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 October 8, 2004.

A. Federal Reserve Bank of New York (Jay Bernstein, Bank Supervision Officer) 33 Liberty Street, New York, New York 10045–0001:

1. Excel Bancorp LLC, New York, New York to become a bank holding company by acquiring 96.93 percent of the voting shares of Excel Bank, National Association, New York, New York.

B. Federal Reserve Bank of Minneapolis (Jacqueline G. Nicholas, Community Affairs Officer) 90 Hennepin Avenue, Minneapolis, Minnesota 55480–0291:

1. First National Bancorp, Inc., Brewster, Minnesota; to become a bank holding company by acquiring 100 percent of the voting shares of Nobles Agency, Inc., Brewster, Minnesota, and thereby indirectly acquire voting shares of The First National Bank of Brewster, Brewster, Minnesota. Applicant also proposes through the acquisition of Nobles Agency, Inc., Brewster, Minnesota, to engage in insurance agency activities in a town with a population not exceeding 5,000, pursuant to section 225.28(b)(11)(iii)(A) of Regulation Y.

Board of Governors of the Federal Reserve System, September 9, 2004.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. 04–20733 Filed 9–14–04; 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 October 12, 2004.

A. Federal Reserve Bank of Atlanta (Sue Costello, Vice President) 1000 Peachtree Street, N.E., Atlanta, Georgia 30303:

1. United Community Banks, Inc., Blairsville, Georgia; to merge with Liberty National Bancshares, Inc., and thereby indirectly acquire voting shares of Liberty National Bank, both of Conyers, Georgia.

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

1. Country Bancshares, Inc., Jamesport, Missouri; to retain 9.14 percent of the voting shares of Branson Bancshares, Inc., and thereby indirectly retain voting shares of Branson Bank, both of Branson, Missouri.

Board of Governors of the Federal Reserve System, September 10, 2004.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. 04–20803 Filed 9–14–04; 8:45 am]

BILLING CODE 6210–01–S

FEDERAL RESERVE SYSTEM

Notice of Proposals to Engage in Permissible Nonbanking Activities or to Acquire Companies that are Engaged in Permissible Nonbanking Activities

The companies listed in this notice have given notice under section 4 of the Bank Holding Company Act (12 U.S.C. 1843) (BHC Act) and Regulation Y (12 CFR Part 225) to engage *de novo*, or to acquire or control voting securities or assets of a company, including the companies listed below, that engages either directly or through a subsidiary or other company, in a nonbanking activity that is listed in § 225.28 of Regulation Y (12 CFR 225.28) or that the Board has determined by Order to be closely related to banking and permissible for bank holding companies. Unless otherwise noted, these activities will be conducted throughout the United States.

Each notice is available for inspection at the Federal Reserve Bank indicated. The notice also will be available for inspection at the offices of the Board of Governors. Interested persons may express their views in writing on the question whether the proposal complies with the standards of section 4 of the BHC Act. 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 the applications must be received at the Reserve Bank indicated or the offices of the Board of Governors not later than October 12, 2004.

A. Federal Reserve Bank of Cleveland (Cindy C. West, Banking Supervisor) 1455 East Sixth Street, Cleveland, Ohio 44101–2566:

1. Park National Corporation, Newark, Ohio; to acquire First Federal Bancorp, Inc., and thereby indirectly acquire First Federal Savings Bank of Eastern Ohio, both of Zanesville, Ohio, and thereby engage in operating a savings association, pursuant to section 225.28(b)(4)(ii) of Regulation Y.

Board of Governors of the Federal Reserve System, September 10, 2004.

Robert deV. Frierson,

Deputy Secretary of the Board.

[FR Doc. 04–20802 Filed 9–14–04; 8:45 am]

BILLING CODE 6210–01–S

FEDERAL TRADE COMMISSION

Email Authentication Summit

AGENCIES: The Federal Trade Commission (''FTC'' or the ''Commission'') and the National Institute of Standards and Technology (''NIST''), United States Department of Commerce.

ACTION: Notice announcing email authentication summit, request for comments, and solicitation of requests to participate.

DATES: The Email Authentication Summit will be held on November 9–10, 2004, from 8:30 a.m. to 5:30 p.m. at the Federal Trade Commission, Satellite

Building, 601 New Jersey Ave., NW., Washington, DC 20001. The event is open to the public, and there is no fee for attendance. Pre-registration is not required.

