
DATE: Comments should be submitted no later than May 23, 1991.

ADDRESS: Send written comments to the
Mr. Robert N. Veeder at 202-395-7285.

For further information contact:
Mr. Robert N. Veeder, Information
Policy Branch (Attention
NEOB, Washington, DC 20503.

For further details with respect to this
amendment, see (1) The application for
amendment dated October 31, 1989, as
supplemented January 25, March 8, June
27, August 23, November 8, and
November 22, 1990, and (2) Amendment

These documents are available for
public inspection at the Commission's
Public Document Room, the Gorman
Building, 2120 L Street, NW,
Washington, DC and at the Coastal
Region Library, 8619 W. Crystal Street,
Crystal River, Florida 32324.

Dated at Rockville, Maryland, this 15th day
of April 1991.

For the Nuclear Regulatory Commission,
Harley Silver,
Project Manager, Project Directorate II-2,
Division of Reactor Projects II/D, Office of
Nuclear Reactor Regulation.

OFFICE OF MANAGEMENT AND BUDGET

The Computer Matching and Privacy Protection Amendments of 1990 and
The Privacy Act of 1974

AGENCY: Office of Management and
Budget (OMB).

ACTION: Proposed guidance.

SUMMARY: OMB request public
comments on proposed guidance to
Federal, State and local agencies on
implementing certain provisions of the
Privacy Act of 1974, as amended. This
guidance focuses especially on the
recently enacted Computer Matching
and Privacy Protection Amendments of
1990, which alter the due process
provisions of the Computer Matching
and Privacy Protection Act of 1988. This
latter Act amended the Privacy Act of
1974. The guidance also addresses
another issue suggested by agencies in
reporting to OMB their activities in
implementing the Computer Matching
and Privacy Protection Act.

As implementation took place, it
became apparent that the due process
provisions in some instances conflicted
with existing protections that had
arguably been working well prior to the
Computer Matching and Privacy
Protection Act. This was especially true
in programs such as Food Stamps, Aid to
Families with Dependent Children,
and Medicaid, all of which had well-
established due process traditions
provided by statute, regulation, or both.

The consequence of providing
individuals with 30 days to respond to a
notice of adverse finding was to
automatically overpay some
beneficiaries.

As to independent verification, the
House Report on the amendment noted
that "The purpose of the independent
verification requirement is to assure that
the rights of individuals are not affected
automatically by computers without
human involvement and without taking
reasonable steps to determine that the
information relied upon is accurate," (House
Report 101-788, p. 4) Again, the goal was to
assure fairness to the individual.

Indeed, as they implemented the
Computer Matching and Privacy Protection
Act, agencies discovered instances where strict adherence to the
independent verification requirement
could have serious financial and
administrative implications for the
management of their programs. For
example, in the case of data exchanges
between State agencies and the Social
Security Administration (SSA) under the
Income Eligibility Verification System (IEVS), the States have no
independent procedure through which they
can verify the SSA data. IEVS
recognizes this problem by excluding
educational benefit programs from its own
independent verification requirement.
Similarly, automated data exchanges
between the Department of Defense and the
Department of Veteran's Affairs to
determine eligibility for certain
educational benefit programs would be
jeopardized if, in each instance, before
taking an action, the recipient agency
had to examine the source agency's
underlying paper record.

The Computer Matching and Privacy
Protection Amendments of 1990 change
both the independent verification and
30-day notice due process protection
provisions. These changes are described
below, accompanied by proposed
guidance.

1. Notification of Adverse Finding:
Under the 1988 provisions, before taking
an adverse action, an agency was
required to notify the individual of any
information relied upon is accurate.
Under the 1988 provisions, before taking
an adverse action, an agency was
required to notify the individual of any
information relied upon is accurate.
Under the 1988 provisions, before taking
an adverse action, an agency was
required to notify the individual of any
information relied upon is accurate.
Under the 1988 provisions, before taking
an adverse action, an agency was
required to notify the individual of any
information relied upon is accurate.
Under the 1988 provisions, before taking
an adverse action, an agency was
required to notify the individual of any
information relied upon is accurate.
Under the 1988 provisions, before taking
an adverse action, an agency was
required to notify the individual of any
The amendment allowing agencies to substitute existing alternative time periods for new ones was effective immediately upon enactment and did not require specific OMB interpretive guidance. OMB invites comment, therefore, on related guidance on this provision:

- Under what circumstances should an agency be permitted to establish a new time period by regulation? OMB interprets the amendments to indicate that agencies should be able to adopt new time periods that are shorter than the 30 day threshold the CMPPA provides. What safeguards are needed for this process?

