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.

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

ADDRESS: Send written comments to the Information Policy Branch (Attention Robert N. Veeder), Office of Information and Regulatory Affairs, Office of Management and Budget, Room 3235 NEOB, Washington, DC 20503. Comments may be sent by Fax to Robert N. Veeder at 202-395-7285.

FOR FURTHER INFORMATION CONTACT: Mr. Robert N. Veeder, Information Policy Branch, Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503 (202) 395-3785.

SUPPLEMENTARY INFORMATION: Section (v) of the Privacy Act of 1974 (5 U.S.C. 552a) charges OMB with overseeing agencies' implementing activities and issuing regulations and guidelines. In addition, Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988 (CMPPA), and Public Law 101-508, the Computer Matching and Privacy Protection Amendments of 1990 (amendments) require OMB to provide guidance on their implementation. Where the proposed guidance below contradicts earlier guidance on specific points of interpretation, it is intended that the most recent guidance should be relied upon.

The changes made by the Computer Matching and Privacy Protection Amendments of 1990 addressed agencies' problems in implementing the due process provisions of the Computer Matching and Privacy Protection Act of 1988. (See 5 U.S.C. 552a(p), "Verification and Opportunity to Contest Findings".) Under the 1988 provisions, before taking an adverse action, an agency was required to verify independently any information developed through a matching program that indicated ineligibility. The agency was also required to notify the individual of any proposed action and wait thirty days for the individual to respond. These provisions were intended to ensure fairness in the determination process.

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, complete and timely." (House Report 101-768, 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 and Verification System (IEVS), the States have no independent procedure through which they can verify the SSA data. IEVS recognizes this problem by excluding Social Security and Supplemental Security Income (SSI) data 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:* The 1990 amendments authorize agencies that have in law or regulation a different time period for notification than thirty days, to substitute that other period. Agencies without alternative periods must wait thirty days.

The amendment allowing agencies to substitute existing alternative time periods were 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: "Where a program statute is silent or permits, agencies may also establish a new notification period through rulemaking that involves the public in the process, either through hearings or publication in the Federal Register for notice-and-comment. Agencies should not establish periods that are shorter than the CMPPA's thirty day standard unless they can ensure that such periods are adequate to give individuals meaningful notice and sufficient time to respond.

Moreover, whatever the time period used, agencies must disclose not merely the fact that they have information that indicates ineligibility, but what that information is. This will give individuals meaningful notice and permit them to understand exactly what the discrepant information is and to provide any explanatory information. In either case, the period begins to run from the date of the notice that describes the agency's findings to the individual or the date on which the agency provides a copy in person."

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 a 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.*, it consists of underlying eligibility information—amount of earned income, amount of unearned income, number of dependents) and is different for each participant, such data is not a candidate for the waiver procedure.

• 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 assert 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 daa 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). 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 data base is updated.

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. 552a(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. MacRae, Jr.,

Acting Administrator and Deputy Administrator, Office of Information and Regulatory Affairs.

[FR Doc. 91-9475 Filed 4-22-91; 8:45 am]

BILLING CODE 3110-01