Comments: Written comments should be submitted on or before September 30, 2004. For further information, please see the ''Request for Comments'' section of this Notice.

Participants: Written Requests to Participate in the Email Authentication Summit must be filed by September 30, 2004. For further information, please see the ''Requests to Participate'' section of this Notice. Parties submitting Requests to Participate will be notified by October 15, 2004, if they have been selected.

ADDRESSES: Written comments should be identified as ''Email Authentication Summit-Comments,'' and written requests to participate in the Email Authentication Summit should be identified as ''Email Authentication Summit-Request to Participate.'' Written Comments and Requests to Participate should be submitted to: Secretary, Federal Trade Commission, Room 159–H (Annex V), 600 Pennsylvania Ave., NW., Washington, DC 20580. If submitting in paper form, parties must submit an original and three copies of each document. The FTC requests that any comment filed in paper form be sent by courier or overnight service, since U.S. postal mail in the Washington area and at the Commission is subject to delay due to heightened security precautions.

In the alternative, parties may email Comments and Requests to Participate to *authenticationsummit@ftc.gov*. To ensure that the Commission considers an electronic comment, you must file it with the FTC at this email address.

For further requirements concerning the filing of Comments and Requests to Participate, please see the Request for Comments and Requests to Participate sections of this Notice.

FOR FURTHER INFORMATION CONTACT: Sana D. Coleman, Attorney, (202) 326–2249. A detailed agenda and additional information on the Email Authentication Summit will be posted on the FTC's Website, *http://www.ftc.gov*, by November 7, 2004.

SUPPLEMENTARY INFORMATION:

Section A. Introduction

In the Commission's June 15, 2004 National Do Not Email Registry Report to Congress, the Commission explained that significant security, enforcement, practical, and technical challenges rendered a registry an ineffective solution to the spam problem.[1] The Report, however, identified domain-level authentication as a promising technological development that would enable Internet Service Providers (''ISPs'') and other domain holders to better filter spam, and that would provide law enforcement with a potent tool for locating and identifying spammers. The Report concluded that the Commission could play an active role in spurring the market's development, testing, evaluation, and deployment of domain-level authentication systems. As a first step, the Report explained that the Commission, with other relevant government agencies, would host an Email Authentication Summit in the Fall of 2004. This **Federal Register** Notice explains that the Commission and the Department of Commerce's National Institute of Standards and Technology (''NIST'') will be hosting the Summit on November 9–10, 2004, asks for comments on a number of issues concerning email authentication standards, and solicits requests to participate in the Summit.

Section B. Background

The Simple Mail Transfer Protocol (''SMTP''), the Internet protocol for the email system, allows information to travel freely with relative anonymity and ease. SMTP facilitates the proliferation of spam by making it possible and cost-efficient for illegitimate marketers to send spam to billions of email accounts worldwide, while allowing them to hide their identities and the origins of their email messages.

Spammers use many techniques to hide, including ''spoofing,'' open relays, open proxies, and ''zombie drones,'' including ''zombie nets.'' First, spammers use spoofing to falsify header information and hide their identities. This technique disguises an email to make it appear to come from an address other than the one from which it actually comes. A spammer can falsify portions of the header or the entire header. The SMTP system facilitates this practice because it does not require accurate routing information except for the intended recipient of the email. By failing to require accurate sender identification, SMTP allows spammers to send email without accountability, often disguised as personal email. A spammer can send out millions of spoofed messages, but any bounced messages—messages returned as undeliverable—or complaints stemming from the spoofed emails will only go to the person whose address was spoofed. The spammer never has to deal with them. As a result, an innocent email user's inbox may become flooded with undeliverable messages and angry, reactive email, and the innocent user's Internet service may be shut off due to the volume of complaints.

Second, many spammers use open relays to disguise the origin of their email. A computer must be connected to a mail server to send or receive mail. When someone sends an email message using an email server that is ''secure,'' the mail server's software checks to make sure that the sender's computer and email account are authorized to use that server. If this authorization is in order, then the server sends the email. If the computer and email account are not listed as authorized, the server refuses to accept and send the email message. On the other hand, if a mail server is not secure, *i.e.*, some of its settings allow it to stay open, it will forward email even though the sender is not an authorized user of that server. An open server is called an open relay because it will accept and transfer email on behalf of any user anywhere.

