

This AGREEMENT is made this 7th day of OCTOBER, 1999, by and between: AT&T CORP., BRITISH TELECOMMUNICATIONS PLC, TNV (NETHERLANDS) BV, VLT CO. LLC, VIOLET LICENSE CO. LLC, THE UNITED STATES DEPARTMENT OF DEFENSE (the "DoD"), the UNITED STATES DEPARTMENT OF JUSTICE (the "DoJ") and the FEDERAL BUREAU OF INVESTIGATION (the "FBI") (collectively "the Parties").

RECITALS

WHEREAS, the U.S. telecommunications system is essential to U.S. national security, law enforcement, and public safety;

WHEREAS, the U.S. Government considers it critical to maintain the viability, integrity, and security of that system (see e.g., Presidential Decision Directive 63 on Critical Infrastructure Protection);

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

WHEREAS, AT&T Corp. ("AT&T") operates a major U.S. telecommunications network under licenses granted to it and its subsidiaries by the Federal Communications Commission ("FCC");

WHEREAS, British Telecommunications plc ("BT"), a major telecommunications company registered under the laws of England and Wales, and AT&T intend to establish a joint venture, (the "Parent Corporation" as defined in Section 8.1.14, below), to provide international telecommunications services;

WHEREAS, AT&T and BT will each own 50% of the outstanding shares of the Parent Corporation;

WHEREAS, certain license applications related to the formation of the joint venture have been filed with the FCC in Docket No. 98-212 on 11/10/1998 and will require approval by the FCC, and such approval may be made subject to conditions relating to national security, law enforcement, and public safety;

WHEREAS, on January 8, 1999, the Federal Bureau of Investigation ("FBI") filed comments with the FCC expressing national security, law enforcement and public safety concerns about the approval of such license applications;

WHEREAS, on January 19, 1999, the Department of Defense ("DoD") filed comments with the FCC expressing national security concerns about the approval of such license applications;

WHEREAS, the Parent Corporation will establish direct or indirect United States subsidiaries (collectively, the "Company," as defined in Section 8.1.3 of this Agreement), including VLT Co. LLC and Violet License Co. LLC, which will be located in the United States and which will own and operate the Domestic Telecommunications Infrastructure (as defined in Section 8.1.7 of this Agreement) directly or indirectly owned by the Parent Corporation;

WHEREAS, the Parent Corporation will directly or indirectly own all of the outstanding shares of the Company;

WHEREAS, the Parties agree that the Company will be required to obtain facility security clearances issued under the National Industrial Security Program ("NISP") (Executive Order 12829, January 6, 1993) in order to conduct any of its business that requires access to Classified Information;

WHEREAS, the NISP requires that in order to maintain a facility security clearance a corporation must be effectively insulated from foreign ownership, control or influence ("FOCI");

WHEREAS, the DoD intends to grant, in accordance with the National Industrial Security Program Operating Manual ("NISPOM"), a facility security clearance to the Company in consideration of the Parties' execution and compliance with the provisions of this Agreement; and

WHEREAS, because it is difficult to predict exactly how AT&T and BT may wish to conduct their business in the future, the Parties intend to work closely together and to share information to permit the Government to monitor the implementation of this Agreement over time;

NOW THEREFORE, the Parties are entering into this Agreement to address all objections that the DoD, the DoJ and the FBI might otherwise have to the grant of FCC licenses to the Company and transfer of ultimate control of FCC licenses to the Parent Corporation.

ARTICLE I - ORGANIZATION

1.1 Members and Principal Managers of the Company

Except as specifically provided herein, the Member or Members of the Company shall have all of the rights, powers, and responsibilities conferred or imposed upon Members of the Company by the applicable statutes and regulations, and by the Company's charter documents. The Company's Principal Managers shall be resident citizens of the United States who have personnel security clearances at the level of the Company's facility security clearance. The Defense Security Service ("DSS") or the designated security component for the FBI (hereinafter, "FBISC") may authorize temporary appointment of a Principal Manager for whom a personnel security clearance is under consideration. Further, all officers (including but not limited to Principal Managers) and employees of the Company having access to Classified or Sensitive

Information shall be resident citizens of the United States cleared to the level of the Classified or Sensitive Information to which they have access.

1.2 Within 90 days after the Effective Date (as defined in Section 7.1) of this Agreement, the Company shall promulgate written policies and procedures establishing a formal organizational structure, further described in Article III hereof, to ensure the protection of Classified, Controlled Unclassified, and Sensitive Information entrusted to it and to place the responsibility therefor with a committee of its Principal Managers to be known as the Government Security Committee ("GSC"), as hereinafter provided. The GSC shall be established no later than 30 days after the last of its members has received the appropriate security clearance. Until that time, oversight of the Company's protection of Classified, Controlled Unclassified, and Sensitive Information shall be the responsibility of the Company's designated representative identified in Section 7.3 of this Agreement.

