Summary: EPA has no objections to the proposed project.

EIS No. 20050254, ERP No. FS–NOA–C91004–00, Amendment to the Fishery Management Plans (FMPs), Amendment 2 for the Spiny Lobster Fishery; Amendment 1 for the Queen Conch Resources; Amendment 3 for the Reef Fish Fishery; Amendment 2 Corals and Reef Associated Invertebrates, U.S. Caribbean to Address Required Provisions MSFCMA, Puerto Rico and the U.S. Virgin Island.

Summary: EPA has no objections to the proposed project.

Dated: August 2, 2005.

Robert W. Hargrove,

Director, NEPA Compliance Division, Office of Federal Activities.

[FR Doc. 05–15521 Filed 8–4–05; 8:45 am]

BILLING CODE 6560–50–P

FEDERAL RESERVE SYSTEM

Change in Bank Control Notices; Acquisition of Shares of Bank or Bank Holding Companies

The notificants listed below have applied under the Change in Bank Control Act (12 U.S.C. 1817(j)) and § 225.41 of the Board's Regulation Y (12 CFR 225.41) to acquire a bank or bank holding company. The factors that are considered in acting on the notices are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The notices are available for immediate inspection at the Federal Reserve Bank indicated. The notices also will be available for inspection at the office of the Board of Governors. Interested persons may express their views in writing to the Reserve Bank indicated for that notice or to the offices of the Board of Governors. Comments must be received not later than August 19, 2005.

A. Federal Reserve Bank of Kansas City (Donna J. Ward, Assistant Vice President) 925 Grand Avenue, Kansas City, Missouri 64198-0001:

1. Kenneth D. Klehm, Edmond, Oklahoma, and G. Blake Hogan, Houston, Texas, as trustees of the William M. Cameron 2004 Family Trusts, Oklahoma City, Oklahoma; and John W. Rex and Theodore M. Elam, as trustees of the Lynda L. Cameron 2004 Trust, all of Oklahoma City, Oklahoma, to retain voting shares of First Fidelity Bancorp, Inc., and thereby indirectly retain voting shares of First Fidelity Bank, N.A., both in Oklahoma City, Oklahoma.

Board of Governors of the Federal Reserve System, August 1, 2005.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. 05–15502 Filed 8–4–05; 8:45 am]

BILLING CODE 6210–01–S

FEDERAL RESERVE SYSTEM

Formations of, Acquisitions by, and Mergers of Bank Holding Companies

The companies listed in this notice have applied to the Board for approval, pursuant to the Bank Holding Company Act of 1956 (12 U.S.C. 1841 *et seq.*) (BHC Act), Regulation Y (12 CFR Part 225), and all other applicable statutes and regulations to become a bank holding company and/or to acquire the assets or the ownership of, control of, or the power to vote shares of a bank or bank holding company and all of the banks and nonbanking companies owned by the bank holding company, including the companies listed below.

The applications listed below, as well as other related filings required by the Board, are available for immediate inspection at the Federal Reserve Bank indicated. The application also will be available for inspection at the offices of the Board of Governors. Interested 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 August 29, 2005.

A. Federal Reserve Bank of St. Louis (Glenda Wilson, Community Affairs Officer) 411 Locust Street, St. Louis, Missouri 63166-2034:

1. Lonoke Bancshares, Inc., Lonoke, Arkansas; to acquire 14.68 percent of the voting shares of First Southern Bank, Batesville, Arkansas (in organization).

B. Federal Reserve Bank of San Francisco (Tracy Basinger, Director, Regional and Community Bank Group) 101 Market Street, San Francisco, California 94105-1579:

1. Cowlitz Bancorporation, Longview, Washington; to merge with AEA Bancshares, Inc., Seattle, Washington, and thereby indirectly acquire voting shares of Asia–Europe–Americas Bank, Seattle, Washington.

Board of Governors of the Federal Reserve System, August 1, 2005.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. 05–15501 Filed 8–4–05; 8:45 am]

BILLING CODE 6210–01–S

GENERAL SERVICES ADMINISTRATION

National Travel Forum 2006: Where the Travel Stars Shine

(NTF 2006)

AGENCY: Office of Governmentwide Policy, General Services Administration (GSA).

