entrance between 20th and 21st Streets, NW., Washington, DC 20551.

STATUS: Closed.

MATTERS TO BE CONSIDERED:

1. Personnel actions (appointments, promotions, assignments, reassignments, and salary actions) involving individual Federal Reserve System employees.

2. Any items carried forward from a previously announced meeting.

CONTACT PERSON FOR MORE INFORMATION: Mr. Joseph R. Coyne, Assistant to the Board; (202) 452–3204. You may call (202) 452–3207, beginning at approximately 5 p.m. two business days before this meeting, for a recorded announcement of bank and bank holding company applications scheduled for the meeting.

Dated: July 18, 1997.

Jennifer J. Johnson,

Deputy Secretary of the Board.

[FR Doc. 97–19433 Filed 7–18–97; 8:45 am]

BILLING CODE 6210–01–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

Agency Information Collection Activities: Proposed Collections; Comment Request

The Department of Health and Human Services, Office of the Secretary will periodically publish summaries of proposed information collections projects and solicit public comments in compliance with the requirements of Section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995. To request more information on the project or to obtain a copy of the information collection plans and instruments, call the OS Reports Clearance Officer on (202) 690–6207.

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, utility and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the sue of automated collection techniques or other forms of information technology.

Proposed Project 1

Responsibilities of Awardees and Applicant Institutions for Reporting Possible Misconduct in Science (42 CFR part 50 and PHS 6349)—0937–0198—Revision—As required by Section 493 of the Public Health Service Act, the Secretary by regulation shall require that applicant and awardee institutions receiving PHS funds must investigate and report instances of alleged or apparent misconduct in science. *Respondents:* State or local governments; Businesses or other for-profit; Non-profit institutions—Reporting Burden Information—*Number of Respondents:* 3607; *Number of Annual Responses:* 3,700; Average Burden per Response; 29.85 minutes; *Total Reporting Burden:* 1,841 hours—Disclosure Burden Information—*Number of Respondents:* 3607; *Number of Annual Responses:* 3,667; *Average Burden per Response:* 30 minutes; *Total Disclosure Burden:* 1,834 hours—Recordkeeping Burden Information—Number of Respondents: 40; *Number of Annual Responses:* 140; *Average Burden per Response:* 7,03 hours; *Total Recordkeeping Burden:* 984 hours—Total Burden—4,659 hours.

Send comments to Cynthia Agens Bauer, OS Reports Clearance Officer, Room 503H, Humphrey Building, 200 Independence Avenue S.W., Washington DC, 20201. Written comments should be received within 60 days of this notice.

Dated: July 10, 1997.

Dennis P. Williams,

Deputy Assistant Secretary, Budget.

[FR Doc. 97–19138 Filed 7–21–97; 8:45 am]

BILLING CODE 4150–04–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Committee on Vital and Health Statistics: Meetings

Pursuant to the Federal Advisory Committee Act, the Department of Health and Human Services announces the following advisory committee meetings.

Name: National Committee on Vital and Health Statistics (NCVHS), Subcommittee on Health Data Needs, Standards, and Security. Workgroup on Data Standards and Security.

Times and Dates: 9:00 a.m.–4:30 p.m., August 5, 1997; 8:30 a.m.–4:30 p.m., August 6, 1997; 8:30 a.m.–4:00 p.m., August 7, 1997.

Place: Capital Hilton, 16th and K Streets, NW., Washington, DC 20201.

Status: Open.

Purpose: Under the Administrative Simplification provisions of P.L. 104–191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Secretary of Health and Human Services is required to adopt standards for specified transactions to enable health information to be exchanged electronically. The law requires that, within 24 months of adoption, all health plans, health care clearinghouses, and health care providers who choose to conduct these transactions electronically must comply with these standards. The law also requires the Secretary to adopt a number of supporting standards including standards for code sets and classification systems and standards for security to protect health information. The Secretary is required to consult with the National Committee on Vital and Health Statistics (NCVHS) in complying with these provisions. The NCVHS is the Department's federal advisory committee on health data, privacy and health information policy.

To assist in the development of the NCVHS recommendations to HHS, the NCVHS Subcommittee on Health Data Needs, Standards, and Security has been holding a series of public meetings to obtain the views, perspectives and concerns of interested and affected parties.

On August 5, and August 6, 1997, the Subcommittee's Working Group on Data Standards and Security will hold a public meeting at which they will receive input from the health care industry on recommendations for security standards. The Subcommittee is interested in receiving testimony that will provide an understanding of the foundation of information security in health care as well as the issues, barriers, and challenges that face the industry. Representatives of the health care industry—health care providers, payers, professional associations, vendors, and standards development organizations—are being invited to testify and respond to the Subcommittee's question on security issues in the implementation of the administrative simplification provisions of P.L. 104–191. The industry representatives are being asked to address the questions (below) in writing, to make brief oral presentations of their answers, and to answer further questions from the Subcommittee. Other organizations that would like to submit written statements on these issues are invited to do so.

On August 7, 1997, the Subcommittee will discuss issues, recommendations, and its proposed workplan for the supporting standards for the nine financial and administrative health care transactions. The full NCVHS has already forwarded its recommendations on the architecture for these nine transactions to the Secretary.

Questions to be Addressed: Whereas not all questions are applicable to all participants or their organizations, the following set of questions illustrates the scope and complexity of the security issues to be addressed by the Committee.