Spammers who use open relays effectively bypass the email servers to which their computers are connected. Once the spam passes through an open relay, a routing header from that server is added to the email. Thus, the email will appear as if it originated from the relay mail server. This allows spammers to obscure their tracks, making it difficult to trace the path their message takes from sender to recipient.

Third, many spammers use ''open proxies.'' They began doing this after ISPs and other mail server operators realized the negative impact of open relays and made efforts to identify and close them. Most organizations have multiple computers on their networks, but have a smaller number of proxy servers that are the only machines on the network that directly interact with the Internet. This system provides more efficient web browsing for the users within that organization and secures the organization's network against unauthorized Internet users from outside the organization. If the proxy is not configured properly, it is considered to be ''open,'' and may allow an unauthorized Internet user to connect through it to other hosts (computers that control communications in a network or administer databases) on the Internet.

Fourth, the most recent escalation in this cat-and-mouse game involves the exploitation of millions of home

[1] ''National Do Not Email Registry, A Report to Congress,'' by the Federal Trade Commission, June 2004. The Report is posted online at *http://www.ftc.gov/reports/dneregistry/report.pdf*.

computers, using malicious viruses, worms, or ''Trojans.'' These infections, often sent via spam, turn any computer into an open or compromised proxy called ''zombie drones.'' When large collections of zombie drones are under centralized command, they are called ''zombie nets.'' Once a computer is infected with one of these programs, a spammer can remotely hijack and send spam from that computer. Spammers target home computers with high speed Internet connections, such as DSL or cable modem lines, that are poorly secured. Spam sent via zombie drones will appear to originate (and actually will originate) from these infected computers. This practice is all the more pernicious because users often do not know that their home computers are infected. The outgoing spam does not show up in their outbox. Once an ISP realizes spam is coming from one of its customer's machines, the ISP must shut off the customer's Internet service even though the customer had no knowledge that the spammer was using his or her machine.

Obfuscatory techniques such as spoofing, open relays, open proxies, and zombie drones make it more difficult for ISPs to locate spammers. When ISPs and domain holders implement technologies designed to stop one exploitative technique, spammers quickly adapt, finding new methods to avoid detection. If the cloak of anonymity were removed, however, spammers could not operate with impunity. ISPs and domain holders could filter spam more effectively, and the government and ISPs could more effectively identify and prosecute spammers who violate the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the ''CAN–SPAM Act''), 15 U.S.C. 7708, or other statutes.[2]

To remove this cloak of anonymity, ISPs and others involved with the email system have proposed domain-level authentication systems—systems that would enable a receiving mail server to verify that an email message actually came from the sender's purported domain. In other words, if a message claimed to be from *abc@ftc.gov*, the private market authentication proposals would authenticate that the message came from the domain ''ftc.gov,'' but would not authenticate that the message came from the particular email address ''abc'' at this domain.

There are two well-publicized private market authentication proposals, ''Sender ID'' and ''DomainKeys.'' Sender ID, a combination of an earlier proposed authentication standard called SPF (''sender policy framework'') and Microsoft's ''Caller ID for Email,'' would require senders of email to list the IP addresses from which they send email in the domain name system (the ''DNS system''). Receiving servers would compare the IP addresses listed in a message's header with those listed in the DNS system to determine if the message was coming from an authenticated IP address.

DomainKeys uses public key/private key cryptography to authenticate email messages. A domain that sends email would create a public/private key pair and post the public key in the DNS system. For each message, the sending domain would generate a digital signature by applying the private key algorithm to the entire message. The sending domain would then add the digital signature in the message's header. The receiving mail server would then use the public key to verify that the digital signature was generated by the matching private key.

While Sender ID and DomainKeys are the best known of the proposed authentication standards, other participants in the email system have proposed or intend to propose other domain-level authentication standards. For example, this Fall, the Internet Engineering Task Force, the Internet's standards setting body, is expected to forward an SPF-modeled authentication standard to one of its internal committees, the Internet Engineering Steering Group, which will decide whether to accept any such SPF-based model as a proposed or experimental standard or send it back for revision.

