The points of contact shall be resident U.S. citizens who, based on the information in Telstra's possession, are eligible for appropriate U.S. security clearances. Telstra shall cooperate with any request by a Government Authority within the United States that a background check, security clearance process or both be completed for a designated point of contact.

3.7 **Information Security Plan.** Within **ninety (90) calendar days** of the Effective Date, Telstra shall:

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

(b) assign U.S. citizens, who meet high standards of trustworthiness for maintaining the confidentiality of Sensitive Information, to positions that handle or that regularly deal with information identifiable to such person as Sensitive Information;

(c) upon request from DHS provide the name, date of birth, and other relevant requested identifier information of each person who regularly handles or deals with Sensitive Information;

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

(e) provide that the points of contact described in Section 4.6 of this Agreement shall have sufficient authority over any of Telstra's employees who may handle Classified or Sensitive Information to maintain the confidentiality and security of such information in accordance with applicable U.S. legal authority and the terms of this Agreement; and

(f) maintain appropriately secure facilities (e.g., offices) for the handling and storage of any Classified or Sensitive Information.

3.8 **Nondisclosure of Protected Data.** Telstra shall not directly or indirectly disclose information concerning Lawful U.S. Process, Classified Information, or Sensitive Information to any third party, or to any officer, director, shareholder, employee, agent, or contractor of Telstra, including those who serve in a supervisory, managerial or executive role with respect to the employees working with the information, unless disclosure has been approved by prior written consent obtained from DHS, or there is an need for disclosure of the information in order to fulfill an obligation consistent with the purpose for which the information is collected or maintained.

3.9 **Notice of Obligations.** Telstra shall instruct appropriate officials, employees, contractors, and agents as to Telstra's obligations under this Agreement, including the individuals' duty to report any violation of this Agreement and the reporting requirements in Article 4 of this Agreement, and shall issue periodic reminders to them of such obligations. Telstra shall have issued these instructions in writing within **forty-five (45) calendar days** of the

Effective Date, and shall submit them to the U.S. Government parties at the same time as it issues the instructions to officials, employees, contractors, and agents.

3.10 **Access to Classified or Sensitive Information**. Nothing contained in this Agreement shall limit or affect the authority of a U.S. Government Authority to deny, limit or revoke whatever access Telstra might have to Classified or Sensitive Information under that Government Authority's jurisdiction.

ARTICLE 4: REPORTING AND NOTICE

4.1 **Filings Concerning *de jure* or *de facto* Control of Telstra**. If Telstra makes any filing with the FCC or any other Government Authority relating to the *de facto* or *de jure* control of Telstra or the Cable System except for filings with the FCC for assignments or transfers of control that are *pro forma*, Telstra shall promptly provide to DHS written notice and copies of such filing.

4.2 **Change in Control**. If any member of the management of Telstra (including officers and members of the Board of Directors) acquires any information that reasonably indicates that any single foreign entity or individual, other than those already identified in connection with Telstra's pending FCC Application, has or will likely obtain an ownership interest (direct or indirect) in Telstra or the Cable System above ten (10) percent, as determined in accordance with 47 C.F.R. § 63.09, or if any foreign entity or individual, singly or in combination with other foreign entities or individuals, has or will likely otherwise gain either: (i) Control; or (ii) *de facto* or *de jure* control of Telstra, then such officer or director shall promptly cause Telstra to notify DHS in writing within **ten (10) business days**. Notice under this Section shall, at a minimum:

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

(b) identify the beneficial owners of the increased or prospective increased interest in Telstra by the entity or individual(s) (specifying the name, addresses, and telephone numbers of each beneficial owner); and

(c) quantify the amount of ownership interest that the entity or individual(s) has or will likely obtain in Telstra and, if applicable, the basis for their prospective Control of Telstra.