Policies and Procedures

- What policies and procedures should be employed to safeguard information?
- How should these policies and procedures be communicated to internal and external users as well as consumers?
- How frequently are policies reviewed?

- Do employees, agents, independent contractors, medical staff, and vendors sign confidentiality statements?
- What are the consequences of a security breach by an individual? What type of disciplinary action is taken?
- How do you protect employee health information, particularly if you self-administer a benefit plan?
- How do you monitor electronic files to detect unauthorized changes or systematic corruption?
- How do you protect backups? What abilities do you have to recover files that become corrupted or lost?

Organization Commitment

- What approaches have been successful in your organization in obtaining upper management commitment to data security? What approaches have been less than successful?
- Who is accountable to manage the information security program in your organization?
- What level of authority should review and approve policies?
- Has your organization assigned staff dedicated to information security? Please describe the reporting structure for information security at your organization.
- How do you determine who can have access to health information? Do you have different classes of access based on the sensitivity of the health information (e.g., more restrictive access to HIV status or mental health diagnoses)?
- Has cost been a factor in limiting your information security program? How would you determine the appropriate cost of security?
- What factors should be considered in assessing the costs and benefits of security? How should these factors be weighted?
- Based on your experience, what are the impediments to implementing health information security measures?
- How would federal legislation or regulations requiring the protection of health information affect the information security program at your organization?

Training

- What are the objectives of your data security training program?
- Who receives training in information security?
- How is training delivered?
- Is training customized to user class?
- How often is training repeated?

Technical Practices

- Are unique passwords used?
- Are tokens, smart cards, or biometrics used for authentication?
- Is access control handled through technology or through policy?
- How do you protect remote access points?
- Is encryption used for internal or external transmissions?
- If you use encryption, do you use it for your password, your patient identifier, your clinical information, or the entire patient record message?
- When you use encryption, do you use secure socket layer (SSL), data encryption standard (DES), or another encryption standard? Why did you select this particular encryption standard?
- What are the initial and ongoing costs associated with encryption?
- Do you transmit or plan to transmit patient identifiable information over the Internet? How is the information to be safeguarded?
- What physical security measures do you use?
- Are different security practices required for a private network?
- What type of unique identifier do you use to identify patient information?
- Do you use electronic signatures? If yes, explain the applications, the type of technology used, and liability issues, if any.

Patient Awareness/Authorization

- Are patients informed of your organization's policies and procedures on information security? If so, how? Do you have specific educational tools that you use to educate patients/consumers?
- Do patients review their information? How do patients amend incorrect information (particularly if maintained electronically)?
- Do patients have access to the audit trail of all those who have looked at their patient record?
- Can patients request that their information not be computerized?

Vendors and Data Security Consultants

- What security features do your products employ?
- What security features are customers asking for?
- Is cost a factor?
- Can security technology being used in other industries be integrated into your products?
- How do you help a client identify their data security risks, threats, and exposures?
- How do you help a client develop an effective data security strategy, design, or architecture?
- How do you avoid technology-dependent security procedures and systems?

SDOs/Accreditation Organizations

- What standards presently exist regarding security?
- Are the existing standards adequate for adoption by the Security of HHS?
- What standards must organizations meet in order to be accredited by your organization?
- What plans are underway to address security requirements?
- Do you feel that there is a need for the federal government to provide leadership in this area?

Contact Person for More Information: Substantive program information as well as summaries of the meeting and a roster of committee members may be obtained from Judy K. Ball, Committee staff, Office of the Assistant Secretary for Planning and Evaluation, DHHS, Room 440–D. Humphrey Building, 200 Independence Avenue SW, Washington, DC 20201, telephone (202) 690–7100, or from Marjorie S. Greenberg, Executive Secretary, NCVHS, NCHS, CDC, Room 1100, Presidential Building, 6525 Belcrest Road, Hyattsville, MD 20782, telephone (301) 436–7050. Information is also available on the NCVHS home page of the HHS website: http://aspe.os.dhhs.gov/ncvhs/.

Dated: July 14, 1997.

James Scanlon,

Director, Division of Data Policy, Office of the Assistant Secretary for Planning and Evaluation.

[FR Doc. 97–19137 Filed 7–21–97; 8:45 am]

BILLING CODE 4151–04–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Proposed Information Collection Activity; Comment Request

Proposed Projects:

Title: Voluntary Establishment of Paternity.

OMB No.: New Request.

Description: Public Law 104–193 requires the Secretary of the Department of Health and Human Services to specify the minimum data requirements of an affidavit to be used for the voluntary acknowledgment of paternity. Public Law 104–193 also requires States to enact laws requiring the development and use of an affidavit which met the minimum requirements specified by the Secretary and to give full faith and credit to such an affidavit signed in any other State according to its procedures. The Department established a task group composed of Federal and State staff to recommend minimum data elements for all State paternity acknowledgment affidavits. The minimum data elements were crafted to balance the need for a tool for collecting information necessary to the establishment of a child support order and the need for a user-friendly form that addresses only the data necessary to establish legal paternity. The minimum data elements are: The current full name, social security number and date of birth of mother, father, and child; address of mother and father, birthplace of child; an explanation of the legal consequences of signing the affidavit; a statement indicating both parents understand their rights, responsibilities, alternatives and the consequences of signing the affidavit; the place the affidavit was completed; and signature lines for mother, father and witnesses or notaries.

Respondents: States and Other Entities.

Annual Burden Estimates: