EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

August 16, 2013

M-13-20

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Sylvia M. Burwell
Director

SUBJECT: Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative

This Memorandum implements section 5 of the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA)[1] and provides guidance to help Federal agencies protect privacy while reducing improper payments with the Do Not Pay (DNP) Initiative.

In Executive Order 13520 of November 20, 2009 (*Reducing Improper Payments*), the President directed agencies to identify "ways in which information sharing may improve eligibility verification and pre-payment scrutiny."[2] To help agencies implement the Executive Order, the President issued memoranda on finding and recapturing improper payments[3] and enhancing payment accuracy through a "Do Not Pay List."[4] The President directed the establishment of a "single point of entry" through which agencies would access relevant data in order to determine eligibility for a Federal award or payment.

In April 2012, OMB released a memorandum describing the efforts of OMB and the Department of the Treasury (Treasury) to establish the DNP Initiative.[5] The memorandum directed agencies to develop a plan for using the DNP Initiative for pre-payment eligibility reviews. In January 2013, the President signed IPERIA into law, codifying the ongoing efforts to develop and enhance the DNP Initiative. As the Federal Government takes these important steps to prevent waste, fraud, and abuse in Federal spending, it is vital for agencies to ensure that individual privacy is fully protected.

---

[1] Pub. L. No. 112-248, 126 Stat. 2390 (2013).
[2] 74 Fed. Reg. 62201 (Nov. 20, 2009), *available at* http://www.gpo.gov/fdsys/pkg/FR-2009-11-25/pdf/E9-28493.pdf.
[3] Memorandum of March 10, 2010, Finding and Recapturing Improper Payments, 75 Fed. Reg. 12119 (Mar. 10, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/financial_improper/03102010_improper_payments.pdf.
[4] Memorandum of June 18, 2010, Enhancing Payment Accuracy Through a "Do Not Pay List," 75 Fed. Reg. 35953 (June 18, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/financial_improper/06232010_donotpaylist.pdf.
[5] *See* OMB Memorandum M-12-11, Reducing Improper Payments through the "Do Not Pay List" (Apr. 12, 2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-11_1.pdf.

As required by IPERIA, this Memorandum sets forth implementation guidance for the DNP Initiative to help ensure that the Federal Government's efforts to reduce improper payments comply with privacy laws and policies.

1. Background

On January 10, 2013, the President signed IPERIA into law. Among other things, the law codified the Administration's DNP Initiative already underway across the Federal Government. The DNP Initiative includes multiple resources that are designed to help agencies confirm that the right recipient receives the right payment for the right reason at the right time. IPERIA provides the Federal Government with new tools and authorities to help agencies effectively implement the DNP Initiative.

Section 5(e)(3) of IPERIA requires OMB to issue guidance implementing the relevant parts of the law. In particular, the statute requires OMB to provide guidance to agencies on reimbursement of costs between agencies, retention and timely destruction of records, and prohibiting the duplication and redisclosure of records. Furthermore, under IPERIA, OMB must also provide guidance to help improve the effectiveness and responsiveness of agencies' Data Integrity Boards (DIBs). This Memorandum addresses all of these points and provides additional guidance on several other issues that are relevant to the DNP Initiative.

This Memorandum builds on previous OMB guidance. In 1988, Congress amended the Privacy Act of 1974[6] to establish procedural safeguards for agencies' use of computer matching programs.[7] The following year, OMB issued guidance to help agencies interpret the law and meet the new requirements.[8] Since releasing the original computer matching guidance, OMB has issued additional guidance regarding computer matching.[9] This Memorandum supplements the existing OMB documents and provides new guidance to help agencies protect privacy while reducing improper payments with the DNP Initiative.

2. Scope and Applicability

This Memorandum implements section 5 of IPERIA and applies to agencies' activities related to the DNP Initiative.[10] Some of the requirements in this Memorandum apply to all DNP Initiative activities (indicated by the term "DNP Initiative"), while other requirements are specific to Treasury's Working System (indicated by the term "Treasury's Working System"), as

---

[6] 5 U.S.C. § 552a.

[7] Computer Matching and Privacy Protection Act of 1988, Pub. L. No.100-503, 102 Stat. 2507 (1988).

[8] Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818 (June 19, 1989), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/final_guidance_pl100-503.pdf.

[9] *See* OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy (Dec. 20, 2000), *available at* http://www.whitehouse.gov/omb/memoranda_m01-05/; *see also* OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals, *available at* http://www.whitehouse.gov/omb/circulars_a130_a130trans4.

[10] IPERIA applies only to executive agencies of the Federal Government, not to State or local governments or non-executive Federal agencies.

defined in section 3 of this Memorandum. As required by section 5(e)(3)(B) of IPERIA, this guidance also clarifies some issues regarding matching programs in general.[11]

Although this Memorandum creates new policy requirements, nothing in this document extends the legal requirements of the Privacy Act to information or activities that would not otherwise be covered under the statute.[12] Notably, IPERIA does not modify the definitions in the Privacy Act. For example, the matching requirements of the Privacy Act only apply to a "matching program," and only apply to a Federal benefit match if the match involves a "Federal benefit program," as defined in the statute. Agencies should consult with their counsel and senior agency official for privacy to determine whether an activity is covered by the requirements in the Privacy Act and the corresponding requirements in this Memorandum.

