persons may express their views in writing on the standards enumerated in the BHC Act (12 U.S.C. 1842(c)). If the proposal also involves the acquisition of a nonbanking company, the review also includes whether the acquisition of the nonbanking company complies with the standards in section 4 of the BHC Act (12 U.S.C. 1843). Unless otherwise noted, nonbanking activities will be conducted throughout the United States. Additional information on all bank holding companies may be obtained from the National Information Center website at *www.ffiec.gov/nic/*.

Unless otherwise noted, comments regarding each of these applications must be received at the Reserve Bank indicated or the offices of the Board of Governors not later than March 29, 2007.

A. Federal Reserve Bank of Atlanta (David Tatum, Vice President) 1000 Peachtree Street, N.E., Atlanta, Georgia 30309:

1. Banco de Sabadell, S.A., Sabadell, Spain; to become a bank holding company by acquiring 100 percent of the voting shares of TransAtlantic Holding Corp., and thereby indirectly acquire TransAtlantic Bank, both of Miami, Florida.

2. United Community Banks, Inc., Blairsville, Georgia; to merge with Gwinnett Commercial Group, Inc., and thereby indirectly acquire First Bank of The South, both of Lawrenceville, Georgia.

Board of Governors of the Federal Reserve System, February 27, 2007.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. E7–3668 Filed 3–1–07; 8:45 am]

BILLING CODE 6210–01–S

FEDERAL TRADE COMMISSION

Transfer of Delegations of Authority To Disclose Certain Nonpublic Information to Foreign Law Enforcement Agencies and To Sign Confidentiality Agreements With Certain Foreign Agencies

AGENCY: Federal Trade Commission.

ACTION: Transfer of delegation of authority.

SUMMARY: The Commission has delegated authority to share information with certain law enforcement agencies in Canada, Australia, the United Kingdom, Ireland, Mexico, Costa Rica, and Spain to the Director of the Bureau of Consumer Protection. The Commission has also delegated to the Director of International Affairs authority to execute confidentiality agreements with certain foreign agencies, as a condition of their being granted access to nonpublic databases. These delegations include authority previously delegated to the Associate Director for International Consumer Protection.

EFFECTIVE DATE: February 26, 2007.

FOR FURTHER INFORMATION CONTACT: Lisa M. Harrison, Attorney, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington, DC 20580, (202) 326–3204, *lharrison@ftc.gov,* or Michael L. Shore, Attorney, Office of International Affairs, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington, DC 20580, (202) 326–2708, *mshore@ftc.gov*.

SUPPLEMENTARY INFORMATION: Notice is hereby given, pursuant to Reorganization Plan No. 4 of 1961, 26 FR 6191, that the Commission has transferred from the Associate Director for International Consumer Protection to the Director of the Bureau of Consumer Protection (BCP Director) its prior delegations of authority to: (1) Disclose to Canadian law enforcement agencies, information regarding consumer protection investigations involving Canadian businesses or consumers (67 FR 45738–01 (July 10, 2002)); (2) disclose to the Australian Competition and Consumer Commission, information regarding consumer protection investigations involving Australian businesses or consumers (67 FR 45738–01 (July 10, 2002)); (3) disclose to Australian law enforcement agencies, information contained in the Consumer Sentinel database of consumer complaints and law enforcement information (67 FR 45738–01 (July 10, 2002)); (4) disclose to the United Kingdom Office of Fair Trading and the United Kingdom Directorate for Trade and Industry, information regarding consumer protection investigations involving U.K. businesses or consumers (67 FR 45738–01 (July 10, 2002)); (5) disclose to Ireland's Office of the Director of Consumer Affairs, information regarding consumer protection investigations involving Ireland (68 FR 60107–01 (Oct. 21, 2003)); (6) disclose to Mexico's Procuraduría Federal del Consumidor, information regarding consumer protection matters involving Mexico (70 FR 6442–01 (Feb. 7, 2005)); (7) disclose to Costa Rica's Ministry of Economy, Industry, and Commerce, information regarding consumer protection matters involving Costa Rica (71 FR 14895–01 (Mar. 24, 2006)); (8) disclose to the United Kingdom's Office of Fair Trading, the United Kingdom's Information Commissioner, Her Majesty's Secretary of State for Trade and Industry in the United Kingdom, the Australian Competition and Consumer Commission, and the Australian Communications Authority, information regarding commercial e-mail investigations that involve consumers, businesses, commerce or markets in the United Kingdom or Australia (69 FR 44008–01 (July 23, 2004)); and (9) disclose to Spain's Agencia Espanola de Proteccion de Datos, information regarding commercial e-mail investigations that involve consumers, businesses, commerce or markets in Spain (70 FR 12487–03 (Mar. 14, 2005)). The BCP Director's authority may be redelegated.