To encourage the development, testing, evaluation and implementation of domain-level authentication systems, the Commission will conduct a two-day Email Authentication Summit. This Summit will be co-sponsored with NIST. The Summit will be held on November 9–10, 2004 in Washington, DC. The purpose of the Summit is to facilitate a discussion among technologists from ISPs, businesses and individuals who operate their own mail servers, computer scientists, and other interested parties regarding technological challenges of the various authentication proposals, the ability of small ISPs and domain holders to participate in the authentication systems, the costs associated with the various proposals, the international implications associated with the proposals, and other issues that impact the time frame for and viability and effectiveness of wide-scale adoption of domain-level authentication systems for email.

Section C. Request for Comments

Parties who wish to submit written comments addressing the Email Authentication Summit must do so by September 30, 2004. Written comments may be filed in either paper or electronic form. Written comments should refer to ''Email Authentication Summit—Comments, (Matter Number P044411)'' to facilitate the organization of comments. A comment filed in paper form should include this reference both in the text and on the envelope, and the original and three copies should be mailed or delivered to the following address: Federal Trade Commission/ Office of the Secretary, Room 159–H (Annex V), 600 Pennsylvania Avenue, NW., Washington, DC 20580. If the comment contains any material for which confidential treatment is requested, it must be filed in paper (rather than electronic) form, and the first page of the document must be clearly labeled ''Confidential.'' The FTC is requesting that any comment filed in paper form be sent by courier or overnight service, if possible, because U.S. postal mail in the Washington area and at the Commission is subject to delay due to heightened security precautions. Comments filed in electronic form (except comments containing any confidential material) should be sent to the following email box: *authenticationsummit@ftc.gov.*

Written comments may address the issues identified below and any other issues in connection with the adoption and implementation of any of the proposed authentication standards.

1. Whether any of the proposed authentication standards (either alone or in conjunction with other existing technologies) would result in a significant decrease in the amount of spam received by consumers.

2. Whether any of the proposed authentication standards would require modification of the current Internet protocols and whether any such modification would be technologically and practically feasible.

3. Whether any of the proposed authentication standards would function with the software and hardware currently used by senders and recipients of email and operators of sending and receiving email servers. If not, what additional software or hardware would the sender and recipient need, how much it would cost, whether it would be required or optional, and where it would be obtained.

[2] SMTP, its abuse by spammers, and the benefits of domain-level authentication are discussed in detail in the Commission's June 2004 National Do Not Email Registry Report to Congress, available at *http://www.ftc.gov/reports/dneregistry/report.pdf.*

4. How operators of receiving email servers are likely to handle un-authenticated messages.

5. Whether any of the proposed authentication standards could result in email being incorrectly labeled as authenticated or unauthenticated (false negatives and false positives), and the steps that could be taken to limit such occurrences.

6. Whether the authentication standards are mutually exclusive or interoperable. Whether any of the proposed authentication standards would integrate with any other standards. For example, if Mail Server A is using standard X, will it accept email easily from Mail Server B that is using standard Y?

7. Whether any of the proposed authentication standards would have to be an open standard (i.e., a standard with specifications that are public).

8. Whether any of the proposed authentication standards are proprietary and/or patented.

9. Whether any of the proposed authentication standards would require the use of goods or services protected by intellectual property laws.

10. How any of the proposed authentication standards would treat email forwarding services.

11. Whether any of the proposed authentication standards would have any implications for mobile users (e.g., users who may be using a laptop computer, an email-enabled mobile phone, or other devices, and who legitimately send email from email addresses that are not administratively connected with their home domain).

12. Whether any of the proposed authentication standards would have any implications for roving users (i.e., users who are obliged to use a third-party submission service when unable to connect to their own submission service).

13. Whether any of the proposed authentication standards would affect the use of mailing lists.

14. Whether any of the proposed authentication standards would have any implications for outsourced email services.

15. Whether any of the proposed authentication standards would have an impact on multiple apparent responsible identities (e.g., in cases where users send email using their Internet Service Provider's SMTP network but have their primary email account elsewhere).

16. Whether any of the proposed authentication standards would have an impact on web-generated email.

17. Whether the proposed authentication standards are scalable. Whether the standards are computationally difficult such that scaling over a certain limit becomes technologically impractical. Whether the standards are monetarily expensive due to hardware and resource issues so that scaling over a certain limit becomes impractical.

