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

1. Southeastern Bank Financial Corporation, Augusta, Georgia; to acquire Southern Bank and Trust, Aiken, South Carolina, and thereby engage *de novo* in operating a savings association, pursuant to section 225.28(b)(4)(ii) of Regulation Y.

Board of Governors of the Federal Reserve System, July 20, 2006.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. E6–11819 Filed 7–24–06; 8:45 am]

BILLING CODE 6210–01–S

FEDERAL RESERVE SYSTEM

[Docket No. OP–1260]

Federal Reserve Payment System Risk Policy: Modified Procedures for Measuring Daylight Overdrafts

AGENCY: Board of Governors of the Federal Reserve System.

ACTION: Policy Statement.

SUMMARY: The Board of Governors of the Federal Reserve System (Board) has adopted changes to its Policy on Payments System Risk affecting the procedures for measuring daylight overdrafts. Funds transfers that the Reserve Banks function for certain international organizations using systems other than their payments processing systems will be posted throughout the business day, which is the same treatment as for Fedwire funds transfers.

DATES: *Effective Date:* July 20, 2006.

FOR FURTHER INFORMATION CONTACT: Lisa Hoskins, Assistant Director (202–452–3437) or Susan Foley, Manager (202–452–3596), Division of Reserve Bank Operations and Payment Systems, Board of Governors of the Federal Reserve System; for users of Telecommunications Device for the Deaf (''TDD'') only, contact (202) 263–4869.

SUPPLEMENTARY INFORMATION:

I. Background

The Board's Payment System Risk Policy establishes maximum limits (net debit caps) and fees on daylight overdrafts in depository institutions' accounts at Reserve Banks. When the Board adopted daylight overdraft fees, the Reserve Banks began measuring depository institutions' intraday account balances according to a set of ''posting rules'' established by the Board. These rules comprise a schedule for the posting of debits and credits to institutions' Federal Reserve accounts for different types of payments.[1] The Board's objectives in designing the posting rules include minimizing intraday float, facilitating depository institutions' monitoring and control of their cash balances during the day, and reflecting the legal rights and obligations of parties to payments.

Under these posting rules, certain transactions, including Fedwire funds transfers, Fedwire book-entry securities transfers, and National Settlement Service transactions, are posted as they are processed during the business day. The posting rules do not currently address instances when the Reserve Banks, acting as fiscal agents for certain international organizations, process funds transfers using internal systems other than their payments processing systems, such as Fedwire, to function payments in these institutions' accounts. The legal rights and obligations of the parties to these payments enable the Reserve Banks to treat these funds transfers as final once the accounting entries are made in internal systems. The Board believes that these funds transfers should be treated consistent with Fedwire funds transfers, which are posted throughout the business day, for daylight overdraft measurement purposes. A footnote has been added to the posting rules under Fedwire funds transfers to clarify this treatment of funds transfers processed on internal systems by the Federal Reserve Banks for certain international organizations.

II. Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. ch. 3506; 5 CFR Part 1320, Appendix A.1), the Board has reviewed the policy statement under the authority delegated to the Board by the Office of Management and Budget. No collections of information pursuant to the Paperwork Reduction Act are contained in the policy statement.

Policy on Payments System Risk

In the Federal Reserve Policy on Payments System Risk, section II.A., under heading ''Procedures for Measuring Daylight Overdrafts'' and sub heading ''Post Throughout Business Day'', a new footnote under Fedwire funds transfers will be added. The new footnote will read

[25] Funds transfers that the Reserve Banks function for certain international organizations using internal systems other than payment processing systems such as Fedwire will be posted throughout the business day for purposes of measuring daylight overdrafts.

All subsequent footnotes will be renumbered to accommodate the addition of footnote number 25.

By order of the Board of Governors of the Federal Reserve System, acting through the Director of the Division of Reserve Bank Operations and Payment Systems under delegated authority, July 19, 2006.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. E6–11765 Filed 7–24–06; 8:45 am]

BILLING CODE 6210–01–P

[1] See ''Federal Reserve Policy Statement on Payments System Risk,'' section I.A (57 FR 47093, October 14, 1992).

GENERAL SERVICES ADMINISTRATION

[OMB Control No. 3090–0270]

Federal Acquisition Service; Information Collection; Access Certificates for Electronic Services (ACES)

AGENCY: Office of the Commissioner, GSA.

