S1–05–06, 7500 Security Boulevard, Baltimore, MD 21244.

If a contractor receives a request to escalate an appeal to the ALJ hearing level (or the MAC level) because the contractor (or the ALJ) has not issued a timely decision on the appeal, the contractor should inform the appellant of the delay in implementation of the BIPA provisions, referencing this Ruling, and explain that the appeal will be processed under the existing appeals procedures. The contractor should note that the contractor (or the ALJ) will notify the appellant of its decision on the case and of any subsequent right the appellant may have to an ALJ hearing (or MAC review) on the decision. If the appellant makes such an appeal, a copy of the contractor's correspondence with the appellant should be sent to the ALJ (or the MAC), including a copy of the appellant's request for escalation.

If an ALJ or the MAC requests case files from a contractor in order to process a request to escalate an appeal, the contractor should notify the ALJ or the MAC, in writing, that the case file is currently being used to process a request for appeal at the review, reconsideration or fair hearing level, as appropriate. In that situation, contractors should indicate that the case file will be transmitted when the carrier, FI or hearing officer completes its review. Contractors should retain a copy of the request onsite and mail a copy of the request to: BIPA Lead, CMS, Mail Stop S1–05–06, 7500 Security Boulevard, Baltimore, MD 21244.

Finally, QIOs should continue to review hospital discharges in accordance with §§ 1154(a) and 1154(e) of the Act, with respect to time frames and financial liability.

Authority: Section 1154, 1869, and 1879 of the Social Security Act (42 U.S.C. 1395ff) and section 521 of the Medicare, Medicaid, and SCHIP Benefits Improvement and Protection Act of 2000, Pub. L. 106–554.

(Catalog of Federal Domestic Assistance Program No. 93.778, Medical Assistance Program; No. 93.773 Medicare—Hospital Insurance Program; and No. 93.774, Medicare—Supplementary Medical Insurance Program)

Dated: September 12, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

[FR Doc. 02–25351 Filed 10–1–02; 4:05 pm]

BILLING CODE 4120–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Medicare & Medicaid Services

Privacy Act of 1974; Report of New System

AGENCY: Department of Health and Human Services (HHS), Centers for Medicare & Medicaid Services (CMS).

ACTION: Notice of new System of Records (SOR).

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, we are proposing to establish a new system of records, called the ''Privacy Accountability Database (PAD),'' HHS/CMS/OIS No. 09–70–0540. The primary purpose of the system of records is to aid CMS in tracking, reporting, and accounting the disclosures made from all CMS system of records as permitted by the Privacy Act of 1974 and The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Information retrieved from this system of records will be used to support regulatory, reimbursement, and policy functions performed within the agency or by a contractor or consultant; support constituent requests made to a Congressional representative; and support litigation involving the agency.

We have provided background information about the proposed system in the SUPPLEMENTARY INFORMATION section, below. Although the Privacy Act requires only that the ''routine use'' portion of the system be published for comment, CMS invites comments on all portions of this notice. See ''Effective Dates'' section for comment period.

EFFECTIVE DATES: CMS filed a new system report with the Chair of the House Committee on Government Reform and Oversight, the Chair of the Senate Committee on Governmental Affairs, and the Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) on September 19, 2002. In any event, we will not disclose any information under a routine use until forty (40) calendar days after publication. We may defer implementation of this system of records or one or more of the routine use statements listed below if we receive comments that persuade us to defer implementation.

ADDRESSES: The public should address comments to: Director, Division of Data Liaison and Distribution (DDLD), CMS, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850. Comments received will be available for review at this location, by appointment, during regular business hours, Monday through Friday from 9 a.m.–3p.m., eastern time zone.

FOR FURTHER INFORMATION CONTACT: Kimberly Elmo, Division of Data Liaison and Distribution (DDLD), CMS, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland 21244–1850.

SUPPLEMENTARY INFORMATION:

I. Description of the New System of Records

A. Statutory and Regulatory Basis for System of Records

42 CFR 401.101–401.148 and 1106(a) of the Social Security Act, 42 U.S.C. 1306(a), 45 CFR 552a(c) of the Privacy Act and 45 CFR 164.528 of the Health Insurance Portability and Accountability Act.

B. Background

CMS administers the Medicare, Medicaid, and the State Children's Health Insurance Program to accomplish its mission of ensuring health care security for beneficiaries. Accordingly, CMS possesses the nation's largest collection of health care data (consisting of over 60 system of records), with information on over 74 million Americans. Having in place adequate electronic and procedural controls to address confidentiality will protect this personally identifiable data.