1.3 Departure and Replacement of Principal Managers

1.3.1 The Company shall provide written notification to the DSS and the FBISC in advance, to the extent feasible, of the departure of a Principal Manager of the Company, and of any replacement for the departed Principal Manager. Any replacement for any departed Principal Manager shall meet the qualifications set forth in this Agreement.

1.3.2 The obligation of a Principal Manager to enforce this Agreement shall terminate when the Principal Manager leaves his/her position. Nothing herein shall relieve the departing Principal Manager of the responsibility not to disclose Classified, Controlled Unclassified, and Sensitive Information obtained while a Principal Manager of the Company. Such responsibility shall not terminate by virtue of leaving a position of Principal Manager. The Company shall advise the departing Principal Manager of such responsibility, but failure of the Company to so advise shall not relieve the Principal Manager of such responsibility.

ARTICLE II - FACILITIES AND RECORDS

2.1 Except to the extent and under conditions concurred in by the DoD, the DoJ and the FBI in writing: (1) all Domestic Telecommunications Infrastructure owned directly or indirectly by the Parent Corporation will be owned and controlled by the Company and shall at all times be located in the United States, and (2) all telecommunications of U.S. Joint Venture Subscribers carried over the Company's facilities shall pass through a facility, from which Electronic Surveillance can be conducted, that is physically located in the U.S. and under the control of either the Company or a licensed U.S. carrier.

2.2 The Company's Domestic Telecommunications Infrastructure shall, to the extent required under U.S. law, be capable of complying and configured to comply, and the Company's officials in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with:

- (1) 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),
- (2) National Security and Emergency Preparedness rules, regulations and orders issued by the FCC pursuant to the Communications Act of 1934, as amended (47 U.S.C. § 151 *et seq.*), and
- (3) lawful requests by U.S. federal, state or local law enforcement agencies or U.S. intelligence agencies, certifications, and court orders regarding Electronic Surveillance and the acquisition of Subscriber Information.

2.3 The Company shall maintain within the United States its principal business office and security office. If the Parent Corporation or the Company stores Subscriber Information concerning U.S. Joint Venture Subscribers for any reason:

- a. the Company shall maintain a current copy of such information in an office in the United States, and
- b. other copies of such information may be stored, and databases concerning same may be maintained, outside of the United States.

2.4 The Company shall store exclusively in the United States if stored by the Company for any reason:

- a. all Classified and Sensitive Information; and
- b. the copy of any Wire Communication or Electronic Communication Intercepted by U.S. federal, state or local government agents within the United States to which the Company may have access.

2.5 Content of Wire and Electronic Communications

2.5.1 The Company shall maintain within its Domestic Telecommunications Infrastructure the technical ability to access, and shall make available technical access to or provide the stored Electronic Communications and Wire Communications of U.S. Joint Venture Subscribers pursuant to Lawful U.S. Process.

2.5.2 In the event that the Parent Corporation, the Company or any of their subsidiaries proposes to store Electronic Communications or Wire Communications of U.S. Joint Venture Subscribers at locations outside of the United States, the Company will give prior notice of not less than 90 days to the DoJ. Within 30 days after receipt of such notice, the DoJ may

request that the Company consider the DoJ's views or concerns regarding the potential impact on the DoJ's authorities. Upon receipt of such request, the Company will consider both the availability and suitability, from a cost, technical and business perspective, of any reasonable alternatives, including retaining storage in the U.S. Notwithstanding this process or any other provision of this Agreement, at the end of the 90-day period the Parent or subsidiary may proceed with any action not prohibited by law. The foregoing prior notice and consultative process shall not apply to: (1) situations where Electronic Communications or Wire Communications of U.S. Joint Venture Subscribers are already stored outside of the United States; or (2) situations where an individual customer's requirements result in the storage of that customer's Electronic Communications or Wire Communications outside of the United States.

2.5.3 AT&T, BT and the Company shall participate in an industry forum that is sponsored by the DoJ, and that includes representatives from telecommunications carriers, equipment suppliers and Internet service providers, to examine law enforcement policy in the context of global communications. AT&T, BT and the Company also will encourage the participation of other domestic and international industry members in such discussions.

2.5.4 Nothing in this Agreement shall require the Company to store any information or data for a longer period than such information and data are stored in the ordinary course of the Company's business. Nothing in this Agreement shall exempt the Company from compliance with U.S. legal requirements for the retention or preservation of such information or data.

2.6 Except as provided below, the Company shall not provide access to the Wire Communications, Electronic Communications, or Subscriber Information of U.S. Joint Venture Subscribers maintained by the Company to any person if the purpose of such access is to respond to legal process or a request of a foreign government or a component or subdivision thereof.