While IPERIA does not explicitly amend the definitions in the Privacy Act, it nonetheless changes how the Privacy Act applies for purposes of the DNP Initiative.[13] Specifically, IPERIA establishes new standards and procedures that apply to matching programs conducted exclusively for purposes of the DNP Initiative. The DNP-specific standards and procedures do not apply to other efforts to combat improper payments or matching programs that are not part of the DNP Initiative. For all matching programs, agencies shall continue to follow the existing standards and procedures in law and OMB policies unless directed otherwise in this guidance. In particular, agencies shall follow OMB's *Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988*,[14] OMB Circular A-130,[15] and OMB Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy*.[16]

3. Definitions

a. The terms "agency," "individual," "maintain," "record," "system of records," "routine use," "recipient agency," "non-Federal agency," and "source agency," as used in this Memorandum, are defined in the Privacy Act.[17]

---

[11] For example, section 13 of this Memorandum establishes some general requirements regarding the performance of agencies' Data Integrity Boards.

[12] As provided in OMB guidance, agencies shall consider applying the matching principles in contexts other than those covered by the matching requirements. *See* OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy (Dec. 20, 2000) ("Although this guidance applies directly only to programs covered by the Matching Act, agencies should consider applying these principles in other data sharing contexts.").

[13] For example, section 5(e)(2)(D) of IPERIA provides that, for the purposes of IPERIA, section 552a(o)(1) of the Privacy Act shall be applied by substituting "between the source agency and the recipient agency or non-Federal agency or an agreement governing multiple agencies" for "between the source agency and the recipient agency or non-Federal agency" in the matter preceding subparagraph (A).

[14] Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818 (June 19, 1989), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/final_guidance_pl100-503.pdf.

[15] OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals, *available at* http://www.whitehouse.gov/omb/circulars_a130_a130trans4.

[16] OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy (Dec. 20, 2000), *available at* http://www.whitehouse.gov/omb/memoranda_m01-05/

[17] *See* 5 U.S.C. § 552a(a)(1)-(5), (7), (9)-(11).

b. ***Computer matching agreement.*** The term "computer matching agreement" (CMA) means a written agreement between a source agency and a recipient agency (or multiple source and/or recipient agencies, as appropriate) or a non-Federal agency that allows the parties to engage in a matching program. In a Do Not Pay matching program, original source agencies need not be a party to a computer matching agreement between Treasury and a payment-issuing agency. Computer matching agreements are described in more detail in the Privacy Act, 5 U.S.C. § 552a(o), and in OMB guidance.[18]

c. ***Data Integrity Board.*** The term "Data Integrity Board" (DIB) means the board of senior personnel designated by the head of an agency that is responsible for reviewing the agency's proposals to conduct or participate in a matching program, and for conducting an annual review of all matching programs in which the agency has participated.

d. ***Do Not Pay Initiative.*** The term "Do Not Pay Initiative" (DNP Initiative) means the initiative codified by section 5 of IPERIA to facilitate Federal agencies' review of payment or award eligibility for purposes of identifying and preventing improper payments. The initiative may include other activities, as designated by OMB.

e. ***Do Not Pay matching program.*** The term "Do Not Pay matching program" (DNP matching program) means a matching program (as defined in this Memorandum) that is conducted for purposes of the Do Not Pay Initiative and involves at least one of the five databases enumerated in section 5(a)(2) of IPERIA and/or a database designated by OMB pursuant to section 5(b) of this Memorandum. Do Not Pay matching programs are subject to alternative standards and procedures (as provided in this Memorandum) that are different from the standards and procedures that apply to matching programs outside of the Do Not Pay Initiative.

f. ***Federal benefit program.*** The term "Federal benefit program" is defined in the Privacy Act[19] and refers to any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.

g. ***Improper payment.*** The term "improper payment" is defined in the Improper Payments Information Act of 2002[20] and refers to a payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. The definition includes any payment made to an ineligible recipient, any payment for an ineligible service, any duplicate payment, payments for services not rendered, and any payment that does not account for credit for applicable discounts.

---

[18] *See* Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818, 25826 (June 19, 1989).
[19] *See* 5 U.S.C. § 552a(a)(12).
[20] Pub. L. No. 107-300 (2002) (codified at 31 U.S.C. § 3321 note).

h. ***Inspector General.*** The term "Inspector General" means a Federal agency official described in subparagraph (A), (B), or (I) of section 11(b)(1) of the Inspector General Act of 1978[21] and any successor Inspector General.

i. ***Matching program.*** The term "matching program" is defined in the Privacy Act[22] and generally refers to a computerized comparison of records from two or more automated systems of records, or an automated system of records and automated records maintained by a non-Federal agency (or agent thereof). A matching program either pertains to Federal benefit programs or Federal personnel or payroll records. A Federal benefit match is performed for purposes of determining or verifying eligibility for payments under Federal benefit programs, or recouping payments or delinquent debts under Federal benefit programs. A matching program involves not just the matching activity itself, but also the investigative follow-up and ultimate action, if any.

j. ***Multilateral computer matching agreement.*** The term "multilateral computer matching agreement" (multilateral CMA) means a computer matching agreement that involves more than two agencies.[23] For the purposes of a Do Not Pay matching program involving Treasury's Working System, a multilateral computer matching agreement involves Treasury and more than one payment-issuing agency.

k. ***Original source agency.*** The term "original source agency" means a Federal agency that discloses records from a system of records to another agency in order to allow that

---

[21] 5 U.S.C. App.

[22] The term "matching program" (A) means any computerized comparison of – (i) two or more automated systems of records or a system of records with non-Federal records for the purpose of –

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or

(II) recouping payments or delinquent debts under such Federal benefit programs . . .

(B) but does not include –

(i) matches performed to produce aggregate statistical data without any personal identifiers; (ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals; (iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons; (iv) matches of tax information . . . (v) matches –

(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes . . .

(II) conducted by an agency using only records from systems of records maintained by that agency if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; or (vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel; (vii) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986; or (viii) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. § 402(x)(3), § 1382(e)(1).

5 U.S.C. § 552a(a)(8).

[23] The term "multilateral" simply refers to an agreement with multiple parties; it does not refer to an agreement that involves databases outside the United States that are not under the control of a Federal (or non-Federal) agency.

agency to use the records in a matching program with a payment-issuing agency. For the purposes of a Do Not Pay matching program involving Treasury's Working System, an original source agency discloses records to Treasury in order to allow Treasury to engage in a Do Not Pay matching program with payment-issuing agencies. In a Do Not Pay matching program, original source agencies need not be a party to a computer matching agreement between Treasury and a payment-issuing agency.

l. ***Payment-issuing agency.*** The term "payment-issuing agency" means a Federal agency that has the authority to issue a payment or award and engages in a matching program for the purposes of determining or verifying eligibility for the payment or award under a Federal benefit program or of recouping the payment under a Federal benefit program. Generally, the payment-issuing agency will be the agency that benefits from the matching program. The payment-issuing agency is responsible for conducting the cost-benefit analysis and meeting the reporting and publication requirements in the matching provisions of the Privacy Act. If more than one payment-issuing agency is a party to a matching program, the payment-issuing agencies may assign these responsibilities as described in section 12(c) of this Memorandum.[24]

m. ***Treasury's Working System.*** The term "Treasury's Working System" means the Do Not Pay Initiative functions performed by the Department of the Treasury that are authorized by section 5 of IPERIA. Treasury's Working System includes Treasury's system of records for Do Not Pay, as well as other activities such as investigation activities for fraud and systemic improper payments detection through analytic technologies and other techniques.

4. <u>Roles and Responsibilities</u>

a. ***Office of Management and Budget.*** OMB is responsible for:

1. Implementing the DNP Initiative and providing guidance, oversight, and continued assistance to agencies.
2. Establishing a working system for pre-payment and pre-award review as part of the DNP Initiative.
3. Submitting annual reports to Congress regarding the operation of the DNP Initiative.

b. ***Department of the Treasury.*** Treasury is responsible for:

1. Hosting a working system (Treasury's Working System) for the DNP Initiative that includes a system of records for DNP that allows agencies to perform pre-payment eligibility reviews, as required in IPERIA.
2. Developing memoranda of understanding (MOUs) with original source agencies, as described in this Memorandum, and periodically reviewing the MOUs to determine whether the terms are sufficient.

[24] For guidance on the publication and reporting requirements of the Privacy Act, see OMB Circular A-130, Appendix I.

3. Entering into CMAs with payment-issuing agencies, as described in this Memorandum.
4. Periodically reassessing whether all of the data in Treasury's Working System are relevant and necessary to meet the objectives in section 5 of IPERIA and deleting or expunging any data that are not.
5. Taking reasonable steps to ensure that records in Treasury's Working System are sufficiently accurate, complete, and up-to-date as is reasonably necessary to ensure fairness to the individual record subjects.
6. Coordinating with original source agencies to develop a process that allows individuals to request the correction of data.
7. Preparing and submitting to OMB a written assessment to document the suitability of any commercial databases that could be designated for use in Treasury's Working System.
8. Maintaining the central DNP Initiative website that includes all relevant information, including all relevant CMAs, system of records notices, and privacy impact assessments.
9. Complying with all applicable requirements in the Privacy Act and other applicable laws, regulations and policies, as well as with the terms of all relevant CMAs and MOUs.
10. Submitting periodic reports to OMB.

c. ***Original source agencies***. Original source agencies are responsible for:

1. Ensuring that they have sufficient legal authority and a specific designation from OMB (except as provided by law) before disclosing records to Treasury for Treasury's Working System.
2. Entering into a written MOU with Treasury that describes how Treasury may use the records in question and provides rules for protecting and correcting the information and for the retention and destruction of records.
3. Confirming that Treasury has the appropriate level of security controls before sharing any records with Treasury.
4. Coordinating with Treasury to develop a process that allows individuals to request the correction of data, and promptly reviewing any request for correction.
5. Complying with all applicable requirements in the Privacy Act and other applicable laws, regulations, and policies, as well as with the terms of all relevant MOUs.

d. ***Payment-issuing agencies***. Payment-issuing agencies are responsible for:

1. Ensuring that they have sufficient legal authority to engage in a matching program for purposes of the DNP Initiative.
2. Entering into CMAs with Treasury, as described in this Memorandum.
3. Conducting the cost-benefit analysis and meeting the reporting and publication requirements in the matching provisions of the Privacy Act.
4. Ensuring that they only match against data sources that are relevant and necessary for the specific matching purpose.

5. Making determinations about the disbursement of payments or awards, consistent with legal authority.
6. Complying with all applicable requirements in the Privacy Act and other applicable laws, regulations, and policies, as well as with the terms of all relevant CMAs.

e. ***Senior agency officials for privacy.*** All agencies' senior agency officials for privacy are responsible for:

1. Developing a training program for the agency's DIB to ensure that all members of the DIB are properly trained and prepared to fulfill their duties with respect to all matching activities at the agency.
2. Periodically reviewing the effectiveness and responsiveness of the agency's DIB to determine whether the DIB needs additional support or instruction.

5. <u>Including Databases in Do Not Pay</u>

a. ***Enumerated databases.*** Section 5(a)(2) of IPERIA lists five databases that shall be included in the DNP Initiative without the need for OMB designation – the Social Security Administration's Death Master File, the General Services Administration's System for Award Management (formerly known as the Excluded Parties List System), Treasury's Debt Check Database, the Department of Housing and Urban Development's Credit Alert System or Credit Alert Interactive Voice Response System, and the Department of Health and Human Services Office of the Inspector General's List of Excluded Individuals/Entities.

b. ***OMB designation of additional databases.*** Section 5(b)(1)(B) of IPERIA provides that OMB may designate additional databases for inclusion in the DNP Initiative, in consultation with the appropriate agencies. Treasury may only use or access additional databases for Treasury's Working System once OMB has officially designated such databases for inclusion, except as provided by law. Before designating additional databases, OMB will publish a 30-day notice of the designation proposal in the Federal Register asking for public comment. At the conclusion of the 30-day comment period, if OMB decides to finalize the designation, OMB will publish a notice in the Federal Register to officially designate the database for inclusion in the DNP Initiative.

When considering additional databases for designation, OMB will consider:

1. Statutory or other limitations on the use and sharing of specific data;
2. Privacy restrictions and risks associated with specific data;
3. Likelihood that the data will strengthen program integrity across programs and agencies;
4. Benefits of streamlining access to the data through the central DNP Initiative;
5. Costs associated with expanding or centralizing access, including modifications needed to system interfaces or other capabilities in order to make data accessible; and
6. Other policy and stakeholder considerations, as appropriate.

c. ***Data minimization***. OMB will only consider the inclusion of data in the DNP Initiative if the data are relevant and necessary to meet the objectives of section 5 of IPERIA. In the case of Treasury's Working System, Treasury shall periodically reassess whether all data in Treasury's Working System meet this standard and delete or expunge any data that do not.

d. ***Disclosure from an original source agency to Treasury***. An OMB designation is not sufficient to allow agencies to provide records to Treasury for Treasury's Working System; agencies must also have legal authority to disclose records. This Memorandum alone does not provide agencies with such authority. Whenever OMB designates additional databases for inclusion in Treasury's Working System, the designation is subject to the original source agency's determination that it has the necessary legal authority to share the data with Treasury. In addition:

1. Prior to sharing any records, original source agencies shall confirm that Treasury affords the appropriate level of security controls, comparable to those employed by the original source agency.
2. Original source agencies shall develop a MOU with Treasury that describes all restrictions on the use of a particular dataset, and all security controls and other requirements. Treasury shall describe all of these restrictions, security controls, and requirements in the CMAs with payment-issuing agencies, as applicable.

6. <u>Use, Maintenance, Duplication, and Redisclosure of Records</u>

a. ***Limits on Treasury's use, maintenance, duplication, and redisclosure of records***. Any records provided from an original source agency to Treasury for purposes of Treasury's Working System shall not be used, maintained, duplicated, or redisclosed for any purpose other than those described in section 5 of IPERIA or this Memorandum, except where required by law.[25] All uses of the records shall be clearly described in the MOU between Treasury and the original source agency, as well as in Treasury's system of records notice for DNP. At a minimum, original source agencies shall specify in the MOU that all limitations on the use, maintenance, duplication, or disclosure of the records at the original source agency also apply to Treasury. In addition, Treasury shall ensure that all routine uses listed in the DNP system of records notice are appropriate and properly tailored for every dataset to which they apply in Treasury's Working System.

b. ***Matching with a payment-issuing agency***. In a DNP matching program, Treasury shall allow payment-issuing agencies to match against only those datasets in Treasury's Working System that are relevant and necessary for the specific matching purpose (*e.g.*,

[25] Pursuant to the Privacy Act at 5 U.S.C. § 552a(o)(1)(H), a recipient agency may also duplicate or redisclose records provided by a source agency where "essential to the conduct of the matching program." As explained in OMB guidance, "The essential standard is a strict test that is more restrictive than the 'compatibility' standard the Privacy Act establishes for disclosures made pursuant to section (b)(3): 'for a routine use.' Thus, under the essential standard, the results of the match may be disclosed for follow-up and verification or for civil or criminal law enforcement investigation or prosecution if the match uncovers activity that warrants such a result." *See* Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818, 25826 (June 19, 1989).

payment-issuing agencies shall not be allowed to match against income data if income is not relevant to the payment or award in question). The specific terms of the DNP matching program shall be described in the CMA and reviewed by each payment-issuing agency's DIB. All parties to the CMA shall be responsible for fully adhering to these terms.

c. ***Disclosure from Treasury to payment-issuing agency***. In accordance with IPERIA, Treasury may disclose information (*i.e.*, the results of the match) to the payment-issuing agencies.

7. Retention and Destructions of Records

a. ***General guidelines on retention and destruction of records***. Agencies shall follow all applicable record retention requirements, including those from the National Archives and Records Administration (NARA).

b. ***Specific requirements on retention and destruction of records***. The MOU between Treasury and an original source agency shall specify that Treasury will abide by the same rules for the retention and destruction of records that apply to the original source agency. The rules shall not change simply because records are provided to Treasury. As required in the Privacy Act, the relevant agencies' DIBs shall annually review agency recordkeeping and disposal policies and practices for compliance with the Privacy Act.

8. Correction of Data

a. ***Accuracy of records in Treasury's Working System***. Because the records in Treasury's Working System will be used to help agencies make determinations about individuals, Treasury shall take reasonable steps to ensure that records in Treasury's Working System are sufficiently accurate, complete, and up-to-date as is reasonably necessary to ensure fairness to the individual record subjects. Treasury's MOUs with original source agencies shall describe the means by which the original source agencies will ensure that the records provided to Treasury meet these standards. Treasury's senior agency official for privacy shall periodically review the MOUs to determine whether the terms are sufficient.

b. ***Correction of data***. Section 5(e)(4) of IPERIA requires OMB to establish procedures providing for the correction of data in order to ensure compliance with the Privacy Act. Treasury shall coordinate with original source agencies to develop a process that allows individuals to request the correction of data. The process shall meet the following general requirements:

1. If a request for correction is made directly to Treasury, Treasury shall promptly inform the original source agency (or agencies) of the request. The original source agency shall promptly review the request and determine whether corrections should be made to the data in question. Original source agencies shall follow their existing process for handling such requests. Some original source agencies have laws, regulations, or policies that govern how individuals may request corrections to records in a system of records. Thus, original source

agencies may not be able to make corrections to records solely based on information provided by Treasury. However, original source agencies shall review all information provided by Treasury and, if appropriate, contact the individual making the request.

2. If a request for correction is made to an original source agency, the original source agency shall determine whether corrections should be made to the data and promptly inform Treasury of the determination if the data are included in Treasury's Working System. Whenever an original source agency determines that corrections are needed to data, the data shall be corrected at both the original source agency and in Treasury's Working System. Treasury and the original source agency shall take reasonable steps to avoid discrepancies between two versions of the same dataset. The data correction processes shall be described on Treasury's DNP website, in Treasury's DNP system of records notice, and in all relevant MOUs and CMAs.

c. ***Reporting to OMB***. Treasury shall annually report to OMB the total number of requests made to Treasury for the correction of data in Treasury's Working System. In addition, Treasury shall report to OMB the number of such requests that actually led to corrections of records. OMB will include this information in its annual report to Congress.

9. <u>Procedural Safeguards</u>

a. ***General procedural safeguards***. The Privacy Act, at 5 U.S.C. § 552a(p), establishes certain procedural safeguards that individuals whose records are used in a matching program shall be afforded when matches uncover adverse information about them. As provided in section 5(e)(6) of IPERIA, nothing in IPERIA shall be construed to affect the rights of an individual under the Privacy Act at 5 U.S.C. § 552a(p).

b. ***Verification of adverse information***. Before adverse action is taken against an individual, any adverse information that agencies discover shall be subjected to investigation and verification, unless an agency's DIB waives this requirement pursuant to the Privacy Act at 5 U.S.C. § 552a(p)(1)(A)(ii). Verification requires a confirmation of the specific information that would be used as the basis for an adverse action against an individual. As explained in OMB guidance, "Absolute confirmation is not required; a reasonable verification process that yields confirmatory data will provide the agency with a reasonable basis for taking action."[26] In each case, agencies shall document the specific information on which any determination about an individual is based. For additional guidance on verification of adverse information, agencies shall consult OMB's existing guidance.[27]

c. ***Notice and opportunity to contest***. Once agencies have verified the adverse information, they shall provide the individual with notice and an opportunity to contest before taking adverse action. The notice shall inform the individual of the relevant information and give him or her an opportunity to provide an explanation. Individuals shall have 30 days

[26] *See* Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818, 25827 (June 19, 1989).
[27] *Id.*

to respond to a notice of adverse action, unless a statute or regulation provides a different period of time. For additional guidance on notice and opportunity to contest, agencies shall consult OMB's existing guidance.[28]

d. ***Stopping a payment or award.*** Except as provided by law, only the agency with authority to issue a payment or award may decide to stop the payment or award. Treasury disburses payments only as directed by payment-issuing agencies; IPERIA does not provide Treasury with authority to issue a payment or award. However, the Treasury disbursing official, consistent with his or her responsibility to ensure that payments are issued accurately and correctly, may act on behalf of the certifying agency to stop a payment (*i.e.*, not disburse the payment) only as directed by the certifying agency, in accordance with criteria and instructions specified by the certifying agency. As provided in section 5(b)(4) of IPERIA, there may be circumstances in which the law requires a payment or award to be made to a recipient, regardless of whether that recipient is identified as potentially ineligible under the DNP Initiative.

10. Cost Reimbursement

a. ***Need for cost reimbursement.*** When Federal agencies share data, cost reimbursement may be necessary in order to appropriately support additional work that one agency requests from another.

b. ***General requirements for cost reimbursement.*** In general, cost reimbursement for the DNP Initiative shall reflect the true costs incurred by an agency in order to provide data, recognizing that agencies may sometimes offset costs through reciprocal exchanges of data. Rather than paying for the same data multiple times, cost reimbursement is a mechanism to capture the actual total cost of providing access to the data.

c. ***Specific considerations for cost reimbursement.*** Appropriate cost reimbursement may vary for different data sources based on factors including, but not limited to, statutory obligations and restrictions associated with accessing a specific data source. In accessing and paying for data, agencies shall ensure proper coordination across programs and components.

11. Commercial Databases

a. ***Use of or access to commercial databases.*** Section 5(d)(2)(C) of IPERIA provides that the DNP Initiative may include the use of or access to commercial databases to investigate activities for fraud and systematic improper payments detection. Some commercial databases may help the Federal Government meet the objectives of the DNP Initiative. At the same time, commercial databases may also present new or increased privacy risks, such as databases with inaccurate or out-of-date information. The requirements in this section of the Memorandum shall apply to all information in commercial databases that are not part of a system of records under the Privacy Act.

---

[28] *Id.*

b. ***General standards for the use of or access to commercial databases.*** Treasury may use or access a commercial database for Treasury's Working System only if OMB has officially, previously designated such database for inclusion following a period of public notice and comment, as described in section 5(b) of this Memorandum. Because commercial databases used or accessed for purposes of the DNP Initiative will be used to help agencies make determinations about individuals, it is important that agencies apply safeguards that are similarly rigorous to those that apply to systems of records under the Privacy Act. Thus, commercial data may only be used or accessed for the DNP Initiative when the commercial data in question would meet the following general standards:

1. Information in commercial databases must be relevant and necessary to meet the objectives described in section 5 of IPERIA.
2. Information in commercial databases must be sufficiently accurate, up-to-date, relevant, and complete to ensure fairness to the individual record subjects.
3. Information in commercial databases must not contain information that describes how any individual exercises rights guaranteed by the First Amendment, unless use of the data is expressly authorized by statute.

c. ***Specific requirements for Treasury's use of or access to commercial databases.*** In addition to the general standards provided above, Treasury shall meet the following specific requirements whenever agencies use or access a commercial database as part of Treasury's Working System:

1. Treasury shall establish rules of conduct for persons involved in the use of or access to commercial databases and instruct each person with respect to such rules, including penalties for noncompliance, as appropriate.
2. Treasury shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of information in commercial databases when such information is under Treasury's control.

d. ***Written assessment of the suitability of a commercial database.*** Before OMB considers designating a commercial database for use or access in Treasury's Working System, Treasury shall prepare and submit to OMB a written assessment to document the suitability of the commercial database for use in Treasury's Working System. The assessment shall explain the need to use or access the data, explain how the data will be used or accessed, provide a description of the data (including each data element that will be used or accessed), and explain how the database meets all applicable requirements in this Memorandum. OMB will provide the written assessment to the public as part of the notice of the designation proposal described in section 5(b) of this Memorandum.

e. ***Pilot programs.*** Treasury may use or access commercial databases as part of a pilot program without satisfying the requirements in this section of the Memorandum. A pilot program involves the small scale use of or access to commercial data in order to gather information on which to base a decision about seeking broader use or access. A pilot program shall terminate after a maximum of 6 months. No agency may stop any payments or awards or take any other adverse action against an individual as a result of a

pilot program.

f. ***Compliance with law***. Agencies are reminded that information in commercial databases used in the DNP Initiative may constitute a system of records or become part of a system of records; such information would be subject to all applicable requirements in the Privacy Act. As with all aspects of this guidance, in addition to the Privacy Act, agencies shall comply with all applicable requirements in the Paperwork Reduction Act,[29] the Federal Records Act,[30] the Information Quality Act,[31] and other applicable laws, regulations, and policies.