ACTION: Notice.

SUMMARY: The General Services Administration (GSA) is announcing that it will hold its fourth National Travel Forum. The National Travel Forum 2006: Where the Travel Stars Shine (NTF 2006) will take place June 26–29, 2006 at the Westin Bonaventure Hotel in Los Angeles, California. Nearly 1,500 travel, relocation, financial and other professionals within Federal, State, and local governments, as well as the private sector will attend. To attend, exhibit, or hold an agency-wide meeting, visit the NTF 2006 web site at *http://www.nationaltravelforum.org.*

FOR FURTHER INFORMATION CONTACT Michael Hopkins, Project Manager, Office of Travel, Transportation, and Asset Management, at (202) 208–4421, or by e-mail to *michael.hopkins@gsa.gov.*

SUPPLEMENTARY INFORMATION:

Dated: August 1, 2005.

Peggy DeProspero,

Travel Management Policy.

[FR Doc. 05–15514 Filed 8–4–05; 8:45 am]

BILLING CODE 6820–14–S

GENERAL SERVICES ADMINISTRATION

[C–05–N01]

Notice; Establishment of E-Authentication Service Component

AGENCY: Office of Governmentwide Policy, General Services Administration, GSA.

ACTION: Notice and request for comments.

SUMMARY: In accordance with the Privacy Act of 1974, as amended, the General Services Administration (GSA) proposes to establish the E-Authentication Federation, or ''Service Component.'' The E-Authentication Service Component is a common infrastructure for electronically authenticating the identity of users of Federal E-Government services Governmentwide. Using a common network, this infrastructure links identity suppliers (termed Credential Service Providers or CSPs) and identity consumers (termed Agency Applications or AAs) enabling participating CSPs and AAs to communicate in a standardized way. The E-Authentication Service Component does not create or maintain any new Federal System of Records, but does provide for the authorized exchange of information among systems of records that have been or will be established to support Federal E-Government programs and services.

DATES: Submit comments on or before: September 6, 2005.

FOR FURTHER INFORMATION CONTACT: David Temoshok, Director, Identity Policy and Practices, Office of Governmentwide Policy at telephone (202) 208–7655 or via e-mail to *david.temoshok@gsa.gov*.

ADDRESSES: Comments on this Notice should be addressed to David Temoshok, Director for Identity Policy and Practices, Office of Governmentwide Policy. Comments should be mailed to the attention of Ms. Barbara J. Vitko, GSA 1800 F Street NW, Room 2239, Office of Technology Strategy, Washington, DC, 20405–0002. Comments may be submitted by facsimile to (202) 219–1533.

SUPPLEMENTARY INFORMATION: As part of the President's Management Agenda, the E-Authentication Service Component is established to enable trust and confidence in E-Government transactions through the establishment of an integrated policy and technical infrastructure for electronic authentication. Through this initiative, citizens, businesses, and governmental entities will have simpler access to multiple agency applications through the re-use of credentials and established identities. GSA is making the E-Authentication Service Component (ASC) available to Federal E-Government applications through the Federal Enterprise Architecture. In this way, Federal agencies can use the common policy and technical infrastructure of the ASC without the cost and burden of re-creating the infrastructure individually.

GSA has been designated by the Office of Management and Budget (OMB) as the lead agency for the development, implementation and operation of the Federal electronic authentication infrastructure. GSA has established a Program Management Office (PMO) in the Federal Technology Service for the operation of the ASC. The GSA Office of Governmentwide Policy provides policy support for the initiative.

After careful analyses and proofs-of-concept, GSA determined that the most viable means to implement a common E-Authentication infrastructure was through a decentralized approach. 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. Over time, the E-Authentication Service Component will support multiple protocols and communication schemes and, therefore, is not built around a single scheme or commercial product. The E-Authentication Service Component currently uses the industry standard of SAML 1.0.

The E-Authentication Service Component is aligned with OMB Policy Memorandum M–04–04, E-Authentication 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/SP800–63v6__3__3.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*.

Following are the key requirements and design goals established for the E-Authentication initiative.

Key Requirements:

- *Leverage credentials*: A credential from any approved credential service should be usable at any application of equal or lower assurance level. Agency applications must be able to leverage existing credentials rather than establish new identity management systems.
- *Single Sign-on*: Once a user has authenticated they must be able to move among applications with equivalent assurance levels without re-authenticating. For privacy considerations, the end user is required to take an explicit action to opt into single sign-on for that browser session.
- *Privacy*: There must be no central repository of personal information about end users and no centralized database. Credentialing must be federated among multiple providers. End users can choose to federate their identity information as they determine appropriate.
- *Security controls*: The architecture must provide for explicit control over which applications and credential services can join and participate in the E-Authentication Federation.

Design Goals:

- *Standards*: The architecture should rely on existing industry standards.
- *COTS*: The architecture should employ multiple Commercial-off-the-Shelf (COTS) products that have demonstrated the capability to interoperate.
- *Federation*: Authentication should be federated among multiple credential providers.
- *Durability*: The architecture should be designed to allow for the evolution of technology, providing for easy migration as the industry and technology evolves.
- *Flexibility*: The architecture should not create undue reliance on any single standard, vendor, product, or integrator.

Based on these requirements and design goals, the technical approach for E-Authentication is to allow for multiple identity management schemes (*e.g.*, identity proofing, credential technology, credential strength, credential management) within a single architecture. The framework includes a methodology and process for the evaluation and adoption of these schemes over time. The goal of the framework is to provide a lasting architectural model for E-Authentication that is not irrevocably bound to a single industry standard, vendor, or product.

The Federal E-Authentication Service Component establishes four levels of authentication assurance, defines risk management guidelines for associating a required level of authentication to applications, and provides a Credential Assessment Framework for evaluating authentication systems to determine whether they meet Federal standards for any of the four specified authentication levels. The initiative also provides a technical architecture that leverages federated identity through the use of Security Assertion Markup Language (SAML) 1.0, PKI (X509 v.3 certificates), and the Federal Bridge Certification Authority.

The E-Authentication Federation:

The E-Authentication Service Component is designed to ensure that government services delivered over the Internet are accessed by and delivered to the intended individual. The E-Authentication Service Component allows authorized participants to share responsibility for federating identity to mutual benefit. Together, the E-Authentication Service Component and the authorized participants of the service component represent the E-Authentication Federation. The participants of the E-Authentication Federation are:

- *Agency Applications (AAs)*: E-Government applications that perform some business function online. If an E-Government application has multiple interfaces (*e.g.*, administration and service application), each interface with distinct authentication requirements is considered a stand-alone AA. Agency Applications manage all business transactions and all end user authorization decisions. One of the principle goals of the E-Authentication initiative is to provide broad authentication services to AAs, making separate credentialing unnecessary.
- *Credential Services Providers (CSPs)*: Commercial or government services which provide end users identity management services which include credentials that can be used at E-Authentication-enabled AAs. Credential Services Providers are authorized to participate in the E-Authentication Federation by the GSA E-Authentication Program Management Office (PMO). Authorized CSPs are presented to the public on the E-Authentication Federation Trust List. The Trust List of Authorized Credential Services is available at the E-Authentication website (*http://www.cio.gov/eauthentication/TCSPlist.htm*) and at the E-Authentication portal.
- *E-Authentication Portal*: A website that helps users locate the CSPs and AAs they need to complete their transactions. The portal is maintained and operated by the E-Authentication PMO.
- *End Users*: Any citizen, Government employee, contractor, business, or governmental entity that uses an AA. One of the principle goals of E-Authentication is to make the end user experience as simple as possible by improving the availability and ease of use of credentials.

Authentication Service Component Operations:

Within the framework of the E-Authentication Service Component, the end user interacts directly with AAs, CSPs, and the E-Authentication Portal. Typically the user starts at the portal in order to locate the appropriate AAs and CSPs which the end user intends to use. The end user can choose the AA that they wish to access and the CSP that they choose to validate their credential(s). In general, AAs are E-Government services that agencies provide end users; typically, the agencies maintain records on individuals' use of the services provided. Authentication of end users is required to allow authorization privileges in accordance with the rules of the AA. The E-Authentication Federation uses the term ''activation process'' to refer to the process of matching the authenticated end user to the correct individual in an AA records system.