2.7 The Company shall not, directly or indirectly, disclose or permit disclosure of, or provide access to any of the following:

- (a) Classified or Sensitive Information,
- (b) the copy of any Wire Communication or Electronic Communication Intercepted by U.S. federal, state or local government agents within the United States, or
- (c) Subscriber Information of U.S. Joint Venture Subscribers maintained by the Company under Section 2.3

to any foreign government or a component or subdivision thereof without the express written consent of the U.S. Department of Justice or the authorization of a court of competent jurisdiction in the United States. Notwithstanding anything contained in the preceding sentence, the Company shall not disclose Classified Information to any person not having the requisite U.S.

Government security clearance. Any requests or any legal process submitted by a foreign government or a component or subdivision thereof to the Company or an Affiliate for the information identified in (a) through (c) above that is maintained by the Company shall be referred to the U.S. Department of Justice as soon as possible and in no event later than five (5) business days after such request. At least every 3 months, the Company shall notify the U.S. Department of Justice in writing of requests by foreign non-governmental entities for access to or disclosure of either the content of a Wire Communication or Electronic Communication, whether or not stored, or Subscriber Information maintained by the Company.

2.8 The Company shall establish and comply with policies and practices to ensure the safeguarding of Classified, Controlled Unclassified and Sensitive Information, as provided in Article III of this Agreement, and designed to prevent any network, electronic, or other access from outside the United States or from facilities not specifically designated within the United States, to Classified and Sensitive Information, and Controlled Unclassified Information requiring a U.S. export license, entrusted to the Company. In addition, as provided in Article III, or in policies and practices to be established as a result of this Agreement, such safeguarding shall include, but is not limited to, technical security protection, personnel security clearances, and the execution of nondisclosure agreements.

2.9 Except to the extent and under conditions concurred in by the DoD, the DOJ and the FBI in writing, the Company shall have no technological capability, including any technological interface or connection, direct or indirect, that would enable the Company to control any part of the Domestic Telecommunications Infrastructure of AT&T or any other telecommunications company. In addition, the Company shall have no technological capability that would enable it to learn (1) of Lawful U.S. Process regarding AT&T's, or any other telecommunications company's, domestic or international networks or (2) about Classified or Sensitive Information maintained by AT&T or any other telecommunications company.

2.10 Sensitive Network Monitoring Personnel

2.10.1 The Company shall verify the recent employment and residence history of persons who assume positions in the category of Sensitive Network Monitoring Personnel working in any part of its Domestic Telecommunications Infrastructure. The Company shall provide this information, as well as personal identifying information for such persons (including name(s), alias(es), date and place of birth, social security number, visa and passport numbers) to the FBI. The purpose of this provision is to ensure the trustworthiness of Sensitive Network Monitoring Personnel.

2.10.2 Following the receipt of this information, if the FBI reasonably believes that a person is not sufficiently trustworthy to occupy a position in the category of Sensitive Network Monitoring Personnel and so notifies the Company, the person shall not be permitted to hold a position in such a category; provided, however, that after fourteen (14) days shall have passed after the provision of required information to the FBI by the Company, and no adverse

notice shall have been received from the FBI, that person shall be deemed suitable to begin work as Sensitive Network Monitoring Personnel.

2.10.3 If the DoD or the FBI provides information to the Company regarding any person occupying a position in the category of Sensitive Network Monitoring Personnel that reasonably would have precluded that person's occupying a position in the category of Sensitive Network Monitoring Personnel at the outset, then the FBI and the Company shall promptly review this information and promptly make a determination concerning that person's trustworthiness and the appropriateness of such person's continuing to occupy such position in the category of Sensitive Network Monitoring Personnel. If adverse information material to the trustworthiness of a person within the category of Sensitive Network Monitoring Personnel comes to the attention of the Company, then the Company shall either remove the person from such position or promptly provide information about the matter to the FBI. The Company may provide such information to the FBI in a manner that maintains the anonymity of such person, to the extent feasible and proper.

ARTICLE III - OPERATION OF THIS AGREEMENT

3.1 Policies and Practices

3.1.1 This Agreement establishes the basis for a facility clearance, which shall be issued to the Company upon satisfaction of the NISPOM review and approval process. The Company shall maintain practices and written policies designed to prevent unauthorized disclosure of or access to the Classified, Controlled Unclassified, and Sensitive Information entrusted to it.

3.1.2 The Company's policies and practices shall provide that the Company shall exclude any person who does not have the requisite U.S. government clearance, whether or not such person is an officer, employee, agent or other representative of an Affiliate, from access to Classified and Sensitive Information. Within 90 days from the Effective Date of this Agreement, the Company shall establish these policies and practices which shall be subject to the review and approval of the DSS and the FBISC. Such policies and practices shall not be repealed or amended without prior written notice to, and agreement of, the DSS and the FBISC.

3.1.3 AT&T agrees not to reveal or transfer Classified or Sensitive Information to the Company or to any other person except with prior written authorization by the DoD or the FBI. Where such authorization is granted, the information will be protected in the same manner as it was by AT&T.