- Should OMB provide guidance on what constitutes “reasonable notice,” including defining when the time period begins to run? What should that guidance say?

- Should OMB mandate what the content of the notices should be? If so, how specific should the content be?

- Reviewers should use the following proposed guidance as a point of departure for commenting on the questions above.

  Proposed Guidance: "Program officials may petition the Data Integrity Board of the recipient Federal agency in the case of a Federal matching program, or the Federal source agency in the case of a Federal/State matching program to waive the independent verification requirement only after they have taken the following steps:
  
  - Identification of the Type of Matching Data Eligible for the Waiver. Eligible data are only information that identifies the individual and the amount of benefits paid to the individual under a Federal benefit program. A clear example of the kind of data exchange that is eligible for waiver consideration is the furnishing to States by the Social Security Administration of Cost of Living Adjustment (COLA) information that consists of the name of the benefit recipient, the benefit amount including amount of the COLA change, and other information. In this example, the name and benefit amount would be eligible for the waiver procedure; the "other information" would not. Another example would be the furnishing by the Department of Defense of information about the Reserve status of military personnel to the Department of Veterans Affairs for purposes of determining credit for educational benefits programs, provided that the information consisted of the name, rank and reserve status, i.e., active or inactive during the reporting time period. In both of these examples, the data that is conveyed is unambiguous: e.g., the COLA increase is five percent for all recipients; here is a list of all reservists who performed duty such that they are eligible for the benefit. Where the information furnished is less precise (E.g., data is 99 percent accurate within one week of receipt, 95 percent accurate within two weeks of receipt, 85 percent accurate within three weeks of receipt). For example, a source agency updates data each quarter. A recipient agency should probably not use data that it received in January to make a determination in March since newer data will be available then. In some cases, the source agency may wish to provide confidence intervals to help the recipient agency determine when the data is so old as to be suspect: e.g., data is 99 percent accurate within one week of receipt, 95 percent accurate within two weeks of receipt, 85 percent accurate within three weeks of receipt. Alternatively, a source agency may wish to warn a recipient agency not to use data after the date on which the database is updated.

  - Conducting Thorough Determinations of Data Accuracy. Once an agency has determined that the data being exchanged qualifies for the waiver procedure, the agency must present convincing evidence to the Data Integrity Board of the recipient agency (or source agency in the case of a Federal/non-Federal Match) to permit the Board to accept a high degree of confidence in the accuracy of the data. Note that the Amendments do not require that the agencies conduct thorough audits of their systems, only that they have information relating to the quality of data. Among the elements an agency may wish to present to a Data Integrity Board are the following, (not all of which may be necessary or appropriate):
  
  - A description of the data bases involved (both source and recipient) including information on how data are acquired and maintained so as to permit accuracy assessments.
  
  - The system managers’ overall assessment of the reliability of the systems and the accuracy of the data they contain (both participants).
  
  - The results of any audits or risk assessments conducted (both participants).
  
  - Any material or significant weaknesses identified in response to requirements of the Federal Managers Financial Integrity Act or related legislation and any applicable OMB Circulars (both participants).
  
  - Any assessments of the effectiveness of the agencies’ Personnel Security Programs (both participants).
  
  - The security controls in place for the systems and the security risks associated with those systems (both participants).
  
  - Any historical data relating to program error rates (recipient agency).
  
  - Any information relating to the currency of the data (source agency).

- Any non-compliance or significant weaknesses identified in response to requirements of the Federal Managers Financial Integrity Act or related legislation and any applicable OMB Circulars (both participants).

2. Independent Verification Requirements: The 1990 amendments authorize an agency’s Data Integrity Board to waive the independent verification procedures when it finds a high degree of confidence in the accuracy of the data.

- The amendments create an alternative to the requirement that agencies independently verify the accuracy of information developed through a matching program before using it to make an adverse determination. According to the House Report, "the alternative procedure permits a Data Integrity Board to waive the independent verification procedure for qualifying disclosures." (House Report 101-768, p. 4).

- Note that this alternative is not a general exception to the requirement; it is available only for a specific type of matching data and only when the agency has taken certain steps.