This delegated authority does not apply to competition-related investigations. This delegated authority includes the authority to respond to disclosure and other requests within the ambit of any memorandum of understanding or agreement concerning consumer protection cooperation between the Commission and an agency listed or described in this notice or within the ambit of any agreement concerning consumer protection cooperation between the United States and any country listed in this notice. For this delegated authority, ''consumer protection investigations involving businesses or consumers'' of a country, ''consumer protection investigations involving'' a country and ''consumer protection matters involving'' a country shall include any consumer protection investigation or matter involving that country or with a nexus to any person, entity, commerce, or market in that country. The phrase ''commercial e-mail investigations that involve consumers, businesses, commerce or markets in'' a country shall include any commercial e-mail investigation or matter involving that country or with a nexus to any person, entity, commerce, or market in that country.

When exercising its delegated authority, the BCP Director will require assurances of confidentiality from the relevant foreign law enforcement agency. Disclosures shall be made only to the extent consistent with limitations on disclosure including, where applicable, sections 6(f) and 21 of the FTC Act, 15 U.S.C. 46(f) and 57b–2 (as amended by sections 4(a) and 6(a) of the U.S. SAFE WEB Act of 2006, Public Law 109–455, 120 Stat. 3372, 3372–73 and 3376–77), Commission Rule 4.10(d), 16 CFR 4.10(d), and with the Commission's enforcement policies and other

important interests. Where the subject matter of the information to be shared raises significant policy concerns, the BCP Director shall notify the Commission before disclosing such information. In addition, the Commission has transferred from the Associate Director for International Consumer Protection to the Director of the Office of International Affairs (OIA Director) its prior delegations of authority to execute econsumer.gov confidentiality agreements with consumer protection authorities from current or future International Consumer Protection and Enforcement Network (ICPEN) member countries, and to execute Consumer Sentinel confidentiality agreements with any foreign law enforcement agency whose access has been authorized or is authorized in the future by the Commission or by the Commission's delegate, including without limitation Canadian and Australian law enforcement agencies (67 FR 45738–01 (July 10, 2002)). When exercising its delegated authority, the OIA Director will require assurances of confidentiality from the relevant foreign law enforcement agency. The OIA Director's authority under these delegations may be redelegated.

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. E7–3719 Filed 3–1–07; 8:45 am]

BILLING CODE 6750–01–P

GENERAL SERVICES ADMINISTRATION

[FMR Bulletin 2007–B1]

Information Technology and Telecommunications Guidelines for Federal Telework and Other Alternative Workplace Arrangement Programs

AGENCY: General Services Administration.

ACTION: Notice.

SUMMARY: This bulletin establishes guidelines for implementing and operating telework and other alternative workplace arrangement programs through the efficient and effective use of information technology and telecommunications. These policies are designed to assist agencies in the implementation and expansion of Federal alternative workplace arrangement programs.

EFFECTIVE DATE: March 2, 2007.

FOR FURTHER INFORMATION CONTACT: For further clarification of content, contact Stanley C. Langfeld, Director, Regulations Management Division (MPR), General Services Administration, Washington, DC 20405; or *stanley.langfeld@gsa.gov*.