Data files consisting of personally identifiable data are disclosed to various entities. These disclosures fall under exceptions of the Privacy Act, routine uses of the applicable system of record or are permitted by HIPAA. Privacy legislation requires CMS to track disclosures from each individual system of records. The PAD will provide the necessary tracking, reporting and accounting capabilities that CMS must have in place to be in compliance with the Privacy Act of 1974 and HIPAA.

II. Collection and Maintenance of Data in the System

A. Scope of the Data Collected

The PAD will contain information on disclosures of CMS data that fall under exceptions of the Privacy Act; routine uses of the applicable system of record or permitted by HIPAA that require tracking. This system may also contain the Medicare Health Insurance Claim Number, Social Security Number, or Railroad Retirement Board Number and a PAD tracking number for Medicare beneficiaries whose CMS data have been disclosed.

The PAD will be implemented in phases. The initial fielding, scheduled to coincide with the April 14, 2003

HIPAA Privacy Rule compliance date, will capture and record applicable disclosure tracking information for enrollment and claims databases only (09–70–0536 Medicare Beneficiary Database and 09–70–0005 National Claims History National Medicare Utilization Database). These two databases contain the information most requested and, subsequently, serve as the source for the most frequently disclosed information. This phased implementation is based on architectural and technical limitations that exist in the CMS data center today. Modernization and reengineering initiatives are ongoing to increase cross-platform compatibility and integration. The PAD will incorporate accounting of additional databases as they are integrated into the new environment. This SOR will be republished as necessary.

B. Agency Policies, Procedures, and Restrictions on the Routine Use

The Privacy Act permits us to disclose information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose(s) for which the information was collected. Any such disclosure of data is known as a ''routine use.'' The government will only release PAD information that can be associated with an individual as provided for under ''Section III. Entities Who May Receive Disclosures Under Routine Use.'' Both identifiable and non-identifiable data may be disclosed under a routine use. Identifiable data includes individual records with PAD information and identifiers. Non-identifiable data includes individual records with PAD information and masked identifiers or PAD information with identifiers stripped out of the file.

CMS will only disclose the minimum personal data necessary to achieve the purpose of the PAD. CMS has the following policies and procedures concerning disclosures of information that will be maintained in the system. In general, disclosure of information from the SOR will be approved only for the minimum information necessary to accomplish the purpose of the disclosure after CMS:

1. Determines that the use or disclosure is consistent with the reason that the data are being collected; *e.g.*, tracking, reporting and accounting the disclosures made from all CMS systems of records as permitted by the Privacy Act and HIPAA.

2. Determines that:

a. The purpose for which the disclosure is to be made can only be accomplished if the record is provided in individually identifiable form;

b. The purpose for which the disclosure is to be made is of sufficient importance to warrant the effect and/or risk on the privacy of the individual that additional exposure of the record might bring; and

c. There is a strong probability that the proposed use of the data would, in fact, accomplish the stated purpose(s).

3. Requires the information recipient to:

a. Establish administrative, technical, and physical safeguards to prevent unauthorized use of disclosure of the record;

b. Remove or destroy at the earliest time all individually, identifiable information; and

c. Agree to not use or disclose the information for any purpose other than the stated purpose under which the information was disclosed.

4. Determines that the data are valid and reliable.

III. Proposed Routine Use Disclosures of Data in the System

A. Entities That May Receive Disclosures Under Routine Use

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the PAD without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. CMS proposes to establish the following routine use disclosures of information maintained in the system:

1. To agency contractors, or consultants that have been contracted by the agency to assist in the performance of a service related to this system of records and that need to have access to the records in order to perform the activity.

CMS contemplates disclosing information under this routine use only in situations in which CMS may enter into a contractual or similar agreement with a third party to assist in accomplishing agency business functions relating to purposes for this system of records.

CMS occasionally contracts out certain of its functions when doing so would contribute to effective and efficient operations. CMS must be able to give a contractor whatever information is necessary for the contractor to fulfill its duties. In these situations, safeguards are provided in the contract prohibiting the contractor from using or disclosing the information for any purpose other than that described in the contract and requires the contractor to return or destroy all information at the completion of the contract.

2. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional Office made at the written request of the constituent about whom the record is maintained.

Individuals sometimes request the help of a Member of Congress in resolving some issue relating to a matter before CMS. The Member of Congress then writes CMS, and CMS must be able to give sufficient information to be responsive to the inquiry.

3. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The agency or any component thereof, or

b. Any employee of the agency in his or her official capacity; or

c. Any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee, or

d. The United States Government;

is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation.

Whenever CMS is involved in litigation, or occasionally when another party is involved in litigation and CMS's policies or operations could be affected by the outcome of the litigation, CMS would be able to disclose information to the DOJ, court or adjudicatory body involved. A determination would be made in each instance that, under the circumstances involved, the purposes served by the use of the information in the particular litigation is compatible with a purpose for which CMS collects the information.

B. Additional Provisions Affecting Routine Use Disclosures

In addition, CMS policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary).

This System of Records contains Protected Health Information as defined by the Department of Health and Human Services' regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 82462 as amended by 66 FR 12434). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information.''

IV. Safeguards

The PAD system will conform to applicable law and policy governing the privacy and security of Federal automated information systems. These include but are not limited to: the Privacy Act of 1974, Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and OMB Circular A–130, Appendix III, ''Security of Federal Automated Information Resources.'' CMS has prepared a comprehensive system security plan as required by OMB Circular A–130, Appendix III. This plan conforms fully to guidance issued by the National Institute for Standards and Technology (NIST) in NIST Special Publication 800–18, ''Guide for Developing Security Plans for Information Technology Systems.'' Paragraphs A-C of this section highlight some of the specific methods that CMS is using to ensure the security of this system and the information within it.

A. Authorized Users

Personnel having access to the system have been trained in Privacy Act requirements. Employees who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data. Records are used in a designated work area and system location is attended at all times during working hours.

To ensure security of the data, the proper level of class user is assigned for each individual user level. This prevents unauthorized users from accessing and modifying critical data. The system database configuration includes five classes of database users:

—*Database Administrator* class owns the database objects (*e.g.*, tables, triggers, indexes, stored procedures, packages) and has database administration privileges to these objects.

—*Quality Control Administrator* class has read and write access to key fields in the database;

—*Quality Index Report Generator* class has read-only access to all fields and tables;

—*Policy Research* class has query access to tables, but are not allowed to access confidential patient identification information; and

—*Submitter* class has read and write access to database objects, but no database administration privileges.

B. Physical Safeguards

All server sites will implement the following minimum requirements to assist in reducing the exposure of computer equipment and thus achieve an optimum level of protection and security for the CMS system:

Access to all servers is to be controlled, with access limited to only those support personnel with a demonstrated need for access. Servers are to be kept in a locked room accessible only by specified management and system support personnel. Each server is to require a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card, key and/or combination, which grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to Automated Information Systems (AIS) resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the workstations, servers and databases include:

—*User Log-on*—Authentication is to be performed by the Primary Domain Controller/Backup Domain Controller of the log-on domain.

—*Workstation Names*—Workstation naming conventions may be defined and implemented at the agency level.

—*Hours of Operation*—May be restricted by Windows NT. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are to be determined and implemented at the agency level.

—*Inactivity Lockout*—Access to the NT workstation is to be automatically locked after a specified period of inactivity.

—*Warnings*—Legal notices and security warnings are to be displayed on all servers and workstations.

—*Remote Access Security*—Windows NT Remote Access Service (RAS) security handles resource access control. Access to NT resources is to be controlled for remote users in the same manner as local users, by utilizing Windows NT file and sharing permissions. Dial-in access can be granted or restricted on a user-by-user basis through the Windows NT RAS administration tool.

C. Procedural Safeguards

All automated systems must comply with Federal laws, guidance, and policies for information systems security. These include, but are not limited to: The Privacy Act of 1974; the Computer Security Act of 1987; OMB Circular A–130, revised; Information Resource Management Circular #10; HHS AIS Security Program; the CMS Information Systems Security Policy, Standards, and Guidelines Handbook; and other CMS systems security policies. Each automated information system should ensure a level of security commensurate with the level of sensitivity of the data, risk, and magnitude of the harm that may result from the loss, misuse, disclosure, or modification of the information contained in the system.

V. Effects of the New System on Individual Rights

CMS proposes to establish this system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. Data in this system will be subject to the authorized releases in accordance with the routine uses identified in this system of records.

CMS will monitor the collection and reporting of PAD data. PAD information is submitted to CMS through standard systems. CMS will use a variety of onsite and offsite edits and audits to increase the accuracy of PAD data.

