KELLEY DRYE & WARREN LLP
A LIMITED LIABILITY PARTNERSHIP

1200 19TH STREET, N.W.
SUITE 500
WASHINGTON, D.C. 20036

(202) 955-9600

FACSIMILE
(202) 955-9792
www.kelleydrye.com

NEW YORK, NY
TYSONS CORNER, VA
CHICAGO, IL
STAMFORD, CT
PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES
JAKARTA, INDONESIA
MUMBAI, INDIA

DIRECT LINE: (703) 918-2320
EMAIL: jgriffin@kelleydrye.com

DOCKET FILE COPY ORIGINAL

December 5, 2005

RECEIVED

DEC - 5 2005

Federal Communications Commission
Office of Secretary

BY HAND AND ECFS

Marlene H. Dortch
Secretary
Federal Communications Commission
Office of the Secretary
445-12th Street, SW
Washington, D.C. 20054

Re: In the Matter of Cypress Communications Operating Company, Inc.
Application for Consent to Transfer of Control of a Company Holding an International Authorization and a Blanket Domestic Authorization Pursuant to Section 214 of the Communications Act of 1934, as Amended
File No. ITC-T/C-20041112-00448
WC Docket No. 04-418

Dear Ms Dortch:

On June 28, 2005, in Public Notice DA 05-1850, the Commission granted the application for transfer of control of Cypress Communications Operating Company, Inc. that is captioned above. Grant of authority was conditioned upon compliance with the terms of the June 17, 2005 agreement ("Agreement") by and between Cypress Communications Holding Company, Inc. ("Cypress Holding"); TechInvest Holding Company, Inc. ("THC"); Arcapita Investment Management Limited ("AIM"); Arcapita Bank B.S.C.(c) ("Arcapita"); the U.S. Department of Justice ("DOJ"), including the Federal Bureau of Investigation ("FBI"); the U.S. Department of Homeland Security ("DHS"); and the U.S. Department of the Treasury ("Treasury"). Cypress Holding, THC, AIM, and Arcapita are referred to collectively herein as "Cypress."

By this letter, Cypress requests that the Commission replace the copy of the Agreement that currently resides in the Commission's docket files with the attached copy. The Agreement that is currently on file with the Commission does not accurately reflect the

No. of Copies rec'd 0+5
List A B C D E

intentions of Cypress in adopting the Agreement, and DOJ, FBI, DHS, and Treasury have recently agreed to modify it to reflect Cypress's position. The modification is essentially a matter of form and does not alter the substantive commitments made by Cypress. Accordingly, the Agreement as revised and attached to this letter is deemed by Cypress, DOJ, FBI, DHS, and Treasury to have been made as of the date of the original Agreement, *i.e.*, June 17, 2005. Thus, the attached Agreement is not an amendment to the original Agreement but a substitute for it. The original Agreement is no longer in effect. As such, Cypress believes the public interest would be served if the Commission were to remove the original Agreement from the Commission's files and replace it with the attached version, as it would prevent the public from mistakenly consulting and relying upon a document that is no longer effective.

I am authorized to state that DHS, DOJ, FBI, and Treasury have no objection to this request. Please contact the undersigned counsel if you have any questions regarding this matter.

Sincerely,

Joan M. Griffin

cc: David Krech
Alex Johns
Susan O'Connell
Jodi Cooper
Louis Brenner (DHS)
John LoGalbo (DOJ)
Joan Koetze (Treasury)

AGREEMENT

This AGREEMENT (the "Agreement") is deemed executed as of June 17, 2005, by and between Cypress Communications Holding Company, Inc. ("Cypress"); TechInvest Holding Company, Inc. ("THC"); Arcapita Investment Management Limited ("AIM"); and Arcapita Bank B.S.C.(c) ("Arcapita"), on the one hand; and the U.S. Department of Justice ("DOJ"), including the Federal Bureau of Investigation ("FBI"); the U.S. Department of Homeland Security ("DHS"); and the U.S. Department of the Treasury ("Treasury"), on the other hand (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, Presidential Decision Directive 63, Critical Infrastructure Protection, and Presidential Homeland Security 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, Cypress has an obligation to protect from unauthorized disclosure the contents of wire and electronic communications;

WHEREAS, Cypress is a provider of bundled telecommunications services (including local, long distance, and international telecommunications services; high-speed Internet connectivity; e-mail services; fully-managed firewall services; web hosting; virtual private networks; feature-rich digital desktop stations; calling cards; audio and web conferencing; and digital business television) to small and medium-sized businesses located in multi-tenant commercial office buildings in major metropolitan markets in the U.S.;

WHEREAS, Cypress may provide or facilitate electronic communication services, remote computing services, and interactive computer services, all of which are subject to U.S. privacy and electronic surveillance laws;

WHEREAS, Cypress has or will have direct physical or electronic access to certain customer facilities, including numerous buildings in numerous U.S. cities containing the servers,

storage media, network connections, bandwidth transport and firewalls Cypress works with in providing its services in those customer facilities, and thereby Cypress also has or will have direct physical or electronic access to a variety of customer and end-user information that is subject to U.S. privacy and electronic surveillance laws;

WHEREAS, Cypress and THC have filed with the Federal Communications Commission ("FCC") an application (including amendments) under Section 214 of the Communications Act of 1934, as amended, seeking authority to transfer control of Cypress Communications Operating Company, Inc. to THC, such application having been assigned FCC File No. ITC-T/C-20041112-00448 and WC Docket No. 04-417 by the FCC (the "FCC Application");

WHEREAS, as disclosed to the FCC, THC is an indirect subsidiary of Arcapita, a joint stock company organized under the laws of the Kingdom of Bahrain;