- Reviewers are invited to comment on the following proposed guidance. OMB is particularly interested in knowing whether its guidance for identifying the types of matching data eligible for waiver is adequate. Also, are the criteria for evaluating a database sufficient?

  Proposed Guidance: “Program officials may petition the Data Integrity Board of the recipient Federal agency in the case of a Federal matching program, or the Federal source agency in the case of a Federal/State matching program to waive the independent verification requirement only after they have taken the following steps:
  
  - Identification of the Type of Matching Data Eligible for the Waiver. Eligible data are only information that identifies the individual and the amount of benefits paid to the individual under a Federal benefit program. A clear example of the kind of data exchange that is eligible for waiver consideration is the furnishing to States by the Social Security Administration of Cost of Living Adjustment (COLA) information that consists of the name of the benefit recipient, the benefit amount including amount of the COLA change, and other information. In this example, the name and benefit amount would be eligible for the waiver procedure; the "other information" would not. Another example would be the furnishing by the Department of Defense of information about the Reserve status of military personnel to the Department of Veterans Affairs for purposes of determining credit for educational benefits programs, provided that the information consisted of the name, rank and reserve status, i.e., active or inactive during the reporting time period. In both of these examples, the data that is conveyed is unambiguous: e.g., the COLA increase is five percent for all recipients; here is a list of all reservists who performed duty such that they are eligible for the benefit. Where the information furnished is less precise (E.g., data is 99 percent accurate within one week of receipt, 95 percent accurate within two weeks of receipt, 85 percent accurate within three weeks of receipt). For example, a source agency updates data each quarter. A recipient agency should probably not use data that it received in January to make a determination in March since newer data will be available then. In some cases, the source agency may wish to provide confidence intervals to help the recipient agency determine when the data is so old as to be suspect: e.g., data is 99 percent accurate within one week of receipt, 95 percent accurate within two weeks of receipt, 85 percent accurate within three weeks of receipt. Alternatively, a source agency may wish to warn a recipient agency not to use data after the date on which the database is updated.

- Conducting Thorough Determinations of Data Accuracy. Once an agency has determined that the data being exchanged qualifies for the waiver procedure, the agency must present convincing evidence to the Data Integrity Board of the recipient agency (or source agency in the case of a Federal/non-Federal Match) to permit the Board to accept a high degree of confidence in the accuracy of the data. Note that the Amendments do not require that the agencies conduct thorough audits of their systems, only that they have information relating to the quality of data. Among the elements an agency may wish to present to a Data Integrity Board are the following, (not all of which may be necessary or appropriate):

  - A description of the data bases involved (both source and recipient) including information on how data are acquired and maintained so as to permit accuracy assessments.
  
  - The system managers’ overall assessment of the reliability of the systems and the accuracy of the data they contain (both participants).
  
  - The results of any audits or risk assessments conducted (both participants).
  
  - Any material or significant weaknesses identified in response to requirements of the Federal Managers Financial Integrity Act or related legislation and any applicable OMB Circulars (both participants).
  
  - Any assessments of the effectiveness of the agencies’ Personnel Security Programs (both participants).
  
  - The security controls in place for the systems and the security risks associated with those systems (both participants).
  
  - Any historical data relating to program error rates (recipient agency).
  
  - Any information relating to the currency of the data (source agency).

- Any non-compliance or significant weaknesses identified in response to requirements of the Federal Managers Financial Integrity Act or related legislation and any applicable OMB Circulars (both participants).

2. Independent Verification Requirements: The 1990 amendments authorize an agency’s Data Integrity Board to waive the independent verification procedures when it finds a high degree of confidence in the accuracy of the data.

- The amendments create an alternative to the requirement that agencies independently verify the accuracy of information developed through a matching program before using it to make an adverse determination. According to the House Report, "the
Note that this list is not meant to be exhaustive, nor will each item be suitable for every matching program. Agencies should use whatever is appropriate to their particular circumstances, so long as the resultant finding is that the Data Integrity Board has a high degree of confidence in the accuracy of the data. Obviously, since much of the data used by the recipient agency in the determination must come from the source, the source should be prepared to cooperate in the development of the waiver determination. The evaluations should be renewed each time the matching agreement is renewed. Moreover, any changes to the data base that would affect data quality should be reported to the Data Integrity Board which must then determine whether to continue its certification.