ACTION: Notice of request for comments regarding a renewal to an existing OMB clearance.

SUMMARY: Under the provisions of the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35), the General Services Administration will be submitting to the Office of Management and Budget (OMB) a request to review and approve a renewal of a currently approved information collection requirement regarding Access Certificates for Electronic Services (ACES). The clearance currently expires on October 31, 2006.

The ACES Program is designed to facilitate and promote secure electronic communications between online automated information technology application systems authorized by law to participate in the ACES Program and users who elect to participate in the program, through the implementation and operation of digital signature certificate technologies. Individual digital signature certificates are issued to individuals based upon their presentation of verifiable proof of identity in an authorized ACES Registration Authority. Business Representative digital signature certificates are issued to individuals based upon their presentation of verifiable proof of identity and verifiable proof of authority from the claimed entity to an authorized ACES Registration Authority.

Public comments are particularly invited on: Whether this collection of

information is necessary and whether it will have practical utility; whether our estimate of the public burden of this collection of information is accurate and based on valid assumptions and methodology; and ways to enhance the quality, utility, and clarity of the information to be collected.

DATES: Submit comments on or before: September 25, 2006.

FOR FURTHER INFORMATION CONTACT: Stephen Duncan, Federal Acquisition Service, at telephone (703) 872–8537 or via e-mail to *stephen.duncan@gsa.gov*.

ADDRESSES: Submit comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to the Regulatory Secretariat (VIR), General Services Administration, Room 4035, 1800 F Street, NW., Washington, DC 20405. Please cite OMB Control No. 3090–0270, Access Certificates for Electronic Services (ACES), in all correspondence.

SUPPLEMENTARY INFORMATION:

A. Background

One of the primary goals of the emerging Government Services Information Infrastructure (GSII) is to facilitate public access to government information and services through the use of information technologies. One of the specific goals of the GSII is to provide the public with a choice of using Internet-based, online access to the automated information technology application systems operated by government agencies; such access will make it easier and less costly for the public to complete transactions with the government. By law, access to some of these automated information technology application systems can be granted only after the agency operating the system is provided with reliable information that the individual requesting such access is who he/she claims to be, and that he/she is authorized such access. The arms-length transactions envisioned by the GSII require implementation of methods for:

1. Reliably establishing and verifying the identity of the individuals desiring to participate in the ACES Program, based primarily upon electronic communications between the applicant and authorized ACES Registration Authority.

2. Issuing to the individuals who have been successfully identified a means that they can use to uniquely identify themselves to the automated information technology application systems participating in the ACES Program.

3. Electronically and securely passing that identity to the automated information technology application system to which the individual is requesting access.

4. Electronically and securely authenticating that identity, through a trusted third party, each time it is presented to an automated information technology application system participating in the ACES Program.

5. Ensuring that the identified individual requesting access to an automated information technology application system has been duly authorized, by the management of that automated information technology application system, to access that system and perform the transactions desired.

6. Ensuring that the information being exchanged between the individual and the automated information technology application system has not been corrupted during transmission.

7. Reducing the ability of the parties to such transactions to repudiate the actions taken.

The current state-of-the-art suggests that digital signature certificate technologies (often referred to as part of ''Public Key Infrastructure, or PKI'') provide a reliable and cost efficient means for meeting many of these GSII requirements. Thus, the ACES Program should be understood to represent an effort to implement and continue a PKI through which members of the public who desire to do so can securely communicate electronically with the online automated information technology application systems participating in the ACES Program.

The initial step for any member of the public to take in order to participate in the ACES Program is to submit an application for an ACES certificate to an authorized ACES Registration Authority. In conjunction with application process, the applicant will be required to submit at least:

a. His/her full name.

b. His/her place of birth.

c. His/her date of birth.

d. His/her current address and telephone number.

e. At least three(3) of the following:

i. Current valid state issued driver license number or number of state issued identification card.

ii. Current valid passport number.

iii. Current valid credit card number.

iv. Alien registration number (if applicable).

v. Social Security Number.

vi. Current employer name, address, and telephone number.

f. If the registration is for a business representative certificate, evidence of authorization to represent that business entity.