4.3 **Procedure and Process on Reporting**. Within **forty-five (45) calendar days** of the Effective Date, Telstra shall adopt and distribute to all officers and directors, a written procedure or process for the reporting by officers and directors of noncompliance with this Agreement. This written procedure or process shall also provide for the reporting by employees, agents and contractors to management of information that must be reported to DHS under this Article. Any violation by Telstra of any material term of such corporate policy shall constitute a breach of this Agreement. By a written statement, Telstra shall notify all employees, contractors and agents that the general categories of information identified in this Article should be disclosed to senior management and shall set forth in a clear and prominent manner the contact information for a senior manager to whom such information may be reported. The written statement informing employees, contractors, and agents of the need to report this information shall also state that Telstra will not discriminate against, or otherwise take adverse action against, anyone who

reports such information to the Management of Telstra or the United States Government. Telstra shall make such process or procedure documents available to DHS upon request.

4.4 **Non-retaliation**. Within **forty-five (45) calendar days** after the Effective Date, Telstra shall, by duly authorized action of its Board of Directors, adopt and distribute to all officers and directors an official corporate policy that strictly prohibits Telstra from discriminating or taking any adverse action against any officer, director, employee, contractor, or agent because he or she has in good faith initiated or attempted to initiate a notice or report under this Article, or has notified or attempted to notify the management to report information that he or she believes in good faith is required to be reported to DHS under either this Article or under Telstra's written notice to employees on the reporting of any such information. Any violation by Telstra of any material term of such corporate policy shall constitute a breach of this Agreement. Telstra shall make such process or procedure documents available to DHS upon request.

4.5 **Reporting of Incidents**. Telstra shall report to DHS any information acquired by Telstra or any of its officers, directors, employees, contractors or agents that reasonably indicates:

(a) a breach of this Agreement;

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

(c) access to or disclosure of CPNI or Subscriber Information in violation of federal, state or local law or regulation (except for violations of FCC regulations relating to improper commercial use of CPNI); or

(d) improper access to or disclosure of Classified or Sensitive Information.

This report shall be made in writing by the appropriate Telstra officer to DHS, no later than **ten (10) calendar days** after Telstra acquires information indicating a matter described in this Section. Telstra shall lawfully cooperate in investigating the matters described in this Section. Telstra 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.

4.6 **Access to Information and Facilities**. DHS or its designees may visit, at any time upon reasonable request, any part of Telstra's Domestic Communications Infrastructure and security offices located in the United States 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 DHS to verify compliance with the terms of this Agreement.

4.7 **Access to Personnel**. Upon reasonable notice from DHS, Telstra shall make available for interview any officers or employees of Telstra and any contractor of Telstra located in the United States, who is in a position to provide information to verify compliance with the terms of this Agreement.

4.8 **Annual Report**. On or before the last day of January of each year, a designated senior corporate officer of Telstra shall submit to DHS a report assessing Telstra's compliance with the terms of this Agreement for the preceding calendar year. The report shall include:

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

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

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

(d) identification of any other issues that, to Telstra's knowledge, will or reasonably could affect the effectiveness of or its compliance with this Agreement.

4.9 **Notices**. Effective upon execution of this Agreement by all the Parties, all notices and other communications relating to this Agreement, such as a proposed modification, shall be in writing and shall be deemed given as of the date of receipt and shall be sent by electronic mail (if an email is specified below or in a subsequent notice) and one of the following methods: (a) delivered personally, (b) sent by facsimile, (c) sent by documented overnight courier service, or (d) sent by registered or certified mail, postage prepaid, addressed to the Parties' designated representatives at the addresses shown below, or to such other representatives at such addresses as the Parties may designate in accordance with this Section:

Department of Homeland Security
ip-fcc@dhs.gov

With a copy to:

General Counsel
Telstra Incorporated
40 Wall Street
40th Floor
New York, NY 10005

Kelley Drye & Warren LLP
3050 K Street, N.W., Suite 400
Washington, D.C. 20007-5108
ATTN: Robert J. Aamoth

ARTICLE 5: FCC CONDITION

5.1 **FCC Approval**. Upon the execution of this Agreement by all the Parties, DHS shall, on its own motion at an appropriate time or at the request of Telstra, 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**"), DHS has no objection to the FCC's grant of the pending Application described in the Recitals of this Agreement. This Section is effective upon the Effective Date, provided however that in the case of a material modification or withdrawal of the Application after the execution of this Agreement the effectiveness of this Section may be suspended by DHS and any such FCC filing is subject to the right to object reserved in Section 5.2.