12. Computer Matching Agreements for Do Not Pay

a. ***Multilateral CMAs***. Section 5(e)(2)(D) of IPERIA authorizes CMAs "governing multiple agencies" for purposes of the DNP Initiative.[32] Agencies' default for a matching program shall always be traditional CMAs between one source agency and one recipient agency. However, in certain circumstances there may be advantages to using a multilateral CMA.

b. ***Considerations for the use of multilateral CMAs***. Agencies may consider using multilateral CMAs if both the matching purpose and the specific data elements that will be matched are sufficiently similar across each of the agencies to allow all parties to satisfy the requirements in a single CMA that is clear to all relevant agencies and to the public. In making this determination, agencies shall consider whether using a multilateral CMA would lead to unnecessary complexities or inefficiencies that may offset the benefits. For example, it is possible that a multilateral CMA would make it more cumbersome for the agencies to alter or amend the CMA.

c. ***Reporting and publication requirements***. Whenever agencies enter into a multilateral CMA, each of the payment-issuing agencies is responsible for meeting the reporting and publication requirements associated with the matching program.[33] However, the payment-issuing agencies may designate a single agency to report the CMA to OMB and Congress and publish the notice in the Federal Register on behalf of the other agencies, if such designation is clear in the report and notice. Each agency's DIB shall review the designation and determine that the arrangement is sufficient to meet the requirements in the Privacy Act and provide adequate notice to the public.

d. ***Termination date of CMAs***. Section 5(e)(2)(C) of IPERIA provides that a CMA for a DNP matching program shall have a termination date of "less than 3 years." Furthermore, during the 3-month period leading up to the scheduled termination of a CMA, agencies may renew the CMA for a maximum of 3 years. These new termination

---

[29] 44 U.S.C. § 3501 *et seq.*
[30] 44 U.S.C. Chapters 21, 22, 29, 31, and 33.
[31] Consolidated Appropriations Act of 2001, Pub. L. No. 106-554, § 515, 114 Stat. 2763, 2763A154 (2000) (codified at 44 U.S.C. § 3516 note).
[32] As a matter of policy, agencies may use multilateral CMAs for non-DNP matching programs, as appropriate.
[33] For guidance on the publication and reporting requirements of the Privacy Act, see OMB Circular A-130, Appendix I.

periods apply only to DNP matching programs; CMAs outside of the DNP Initiative remain subject to the original termination periods in the Privacy Act.[34] Before a matching program may be renewed, each party shall certify that the matching program has been conducted in compliance with the CMA, and the participating agencies' DIBs shall review the request for renewal and make a determination that the matching program will be conducted without change.[35]

e. ***Additional guidance on CMAs***. If agencies currently have CMAs with Treasury (or any other agency) that involve records that will be provided for Treasury's Working System, the agencies may be required to develop new CMAs in order to accommodate the DNP framework. Like system of records notices, CMAs shall be published and reported to OMB and Congress at the departmental or agency level, even if the records involved are maintained at a component level. For example, the Department of Health and Human Services would publish and report a CMA to OMB and Congress on behalf of the Centers for Medicare and Medicaid Services (CMS), even if the match involves only CMS records.

13. <u>General Guidance on Review by Data Integrity Boards</u>

a. ***General guidance for DIBs***. Agencies' DIBs are responsible for approving or disapproving proposed matching programs based on an assessment of the adequacy of the CMA and other relevant information. When DIBs review a proposed matching program, they shall assess the CMA to ensure that it fully complies with the Privacy Act, as well as any other applicable laws, regulations, and policies. When making a determination, DIBs shall document in writing their reasons for approving or disapproving a matching program. This documentation shall be provided to the appropriate agency officials.

b. ***Training for DIBs***. The senior agency official for privacy shall ensure that all members of the DIB are properly trained and prepared to fulfill their duties with respect to all matching activities at the agency. The senior agency official for privacy shall develop a training program that members of the DIB shall be required to complete, as appropriate. In particular, all DIB members shall receive training regarding the requirements in the Privacy Act, other relevant laws, and guidance from OMB, NARA, and the Department of Commerce's National Institute of Standards and Technology.

c. ***Effectiveness and responsiveness of DIBs***. Agencies' DIBs shall meet with sufficient frequency to ensure that matching programs are carried out efficiently, expeditiously, and in compliance with the law. At a minimum, DIBs shall meet annually to evaluate ongoing matching programs and consider whether any modifications are warranted. In addition, agencies shall ensure that DIBs review matching proposals expeditiously so as not to cause delays to necessary programs. The senior agency official for privacy shall

[34] Pursuant to 5 U.S.C. § 552a(o)(2)(C)-(D), a CMA outside of the DNP Initiative may only remain in effect for a maximum of 18 months, with an optional renewal period of one year. All termination dates and renewals are subject to approval by agencies' DIBs.
[35] *See* 5 U.S.C. § 552a(o)(2)(D).

periodically review the effectiveness and responsiveness of the agency's DIB to determine whether the DIB needs additional support or instruction.

d. ***60-day deadline for review of a CMA***. Section 5(e)(2)(B) of IPERIA requires DIBs to respond to a proposed CMA for the DNP Initiative no later than 60 calendar days after the proposal has been presented to the DIB. This 60-day deadline shall apply to new CMAs, as well as requests for the renewal of an established CMA. The 60-day clock shall begin as soon as the agency provides the DIB with the materials required for the DIB's review. Although the 60-day deadline in the law applies only to DNP matching programs, agencies are encouraged to adopt this timeframe as a general practice for all matching programs, as appropriate.