3.2 Government Security Committee Compliance Programs

3.2.1 There shall be established within the Company a permanent Government Security Committee ("GSC") consisting of no fewer than three Principal Managers and at least one other cleared manager (other than a Principal Manager of the Company). The members of the

GSC shall ensure that the Company complies with the policies and practices established pursuant to section 3.1, and shall establish policies and procedures for oversight and monitoring of the Company's compliance with this Agreement.

3.2.2 The Chairman of the GSC shall be a Principal Manager of the Company. The chairman shall designate a GSC member to serve as secretary of the GSC. The secretary shall be responsible for ensuring that all records, journals and minutes of GSC meetings and other documents sent to or received by the GSC are prepared and retained for inspection by the DSS and the FBISC.

3.2.3 A Facility Security Officer ("FSO") shall be appointed by the Company and shall be the principal advisor to the GSC concerning the safeguarding of Classified and Sensitive Information. The FSO shall be responsible for the oversight of the Company's compliance with the requirements of the NISP and this Agreement.

3.2.4 The Company shall develop and implement a Technology Control Plan ("TCP"), which shall be subject to review by the DSS and shall prescribe measures to prevent the unauthorized disclosure or export of Controlled Unclassified Information consistent with applicable United States laws and this Agreement.

3.2.5 A Technology Control Officer ("TCO"), who may be the same person as the FSO, shall be appointed by the Company and shall be the principal advisor to the GSC concerning the protection of Controlled Unclassified Information. The TCO shall be responsible for the establishment and administration of all intra-company procedures, including employee training and oversight programs, to prevent the unauthorized disclosure or export of Controlled Unclassified Information and to ensure that the Company complies with the requirements of United States export control laws and this Agreement.

3.2.6 Upon taking office, the GSC members, the FSO and the TCO shall be briefed by a DSS and a FBISC representative on: (1) their responsibilities under the NISP; (2) the laws related to Electronic Surveillance and the acquisition of Subscriber Information; (3) United States export control laws; and (4) this Agreement.

3.2.7 A member of the GSC shall advise the DSS and the FBISC telephonically as soon as possible after any member of the GSC is aware of or otherwise believes there has been a violation of, or an attempt to violate: (1) any provision of this Agreement; (2) contract provisions regarding security; (3) United States export control laws; (4) the laws relating to Electronic Surveillance and the acquisition of Subscriber Information; or (5) the NISP. Such GSC member shall provide a written report of any such violation to the FBISC, and if appropriate, also to the DSS within 5 business days of the date upon which the GSC becomes aware of the violation.

3.2.8 Upon accepting his or her appointment and thereafter at each annual meeting of the Company with the DSS and the FBISC as provided in subsection 3.3.1, each member of the GSC shall execute and deliver to the DSS and the FBISC an acknowledgment of the obligations imposed by this Agreement and his or her obligations to enforce this Agreement, and a certification regarding the Member's best efforts to ensure compliance by the Company with this Agreement.

3.3 Annual Review and Certification

3.3.1 Representatives of the DSS, the FBISC, the GSC, the FSO and the TCO shall meet annually to review this Agreement and to establish a common understanding of the obligations of this Agreement and the manner in which the Agreement is being implemented.

3.3.2 One year from the effective date of this Agreement and annually thereafter, the Chairman of the GSC shall submit to the DSS and the FBISC an implementation and compliance report. The report shall include the following information:

- a. a detailed description of the manner in which the Company is carrying out its obligations under this Agreement;
- b. a detailed description of changes to the Company's security procedures, implemented or proposed, relating to the Affiliates and the reasons for those changes;
- c. a summary of any acts of noncompliance with the terms of this Agreement, whether inadvertent or intentional, which have occurred in the previous year, whether previously reported or not, with a discussion of any steps taken by the Company to prevent such acts;
- d. a detailed chronological summary of all disclosures or transfers, if any, of Classified and Sensitive Information, and Controlled Unclassified Information requiring a U.S. export license, from the Company to the Affiliates, with an explanation of the United States governmental authorization relied upon for such disclosures or transfers. Copies of any approved export licenses covering the reporting period shall be appended to the report; and
- e. a discussion of any other issues that could have a bearing on the effectiveness or implementation of this Agreement.

3.4 Access to Facilities and Information

3.4.1 Upon reasonable notice, the DoD, the DoJ or the FBI may visit any facility of the Company or its subsidiaries in the United States and may inspect any part of such facility for the purpose of verifying compliance with the terms of this Agreement.

3.4.2 Upon reasonable request from the DoD, the DoJ or the FBI, the Company, on behalf of itself and the other Parties shall be authorized to and shall,

- a. provide access to information, and
- b. make available for interview any officer or employee located in the United States who may be able to provide information

to assist the DoD, the DoJ and the FBI in assessing and verifying the other Parties' compliance with their obligations under this Agreement and in determining whether additional measures are needed.

3.5 Forms, Reports, Certifications

The GSC shall prepare and submit any form, report, or certification required by the DSS or the FBISC.

3.6 Cooperation in Investigations

The Company shall, under this Agreement, cooperate with the DoD, the DoJ and the FBI in investigating, inter alia: (i) breaches of this Agreement; (ii) Electronic Surveillance conducted in violation of Federal or state law or regulation; (iii) access to or disclosure of Subscriber Information in violation of Federal or state law or regulation or this Agreement; or (iv) improper access to or disclosure of Classified Information or Sensitive Information by the Company or any Affiliate.

ARTICLE IV DISPUTES AND NON-IMPACT ON OTHER GOVERNMENT ACTIONS

4.1 Dispute Resolution

The Parties shall use their best efforts to resolve any disagreements that may arise under this Agreement. Disagreements will 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 higher authorized officials, unless the DoD, the DoJ or the FBI believes that important national interests can be protected, or the Company believes that paramount commercial interests can be resolved, only by resorting to the measures set forth in

section 4.3.1 below. If, after meeting with higher authorized officials, either party determines that further negotiation would be fruitless, then either party may resort to the remedies set forth in Section 4.3.1 below. If resolution of a disagreement requires access to Classified Information, the designees of all Parties shall possess the appropriate security clearances.

4.2 Denial of Access to Information

Nothing contained in this Agreement shall limit or affect the authority of the head of a United States Government agency to deny, limit or revoke the Company's access to Classified, Controlled Unclassified, and Sensitive Information under its jurisdiction.

4.3 Enforcement of Agreement

4.3.1. Remedies for Breach. Subject to section 4.1 of this Agreement, if any Party believes that any other Party has breached or is about to breach this Agreement, that Party may bring an action against the other Party for appropriate judicial relief. Alternatively, (1) the DoJ, the FBI or the DoD may bring an action for relief (including equitable relief) before the FCC, and (2) the Affiliates and the Company may petition the FCC for a declaratory ruling with respect to the Affiliates' or the Company's obligations under this Agreement. Nothing in this Agreement shall waive any defenses to or immunities from suit that a Party may otherwise have. Nothing in this Agreement shall limit or affect the right of the head of a U.S. Government agency to seek revocation by the FCC of any license, permit or other authorization granted or given by the FCC to the Parent Corporation or the Company, or any other sanction by the FCC against the Parent Corporation or the Company, or the right to seek civil sanctions from a U.S. Federal District Court Judge or Magistrate, for any violation by the Parent Corporation or the Company of any U. S. law or regulation or term of this Agreement.

4.3.2 No Waiver of Other Remedies. Subject to section 4.3.3 of this Agreement, the availability of any civil remedy under this Agreement shall not preclude 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 the DoD, the DoJ, or the FBI 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 the DoD, the DoJ or the FBI of any provision or right shall be valid unless it is in writing and signed by the DoD, the DoJ or the FBI.

4.3.3 Forum Selection. It is agreed by and between the Parties that a civil action for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement that is not resolved under section 4.1 of this Agreement shall be brought, if at all, in and before a Federal court of competent jurisdiction in the United States, to the exclusion of the courts of any state, territory, or other nation.

4.4 Criminal Sanctions.

Nothing in this Agreement limits the right of the United States Government to pursue criminal sanctions against the Company or any Affiliate, or any director, Member, officer, employee, representative, or agent of any of these companies, for violations of the criminal laws of the United States.

ARTICLE V - TERMINATION

5.1 Terminations by the DoD, the DoJ, and the FBI

This Agreement may be terminated only by the DoD, the DoJ, and the FBI. The circumstances in which termination may be considered are:

- a. when the DoD, the DoJ, and the FBI determine that:
 - i). existence of this Agreement is no longer necessary to maintain a facility security clearance for the Company;
 - ii). continuation of a facility security clearance for the Company is no longer necessary;
 - iii). there has been a material breach of this Agreement that requires it to be terminated;
- b. in the event of a sale of the Company to a company or person not under FOCI;
- c. when the DoD, the DoJ, and the FBI otherwise determine that termination is in the national interest; or
- d. when the Company petitions the DSS and the FBISC to terminate. A petition shall contain the reason termination is requested. The DoD, the DoJ, and the FBI will determine, in their sole discretion, whether termination is in the interests of the United States.

5.2 Notice of Termination by the DoD, the DoJ, and the FBI

If the DoD, the DoJ, and the FBI elect to terminate this Agreement, the DoD, the DoJ, and the FBI shall provide the Company with thirty (30) calendar days written advance notice stating the reason for termination.

ARTICLE VI - NON-OBJECTION BY DoD, DoJ AND FBI TO THE GRANT OF FCC LICENSES

6.1 Non-Objection

6.1.1 Upon the execution of this Agreement, the DoD, the DoJ and the FBI will notify the FCC that, provided the FCC approves this Agreement and adopts the Condition to FCC Licenses attached hereto as Exhibit A, the DoD, the DoJ and the FBI have no objection to the grant of licenses that are the subject of the application filed with the FCC in Docket Number 98-212 on 11/10/1998.