WHEREAS, as disclosed to the FCC, (a) approximately 75.96 percent of the non-voting common stock of THC will be held by four (4) offshore investment companies – TechAccess Capital Limited, TechShield Capital Limited, TechNet Capital Limited, and TechTVCapital Limited (collectively, the "Non-Voting Cayman Entities") – each of which is a wholly-owned subsidiary of Arcapita Investment Holdings Limited ("AIH"), which is itself a wholly-owned subsidiary of Arcapita; (b) approximately 3.28 percent of the non-voting common stock of THC will be held by Arcapita Incentive Plan Limited ("AIP"); and (c) approximately 18.76 percent of the non-voting common stock of THC will be held by TechInvest Holdings Limited ("THL"), a wholly-owned subsidiary of Arcapita;

WHEREAS, as disclosed to the FCC, 100 percent of the voting common stock of THC, representing less than two (2) percent of the equity interest in THC, will be held by five (5) U.S. citizens in equal shares (the "5 Voting Stockholders;" each, a "Voting Stockholder");

WHEREAS, as disclosed to the FCC, AIM (a wholly-owned subsidiary of Arcapita) will have a call option on the voting common stock of THC held by the 5 Voting Stockholders that can be exercised by AIM under the circumstances set forth in this Agreement for the nominal value of the shares (the "Call Option");

WHEREAS, the FCC's grant of the FCC Application may be made subject to conditions relating to national security, law enforcement, and public safety;

WHEREAS, by Executive Order 12661, the President of the United States, pursuant to Section 721 of the Defense Production Act, as amended, has authorized the Committee on Foreign Investment in the United States ("CFIUS") to review, for national security purposes, foreign acquisitions of U.S. companies (*see* 50 App. U.S.C. § 2170 and 31 C.F.R. Part 800);

WHEREAS, Cypress and THC collectively have submitted a voluntary notice to CFIUS regarding the proposed acquisition of Cypress, and Arcapita, AIM, THC, and Cypress have agreed to enter into this Agreement and the associated financial compliance measures agreement as specific consideration for the obligations accepted herein by DHS, DOJ, FBI, and Treasury, and to address national security issues that these agencies might raise, including in the CFIUS review process, and to request that the FCC condition the authorization granted by the FCC on

its compliance with this Agreement;

WHEREAS, representatives of Arcapita, THC, and Cypress have held discussions with U.S. Government officials. During those discussions, Arcapita, THC, and Cypress have represented that: (a) no Party has any present plans, nor is any Party aware of present plans of any other entity, that would result in Cypress providing Domestic Communications through facilities located outside the United States; and (b) no Party has any present plans, nor is any Party aware of present plans of any other entity, that would result in Cypress providing Domestic Communications or Hosting Services in the United States through any Affiliate other than Cypress or its subsidiaries, divisions, departments, or branches; and Arcapita and THC have represented that: (a) two separate but related shareholders – Jasmine Quadrilateral Investment Corporation, a corporation organized under the laws of the British Virgin Islands, and Al-Jomaih Company Limited, a limited liability company organized under the laws of Saudi Arabia -- hold in total approximately 10.5 percent of the ownership interest in Arcapita; (b) the Securities House K.S.C.C., a corporation organized under the laws of Kuwait, holds approximately 5 percent of the ownership interest in Arcapita; (c) the employees of Arcapita and its subsidiaries collectively and indirectly hold approximately 11 percent of the ownership interest in Arcapita; (d) no shareholder or group of shareholders holds a controlling interest in Arcapita, and there are no voting or other agreements that would give control to one shareholder or group of shareholders; (e) following consummation of the transactions described in the FCC Application, no person or entity other than (i) Arcapita or its Affiliates or (ii) the shareholders listed in (a) and (b) above will hold interests sufficient to constitute a 5 percent or greater equity interest in Cypress, determined in accordance with the FCC's ownership attribution rules set forth in 47 CFR § 63.09; (f) following consummation of the transactions described in the FCC Application, no person or entity other than Arcapita or its Affiliates will hold interests sufficient to confer the ability to Control Cypress; and (g) no Foreign government holds an ownership interest in Arcapita;

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 "5 Voting Stockholders" means the five (5) U.S. citizens that will hold 100 percent of the voting common stock of THC in equal shares. Each such individual is a "Voting Stockholder."

1.2 "Affiliate" (a) with respect to Cypress, means any entity that Cypress Controls; (b) with respect to THC, means any entity that THC Controls or is Controlled by; (c) with respect to AIM, means Arcapita, AIH, the Non-Voting Cayman Entities, THC, Arcapita Employee Stock Option Plan I Limited, Arcapita Employee Stock Option Plan II Limited, any entity whose ownership interests are held only by the employees of Arcapita or its subsidiaries (including but not limited to AIP), and any entity that is a wholly-owned subsidiary of AIM; and (d) with respect to Arcapita, means AIM, AIH, the Non-Voting Cayman Entities, THC, Arcapita Employee Stock Option Plan I Limited, Arcapita Employee Stock Option Plan II Limited, any

entity whose ownership interests are held only by the employees of Arcapita or its subsidiaries (including but not limited to AIP), any entity that Controls Arcapita, and any entity that is a wholly-owned subsidiary of Arcapita, but does not include Cypress.

1.3 "AIH" means Arcapita Investment Holdings Limited, a Cayman Islands company limited by shares that was formerly known as First Islamic Investment Holdings Limited and that is a wholly-owned subsidiary of Arcapita.

1.4 "AIM" means Arcapita Investment Management Limited, a Cayman Islands company limited by shares that was formerly known as First Islamic Investment Management Limited.

1.5 "AIP" means Arcapita Incentive Plan Limited, a Cayman Islands company limited by shares whose shares are held only by the employees of Arcapita or its subsidiaries and that was formerly known as FIIP Limited.

1.6 "Arcapita" means Arcapita Bank B.S.C. (c), a joint stock company organized under the laws of the Kingdom of Bahrain that was formerly known as First Islamic Investment Bank, B.S.C. (c).

1.7 "Arcapita Employee Stock Option Plan I Limited" and "Arcapita Employee Stock Option Plan II Limited" are each a shareholder of Arcapita through which management's interest in Arcapita is held.