18. Identify any costs that would arise as a result of implementing any of the proposed authentication standards, and identify who most likely would bear these costs (e.g., large ISPs, small ISPs, consumers, or email marketers).

19. Whether ISPs that do not participate in an authentication regime would face any challenges providing email services. If so, what types of challenges these ISPs would face and whether these challenges would in any way prevent them from continuing to be able to provide email services.

20. Whether an Internet-wide authentication system could be adopted within a reasonable amount of time. Description of industry and standard-setting efforts, whether there is an implementation schedule in place and, if so, the time frames of the implementation schedule.

21. Whether any of the authentication standards would delay current email transmission times, burden current computer mechanisms, or otherwise adversely affect the ease of email use by consumers.

22. Whether any of the proposed authentication standards would impact the ability of consumers to engage in anonymous political speech.

23. Whether any safeguards are necessary to ensure that the adoption of an industry-wide authentication standard does not run afoul of the antitrust laws.

24. Whether a spammer or hacker could compromise any of the proposed authentication standards by using, for example, zombie drones, spoofing of originating IP addresses, misuse of public/private key cryptography, or other means.

25. Whether any of the proposed authentication systems would prevent ''phishing,'' a form of online identity theft.

26. Whether the operators of small ISPs and business owners would have the technical capacity to use any of the proposed authentication standards. Whether any of the authentication standards could be reasonably implemented by smaller ISPs.

27. Whether any of the proposed authentication standards would have cross-border implications.

28. Whether any of the proposed authentication standards would require an international civil cryptographic standard or other internationally adopted standard and, if so, the implications of this requirement.

29. Description of how the Email Authentication Summit can support industry or standard-setting efforts.

30. Assuming a domain-level authentication system is established in the near term, future measures that the private market should develop and implement in order to combat spam.

Section D. Requests To Participate

Parties who wish to participate in the Email Authentication Summit must notify the FTC and NIST in writing of their interest by September 30, 2004 either by mail to the Secretary of the FTC or by email to *authenticationsummit@ftc.gov.* The Request to Participate must include a statement setting forth the requesting party's expertise in or knowledge of any or all of the issues identified in the Request for Comments section of this Notice and their contact information, including a telephone number, facsimile number, and email address (if available), to enable the FTC to notify them if they are selected. Requests to participate as a panelist should be captioned ''Email Authentication Summit—Request to Participate, (Matter Number P044411), and should be filed in the same manner as prescribed for written comments in the ''Request for Comments'' section. For requests filed in paper form, an original and three copies of each document should be provided. Panelists will be notified on or before October 15, 2004, whether they have been selected.

Using the following criteria, the FTC and NIST staff will select a limited number of participants:

1. The party submitted a complete Request to Participate by September 30, 2004.

2. The party has expertise in or knowledge of some or all of the issues that are the focus of the Summit.

3. The party's participation would promote the representation of a balance of interests at the Summit.

If it is necessary to limit the number of participants, parties who request to participate but are not selected may be afforded an opportunity, if at all possible, to present statements during a limited time period. The time allotted for these statements will be based on the amount of time necessary for discussion of the issues by the selected parties and on the number of persons wishing to make statements.

Section E. Availability of Comments and Requests To Participate as Panelists

The FTC Act and other laws the Commission administers permit the collection of public comments and requests to participate as panelists, to consider and use in this proceeding as appropriate. All timely and responsive public comments and requests to participate, whether filed in paper or electronic form, will be considered by the Commission, and will be available to the public on the FTC website, to the extent practicable, at *http://www.ftc.gov*. As a matter of discretion, the FTC makes every effort to remove home contact information for individuals from the public comments and requests to participate it receives before placing those comments on the FTC website. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at *http://www.ftc.gov/ftc/privacy.htm.*

By direction of the Commission.

Donald S. Clark,

Secretary.

[FR Doc. 04–20839 Filed 9–14–04; 8:45 am]

BILLING CODE 6750–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Assistant Secretary for Planning and Evaluation; Medicare Program; Meeting of the Technical Advisory Panel on Medicare Trustee Reports

AGENCY: Assistant Secretary for Planning and Evaluation, HHS

ACTION: Notice of meeting.

