



January 12, 2005

**BY HAND DELIVERY**

Ms. Laura H. Parsky  
Deputy Assistant Attorney General  
United States Department of Justice  
950 Pennsylvania Avenue, N.W.  
Washington, D.C. 20530

Ms. Tina W. Gabbrielli  
Director of Intelligence Coordination and  
Special Infrastructure Protection Programs  
United States Department of Homeland Security  
Washington, D.C. 20528

Mr. Patrick W. Kelley  
Deputy General Counsel  
Federal Bureau of Investigation  
935 Pennsylvania Avenue, N.W.  
Washington, D.C. 20535

Dear Ms. Parsky, Ms. Gabbrielli and Mr. Kelley:

As you know, British Telecommunications plc ("BT"), a United Kingdom company engaged in the provision of global communications services and solutions, plans to acquire Infonet Services Corporation ("Infonet"), a Delaware corporation offering value-added network communications services.

BT and Infonet have met with representatives of the U.S. Department of Justice ("DOJ"), including the Federal Bureau of Investigation ("FBI"), and the U.S. Department of Homeland Security ("DHS") to discuss BT's security arrangements with respect to the planned transaction. Further to those discussions, this letter now sets forth certain security assurances of BT to the DOJ, FBI and DHS in connection with BT's acquisition of Infonet. These security assurances relate to the combined network facilities of BT and Infonet physically located in the United States ("BT U.S. Facilities") and will be effective immediately upon consummation of the acquisition of Infonet by BT.

Specifically, following consummation of the transaction, BT will maintain security policies designed to protect BT U.S. Facilities, safeguard U.S. Customer Data, as hereinafter defined, respond to security incidents, and comply with U.S. law enforcement requests. In furtherance of the foregoing security objectives, BT undertakes the following:

**Maintenance of U.S. Security Policy and Operational Plan.** BT will maintain a security policy and operational plan for the BT U.S. Facilities (the "Security Policy"), including all of the elements set forth below. The Security Policy will address BT's broad security objectives with respect to its U.S. Facilities as well as specific standards and practices to be applied in the BT organization including, but not limited to, facility access, security management, employee screening, cooperation with U.S. law enforcement and related matters.

**Designation of U.S. Security Committee.** BT will designate at least two (2) persons to serve as members of a security committee (the "Security Committee"). BT contemplates that the Security Committee initially will be comprised of four persons: (i) the BT Americas General Counsel; (ii) the Head of U.S. Network Operations; (iii) the U.S. Security Officer; and (iv) the U.S. Law Enforcement Primary Contact Person. BT expects that the composition and number of members of the Security Committee may change from time to time, but in any event will have a minimum of two members, one of which will be the BT Americas General Counsel and one of which will be the Head of U.S. Network Operations. The Security Committee will meet periodically (no less than quarterly) to review the Security Policy and confirm that BT is in operational compliance with the Security Policy. The Security Committee will be responsible for ensuring that the Security Policy is followed in the event of a high level threat or national emergency in the United States. The Security Committee will also be responsible for making appropriate revisions to the Security Policy as needed in light of changes and modifications to the BT global network. The members of the Security Committee will be resident U.S. citizens and will be subject to the third-party, pre-employment screening process at the higher level described below.

3. **Designation of U.S. Security Officer.** BT will designate a Security Officer for the BT U.S. Facilities. The Security Officer will oversee the day-to-day implementation and maintenance of the Security Policy for the BT U.S. Facilities. The Security Officer will report to the Security Committee. The Security Officer will be a resident U.S. citizen and will be subject to the pre-employment screening process at the higher level described below.

**Designation of U.S. Network Security Response Team.** BT will designate a U.S. Network Security Response Team to support and manage BT's U.S. Facilities. The U.S. Network Security Response Team will consist of key personnel from across BT Americas and will have the primary responsibility of assuming ultimate control of BT U.S. Facilities in the event of a high level threat or U.S. national emergency, including (i) terminating control of U.S. Facilities by persons outside the United States; (ii) performing network changes as required, and (iii) maintaining functions to minimize the impact of such threat or emergency to BT's customers. For purposes of the foregoing, to "assume control" in this context means to take necessary action to prohibit personnel physically located outside the United States from performing activities directly related to the physical operation of BT's U.S. Facilities, including but not limited to surveillance, maintenance, integration, commissioning and network management functions.