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

1.9 "Call Option" means the call option held by AIM on the voting common stock of THC that can be exercised by AIM for the nominal value of the shares in accordance with the requirements of Section 5.15 *infra*.

1.10 "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.

1.11 "Contract," "Contracted," or "Contracting" means an agreement between Cypress and an individual or entity that Arcapita, AIM, THC, or Cypress does not Control to perform, in part or in whole, the ordinary operation of Cypress's business and the obligations of Cypress under this Agreement. "Contract," "Contracted," or "Contracting" as used in this Agreement includes outsourcing or sub-contracting.

1.12 "Contractor" means an individual or entity that is not Controlled by Arcapita, AIM, THC, or Cypress and that has entered into an agreement with Cypress to perform duties described in Section 1.11 above.

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

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

(b) the dissolution of the entity;

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

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

(e) the amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in Section 1.13(a) through (d); or

(f) the obligations under this Agreement.

1.14 "Customer Identifying Information" means information that includes but is not limited to: customer identities, customer street addresses and room or suite numbers, and customer phone numbers, web sites, email addresses or other logical addresses.

1.15 "Cyber Attacks" includes, but is not limited to, the malicious insertion of malicious code, insertion and/or transmittal of viruses or worms, denial of service attacks, use of botnets, "phishing," identity theft, alteration or deletion of data, redirection or misdirection of Internet page requests, and establishment of unauthorized covert communications channels.

1.16 "Cypress" means Cypress Communications Holding Co., Inc., a Delaware corporation, and its Affiliates.

1.17 "Cypress Employee" means, for purposes of this Agreement, any person that is an employee, officer, or director of Cypress or its Affiliates. An "employee" means a person who is hired by another to perform a service for wages or salary and is under the other's direction and control.

1.18 "Data Centers" means (a) equipment (including firmware, software and upgrades), facilities, and premises used by (or on behalf of) Cypress 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 Cypress that is leased or owned by a Hosting Services customer.

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

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

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

1.22 "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.

1.23 "Domestic Communications Infrastructure" means (a) transmission, switching, bridging and routing equipment (including software and upgrades) used by or on behalf of Cypress to provide, process, direct, control, supervise or manage Domestic Communications; (b) facilities and equipment used by or on behalf of Cypress that are physically located in the United States; and (c) facilities used by or on behalf of Cypress 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 affiliated with Arcapita, THC, or Cypress and that are:

(1) interconnecting communications providers; or

(2) providers of services or content that are

(A) accessible using the communications services of Cypress or its Affiliates, and

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

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

1.24 "Effective Date" means the date on which the transactions described in the Merger Agreement are consummated.

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

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

1.27 "FBI" means the Federal Bureau of Investigation.

1.28 "FCC" means the Federal Communications Commission.

1.29 "FCC Application" means the application (including amendments) in FCC File No. ITC-T/C-20041112-00448 and WC Docket No. 04-417 under Section 214 of the Communications Act of 1934, as amended, seeking authority to transfer control of Cypress Communications Operating Company, Inc. to THC.

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

1.31 "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.

1.32. "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 Cypress or any of its subsidiaries, affiliates, divisions, departments, branches or other components.

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

1.34 "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.

1.35 "Merger Agreement" means the Agreement and Plan of Merger by and between TechInvest Acquisition, Inc., THC and Cypress, dated November 5, 2004.

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

1.37 "Non-Voting Cayman Entities" means TechAccess Capital Limited, TechShield Capital Limited, TechNet Capital Limited, and TechTVCapital Limited, all Cayman Island companies limited by shares.

1.38 "Non-U.S. Person" means a person who is not a citizen of the United States. For the purposes of this Agreement, Cypress Employees who are not U.S. citizens and who are employed directly by Cypress shall not be considered Non-U.S. Persons.

1.39 "Non-Voting Stockholder" means (a) any shareholder in Arcapita, unless that person or entity is also an employee of Arcapita or its Affiliates, a member of the Board of Directors of Arcapita or its Affiliates, or an entity whose voting or ownership interests are held only by the employees of Arcapita or its subsidiaries, or (b) any shareholder in the Non-Voting Cayman Entities, unless that shareholder is Arcapita or its Affiliates. A Non-Voting Stockholder is a passive investor to the extent described in the FCC Application.

1.40 "OFAC List" means the list of Specially Designated Nationals and Blocked Persons issued by the Office of Foreign Assets Control, U.S. Department of Treasury.

1.41 "Screened Contractor Personnel" shall have the meaning set forth in Section 3.16 of this Agreement.

1.42 "Screened Cypress Personnel" shall have the meaning set forth in Section 3.16 of this Agreement.

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

1.44 "*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).

1.45 "Security Officer" means the person designated pursuant to Section 3.11 of this Agreement.

1.46 "Sensitive Information" means information that is not Classified Information regarding (a) the persons or facilities that are the subjects of Lawful U.S. Process, (b) the identity of the government agency or agencies serving such Lawful U.S. Process, (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance pursuant to Lawful U.S. Process, (d) the means of carrying out Electronic Surveillance pursuant to Lawful U.S. Process, (e) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process, and (f) other information that is not Classified Information 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." The designation of "Sensitive Information" in this paragraph may reference "Official Use Only," "Limited Official Use Only," "Law Enforcement Sensitive," "Sensitive Security Information," or other similar terms, and shall be deemed "Sensitive Information" for purposes of this Agreement. Cypress 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 Cypress's favor.

1.47 "Subscriber Information" means information relating to subscribers or customers of Cypress 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.

1.48 "THC" means TechInvest Holding Company, Inc., a Delaware corporation.

1.49 "THL" means TechInvest Holdings Limited, a Cayman Islands company limited by shares and a subsidiary of Arcapita.