Dated: February 21, 2007.

Kevin Messner,

Acting Associate Administrator, Office of Governmentwide Policy.

General Services Administration

[FMR Bulletin 2007–B1]

Real Property

TO: Heads of Federal Agencies

SUBJECT: Information Technology and Telecommunications Guidelines for Federal Telework and Other Alternative Workplace Arrangement Programs

1. *Purpose:* This bulletin establishes guidelines for implementing and operating telework and other alternative workplace arrangement (AWA) programs through the efficient and effective use of information technology and telecommunications.

2. *Expiration Date:* This bulletin will remain in effect indefinitely until specifically cancelled.

3. *Definitions:* Following are terms and definitions used in and for the purpose of this bulletin:

a. Agency Worksite—An agency worksite is the post of duty to which an employee would report if not teleworking.

b. Alternative Worksite—An alternative work location used by teleworkers while teleworking.

c. Broadband—Broadband is a term that commonly and loosely refers to high speed data transmission service. When such service is used for connections to the internet, the Federal Communications Commission (FCC) defines two types of connections: (1) high-speed lines that deliver services at speeds exceeding 200 kilobits per second (kbps) in at least one direction, and (2) advanced services lines that deliver services at speeds exceeding 200 kbps in both directions (see FCC News Release entitled ''Federal Communications Commission Releases Data On High-Speed Services for Internet Access, High-Speed Connections to the Internet Increased by 33% in 2005,'' dated July 26, 2006, *http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-266593A1.doc%3E*).

d. Dial-up—Dial-up refers to the use of an analog telephone line for accessing the internet and remotely connecting to and from an alternative worksite to an agency Information Technology (IT) system. Dial-up access uses normal telephone lines for data transmission and generally has a lower data transfer rate as compared to other internet services.

e. Docking Station—A docking station is a piece of equipment that is used with a laptop computer to allow for the convenient and quick connection of peripheral and/or telecommunications (internet access, for example) equipment by providing the laptop with additional ports, expansion slots, and bays for various types of peripherals and other connections. Typically, the docking station is continuously located in a given workstation and continuously connected to peripherals and telecommunications access; the laptop is slipped in and out of the docking station, as needed. A docking station also enables use of the laptop to resemble the use and convenience of a desktop computer by enabling the user to operate the laptop with a full size external keyboard, monitor, and/or mouse. Thus, a docking station maintains the flexibility of a laptop while giving it the functionality of a desktop computer.

f. External Information Systems—Information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately-owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers or airports); information systems owned or controlled by non-federal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.

g. One Computer Model—Teleworker use of a single computer, usually a laptop, that is transported to all worksites (typically back and forth between an alternative worksite and the agency worksite). The One Computer Model contrasts with multi-computer situations in which the teleworker has a separate computer for use at each worksite and, typically, each of these computers remains at the worksite and is not transported around.

h. Remote Access Servers (RAS)—Remote access servers provide internet and dialup access to the office local area network (LAN). The RAS authenticates the user through a password or stronger mechanism; it then allows the user to access files, printers, or other resources on the LAN. The chief benefit of a RAS is in providing a conveniently packaged comprehensive solution to offsite access needs. Typically, the servers include support for internet-based voice communications, virtual private networks (defined below), and authentication in a package designed to make it easier for administrators to establish and maintain user privileges.

i. Telework—Telework is work performed by an employee at an alternative worksite, which reduces or eliminates the employee's commute or travel to the agency worksite. Alternative worksites may include the employee's home, telework center, satellite office, field installation, or other location.

j. Virtual Private Network (VPN)—The National Institute of Standards and Technology (NIST) defines VPN as ''a logical network that is established, at the application layer of the Open Systems Interconnection (OSI) model, over an existing physical network and typically does not include every node present on the physical network.'' Further, NIST describes how VPN technology uses the internet as the transport medium