6.1.2 Provided that the FCC approves this Agreement and adopts the Condition to FCC Licenses, neither the DoD nor the DoJ shall make any objection they otherwise would have made concerning the formation of the Parent Corporation to the Committee on Foreign Investment in the United States or the President.

ARTICLE VII -- GENERAL

7.1 Effective Date.

The Effective Date of this Agreement shall be the date of the closing of the transaction establishing the Parent Corporation or the date upon which the Parent Corporation, the Company or any of their subsidiaries begin operations pursuant to the authorities granted by the FCC in Docket No. 98-212, whichever is sooner.

7.2 Right to Make and Perform Agreement.

AT&T and BT represent that, to the best of their knowledge, they have and will continue to have throughout the term of this Agreement the full right to enter into this Agreement and perform their obligations hereunder and that this Agreement is a legal, valid, and binding obligation of AT&T, BT, the Parent Corporation and the Company enforceable in accordance with its terms.

7.3 Notices.

With the exception of service of Lawful U.S. Process, all requests for information, visits, interviews and all reports, notices, and proposed modifications provided under this Agreement shall be made to the parties' designated representatives. All reports, notices and proposed modifications under this Agreement shall be delivered by (1) registered or certified U.S. mail; (2) overnight courier (receipt requested); or (3) facsimile (confirmed by mail) addressed to the addresses shown below, or to such other addresses as the Parties may designate by agreement. The representatives shall be:

For AT&T: Steven W. DeGeorge
c/o AT&T Corp.
2020 K Street, N.W.
Suite 712
Washington, D.C. 20006

For BT: Alan Whitfield
British Telecommunications plc
BT Centre (BTC-EC)
81 Newgate Street
London EC1A7AJ ENGLAND

For the Parent Corporation: Walter Desocio
General Counsel
AT&T- BT Global Venture
Room 6110
1200 Peachtree Street, N.E.
Atlanta, GA 30309

For the Company: Steven W. DeGeorge
c/o AT&T Corp.
2020 K Street, N.W.
Suite 712
Washington, D.C. 20006

For DSS: Defense Security Service
1340 Braddock Place
Alexandria, Virginia 22314-1651

with a copy to:

General Counsel
Department of Defense
The Pentagon
Washington, D.C. 20301 - 1600

For FBISC: National Security Division
Attn: Unit Chief, NSU, NS-5A
Room 1B045
FBI Headquarters
935 Pennsylvania Ave., N.W.
Washington, D.C. 20535

with a copy to:

FBI General Counsel
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

For the DoJ:

Assistant Attorney General
Criminal Division
Main Justice Building
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

7.4. Other Laws.

Nothing in this Agreement is intended to limit or constitute a waiver of (i) any obligation imposed by Federal or state law or regulation on Affiliates and the Company; (ii) any obligation imposed by Federal law or regulation on the DoD, the DoJ, or the FBI; (iii) any enforcement authority available under Federal or state law or regulation; (iv) the sovereign immunity of the United States; or (v) any authority over Affiliates' activities or facilities that the U.S. Government may possess. Nothing in this Agreement is intended to benefit or confer a right upon any person other than a Party to this Agreement or other U.S. federal, state or local government entities entitled to conduct Electronic Surveillance. Nothing in this agreement shall require, expressly or by implication, the violation of any domestic or foreign law.

7.5. Statutory References.

All references to statutory provisions or to Executive Orders shall include any future amendments to such authorities.

7.6. Precedence of Agreement.

In the event that any resolution, regulation or provision of the charter documents of the Company is inconsistent with any provision of this Agreement, this Agreement shall control.

7.7. Amendment and Modification of Agreement.

7.7.1 Amendment. This Agreement may be modified only by a written agreement signed by all of the Parties. Any substantial modification to this Agreement shall be reported to the FCC within thirty (30) days after approval by the Parties.

7.7.2 Modification. Beginning on the date which is eighteen months after execution of this Agreement, the Parties agree to consider in good faith possible modifications to this Agreement as may be required for the consistent application of U.S. national security, law enforcement and public safety laws and policies to the Company vis-a-vis other international communications services in like circumstances.

7.8 Headings.

The headings contained in this Agreement are for reference purposes only, and do not in any way affect the meaning or interpretation of the provisions.

7.9 Location of Agreement.

Until the termination of this Agreement, one original counterpart shall be kept at the principal office of the Company.