1.50 "Transactional Data" means:

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

(b) any information possessed by Cypress, or an entity acting on behalf of Cypress, 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 (d) below;

(c) the time, date, size, or volume of data transfers, duration, domain names, Media Access Control ("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, including electronic mail headers showing From: and To: addresses; and

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

The term includes all records or other information of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c)(1) and (d) but does not include the content of any communication. The phrase "on behalf of" as used in this Section does not include entities with which Cypress or any of its Affiliates has contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree.

1.51 "Treasury" means the United States Department of the Treasury.

1.52 "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 jurisdictions of the United States.

1.53. "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.

1.54. "U.S. Hosting Services Customer" is a customer or subscriber that receives Hosting Services from Cypress 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.

1.56 "Voting Stockholder" means one of the five (5) U.S. citizens that will hold 100 percent of the voting common stock of THC in equal shares.

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

1.58 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 terms. 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 DHS, DOJ, and FBI in writing:

(a) all Domestic Communications Infrastructure shall at all times be located in the United States and will be directed, controlled, supervised and managed by Cypress;

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

(c) Cypress shall use industry best practices (*e.g.*, Network Reliability Interoperability Council – NRIC series for service providers or ISO information security standards) for monitoring both signaling and traffic for unauthorized access, network

intrusion, Cyber Attacks, and other malicious activity. Such practices, including the timing of the implementation of any such practices, shall be jointly determined by Cypress, DHS, and FBI.

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

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

(b) Cypress 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 Cypress and physically located in the United States, from which Electronic Surveillance can be conducted in a timely manner. Cypress will provide technical or other assistance to facilitate such Electronic Surveillance.

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

(a) Lawful U.S. Process;
(b) the orders of the President in the exercise of his/her authority under § 706 of the Communications Act of 1934, as amended, (47 U.S.C. § 606), and under § 302(e) of the Aviation Act of 1958 (49 U.S.C. § 40107(b)) and Executive Order 11161 (as amended by Executive Order 11382); and
(c) National Security and Emergency Preparedness rules, regulations and orders issued pursuant to the Communications Act of 1934, as amended (47 U.S.C. § 151 et seq.).

2.4 Information Storage and Access. Cypress, effective as of June 17, 2005, shall store exclusively in the United States the following:

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

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

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

(f) Network Management Information; and

(g) Customer Identifying Information.

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

2.5. U.S. Hosting Data Storage and Access. Cypress 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 Cypress-controlled space in a Data Center. Cypress shall ensure that such data shall not be stored outside of the United States. In any event, Cypress 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. Cypress shall store for at least two years all billing records described in Section 2.4(e) above, and all billing records relating to U.S. Hosting Services, and shall make such records available in the U.S. Nothing in this paragraph shall require Cypress to store such records for longer than two years.

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 Government Authority within the United States to preserve any information in the possession, custody, or control of Cypress that is listed in Section 2.4 above or any U.S. Hosting Data, Cypress shall store such information or U.S. Hosting Data in the United States.

2.8 Compliance with U.S. Law. Nothing in this Agreement shall excuse Cypress from its obligation to comply with U.S. legal requirements, including but not limited to those requiring the retention, preservation, or production of information, records or data, those not to unlawfully intercept telecommunications or unlawfully access stored telecommunications, Chapters 119 and 121, of Title 18, United States Code, and the requirements of the Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1001, *et seq.* Similarly, in any action to enforce Lawful U.S. Process, Cypress has not waived any legal right it might have to resist such process.

2.9 Routing of Domestic Communications and U.S. Hosting Data. Cypress shall not route Domestic Communications or U.S. Hosting Data outside the United States.

2.10 CPNI. Cypress 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).

2.11 Storage of Protected Information. The storage of Classified and Sensitive Information by Cypress or its contractors at any location outside of the United States is prohibited, unless the storage is in an appropriately secured location within the offices of a U.S. military facility, a U.S. Embassy or Consulate or other U.S. Government Authority.

ARTICLE 3: SECURITY

3.1 Measures to Prevent Improper Use or Access. Cypress shall take all reasonable measures to prevent physical and virtual or remote access to (i) Domestic Communications Infrastructure and Data Centers, including Domestic Communications Infrastructure and Data Centers located in customer buildings, offices, or premises and (ii) customer buildings, offices, and premises that contain Domestic Communications Infrastructure or Data Centers, to conduct Cyber Attacks, Electronic Surveillance, or to obtain, disclose or use Domestic Communications, U.S. Hosting Data, Classified Information, or Sensitive Information, in violation of any U.S. federal, state, or local laws or the terms of this Agreement. These measures shall include creating and complying with detailed technical, organizational, operational, and personnel controls, written policies and procedures, necessary implementation plans, and physical security measures; they shall also include special measures tailored to prevent improper use and access in the context of outsourcing and joint ventures. Cypress shall submit these written policies and procedures to prevent improper access and use to DHS and FBI within ninety (90) days after the Effective Date for review and approval. If DHS or FBI disapproves the written policies and procedures, then Cypress shall meet and confer with the Party or Parties involved and shall modify the terms appropriately. DHS, DOJ, and FBI acknowledge that Cypress does not control access to its customers' premises or the buildings or offices in which its customers are located and, therefore, that Cypress has limited ability to prevent or control physical access to public areas of those buildings, offices, and premises. With respect to Cypress Employees and other persons or entities, including Contractors, acting on behalf of Cypress, Cypress shall permit only Screened Cypress Personnel or Screened Contractor Personnel to access (i) Domestic Communications Infrastructure or Data Centers or (ii) any customer building, office, or premise in which Domestic Communications Infrastructure or Data Center is located.

3.2 Visitation Policy. No later than ninety (90) days after the Effective Date, Cypress shall submit for DHS, DOJ, and FBI approval a visitation policy. The policy shall apply to all visits by Non-U.S. Persons to (i) Domestic Communications Infrastructure and Data Centers and (ii) any customer building, office, or premise in which Domestic Communications Infrastructure or Data Centers are located, except for Routine Business Visits by Non-U.S. Persons to Cypress Offices, as defined in Section 3.3. The visitation policy shall require that:

(a) The Security Officer shall review and either approve or deny on security or related grounds any requests for visits by Non-U.S. Persons to any Domestic Communications Infrastructure or Data Center (provided that, with respect to

carrier hotels and other shared facilities, the policy will apply solely to that portion of the facility controlled by Cypress).