The end user interacts directly with the CSP to obtain, manage, and validate their credentials. The CSP interacts directly with the AA in order to pass the end users' identity information. The identity information that is passed between the CSP and the AA is standardized for the E-Authentication Federation through the requirements of the E-Authentication Technical Interface Specifications. The ASC currently uses the OASIS standard Security Assertion Mark-up Language (SAML) 1.0 to express authentication identity assertions. Technical documents describing the E-Authentication architecture and the E-Authentication Interface Specifications for the SAML Artifact Profile can be found at *http://www.cio.gov/eauthentication/TechSuite.htm*. 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 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 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 E-Authentication 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 E-Authentication 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 E-Authentication Federation (AAs, CSPs and End users) is core to the mission of the E-Authentication initiative. The E-Authentication 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 E-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.

System of Records Notice Requirements:

The purpose of the notice is to explain the E-Authentication Service Component, how it operates, and how participants, including end users, in the Federation relate. The E-Authentication Service Component portal merely routes the end user to the AA or CSP which the end user has chosen to access. The portal maintains no personally identifiable information about end users and therefore this notice proposes no new Privacy Act system of records.

However, Federal agency participants in the E-Authentication Service Component may maintain systems of records under the Privacy Act. Federal participants maintaining Privacy Act Systems of Records relating to identity authentication must develop appropriate systems of records notices with routine uses providing for the exchange of information through the Federation. As an initial matter, agencies must ensure they possess the appropriate authority to collect and maintain records in order to interface with the E-Authentication Federation. Additionally, agencies must publish Privacy Act Systems of Records notices in the **Federal Register** in accordance with guidance set out in OMB Circular A–130, Appendix 1. For further information contact, E-Authentication Service Component manager, Stephen Timchak, Director, E-Authentication Program Management Office, Suite 911, 2001 Crystal Drive, Arlington VA 22202. Mr. Timchak can be reached at 703–872–8604 or via email *Stephen.timchak@gsa.gov.*

Dated: August 1, 2005

June V. Huber,

Director, Office of Information Management.

[FR Doc. 05–15515 Filed 8–4–05; 8:45 am]

BILLING CODE 6820–34–S

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Agency for Healthcare Research and Quality

Meeting of the Citizens' Health Care Working Group

AGENCY: Agency for Healthcare Research and Quality (AHRQ), HHS.

ACTION: Notice of public meeting and hearing.

SUMMARY: In accordance with section 10(a) of the Federal Advisory Committee Act, this notice announces a meeting and hearing of the Citizens' Health Care Working Group mandated by section 1014 of the Medicare Modernization Act.

In addition, the Working Group will sponsor a community forum in which members of the working group will participate.

DATES: The meeting will be held on Tuesday, August 16, 2005, from 1 p.m. to 3:30 p.m. The community forum will be held on Tuesday August 16, 2005, from 5:30 p.m. to 7 p.m. The hearing will be held Wednesday, August 17, 2005, from 8:30 a.m. to 2:30 p.m.

ADDRESSES: Both Tuesday's meeting and Wednesday's hearing will be held at The Conference Center at Harvard Medical, 77 Avenue Louis Pasteur, Boston, MA 02115, in the Harvard Institute of Medicine (HIM) Meeting Room, First Floor.

The community forum will be held at the same address in Harvard Medical's Amphitheater. The amphitheater is located on the ground floor.

The meeting, community forum, and hearing are all open to the public.

FOR FURTHER INFORMATION CONTACT: Caroline Taplin, Citizens' Health Care Working Group, at (301) 443–1515 or *ctaplin@ahrq.gov.* If sign language interpretation or other reasonable accommodation for a disability is needed, please contact Mr. Donald L. Inniss, Director, Office of Equal Employment Opportunity Program, Program Support Center, on (301) 443–1144.

The agenda for these three Working Group events is available on the Citizens' Working Group Web site, *http://www.citizenshealthcare.gov.* Also available at that site is a roster of Working Group members. When transcriptions of the Group's August 16 and 17 meeting and hearing are completed, they will be available on the website.

SUPPLEMENTARY INFORMATION: Section 1014 of Pub. L. 108–173, (known as the