5. **Compliance with U.S. Law Enforcement Requests.** BT will maintain policies and procedures for the provision of, or for providing access to, within the United States, electronic or wire communications (whether stored or real-time), subscriber information, billing and transactional records of U.S. subscribers (the "U.S. Customer Data") requested by U.S. law enforcement agencies, either pursuant to lawful U.S. process or as otherwise permitted by law. BT will designate one or more points of contact at an office within the United States to receive and process, in a secure and efficient manner, requests for assistance from U.S. law enforcement agencies, including requests for interception or surveillance of communications and compliance with subpoenas or other lawful demands for disclosure of, or access to, BT's records. Such assistance will include, but not be limited to, disclosure, if necessary, of technical and engineering information relating to the design, maintenance or operation of BT's systems. BT and the law enforcement agency seeking the assistance will work together to determine what assistance is reasonable, taking into account the investigative needs of the agency and BT's commercial interests. BT will designate a screened technical official to assist, where applicable, in execution of such requests for assistance from law enforcement agencies. BT also will provide for the confidential treatment, and prohibition of unauthorized disclosure, of the record of such requests and all information supplied to law enforcement in response to such requests. Upon designation, BT will notify the FBI, DOJ and DHS in writing of the points of contact, and thereafter will promptly notify the FBI, DOJ and DHS of any change in such designation. The points of contact will be resident U.S. citizens and will be subject to the pre-employment screening process at the higher level described below.
6. **Maintenance of Access Control Policy.** BT will maintain an access control policy (the "Access Control Policy"), which policy will include access control requirements for BT's U.S. Facilities. The Access Control Policy will require in particular that all BT U.S. Facilities be secured and that, while on the premises of BT U.S. Facilities, all employees and visitors must display appropriate identification. The Access Control Policy will also provide that approved visitors are escorted by a BT employee at such times that said visitor has access to U.S. communications or network infrastructure. The minimum requirements for access by any person to any BT U.S. Facility will be that the person (i) is an employee and is based in that particular facility; or (ii) is an expected visitor and has made arrangements for entry with a BT employee host.
7. **Requirement of Unique User Identification.** BT's Access Control Policy will require that each user of computer systems associated with BT's U.S. Facilities be assigned a unique user ID and password for purposes of accessing such systems. Further, access will be granted solely on an "as needed" basis, with individuals obtaining access exclusively to the systems needed to perform their specific job obligations.
8. **Network Monitoring.** BT will monitor its U.S. Facilities in order to detect and prevent malicious access attempts, as well as to resolve technical faults and potential security vulnerabilities. U.S. resident personnel will control the U.S. portions of BT's network with respect to integration, commissioning, and implementation of network

and customer equipment, bandwidth activations, node site management and technical assistance. U.S.-resident personnel will also maintain the ability to assume control over the U.S. portions of the network, including the ability to terminate control by personnel located outside of the U.S. in the event of a high level threat or national emergency.

9. **Maintenance of Screening and Non-Disclosure Requirements.** BT will require pre-employment screening and non-disclosure commitments prior to hiring new employees with access to the BT U.S. Facilities. Higher-level screening will be mandatory for officers of BT and those individuals who already hold, or will hold, particularly sensitive network positions (“Sensitive Network Personnel”), including the members of the Security Committee, the Security Officer, the U.S. Network Security Response Team and the technical official referenced in Paragraph 5 above. The list of positions designated as Sensitive Network Personnel will be reviewed periodically by the Security Officer and approved by the Security Committee to ensure that the appropriate persons are so designated and have been properly screened according to the Security Policy. Prior to such approval, BT will provide DOJ, FBI, and DHS a two week comment period to review the initial list of Sensitive Network Personnel positions and to provide input into the required level of screening for certain sensitive positions. BT will promptly notify DOJ, FBI and DHS of any material changes made in the list thereafter.
10. **Protection of U.S. Customer Data.** BT’s Security Policy will include appropriate policies and procedures, consistent with BT’s compliance with U.S. and foreign laws, to protect U.S. Customer Data from unauthorized access and from mandatory destruction under any foreign laws, and to require prior consent of the DOJ, FBI and DHS before disclosing U.S. Customer Data to non-U.S. persons who are not screened, consistent with BT’s Security Policy, to a level commensurate with the sensitivity of the data to which they have access. Such prior consent is not required for compulsory disclosure pursuant to valid legal process enforceable by a non-U.S. government, in which case BT will give prompt notice to DOJ, FBI and DHS, of the service upon BT of any such process so long as such notice to DOJ, FBI and DHS is not in violation of foreign law. Should any non-U.S. person have access to the content of communications, they would be screened to a substantively identical level as would Sensitive Network Personnel, consistent with the law of the jurisdiction governing such screening. Unauthorized disclosure of U.S. Customer Data will be required to be reported promptly to the Security Committee, which will investigate the matter and make referrals to U.S. law enforcement when it reasonably appears that U.S. law may have been violated, with a copy of any such referral to DOJ, FBI and DHS. BT’s policies regulating the disclosure of U.S. Customer Data will also apply to agents and contractors of BT through non-disclosure agreements, as appropriate.
11. **Reporting of Network Changes.** BT’s Security Policy will require that any major acquisitions, modifications, upgrades or changes made to BT’s U.S. Facilities, including network operating systems, software and access security be promptly reported to the Security Officer and the Head of U.S. Network Operations.

12. **Reporting of Security Breaches.** BT's Security Policy will require that all breaches and suspected breaches of network security that directly and significantly impact the operations or overall management of BT's U.S. Facilities will be promptly reported to the Security Committee. The Security Policy will further require that such matters be investigated by the BT Americas General Counsel and the Security Officer, and that referrals be made to U.S. law enforcement when it reasonably appears that U.S. law may have been violated, with a copy of any such referral to DOJ, FBI and DHS. BT's Security Policy also will require that the Security Officer maintain a record of such actual or suspected breaches. DOJ, FBI and DHS will have a right, with two weeks notice to BT Americas General Counsel and the Security Officer, to inspect the record of reports of all breaches and suspected breaches to the Security Committee, and to obtain on request a brief report of investigation in any matter of concern.

\* \* \*

The assurances provided in this letter reflect BT's commitment to maintaining secure facilities in the United States, as well as BT's desire to continue its strong working relationship with the United States government. Should there be any material changes with respect to BT's security arrangements, or in the facts and circumstances set forth in this letter, or in the letter of November 18, 2004, to DOJ, FBI, DHS, and other U.S. Government agencies, BT will promptly notify DOJ, FBI, and DHS. Should you have any questions regarding any aspect of this letter, please do not hesitate to contact the undersigned.

Very truly yours,

**British Telecommunications plc**

Date: 12/01/05

By: 

Printed Name: TIM COWEN  
Title: GENERAL COUNSEL  
GLOBAL SERVICES