7.10 Freedom of Information Act.

7.10.1 Marking of Information. The DoD, DoJ and the FBI shall take reasonable precautions to protect from improper public disclosure all information submitted by the Affiliates and the Company to the DoD, DoJ and the FBI in connection with or in furtherance of this Agreement and clearly marked with the legend "Company Confidential" or similar designation. Such marking shall represent to the DoD, DoJ and the FBI that the information so marked constitutes "trade secrets" and/or "commercial or financial information obtained from a person and privileged or confidential," or otherwise warrant its protection within the meaning of 5 U.S.C. § 552(b)(4). For purposes of 5 U.S.C. § 552(b)(4), the parties agree that such information is voluntarily submitted. In the event of a request under 5 U.S.C. § 552(a)(3) for information so marked, the DoD, DoJ or the FBI, as appropriate, shall notify the Company of such request and consult with it as to any contemplated release (including release in redacted form) of such information. The DoD, DoJ or the FBI, as appropriate, shall notify the Company five (5) business days in advance of any release of such information under 5 U.S.C. § 552(a)(3).

7.10.2 Use of Information for Government Purposes. Nothing in this Agreement shall prevent the DoD, DoJ or the FBI from lawfully disseminating information as appropriate to seek enforcement of this Agreement, or as otherwise necessary in furtherance of the missions, responsibilities, or obligations of the DoD, DoJ or the FBI, provided that the DoD, DoJ or the FBI shall take reasonable precautions to protect from improper public disclosure information marked as described in the preceding section. Where feasible, the DoD, DoJ and the FBI will make information available for inspection rather than providing copies thereof.

7.11 Partial Invalidity.

If any provision of this Agreement is declared invalid or unenforceable by a court of competent jurisdiction, this Agreement shall be construed as if such provision were reformed or deleted, and the remaining provisions of this Agreement shall remain in full force and effect, unless this construction would constitute a substantial deviation from the Parties's intent as reflected in this Agreement.

7.12 Execution in Counterpart.

This Agreement may be executed in several counterparts, each of which shall be an original.

ARTICLE VIII -- DEFINITION OF TERMS

8.1 Definitions: As used in this Agreement:

8.1.1 "Affiliates" means AT&T, BT, (as described in the Recitals), and the Parent Corporation, individually or collectively, all entities (other than the Company) that Control or are Controlled by the Parent Corporation and all successors and assigns of such parties and entities.

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

8.1.3 "Company" means VLT Co. LLC and Violet License Co. LLC, as described in the Recitals, and any other direct or indirect subsidiaries of the Parent Corporation that own or control any part or portion of the Domestic Telecommunications Infrastructure, and any successor(s) or assigns.

8.1.4 "Control" or "Controlled" as used in Section 8.1.1 of this Agreement, mean 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:

- (1) 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;

- (2) The dissolution of the entity;
- (3) The closing and/or relocation of the production or research and development facilities of the entity;
- (4) The termination or non-fulfillment of contracts of the entity;
- (5) The amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in paragraphs (1) through (4) above; or
- (6) The matters covered by this Agreement.

The terms "control" or "controlled" as used in Sections 2.1, 2.9, 8.1.3 and 8.1.7 mean the ability to direct, supervise or otherwise manage, shut down, interfere with or modify the capabilities of, but does not include routine service maintenance, provisioning or service monitoring.

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

8.1.6 "Domestic Telecommunications" means telecommunications from one U.S. location to another U.S. location.

8.1.7 "Domestic Telecommunications Infrastructure" means the transmission and switching equipment (including software) that is used to provide Domestic Telecommunications or physically located in the United States and any facility that is used to control such equipment.

8.1.8 "Electronic Communication" has the meaning given it in 18 U.S.C. § 25 10(12).

8.1.9 "Electronic Surveillance" means (i) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 25 10(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (ii) access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 et seq.; (iii) acquisition of dialing or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 et seq. and 50 U.S.C. § 1841 et seq.; (iv) acquisition of location-related information concerning a telecommunications service subscriber; (v) preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (vi) including access to, or acquisition or interception of, communications or information as described in (i) through (v) above and comparable State laws.

8.1.10 "FCC" has the meaning given it in the Recitals. It includes any agency or instrumentality of the United States to which, in the future, all or any part of the functions or responsibilities of the FCC may be transferred or assigned.

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

8.1.12 "Lawful U.S. Process" means Electronic Surveillance orders or authorizations, and other orders, legal process, statutory authorizations, and certifications for access to Subscriber Information.

8.1.13 "Member" has the meaning given in Section 18-101(11) of Title 6 of the Delaware Code.

8.1.14 "Parent Corporation" means TNV (Netherlands) BV, as described in the Recitals.

8.1.15 "Parties" has the meaning given it in the Preamble.

8.1.16 "Principal Managers" means those persons occupying positions of director, president, senior vice president, secretary, treasurer and those persons occupying similar positions.

8.1.17 "Sensitive Information" means unclassified information regarding (i) the persons or facilities that are the subjects of Lawful U.S. Process, (ii) the identity of the government agency or agencies serving such Lawful U.S. Process, (iii) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance, (iv) the means of carrying out Electronic Surveillance, (v) the type(s) of service, telephone number(s), records, communications, or facilities subjected to Lawful U.S. Process, and (vi) other unclassified information designated in writing by an authorized official of a federal, state or local law enforcement agency or a U.S. intelligence agency as "Sensitive Information."

8.1.18 "Sensitive Network Monitoring Personnel" means personnel responsible for performing network management, operations, maintenance, or security functions who have regular access to facilities, systems, or equipment which enable monitoring of subscribers' wire or electronic communications, including any such communications that are in electronic storage. This term excludes personnel who (i) perform outside plant operations and maintenance functions, (ii) perform network-level monitoring without the responsibility to monitor the content of a subscriber's communications, or (iii) monitor telemarketing calls by Company personnel or customer-originated calls to the Company.

8.1.19 "Subscriber Information" means information of the type referred to and accessible subject to procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709, or

other legal process established by state law. Subscriber Information does not include the content of any communication.

8.1.20 "United States" means the United States of America including all of its States, districts, territories, possessions, commonwealths, and the special maritime jurisdiction of the United States.

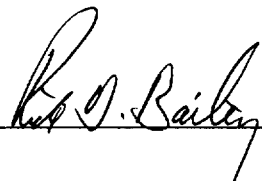
8.1.21 "U.S. Joint Venture Subscriber" means a subscriber, including an employee or similar authorized user of the services provided to a subscriber, of the Parent Corporation or any of its subsidiaries to the extent that such subscriber (i) is regularly provided services at a U.S. location by the Parent Corporation or any of its subsidiaries, and (ii) uses such services at a U.S. location. A customer of a subscriber of the Parent Corporation shall not, by reason of that relationship, be considered a U.S. Joint Venture Subscriber. Neither the Company, nor the subsidiaries of the Parent Corporation or the Company, shall be considered a subscriber of the Parent Corporation.

8.1.22 "Wire Communication" has the meaning given it in 18 U.S.C. § 25 10(1).


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

This Agreement is executed on behalf of the Parties:

VLT CO. LLC

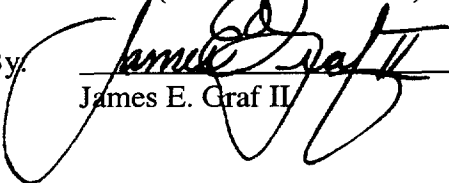
Date: October 1, 1999 By: 

VIOLET LICENSE CO. LLC

Date: October 1, 1999 By: 

TNV (NETHERLANDS) BV

Date: Oct. 1, 1999

By: 
James E. Graf II

AT&T CORP.

Date: October 1, 1999

By: Mary Jane McKeever
Mary Jane McKeever
Vice President

BRITISH TELECOMMUNICATIONS plc

Date: Oct. 1, 1999

By: James E. Graf, II
James E. Graf, II
President, BT North America Inc.

**THE UNITED STATES DEPARTMENT
OF DEFENSE**

Date: _____

By: _____

**THE FEDERAL BUREAU OF
INVESTIGATION**

Date: Oct. 7, 1999

By: Larry R. Parkin

AT&T CORP.

Date: _____ By: _____

BRITISH TELECOMMUNICATIONS plc

Date: _____ By: _____

James E. Graf, II
President, BT North America Inc.

THE UNITED STATES DEPARTMENT OF DEFENSE

Date: **07 OCT 1990** _____ By: _____

Arthur H. Money
Arthur H. Money
Assistant Secretary of Defense for Command,
Control, Communications and Intelligence

THE UNITED STATES DEPARTMENT OF JUSTICE

Date: _____ By: _____

THE FEDERAL BUREAU OF INVESTIGATION

Date: _____ By: _____

**THE UNITED STATES DEPARTMENT
OF JUSTICE**

Date: 10 - 7 - 99

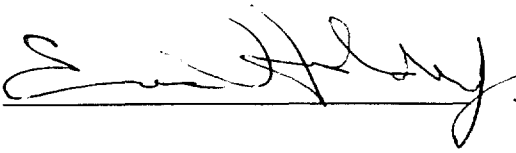
By: 

EXHIBIT A

CONDITION TO FCC LICENSES

IT IS FURTHER ORDERED, that the authorization and the license related thereto are subject to compliance with the provisions of the Agreement attached hereto between AT&T Corp., British Telecommunications PLC, TNV (NETHERLANDS) BV, VLT CO. LLC, and Violet License Co. LLC on the one hand and the Department of Defense (the "DoD"), Department of Justice (the "DoJ") and the Federal Bureau of Investigation (the "FBI") on the other, dated Oct. 7, 1999, which Agreement is designed to address national security, law enforcement, and public safety concerns of the DoD, DoJ and the FBI regarding the licenses granted herein. Nothing in this Agreement is intended to limit any obligation imposed by Federal law or regulation including, but not limited to, 47 U.S.C. § 222(a) and (c)(1) and the FCC's implementing regulations.