   In most cases, the DIB's response to the proposal shall be a definitive approval or disapproval of the matching program. If DIBs have questions about the proposal, those questions shall be submitted to agency officials by day 30 of the 60-day period, if possible. Agency officials shall answer any questions from DIBs in a timely manner. If circumstances do not permit the DIB to approve or disapprove the DNP matching program within 60 days, the DIB shall provide a brief memorandum to the head of the agency (or to the Inspector General in cases where the Inspector General proposed the matching program) describing the necessity for the delay.

e. ***Reporting to OMB***. Agencies shall annually report to OMB the specific number of days that it takes the DIB to approve or disapprove each proposed DNP matching program.

14. <u>Cost-Benefit Analysis</u>

a. ***Specific estimate of savings not required***. The Privacy Act at 5 U.S.C. § 552a(u)(4) requires agencies to perform a cost-benefit analysis for a proposed matching program. This cost-benefit analysis normally includes a specific estimate of any savings, which is included as part of the justification for the matching program in the CMA. However, section 5(e)(2)(E) of IPERIA provides that agencies' cost-benefit analyses for a DNP matching program need not contain a specific estimate of any savings.

b. ***Cost-benefit analysis still required***. Although agencies need not provide a specific estimate of savings, they shall perform a qualitative analysis of the potential costs and benefits of any proposed DNP matching program, unless the cost-benefit analysis is not required pursuant to the Privacy Act at 5 U.S.C. § 552a(u)(4)(B)-(C). This qualitative analysis of potential costs and benefits shall allow the agency to explain in the CMA why there is good reason to believe that the DNP matching program would provide cost savings (or why the matching activity would be justified on other grounds).

c. ***DIBs shall review all relevant data***. When an agency proposes to renew a DNP matching program (or proposes a new DNP matching program that is similar to a previously approved matching program), the agency's DIB shall review all relevant data that was reported to OMB or Congress, including specific data about costs and benefits.

15. Public Availability of Computer Matching Agreements

a. ***Publication of CMAs on a public website.*** Section 5(e)(3)(C) of IPERIA requires OMB to establish rules regarding what constitutes making a DNP Initiative CMA available upon request to the public, pursuant to the Privacy Act at 5 U.S.C. § 552a(o)(2)(A)(ii). The statute provides that these rules shall include requiring publication of the CMA on a public website. As a responsibility of hosting Treasury's Working System, Treasury shall maintain the central DNP Initiative website that includes all of the relevant information about Treasury's Working System. In particular, Treasury shall post (or provide direct links to) all of the CMAs, system of records notices, and privacy impact assessments that pertain to Treasury's Working System. Providing such documents on Treasury's DNP Initiative website will promote transparency and provide examples that other agencies may use to help develop future CMAs and other materials related to Treasury's Working System.

b. ***Removing or redacting sensitive information in CMAs.*** Whenever agencies make CMAs or other materials available to the public, they shall remove or redact any unnecessary personally identifiable information, as appropriate. In addition, agencies shall consider removing or redacting any information that could present security risks, such as specific information about security controls for a system (*e.g.*, password length or complexity).

16. Matching by Inspectors General

a. ***General guidelines for CMAs and Inspectors General.*** Section 5(e)(2)(A) of IPERIA provides that each Inspector General and the head of each agency may enter into CMAs with other Inspectors General and agency heads that allow ongoing data matching (which shall include automated data matching) to assist in the detection and prevention of improper payments. Inspectors General may use the authority provided in IPERIA to enter into CMAs only if the purpose of the match is to detect and prevent improper payments. Although Inspectors General may enter into CMAs, all CMAs shall be published and reported to OMB and Congress at the departmental or agency level.[36]

b. ***Specific requirements for CMAs and Inspectors General.*** CMAs that involve one or more Inspector General are subject to all applicable requirements that pertain to CMAs for the DNP Initiative, including, but not limited to, DIB review, termination dates, correction of data, procedural safeguards, and reporting and notice requirements. If an Inspector General's proposed CMA is disapproved by the agency's DIB, the Inspector General may appeal the disapproval to OMB, pursuant to the Privacy Act at 5 U.S.C. § 552a(u)(5).

17. Matches Involving a Subset of Records from a System of Records

The matching requirements of the Privacy Act shall apply to all matching activities that involve a subset of records from a system of records when the subset of records itself would

[36] For guidance on the publication and reporting requirements of the Privacy Act, see OMB Circular A-130, Appendix I.

meet the definition of "system of records" in the Privacy Act (*i.e.*, it is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual), so long as the other qualifications in the statute are met.

18. For Further Information

If agencies have specific questions regarding this Memorandum, they may contact OMB at privacy-oira@omb.eop.gov. If agencies have general questions regarding Treasury's Working System, they may visit http://donotpay.treas.gov or contact Treasury at donotpay@bpd.treas.gov.