CMS will take precautionary measures (*see* item IV., above) to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other personal or property rights of patients whose data are maintained in the system. CMS will collect only that information necessary to perform the system's functions. In addition, CMS will make disclosure from the proposed system only with consent of the subject individual, or his/her legal representative, or in accordance with an applicable exception provision of the Privacy Act.

CMS, therefore, does not anticipate an unfavorable effect on individual privacy as a result of maintaining this system of records.

Dated: September 19, 2002.

Thomas A. Scully,

Administrator, Centers for Medicare & Medicaid Services.

09–70–0540

SYSTEM NAME:

Privacy Accountability Database (PAD), HHS/CMS/OIS.

SECURITY CLASSIFICATION:

Level 3, Privacy Act Sensitive.

SYSTEM LOCATION:

HCFA Data Center, 7500 Security Boulevard, North Building, First Floor, Baltimore, Maryland 21244–1850. CMS contractors and agents at various locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system will contain the Medicare Health Insurance Claim (HIC) Number, Social Security Number, or Railroad Retirement Board Number for Medicare seneficiaries whose CMS data have been disclosed under exceptions of the Privacy Act, routine uses of the applicable system of record or are permitted by HIPAA. .

CATEGORIES OF RECORDS IN THE SYSTEM:

The PAD will contain information on disclosures of CMS data that fall under exceptions of the Privacy Act; routine uses of the applicable system of record or permitted by HIPAA that require tracking. This system may also contain the Medicare Health Insurance Claim (HIC) Number, Social Security Number, or Railroad Retirement Board Number for Medicare beneficiaries whose CMS data have been disclosed.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 CFR 401.101–401.148 and sec 1106(a) of the Social Security Act, 42 U.S.C. 1306(a), 45 CFR 552a(c) of the Privacy Act and 45 CFR 164.528 of the Health Insurance Portability and Accountability Act.

PURPOSE(S):

The primary purpose of the systems of records is to aid CMS in tracking, reporting, and accounting the disclosures made from all CMS system of records as permitted by the Privacy Act of 1974 and The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OR USERS AND THE PURPOSES OF SUCH USES:

These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may release information from the PAD without the consent of the individual to whom such information pertains. Each proposed disclosure of information under these routine uses will be evaluated to ensure that the disclosure is legally permissible, including but not limited to ensuring that the purpose of the disclosure is compatible with the purpose for which the information was collected. In addition, CMS policy will be to prohibit release even of non-identifiable data, except pursuant to one of the routine uses, if there is a possibility that an individual can be identified through implicit deduction based on small cell sizes (instances where the patient population is so small that individuals who are familiar with the enrollees could, because of the small size, use this information to deduce the identity of the beneficiary). Be advised, this System of Records contains Protected Health Information as defined by the Department of Health and Human Services' (HHS) regulation ''Standards for Privacy of Individually Identifiable Health Information'' (45 CFR parts 160 and 164, 65 FR 8462 as amended by 66 FR 12434). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the ''Standards for Privacy of Individually Identifiable Health Information.''

1. To agency contractors, or consultants that have been contracted by the agency to assist in the performance of a service related to this system of records and that need to have access to the records in order to perform the activity.

2. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional Office made at the written request of the constituent about whom the record is maintained.

3. To the Department of Justice (DOJ), court or adjudicatory body when:

a. The agency or any component thereof, or

b. Any employee of the agency in his or her official capacity; or

c. Any employee of the agency in his or her individual capacity where the DOJ has agreedto represent the employee, or

d. The United States Government; is a party to litigation or has an interest in such litigation, and by careful review, CMS determines that the records are both relevant and necessary to the litigation.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are stored on paper and magnetic media.

RETRIEVABILITY:

The Medicare records are retrieved by Health Insurance Claim Number, Social Security Number, or Railroad Retirement Board Number of the beneficiary and PAD tracking number.

SAFEGUARDS:

CMS has safeguards for authorized users and monitors such users to ensure against excessive or unauthorized use. Personnel having access to the system have been trained in the Privacy Act and systems security requirements. Employees who maintain records in the system are instructed not to release any data until the intended recipient agrees to implement appropriate administrative, technical, procedural, and physical safeguards sufficient to protect the confidentiality of the data and to prevent unauthorized access to the data.