5.2 **Right to Object to Future FCC Filings**. Telstra agrees that in any application or petition by Telstra to the FCC for licensing or other authority filed with or granted by the FCC after the execution of this Agreement, except with respect to *pro forma* assignments or *pro forma* transfers of control, Telstra shall request that the FCC condition the grant of such licensing or other authority on compliance with the terms of this Agreement. Notwithstanding Section 7.9, DHS reserves the right to object, formally or informally, to the grant of any other FCC application or petition of Telstra or its Affiliates for a license or other authorization under Titles II and III of the Communications Act of 1934, as amended, and to seek additional or different terms that would, consistent with the public interest, address any threat to the ability of the United States to enforce the laws, preserve the national security and protect the public safety raised by the services and transactions underlying any such application or petition.

ARTICLE 6: DISPUTES

6.1 **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 Telstra, and the Assistant Secretary for Policy of DHS, or its respective designees, unless DHS believes that important national interests can be protected, or Telstra believes that paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 6.2. If, after meeting with higher authorized officials, any of the Parties determines that further negotiation would be fruitless, then that Party may resort to the remedies set forth in Section 6.2. 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.

6.2 **Enforcement of Agreement**. Subject to Section 6.1 of this Agreement, if any of the Parties believes that any other party has breached or is about to breach this Agreement, that Party may bring an action against the other Party for appropriate judicial relief. Nothing in this Agreement shall limit or affect the right of a U.S. Government Agency to:

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

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

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

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

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

6.3 **Irreparable Injury**. Telstra agrees that the United States would suffer irreparable injury if for any reason Telstra failed to perform any of its obligations under this Agreement, and that monetary relief would not be an adequate remedy. Accordingly, Telstra agrees that, in seeking to enforce this Agreement, DHS shall be entitled, in addition to any other remedy available at law or equity, to specific performance and injunctive or other equitable relief.

6.4 **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.

6.5 **Waiver of Immunity**. Telstra agrees that, to the extent that it or any of its property (including FCC licenses and authorizations and intangible property) is or becomes entitled at any time to any immunity on the ground of sovereignty or otherwise based upon a status as an agency or instrumentality of Government from any legal action, suit or proceeding or from setoff or counterclaim relating to this Agreement, from the jurisdiction of any competent court or the FCC, from service of process, from attachment prior to judgment, from attachment in aid of execution of a judgment, from execution pursuant to a judgment or arbitral award, or from any other legal process in any jurisdiction, it, for itself and its property expressly, irrevocably and unconditionally waives, and agrees not to plead or claim, any such immunity with respect to matters arising with respect to this Agreement or the obligations herein (including any obligation for the payment of money) in any proceeding brought by a U.S. federal, state, or local Government Authority. Telstra agrees that the waiver in this provision is irrevocable and is not subject to withdrawal in any jurisdiction or under any statute, including the Foreign Sovereign Immunities Act, 28 U.S.C. § 1602 *et seq*. The foregoing waiver shall constitute a present waiver of immunity at any time any action is initiated by a U.S. federal, state, or local Government Authority against Telstra with respect to compliance with this Agreement.

6.6 **Forum Selection**. It is agreed by and between the Parties that a civil action among the Parties for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement shall be brought, if at all, in the United States District Court for the District of Columbia.

ARTICLE 7: OTHER

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

7.2 **Headings**. The Article and Section headings and numbering in this Agreement are inserted for convenience only and shall not affect the meaning or interpretation of the terms of this Agreement.

7.3 **Other Laws**. Nothing in this Agreement is intended to limit or constitute a waiver of: (a) any obligation imposed by any U.S. federal, state, or local laws on Telstra, (b) any enforcement authority available under any U.S. or state laws; (c) the sovereign immunity of the United States; or (d) any authority the U.S. Government may possess over the activities or facilities of Telstra located within or outside the United States (including authority pursuant to the International Emergency Economic Powers Act). Nothing in this Agreement is intended to or is to be interpreted to require the Parties to violate any applicable Australian or U.S. law, or to require or compel Telstra to act in a manner that is inconsistent with, or that limits or restricts its ability to comply with, any Lawful Australian Process.

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

7.5 **Non-Parties**. Nothing in this Agreement is intended to confer or does confer any rights on any person other than the Parties and any Government Authorities that utilize Lawful U.S. Process.

7.6 **Entire Agreement; Modifications**. This Agreement constitutes the entire agreement between the Parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations, and discussions, whether oral or written, of the Parties with respect to the subject matter. This Agreement may only be modified by written agreement signed by all of the Parties. DHS agrees to consider promptly and in good faith possible modifications to this Agreement if Telstra believes that the obligations imposed on it 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) calendar days** after approval in writing by the Parties.

7.7 **Severability**. The provisions of this Agreement shall be severable and if any provision thereof or the application of such provision under any circumstances is held invalid by a court of competent jurisdiction, it shall not affect any other provision of this Agreement or the application of any provision thereof.

7.8 **Changes in Circumstances for Telstra**. DHS agrees to negotiate in good faith and promptly with respect to any request by Telstra for relief from application of specific provisions of this Agreement if there is a change in circumstances such that those provisions become unduly burdensome or have a demonstrably adverse effect on Telstra's competitive position.

7.9 **Changes in Circumstances for DHS**. If after the date that all the Parties have executed this Agreement, DHS finds that the terms of this Agreement are inadequate to address national security, law enforcement, or public safety concerns, then the Parties will negotiate in good faith to modify this Agreement to address those concerns.

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

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

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

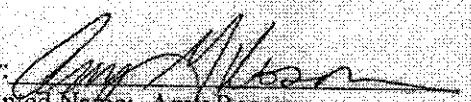
7.13 **Notice of Additional Services**. Telstra shall provide a minimum of **thirty (30) calendar days** advanced notice to DHS in the event that Telstra or any Affiliate changes or intends to change the technical or operational plans set forth in the Recitals to this Agreement such that the material representations made therein are no longer fully accurate, true and complete..

[Signature Pages Follow]

This Agreement is executed on behalf of the Parties:

Telstra Incorporated

Date: 3-06-08

By: 
Printed Name: Amy Rosen
Title: General Counsel

United States **Department of Homeland Security**

Date: _____

By: _____
Printed Name: Stewart A. Baker
Title: Assistant Secretary for Policy

EXHIBIT A
CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that this authorization and any licenses granted thereunder are subject to compliance with the provisions of the agreement (the "**Agreement**") between Telstra and the Department of Homeland Security ("**DHS**"), dated March __, 2008, which Agreement is designed to address national security, law enforcement, and public safety concerns of DHS regarding the authority granted herein. Nothing in the Agreement is intended to limit any obligation imposed by federal law or regulation including, but not limited to, 47 U.S.C. § 222(a) and (c)(1) and the FCC's implementing regulations.

This Agreement is executed on behalf of the Parties:

Telstra Incorporated

Date:_____

By:_____
Printed Name: Amy Rosen
Title: General Counsel

United States Department of Homeland Security

Date: APR 1 6 2008

By:_____
Printed Name: Stewart A. Baker
Title: Assistant Secretary for Policy

EXHIBIT A
CONDITION TO FCC AUTHORIZATION

IT IS FURTHER ORDERED, that this authorization and any licenses granted thereunder are subject to compliance with the provisions of the agreement (the "Agreement") between Telstra and the Department of Homeland Security ("DHS"), dated March __, 2008, which Agreement is designed to address national security, law enforcement, and public safety concerns of DHS regarding the authority granted herein. Nothing in the Agreement is intended to limit any obligation imposed by federal law or regulation including, but not limited to, 47 U.S.C. § 222(a) and (c)(1) and the FCC's implementing regulations.