The information provided during the process of applying for an ACES certificate constitutes the continued information collection activity that is the subject of this Paperwork Reduction Act Notice and request for comments.

B. Description

A detailed description of the current ACES Program is available on the World Wide Web at *http://www.gsa.gov/aces*, or through the ''FOR FURTHER INFORMATION CONTACT '' listed above.

Please note that all ACES identity information collected from the public is covered by the Privacy Act, the Computer Security Act, and related privacy and security regulations, regardless of whether it is provided directly to an agency of the Federal Government or to an authorized ACES Registration Authority providing ACES-related services under a contract with GSA. Compliance with all of the attending requirements is enforced through binding contracts, periodic monitoring by GSA, annual audits by independent auditing firms, and tri-annual re-accreditation by GSA. Only fully accredited Registration Authorities will be permitted to accept and maintain identity information provided by the public.

The identity information collected will be used only to establish and verify the identity and eligibility of applicants for ACES certificates; no other use of the information is permitted.

Participation in the ACES Program is strictly voluntary, but participation will only be permitted upon presentation of identity information by the applicant, and verification of that information by an authorized ACES Registration Authority.

ACES is designed to permit on-line, arms-length registration through the Internet, which significantly reduces the public's reporting burden. Based upon preliminary tests run on similar systems for gathering identity-related information from the public (*e.g.*, U.S. Passports, initial issuance of state-issued driver's license, etc.), the individual reporting burden for providing identity information for the initial ACES certificate is estimated at an average of 15 minutes, including gathering the information together and entering the data into the electronic forms provided by the authorized ACES Registration Authorities.

Service providers participating in the ACES Program may choose to participate in the E-Authentication Services Component (ASC) as a

Credential Service Provider (CSP). As a result and to support the technical requirements of the ASC CSP's may supply attribute information in Security Assertion Markup Language (SAML) Assertions between the CSP and the Agency e-government application. This applies to SAML based use cases only.

The E-Authentication Service Component leverages credentials from multiple credential providers through certifications, guidelines, standards and policies. The E-Authentication Service Component accommodates assertion based authentication (*i.e.*, authentication of PIN and Password credentials) and certificate-based authentication (*i.e.*, Public Key Infrastructure (PKI) digital certificates, and other forms of strong authentication) within the same environment. The E-Authentication Service Component is aligned with OMB Policy Memorandum M–04–04, EAuthentication Guidance for Federal Agencies (*http://www.whitehouse.gov/omb/memoranda/fy04/m04–04.pdf*), which provides policy guidance for identity authentication and establishes four levels of authentication assurance. It is also aligned with National Institute for Standards and Technology (NIST) Special Publication 800–63, Recommendation for Electronic Authentication *http://csrc.nist.gov/publications/nistpubs/800–63/SP800–63V1__0__2.pdf*. This document accompanies and supports OMB M–04–04 and provides technical and procedural requirements for authentication systems which correlate to the four defined authentication assurance levels defined in OMB M–04–04. The E-Authentication Service Component provides the infrastructure for Federal agencies to implement the policies and recommendations of OMB M–04–04 and NIST SP 800–63. These documents as well as other technical, policy, and informational documents and materials can be accessed at the website: *http://www.cio.gov/eauthentication*.

The Interface Specifications require the following information to be contained in the SAML assertion between the Credential Service Provider and an e-Government Agency Application (AA) which is the relying party to the identity assertion:

Common Name: expressed as First Name, Middle Name, Last Name, suffix surname;

User ID: provided by the CSP so that no two subscribers within a credential service can share the same User ID;

Authentication Assurance Level: *i.e.*, assurance level 1, 2, 3, or 4; and

CSP: CSP is identified in the assertion.

Since the SAML assertion contains only common name and user ID of the end user for the selected CSP, most agencies have determined that a separate activation process is necessary to identify the specific individual as represented in the AA. This generally requires creating a separate query process to identify the end user to the AA. To facilitate the activation process and avoid requiring the end user to reenter the same identifying information multiple times, GSA is also proposing to add the following attribute information to the SAML 1.0 Interface Specifications as optional information:

Partial Social Security Number (SSN): the last four digits of the end users' SSN;

Date of Birth (DOB): MM/DD/YYYY; and

Physical Address: street address, city, state, and zip code.