SUMMARY: This notice announces a public meeting of the Technical Advisory Panel on Medicare Trustee Reports (Panel). Notice of this meeting is given under the Federal Advisory Committee Act (5 U.S.C. App. 2, section 10(a)(1) and (a)(2)). The Panel will discuss the long-term rate of change in health spending and may make recommendations to the Medicare Trustees on how the Trustees might more accurately estimate health spending in the long run. The Panel's discussion is expected to be very technical in nature and will focus on the actuarial and economic methods by which Trustees might more accurately measure health spending. Although panelists are not limited in the topics they may discuss, the Panel is not expected to discuss or recommend changes in current or future Medicare provider payment rates or coverage policy.

DATES: September 24, 2004, 8 a.m.–3 p.m. e.d.t.

ADDRESSES: The meeting will be held at HHS headquarters at 200 Independence Ave., SW., 20201, Room 425A.

Comments: The meeting will allocate time on the agenda to hear public comments. In lieu of oral comments, formal written comments may be submitted for the record to Andrew Cosgrove, OASPE, 200 Independence Ave., SW., 20201, Room 443F.8. Those submitting written comments should identify themselves and any relevant organizational affiliations.

FOR FURTHER INFORMATION CONTACT: Andrew Cosgrove (202) 205–8681, *andrew.cosgrove@hhs.gov*. Note: Although the meeting is open to the public, procedures governing security procedures and the entrance to Federal buildings may change without notice. Those wishing to attend the meeting should call or e-mail Mr. Cosgrove by September 17, 2004, so that their name may be put on a list of expected attendees and forwarded to the security officers at HHS Headquarters.

SUPPLEMENTARY INFORMATION: On April 22, 2004, we published a notice announcing the establishment and requesting nominations for individuals to serve on the Panel. The panel members are: Mark Pauly, Edwin Hustead, Alice Rosenblatt, Michael Chernew, David Meltzer, John Bertko, and William Scanlon.

Topics of the Meeting: The Panel is specifically charged with discussing and possibly making recommendations to the Medicare Trustees on how the Trustees might more accurately estimate the long term rate of health spending in the United States. The discussion is expected to focus on highly technical aspects of estimation involving economics and actuarial science. Panelists are not restricted, however, in the topics that they choose to discuss.

Procedure and Agenda: This meeting is open to the public. Interested persons may observe the deliberations and discussions, but the Panel will not hear public comments during this time. The Commission will also allow an open public session for any attendee to address issues specific to the topic.

Authority: 42 U.S.C. 217a; section 222 of the Public Health Services Act, as amended. The panel is governed by provisions of Public Law 92–463, as amended (5 U.S.C. Appendix 2), which sets forth standards for the formation and use of advisory committees.

Dated: September 8, 2004.

Michael J. O'Grady,

Assistant Secretary for Planning and Evaluation.

[FR Doc. 04–20736 Filed 9–14–04; 8:45 am]

BILLING CODE 4150–05–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Submission for OMB review; Comment Request

Title: Survey of Early Head Start Programs.

OMB No.: New collection.

Description: The Head Start Reauthorization Act of 1994 established a special initiative creating funding for services for families with infants and toddlers. In response, the Administration on Children, Youth and Families (ACYF) within the Administration for Children and Families (ACF) developed the Early Head Start program. Early Head Start programs are designed to produce outcomes in four domains: (1) Child development, (2) family development, (3) staff development, and (4) community development. As a requirement of the Reauthorization Act, ACYF funded a rigorous randomized trial to study the effectiveness of Early Head Start programs, sampling from 17 programs funded in the initial years. That research found positive effects of the program overall in a variety of areas, as well as effects for different program types and levels of implementation, and among study participants with different characteristics.

The aim of the current research is to obtain a national picture of Early Head Start. This initiative will begin a process of describing how the Early Head Start initiative has grown over time, how programs are currently implementing services, and who is being served. The study will be conducted between September 2004 and May 2005.

The data will consist of a survey of all Early Head Start programs in October 2004 and site visits to a selected sample of 25 programs in early 2005. All data collection instruments have been designed to minimize the burden on respondents by minimizing the time required to respond. Participation in the study is voluntary.

The results of the research will be used by the Head Start Bureau and ACF to gain a better understanding of changes in program processes and services over time, to identify areas of