(b) A request for approval of a visit must be submitted to the Security Officer in writing or electronically no less than seven (7) days prior to the date of the proposed visit. If a written or electronic request cannot be provided within seven (7) days before the proposed visit because of an unforeseen exigency, the request may be communicated via telephone to the Security Officer and immediately confirmed in writing or electronically; however the Security Officer may refuse to accept any request submitted fewer 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.

(c) Every request shall set forth the purpose and justification for the visit in sufficient detail to enable the Security Officer to make an informed decision concerning the appropriateness of the visit. The Security Officer may refuse to accept any request due to lack of information. Each visit must be reviewed even for persons approved for prior visits. For multiple visits for the same purpose, the Security Officer may approve such visits by the same person or persons for a period not to exceed seven (7) days.

(d) After evaluating a request, the Security Officer shall, as soon as practicable, either approve or disapprove the request, pending the submission of additional information from the requester. The Security Officer shall inform the requester of the decision at least one (1) day prior to the requester's proposed visit. The Security Officer's decision shall also be confirmed in writing or electronically as promptly as possible.

(e) The Security Officer shall keep a record of all visit requests, including the decision to approve or disapprove, and of all consummated visits, including the name, address, business affiliation, citizenship, and dates of birth of the vistor(s) and the Cypress personnel involved. In addition, a chronological file of all documents associated with such visits shall be maintained by Cypress for at least two (2) years from the date of the visits.

(f) All visitors shall be escorted at all times by a Cypress Employee, and visits shall be subject to conditions determined by the Security Officer that are commensurate with the place and purpose of the visit.

3.3 Routine Business Visits by Non-U.S. Persons to Cypress Offices. Notwithstanding Section 3.2, Routine Business Visits by Non-U.S. Persons may occur without prior approval by the Security Officer. "Routine Business Visits by Non-U.S. Persons to Cypress Offices": (1) are made in connection with the regular day-to-day business operations of Cypress; (2) do not involve the transfer or receipt of any information regarding the security of the facilities; (3) pertain only to the commercial aspects of Cypress business; (4) are to (a) the corporate headquarters of Cypress located at 15 Piedmont Center, Atlanta, Georgia 30305, or any subsequent corporate headquarters offices identified by Cypress with notice to DHS, DOJ, and

FBI or (b) the offices listed on Schedule 3.3 to this Agreement and any future offices identified by Cypress with notice to DHS, DOJ, and FBI; and (5) do not involve access to any Domestic Communications Infrastructure or Data Centers. In addition, notwithstanding (1)-(5) in this Section 3.3, visits by Screened Cypress Personnel and Screened Contractor Personnel who are not U.S. citizens and are for the purposes of performing installation, maintenance, repair, and customer service functions on behalf of Cypress at Cypress customer buildings, offices, and premises shall be treated as if they were Routine Business Visits by Non-U.S. Persons to Cypress Offices. Records of such visits shall be maintained by Cypress for at least two (2) years from the date of the visits. Routine Business Visits by Non-U.S. Persons to Cypress Offices may include:

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

(b) visits by customers or commercial suppliers regarding, for example, solicitation of orders, price quotes, or the provision of products or services; and

(c) visits concerning fiscal, financial, or legal matters.

The visitation policy established under Section 3.2 may elaborate on the types of visits that qualify as Routine Business Visits by Non-U.S. Persons to Cypress Offices.

3.3A Records of Communications with Certain Non-U.S. Persons. Cypress shall take all reasonable efforts to maintain a full and complete record of every electronic or written communication by the Cypress directors, officers, employees, and agents with those Non-U.S. Persons that are known by Cypress to be Non-U.S. Persons where the communication is related to security procedures and policy, Domestic Communications Infrastructure, Data Centers, or specific U.S. customers. Such records shall include the names of the correspondents and their business affiliations as well as the substance of the communications. These records shall be maintained for a period of three (3) years by the Security Officer for provision at the request of the third-party auditor identified pursuant to Section 5.7 below, or of DHS, DOJ, or FBI.

3.4 Access to Data by Foreign Entities or Government Authorities. Cypress 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 or on behalf of Cypress in the United States to any person if the purpose of such access is to respond to the legal process or the request of or on behalf of a foreign individual or entity or a foreign government, identified representative, component or subdivision thereof without the express written consent of DHS, DOJ, and FBI or the authorization of a court of competent jurisdiction in the United States; provided, however, that nothing in this section shall require any prior notice or approval for Cypress to disclose or provide access to its subscribers or customers to their Domestic Communications, U.S. Hosting Data, Call Associated Data, Transactional Data, or Subscriber Information. Any such requests or submission of legal process shall be reported to DHS, DOJ, and FBI 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. Cypress shall take reasonable measures to ensure that the Security Officer will promptly learn of all such requests or submission of legal process.