The end user name, partial SSN, physical address and DOB are intended to allow the AA to identify the correct end user during the activation process, without necessarily requiring the AA to query the end user for any additional information. AAs will match the last four digits of the identity information in the SAML assertion against the information currently maintained in application records systems. The Interface specification requires that CSPs which do not collect or maintain SSN, DOB, and/or physical address information to enter a null field for these attribute elements. The attribute information contained in the assertion is intended for the purposes of activation, and will not be provided to agencies that do not already have the authority to maintain this attribute information. AAs/records systems that do not collect or maintain the attribute fields of SSN, DOB, or physical address will not be passed that information in the SAML assertion from the CSPs. The EAuthentication AAs can also determine that they do not want to receive the additional attribute information of partial SSN, DOB and physical address and can opt out of receiving this information in the SAML assertions.

The E-Authentication Federation/Service Component does not involve any new collection of information from end users. If a Federal agency chooses to create or modify a records system to maintain information expressed in the SAML assertion, it must establish or amend a system of records (SOR) notice through publication in the **Federal Register**. Federal agencies that serve as CSPs or AAs may choose to maintain audit logs for browser-based access; such logs may include transaction data associated with the SAML assertion. Such audit logs are used to monitor browser access and are not considered systems of records requiring coverage under the Privacy Act. Once the identity information is known to the AA, the user interacts directly with the AA for business transactions. While the EAuthentication Service Component addresses the need for common infrastructure for authenticating end users to applications, authorization privileges at the application are beyond the scope of the E-Authentication initiative. Authorization and related functionality such as access control and privilege management are left to the application owners. Ensuring trust between the participating entities of the EAuthentication Federation (AAs, CSPs and End users) is core to the mission of the E-Authentication initiative. The EAuthentication Service Component provides:

- Policies and guidelines for Federal authentication;
- Credential assessments and authorizations;
- Technical architecture and documents, including Interface Specifications, for communications within the E-Authentication Federation Network;
- Interoperability testing of candidate products, schemes or protocols;
- Business rules for operating within the Federation; and
- Management and control of accepted federation schemes operating within the environment.

The E-Authentication Service Component technical approach has two different architectural techniques, assertion-based authentication and certificate-based authentication. PIN and Password authentications typically use assertion-based authentication, where users authenticate to the selected CSP, which in turn asserts their identity to the AA. Certificate-based authentication relies on X.509v3 digital certificates in a Public Key Infrastructure (PKI) for authentication, and can be used at any assurance level. PKI credentials offer considerable advantages for authentication. Certificates can be validated using only public information. Standards for PKI are also more mature than other authentication technologies and more widely used than the emerging standards for assertion-based authentication of PIN and password credentials. Nevertheless, the Authentication Service Component incorporates both assertion-based and certificate-based authentication to

provide the broadest range of flexibility and choices to Federal agencies and end users.

C. Purpose

The General Services Administration (GSA) is responsible for assisting Federal agencies with the implementation and use of digital signature technologies to enhance electronic access to government information and services by all eligible persons. In order to ensure that the ACES program certificates are issued to the proper individuals, GSA will continue to collect identity information from persons who elect to participate in ACES.

D. Annual Reporting Burden

Respondents: 1,000,000.
Responses Per Respondent: 1.
Hours Per Response: .25.
Total Burden Hours: 250,000.
Obtaining Copies of Proposals: Requesters may obtain a copy of the information collection documents from the General Services Administration, Regulatory Secretariat (VIR), 1800 F Street, NW., Room 4035, Washington, DC 20405, telephone (202) 501–4755. Please cite OMB Control No. 3090–0270, Access Certificates for Electronic Services (ACES), in all correspondence.

Dated: July 18, 2006

Michael W. Carleton,

Chief Information Officer.

[FR Doc. E6–11760 Filed 7–24–06; 8:45 am]

BILLING CODE 6820–DH–S

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

[Docket No. 2006N–0038]

Agency Information Collection Activities; Announcement of Office of Management and Budget Approval; Irradiation in the Production, Processing, and Handling of Food

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice.

SUMMARY: The Food and Drug Administration (FDA) is announcing that a collection of information entitled ''Irradiation in the Production, Processing, and Handling of Food'' has been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995.

FOR FURTHER INFORMATION CONTACT: Jonna Capezzuto, Office of Management Programs (HFA–250), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857, 301–827–4659.

SUPPLEMENTARY INFORMATION: In the **Federal Register** of May 11, 2006 (71 FR 27503), the agency announced that the proposed information collection had been submitted to OMB for review and clearance under 44 U.S.C. 3507. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. OMB has now approved the information collection and has assigned OMB control number 0910–0186. The approval expires on June 30, 2009. A copy of the supporting statement for this information collection is available on the Internet at *http://www.fda.gov/ohrms/dockets*.

Dated: July 17, 2006.

Jeffrey Shuren,

Assistant Commissioner for Policy.

[FR Doc. E6–11776 Filed 7–24–06; 8:45 am]

BILLING CODE 4160–01–S

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

Anti-Infective Drugs Advisory Committee; Notice of Meeting

AGENCY: Food and Drug Administration, HHS.

ACTION: Notice.

This notice announces a forthcoming meeting of a public advisory committee of the Food and Drug Administration (FDA). The meeting will be open to the public.

Name of Committee: Anti-Infective Drugs Advisory Committee.

General Function of the Committee: To provide advice and recommendations to the agency on FDA's regulatory issues.

Date and Time: The meeting will be held on September 11 and 12, 2006, from 8 a.m. to 5 p.m.

Location: Hilton-Gaithersburg, Salons A, B, and C, 620 Perry Pkwy, Gaithersburg, MD.

Contact Person: Sohail Mosaddegh, Center for Drug Evaluation and Research (HFD–21), Food and Drug Administration, 5600 Fishers Lane (for express delivery, 5630 Fishers Lane, rm. 1093) Rockville, MD 20857, 301–827–7001, fax: 301–827–6776, e-mail: *sohail.mosaddegh@fda.hhs.gov*, or FDA Advisory Committee Information Line, 1–800–741–8138 (301–443–0572 in the Washington DC area), code 3014512530. Please call the Information Line for up-to-date information on this meeting. The background material will become available no later than the day before the meeting and will be posted on FDA's Web site at *http://www.fda.gov/ohrms/dockets/ac/acmenu.htm* under the heading ''Anti-Infective Drugs Advisory Committee (AIDAC).'' (Click on the year 2006 and scroll down to AIDAC meetings.)

Agenda: On September 11, 2006, the committee will discuss new drug applications (NDAs) 21–931, garenoxacin mesylate tablets, 400 milligrams (mg) and 600 mg, and NDA 21–932, intravenous garenoxacin mesylate, 400 mg (200 milliliters (mL) of 2 mg/mL) and 600 mg (300 mL of 2 mg/mL), proposed trade name GENINAX, submitted by Schering Corp., for the proposed treatment indications of acute bacterial exacerbation of chronic bronchitis, acute bacterial sinusitis, community-acquired pneumonia, complicated and uncomplicated skin and skin structure infections, and complicated intra-abdominal infections. On September 12, 2006, the committee will discuss supplemental new drug application (sNDA) 21–158/S–006, Factive (gemifloxacin mesylate) Tablets, submitted by Oscient Pharmaceuticals Corp., for the proposed treatment of acute bacterial sinusitis.

Procedure: Interested persons may present data, information, or views, orally or in writing, on issues pending before the committee. Written submissions may be made to the contact person on or before August 25, 2006. Oral presentations from the public will be scheduled between approximately 1:30 p.m. and 2 p.m. on September 11, 2006, and between approximately 1 p.m. and 1:30 p.m. on September 12, 2006. Time allotted for each presentation may be limited. Those desiring to make formal oral presentations should notify the contact person and submit a brief statement of the general nature of the evidence or arguments they wish to present, the names and addresses of proposed participants and an indication of the approximate time requested to make their presentation on or before August 25, 2006.

Persons attending FDA's advisory committee meetings are advised that the agency is not responsible for providing access to electrical outlets.

FDA welcomes the attendance of the public at its advisory committee meetings and will make every effort to accommodate persons with physical disabilities or special needs. If you require special accommodations due to a disability, please contact Sohail Mosaddegh (see *Contact Person*) at least 7 days in advance of the meeting.