In addition, CMS has physical safeguards in place to reduce the exposure of computer equipment and thus achieve an optimum level of protection and security for the CMS system. For computerized records, safeguards have been established in accordance with HHS standards and National Institute of Standards and Technology guidelines; *e.g.*, security codes will be used, limiting access to authorized personnel. System securities are established in accordance with HHS, Information Resource Management Circular #10, Automated Information Systems Security Program; CMS Information Systems Security, Standards Guidelines Handbook and OMB Circular No. A–130 (revised) Appendix III.

RETENTION AND DISPOSAL:

Records are disposed of in accordance with established CMS, Privacy Act and HIPAA retention guidelines. CMS will conduct periodic reviews to determine if these records are historical and should be placed in permanent files after established retention periods and administrative needs of CMS have elapsed.

Note: The Department of Justice issued a directive in 1992 prohibiting the destruction of Medicare claims/administrative records. Therefore, all Medicare claims-related/ administrative data will be retained until the freeze is lifted.''

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Data Liaison and Distribution, Enterprise Databases Group, Office of Information Services, CMS, Room N2–04–27, 7500 Security Boulevard, Baltimore, Maryland, 21244–1850.

NOTIFICATION PROCEDURE:

For purpose of access, the subject individual should write to the system manager, who will require the system name, the subject individual's name (woman's maiden name, if applicable), social security number (SSN) (furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay), address, date of correspondence and control number.

RECORD ACCESS PROCEDURE:

For purpose of access, use the same procedures outlined in Notification Procedures above. Requestors should also reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2).)

CONTESTING RECORD PROCEDURES:

The subject individual should contact the system manager named above, and reasonably identify the record and specify the information to be contested. State the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7.)

RECORD SOURCE CATEGORIES:

CMS's National Claims History system of records, Enrollment Database system of records, Medicare Beneficiary Database system of records, and Medicaid Statistical Information System of records.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 02–25427 Filed 10–4–02; 8:45 am]

BILLING CODE 4120–03–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Proposed Information Collection Activity; Comment Request

Proposed Projects

Title: Online Interstate Referral Guide (IRG).

OMB No.: 0970–0209.

Description: The IRG is an essential reference maintained by OCSE that provides States with an effective and efficient way of viewing and updating State profile, address, and FIPS code information by consolidation data available through numerous discrete sources into a single centralized, automated repository.

Respondents: State IV–D Child Support Programs.

Annual Burden Estimates:

Instrument	Number of respondents	Number of responses per respondent	Average burden hours per response	Total burden hours
Online IRG	54	18	.3	292

Estimated Total Annual Burden Hours: 292.

In compliance with the requirements of section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995, the Administration for Children and Families is soliciting public comment on the specific aspects of the information collection described above. Copies of the proposed collection of information can be obtained and comments may be forwarded by writing to the Administration for Children and Families, Office of Administration, Office of Information Services, 370 L'Enfant Promenade, SW., Washington, DC 02447, Attn: ACF Reports Clearance Officer. All requests should be identified by the title of the information collection.

The Department specifically requests comments 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) 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 use of automated collection techniques or other forms of information technology. Consideration will be given to comments and suggestions submitted within 60 days of this publication.

Dated: October 1, 2002.

Robert Sargis,

Reports Clearance Officer.

[FR Doc. 02–25424 Filed 10–4–02; 8:45 am]

BILLING CODE 4184–01–M

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Administration for Children and Families

Submission for OMB Review; Comment Request

Title: OCSE–369A: Financial Report; and OCSE–34A: Quarterly Report of Collections.

OMB No.: 0970–0181.

Description: Each State agency administering the Child Support Enforcement Program under Title IV–D of the Social Security Act is required to provide information to the Office of Child Support Enforcement concerning its administrative expenditures and its receipt and disposition of child support payments from non-custodial parents. These quarterly reporting forms enable each State to provide that information, which is used to compute both the quarterly grants awarded to each State and the annual incentive payments earned by each State. This information is also included in a published annual statistical and financial report, available to the general public.

Comments sent to the Office of Child Support Enforcement, both directly and in response to an earlier **Federal Register** Notice (67 FR 39727, *et seq.*), provided many useful recommendations to update and correct these financial reporting forms. However, several comments strongly indicated that State agencies would have inadequate time to incorporate these revisions in time to meet the reporting requirements for the fiscal year beginning October 1, 2002. In addition, legislation has been introduced in Congress that, if enacted, may require additional revisions to these forms.

For these reasons, we have decided to request that the expiration date of the existing forms be extended, without change, through September 30, 2004.

Respondents: State agencies administering the Child Support Enforcement Program.