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

(a) Classified or Sensitive Information; or

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

to any foreign government, identified representative, component or subdivision thereof without satisfying all applicable U.S. federal, state and local legal requirements, and obtaining the express written consent of DHS, DOJ, and FBI 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 Cypress for the communications, data or information identified in this Section 3.5 that is maintained by Cypress shall be referred to DHS, DOJ, and FBI as soon as possible and in no event later than five (5) business days after such request or legal process, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. Cypress 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 [Intentionally Blank]

3.7 Disclosure to Non-Voting Stockholders or Arcapita Employees. Notwithstanding any other provision of this Agreement,

(a) Cypress shall not, directly or indirectly, disclose or permit disclosure of, or provide access to:

(i) Domestic Communications, U.S. Hosting Data, Call Associated Data, Transactional Data, or Subscriber Information;

(ii) Domestic Communications Infrastructure, Network Management Information, or Data Centers;

(iii) Customer Identifying Information; or

(iv) Classified or Sensitive Information,

to any Non-Voting Stockholder or other person who is an employee, officer, board member, shareholder, or investor of Arcapita or its Affiliates; and

(b) Cypress may utilize the following exception to Section 3.7(a) solely with respect to providing disclosure or access to certain Customer Identifying Information to certain persons on the terms described below:

(i) a member of the Cypress Board of Directors who is a U.S. citizen may have access to specific Customer Identifying Information; and

(ii) a member of the AIM Board of Directors who is a U.S. citizen may have access solely to a point of contact for customers of Cypress (unless DHS, DOJ, FBI, and Treasury are specifically notified that Cypress believes there is a need to share additional information with the U.S. citizen AIM board member(s) and approve of such disclosure in advance),

provided Cypress permits such access or disclosure under Section 3.7(b)(i) or (ii) only if:

(I) such member(s) of the Cypress Board of Directors and/or AIM Board of Directors sign a non-disclosure agreement that prohibits the member from providing the specific Customer Identifying Information or point of contact to any person (including a Non-Voting Stockholder or other person who is an employee, officer, board member, shareholder, or investor of Arcapita or its Affiliates other than Cypress) other than a person Controlled by Cypress, the customer itself, or (in the case of a member of the Cypress Board of Directors) another member of the Cypress Board of Directors who is a U.S. citizen and has also signed a non-disclosure agreement of the type discussed in this section;

(II) Cypress keeps a record of any such disclosure and makes it available to DHS, DOJ, FBI or Treasury upon request, and

(III) such disclosure shall not serve as an exception to obligations of Cypress contained in Article 2 of this Agreement, including the storage of information.

3.8 Security of Lawful U.S. Process. Cypress 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. Information concerning Lawful U.S. Process, Classified Information, and Sensitive Information shall be under the custody and control of the Security Officer. Cypress shall ensure that knowledge of the existence of any Lawful U.S. Process served upon Cypress is limited to the Security Officer and those individuals whose assistance is strictly necessary to ensure Cypress's compliance. The Security Officer shall maintain a list of the names, dates and places of birth, and current addresses of each such individual, and the list shall include but not be limited to any technicians assisting in the implementation of electronic surveillance. The Security Officer shall make the list available upon request to any law enforcement agency or officer seeking compliance with Lawful U.S. Process. Cypress will strictly comply with any request by a law enforcement agency or officer to exclude particular individuals from assisting in, or having knowledge of the existence of, Lawful U.S. Process.

3.9 Points of Contact. Within five (5) business days after the Effective Date, Cypress shall designate in writing to DHS, DOJ, and FBI, at least three nominees who are resident U.S. citizens already holding U.S. security clearances granted in accordance with the requirements of Executive Order 12968 (which may include interim clearances) or who Cypress has a reasonable basis to believe are eligible to receive such security clearances to serve as a primary and at least 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 on behalf of Cypress. Cypress shall provide in writing, in accordance with Section 5.14 of this Agreement, to DHS, DOJ, and FBI, the name and contact information for each point of contact. The points of contact shall be assigned to Cypress's security office(s) in the United States, shall be available twenty-four (24) hours per day, seven (7) days per week, and shall be responsible for accepting service and maintaining the security of Classified and Sensitive Information and any Lawful U.S. Process in accordance with the requirements of U.S. law and this Agreement. The points of contact shall undergo the screening process defined in Section 3.16 of this Agreement. If there is any change in the designated points of contact, Cypress shall notify DHS, DOJ, and FBI immediately in writing, providing updated identifying and contact information. Cypress shall comply with any request by a Government Authority in the United States that a background check and/or security clearance process be completed for a designated point of contact.

3.10 Information Security Plan. Not later than ninety (90) days after the Effective Date, Cypress shall develop, document, implement, and maintain an information security plan to:

(a) ensure that the disclosure of or access to Classified or Sensitive Information is limited to those who have the appropriate security clearances and authority;
(b) take appropriate measures to prevent unauthorized access to data or to the section(s), if any, of the facilities that might contain Classified or Sensitive Information;
(c) assign U.S. citizens to positions for which screening is contemplated pursuant to Section 3.16;
(d) upon written request from DHS, DOJ, or FBI, provide the name, social security number and date of birth of each person who regularly handles or deals with Sensitive Information;
(e) require that personnel handling Classified Information shall have been granted appropriate security clearances pursuant to Executive Order 12968;
(f) provide that the points of contact described in Section 3.9 shall have sufficient authority over any of Cypress'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 authorities and the terms of this Agreement;
(g) maintain appropriately secure facilities (*e.g.*, offices) within the United States for the handling and storage of any Classified or Sensitive Information;
(h) establish a formal incident response capability with reference to OMB Circular A-130 and NIST Special Publications 800-18, 800-47 and 800-61; and
(i) identify the types of positions that require screening pursuant to Section 3.16, the required rigor of such screening by type of position, and the criteria by which Cypress will accept or reject screened persons ("Screened Personnel").

3.11 Security Officer Responsibilities and Duties. Within fourteen (14) calendar days after the Effective Date, Cypress shall designate, from among the points of contact selected pursuant to Section 3.9, a Security Officer within the United States with the primary responsibility for carrying out Cypress's obligations under Articles 2, 3 and 5 of this Agreement.

3.12 Nondisclosure of Protected Data. The Security Officer shall not directly or indirectly disclose information concerning Lawful U.S. Process, Classified Information, or Sensitive Information to any third party, or officer, director, shareholder, employee, agent, or contractor of Arcapita, AIM, THC, or Cypress including those who serve in a supervisory, managerial or officer role with respect to the Security Officer, unless disclosure has been approved by prior written consent obtained from DHS, DOJ, and FBI, 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. Any such disclosure shall be in strict compliance with Section 3.8 of this Agreement.

3.13 Establishment of Security Committee of Cypress Board. Not later than ninety (90) days after the Effective Date, the Board of Directors of Cypress shall establish a Security Committee to oversee security matters within Cypress. The Security Committee shall be composed of 2 directors who are U.S. citizens; who shall already possess U.S. security clearances pursuant to Executive Order 12968, or who Cypress has a reasonable basis to believe are eligible to receive such clearances; and who satisfy the independent director requirements of the New York Stock Exchange, unless otherwise agreed by DOJ, DHS, and FBI. 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, DHS, and FBI approval, or pursuant to an interim security clearance. Notice of the proposed appointment of a Security Director, along with appropriate identifying information, shall be provided in writing to DOJ, FBI, and DHS by Cypress. DOJ, FBI, and DHS shall have the opportunity to review and disapprove the proposed appointment of a Security Director within thirty (30) days of receiving notice of the proposed appointment (or such later timeframe as agreed to by the Parties). If DOJ, FBI or DHS objects to the appointment of an individual as Security Director within the 30-day or later agreed timeframe, the proposed appointment shall be withdrawn and a different candidate shall be proposed. DOJ, FBI or DHS may at any time request that a background investigation and/or security clearance process be completed for a Security Director. Cypress shall ensure that any Security Director cooperates fully with any background investigation or security clearance process, and will remove a Security Director who is determined pursuant to such investigation or process to be unsuitable by DOJ, FBI, or DHS. The Security Committee shall have ultimate authority over the establishment, oversight and evolution of policies, practices and procedures related to or materially affecting Cypress's compliance with its obligations under Articles 2, 3 and 5 of this Agreement. To perform its function, the Security Committee shall, among other things, receive reports from the Security Officer on Cypress'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 5.7 of this Agreement and the annual report on compliance issued pursuant to Section 5.11 of this Agreement.

3.14 Notice of Obligations. Cypress shall instruct all officers, directors, employees, contractors, and agents as to Cypress's obligations under this Agreement, including the individuals' duty to report any violation of this Agreement and the reporting requirements in

Sections 5.2, 5.4, 5.5, and 5.8 of this Agreement, and shall issue periodic reminders to them of such obligations.

3.15 Access to Classified or Sensitive Information. Nothing contained in this Agreement shall limit or affect the authority of the U.S. Government to deny, limit or revoke Cypress's access to Classified Information or Sensitive Information under the U.S. Government's jurisdiction.

3.16 Screening of Personnel. Within ninety (90) days after the Effective Date of the Agreement, Cypress shall implement a thorough screening process through the Security Officer or a reputable third party to ensure that all Cypress Employees are subjected to screening commensurate with their job positions and responsibilities and the potential risk posed to national security, law enforcement, and public safety as a result of their access to Domestic Communications, Domestic Communications Infrastructure, or Data Centers. In addition, individuals utilized by Cypress Contractors for the purpose of performing installation, maintenance, repair, and customer service functions on behalf of Cypress and have access to Domestic Communications, Domestic Communications Infrastructure, Data Centers, or the buildings, offices, and premises in which Cypress's customers are located shall be screened pursuant to the policies and procedures established under this Section 3.16 (such personnel are referred to as "Screened Contractor Personnel"). In general, stricter screening procedures may be applied to (1) all individuals who perform security functions; (2) individuals whose job positions and responsibilities enable them to access Domestic Communications, Data Centers, or Domestic Communications Infrastructure that enables those persons to monitor the content of Wire or Electronic Communications (including in electronic storage) or to access U.S. Hosting Data, Network Management Information, Transactional Data, Call Associated Data, or Subscriber Information; (3) individuals whose job positions and responsibilities result in their visiting customer premises or buildings or other facilities occupied by a Cypress customer; (4) individuals who have access to Sensitive Information; (5) Screened Contractor Personnel; and (6) other Cypress Employees mutually agreed to by the Parties. Cypress Employees, including those in these classifications, shall be considered "Screened Cypress Personnel."

(a) Cypress shall consult with the DHS, DOJ, and FBI on the screening procedures required under this Section. DHS, DOJ, and FBI shall take into consideration Cypress's current and proposed screening procedures in its determination of the required screening procedures. Screening procedures may specifically include a background and financial investigation and a criminal record check. Stricter screening procedures shall be consistent with the guidance to U.S. government agencies under Executive Order 10450. The Parties shall consult on whether it is appropriate to obtain security clearances for any positions not currently required to hold them that are assessed at the highest level of risk. The Parties shall consult on whether a financial credit check and criminal record check alone suffice for screening the categories of employees at the lowest level of risk.

(b) Cypress shall provide to DHS, DOJ, and FBI a list of categories of job positions subject to screening under this Section and a proposal for the level of screening Cypress recommends for each category. The Parties shall categorize the job positions according to the risk posed to national security by the level of access of such job positions to Domestic Communications, Data Centers, and Domestic

Communications Infrastructure and shall agree upon the level of screening necessary to satisfy this section for each category. Upon request, Cypress shall provide to the investigation services of DHS, DOJ, or FBI, or in the alternative, to the investigation service of the United States Office of Personnel Management ("OPM"), all the information it collects in its screening process of each candidate, including but not limited to the names, dates of birth, citizenship, addresses, and telephone numbers of all persons holding each position subject to the foregoing screening procedures. Current Cypress Employees in these positions and prospective candidates for these positions shall be informed, and shall consent, that the information collected during the screening process may be provided to the U.S. government. Current and newly hired Cypress Employees subject to stricter screening procedures will be required to sign a non-disclosure agreement approved in advance by DHS, DOJ, and FBI. If DHS, DOJ, or FBI so desires, it may on its own, or through OPM's investigation service, conduct further background checks for personnel subject to stricter screening procedures. Cypress will cooperate with any such further background checks.

(c) Cypress shall immediately notify the Security Committee whenever any Cypress Employee, prospective Cypress Employee, Contractor, or prospective Contractor is deemed unsuitable due to any information developed during the screening process. In the event that the Security Committee determines in its reasonable judgment that any Cypress Employee, prospective Cypress Employee, Contractor, or prospective Contractor presents a potential risk to national security, law enforcement, or public safety, the Security Committee will promptly notify DHS, DOJ, and FBI and, if such person is employed by Cypress, of the transfer, departure, or job modification of such Cypress Employee. Prospective Cypress Employees or prospective Contractors who are rejected by Cypress or by DHS, DOJ, or FBI under the screening requirements of this section will not be hired; Cypress Employees or Contractors who are rejected by Cypress or by DHS, DOJ, or FBI will be immediately removed from their positions, or otherwise have their duties immediately modified so that they are performing the functions of a job position for which they are deemed suitable under that job position's screening requirements.

(d) Cypress shall provide training to instruct Cypress Employees as to their obligations under the Agreement, the maintenance of their trustworthiness determination after screening, and any other requirements agreed upon. Cypress shall monitor on a regular basis the status of Cypress Employees, and shall remove any Cypress Employee who no longer meets the requirements pertaining to their job position and responsibilities.

(e) Cypress shall maintain records relating to the status of screened individuals, and shall provide these records, upon request, to DHS, DOJ, or FBI, or any auditor appointed under the terms of Section 5.7 below.

3.17 Composition of Board of Directors of Cypress and THC.

(a) All directors on the Boards of Directors of Cypress and THC shall be U.S. citizens. Except as provided in (b) or as otherwise agreed by DHS, DOJ, FBI and Treasury, there shall be five (5) Directors on each Board, and the majority of the Directors on each Board shall not be executives or employees with Arcapita, shareholders of Arcapita, or otherwise affiliated with Arcapita.

(b) The Board of Directors of Cypress at the time of closing the transactions described in the Merger Agreement shall consist of Bob Shingler, Stan Allen, and Charles Ogburn. The Board of Directors of THC at the time of closing the transactions described in the Merger Agreement shall consist of Bob Shingler, Stan Allen, and Charles Ogburn.

(c) Not later than September 15, 2005, Arcapita shall give written notice pursuant to Section 5.14 to DHS, DOJ, FBI, and Treasury of all five (5) nominees for Directors of Cypress and all five (5) nominees for Directors of THC. DHS, DOJ, FBI, and Treasury shall have 30 days from receipt of the notice (or such later timeframe as agreed to by the Parties) to review each nomination and provide Arcapita with any objection to a Director nominee. If DHS, DOJ, FBI or Treasury so desires, it may on its own, or through OPM's investigation service, conduct background checks for Director nominees. Arcapita shall cooperate with any such background checks. A nominee or appointee who is objected to by DHS, DOJ, FBI, or Treasury who does not pass the background check, will not be appointed or, if he or she has already been appointed, will be removed immediately as a Director. A nominee to whom DHS, DOJ, FBI, or Treasury does not object shall be promptly appointed to the Board for which the nominee was proposed and shall serve until replaced pursuant to Section 3.18.

This Section shall become effective as of June 17, 2005.

3.18 Changes in Composition of Board of Directors of THC or Cypress. In the event of the death, resignation, removal, or inability to act of any member of the Board of Directors of Cypress or of THC, Arcapita shall give prompt written notice pursuant to Section 5.14 to DHS, DOJ, FBI, and Treasury of the vacancy. Within ninety (90) days after the effective date of the departure of such Director, Arcapita shall notify DHS, DOJ, FBI, and Treasury of its nominee for the successor Director to fill the vacancy. DHS, DOJ, FBI, and Treasury shall have 30 days from receipt of the notice (or such later timeframe as agreed to by the Parties) to review the nomination and provide Arcapita with any objection to the Director nominee. If DHS, DOJ, FBI, or Treasury so desires, it may on its own, or through OPM's investigation service, conduct background checks for Director nominees. Arcapita shall cooperate with any such background checks. A nominee who is objected to by DHS, DOJ, FBI, or Treasury, or who does not pass the background check, will not be appointed. This Section shall become effective as of June 17, 2005.

3.19 Changes in Composition of Board of Directors of AIM. In the event of a proposed change in membership of the Board of Directors of AIM, Arcapita shall give prompt written

notice pursuant to Section 5.14 to DHS, DOJ, FBI, and Treasury of the vacancy and of its nomination of a successor Director to fill the vacancy. DHS, DOJ, FBI, and Treasury shall have 30 days from receipt of the notice to review the nomination and provide Arcapita with any objection to the Director nominee. If DHS, DOJ, FBI, or Treasury so desires, it may on its own, or through OPM's investigation service, conduct background checks for Director nominees. Arcapita shall cooperate with any such background checks. A nominee who is objected to by DHS, DOJ, FBI, or Treasury, or who does not pass the background check, will not be appointed. This Section shall become effective as of June 17, 2005.

3.20 Requirements For Non-Voting Stockholders. No Non-Voting Stockholder other than Jasmine Quadrilateral Investment Corporation, the Securities House K.S.C.C., or the Al-Jomaih Company Limited shall hold directly or indirectly five (5) percent or more of the equity interests in Cypress as calculated in accordance with the FCC's ownership attribution rules set forth in 47 C.F.R. § 63.09.

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 Cypress, the General Counsel of Arcapita, the President of THC, a Director of AIM, the General Counsel of FBI, the Assistant Attorney General for the Criminal Division of DOJ, the Assistant Secretary for Infrastructure Protection of DHS, the Assistant Secretary for International Affairs of Treasury, or their respective designees, unless DHS, DOJ, FBI, or Treasury believes that important national interests can be protected, or Cypress believes that paramount commercial interests can be resolved, only by resorting to the measures set forth in Section 4.2. 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 4.2. 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.

4.2 Enforcement of Agreement. Subject to Section 4.1 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 Authority to:

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

(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 Cypress, or request that the FCC impose any other appropriate sanction, including but not limited to a forfeiture or other monetary penalty, against Cypress; or