Once the Data Integrity Board has found a matching program eligible for waiver, it should notify the program officials expeditiously. It should also notify the source agency. The board should be prepared to include information about any waivers granted as part of its Matching Report to OMB and its agency head.

Supplemental Guidance on the Responsibilities of the “Source” and “Recipient” Agencies [5 U.S.C. 552(a)].

Finally, OMB seeks comment concerning whether it should amend guidance previously given concerning the responsibility of the “source” and “recipient” agencies.

OMB’s initial guidance made the recipient Federal agency responsible for meeting the reporting and publishing requirements of the Computer Matching and Privacy Protection Act. This assignment was based on the assumption that the recipient agency was the one most likely to benefit from the matching program and should, therefore, bear the costs. OMB now believes, however, that in certain limited circumstances, the assumption is not valid. In some cases, a single agency may perform matches for a group of other agencies. The recipient agency in such cases derives no benefit of its own. Nor does it have the information needed to produce the reports and notices the Computer Matching and Privacy Protection Act requires. It merely matches records and gives to the source agencies information, e.g., location of a Federal employee who has defaulted on an obligation incurred under a program operated by the source agency on which they may base some action. In cases like these, OMB intends that its assignment of responsibilities to the recipient agency be interpreted in an equitable way. While it still may make sense from an efficiency standpoint to make one agency responsible for all of the required administrative actions, the matching parties should assign responsibility in a fair and reasonable way.

OMB invites comment on how to clarify the administrative responsibilities of these parties in a fair and equitable manner.

James B. Mackas, Jr.,
Acting Administrator and Deputy Administration, Office of Information and Regulatory Affairs.

[Federal Register Vol. 56, No. 78, Tuesday, April 23, 1991, Notices 18601

BILLING CODE 3110-91

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

President’s Council of Advisors on Science and Technology; Meeting

The President’s Council of Advisors on Science and Technology (PCAST) will meet on May 8-9, 1991. The meeting will begin at 9 a.m. in the Conference Room, Council on Environmental Quality, 722 Jackson Place NW, Washington, DC.

The purpose of the Council is to advise the President on matters involving science and technology.

Proposed Agenda

1. Briefing of the Council on the current activities of the Office of Science and Technology Policy and of the private sector.
3. Discussion of progress of working group panels.
4. Discussion of composition of future working groups.

Portions of the May 8-9 sessions will be closed to the public.

The briefings on some of the current activities of OSTP necessarily will involve discussion of materials that are formally classified in the interest of national defense or foreign policy reasons. This is also true for a portion of the briefing on panel studies. As well, a portion of both of these briefings will require discussion of internal personnel procedures of the Executive Office of the President and information which, if prematurely disclosed, would significantly frustrate the implementation of decisions made requiring agency action. These portions of the meeting will be closed to the public pursuant to 5 U.S.C. 552b(c)(1), (2), and (7)(B).

A portion of the discussion of panel composition will necessitate discussion

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-28037; File No. SR-Amex-90-24]


1. Introduction

On November 7, 1990, the American Stock Exchange, Inc. (“Amex” or “Exchange”) submitted to the Securities and Exchange Commission (“Commission”), pursuant to section 19(b)(3) of the Securities Exchange Act of 1934 (“Act”) 1 and rule 19b-4 thereunder, 2 a proposed rule change designed to amend certain of the Amex’s current arbitration rules and procedures. 3 According to the Exchange, the proposed amendments are designed to codify modifications in the Uniform Code of Arbitration which were approved by the Securities Industry Conference on Arbitration (“SICA”) on.

3 On March 25, 1991, the Amex submitted Amendment No. 1 to File No. SR-Amex-90-24, see letter from James M. Strough, Senior Counsel and Director of Hearings, Legal and Regulatory Policy Division, Amex to James F. Dennis, Office of2, dated March 21, 1991, Amendment No. 1 (Amendment No. 2).
4 See letter from James M. Strough, Senior Counsel and Director of Hearings, Legal and Regulatory Policy Division, Amex to James F. Dennis, Office of2, dated April 2, 1991, Amendment No. 2 (Amendment No. 3).
5 On April 30, 1991, the Amex submitted Amendment No. 3 to the original rule change, see letter from James M. Strough, Senior Counsel and Director of Hearings, Legal and Regulatory Policy Division, Amex to James F. Dennis, Office of2, dated April 30, 1991, Amendment No. 3 (Amendment No. 4).