Guide to the Inspector General Empowerment Act's Computer Matching Exemption

JUNE 2017

Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

Table of Contents

Preface

This Guide is intended to provide an overview of the CMPPA Exemption and to present various matters for Inspectors General to consider when engaging in matching.

This Guide, and the related data match proposal template (Appendix A), data use agreement (DUA) drafting guide (Appendix B), and DUA sample template (Appendix C) are not binding on any Office of Inspector General (OIG). The aforementioned information and guidance also do not represent the official legal interpretation of CIGIE or its members regarding implementation of section 6(j)(2) of the Inspector General Act of 1978 (IG Act) and related provisions of the IG Act, other laws, regulations, and implementing guidance. Each OIG should make its own independent assessment of how to apply the new computerized data matching exemption. Because the legal parameters are not identical across the IG community, OIGs should consult with their respective offices of legal counsel and/or legislative committees for further clarification or to discuss any outstanding issues, as necessary.

Background

The Computer Matching and Privacy Protection Act of 1988[1] (CMPPA) amended the Privacy Act of 1974[2] (the "Privacy Act") and established restrictions on Federal agencies' usage of "matching programs," which generally include computerized comparisons of two or more automated systems of records. The CMPPA also imposed certain procedural requirements on Federal agencies when conducting those matches.

The Inspector General Empowerment Act of 2016[3] (IGEA) exempts certain computerized data comparisons performed by or in coordination with Inspectors General (IGs) from the CMPPA's restrictions and requirements (the "CMPPA Exemption"). Specifically, the IGEA added section 6(j)(2) to the IG Act:

> For purposes of section 552a of title 5, United States Code, or any other provision of law, a computerized comparison of two or more automated Federal systems of records, or a computerized comparison of a Federal system of records with other records or non-Federal records, performed by an Inspector General or by an agency in coordination with an Inspector General in conducting an audit, investigation, inspection, evaluation, or other review authorized under this Act shall not be considered a matching program.

[1] Pub. L. No. 100-503.

[2] Pub. L. No. 93–579, *codified at* 5 U.S.C. § 552a.

[3] Pub. L. No. 114-317, *codified at* 5 U.S.C. § 552a(6)(j)(2).

Matching Under the CMPPA

The CMPPA provisions of the Privacy Act define a "matching program" as:

> [A]ny 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 benefits programs, or
>
> (ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records[.][4]

The CMPPA places various restrictions and requirements on agencies' usage of matching programs, including, but not limited to:

- The CMPPA requires that an agency enter into a computer matching agreement (CMA) with a recipient agency prior to disclosing records to that agency for use in a computer matching program. CMA's need to contain a number of statutorily-defined elements.
- Every agency conducting or participating in a matching program is required to establish a Data Integrity Board (DIB) to oversee and coordinate the agency's implementation of the CMPPA's requirements.
- The CMPPA's requirements provide due process rights to individuals by preventing agencies from taking adverse actions against them without further verification. For example:
  - An agency must independently verify information produced by a matching program prior to taking an adverse action against an individual;
  - An agency's DIB must determine that the information is accurate with a high degree of confidence; and

[4] 5 U.S.C. § 552a(a)(8)(A).

    - An agency must provide individuals with notice containing a statement of findings and informing the individual of opportunities to contest such findings.
- An agency must provide advance notice of any proposal to establish or significantly change a matching program to the House Committee on Government Operations, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB).

The CMPPA also includes several exceptions to the definition of a matching program. If an agency engages in matching that falls under one of these exceptions, the agency is not required to comply with the CMPPA's procedural restrictions and requirements discussed above. These exceptions include, but are not limited to:

- Matches performed to produce aggregate statistical data without any personal identifiers;
- 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;
- Matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to criminal law enforcement, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person for the purpose of gathering evidence against that person;
- Matches of tax information for certain purposes authorized under the Internal Revenue Code of 1986 or the Social Security Act;
- Matches (1) using records predominantly relating to Federal personnel that are performed for routine administrative purposes, or (2) conducted by an agency using only records from systems of records maintained by that agency; but in either case, only if the purpose of the match is not to take any adverse action against Federal personnel; and
- Matches performed for foreign counterintelligence purposes or to produce background checks for security clearances.

Effects of the CMPPA Exemption

The IGEA exempts from the definition of a matching program any computerized data comparisons of Federal systems of records, or of a Federal system of records with other records (including non-Federal records) performed by or in coordination with an OIG so long as the match is performed in connection with an audit, investigation, inspection, evaluation, or other review authorized under the IG Act. As a result, OIGs can engage in matching without adhering to the CMPPA's various restrictions and requirements discussed above. Thus, OIGs are no longer required to enter into CMAs prior to receiving or disclosing records that will be used for matching purposes.

This CMPPA Exemption means that OIGs no longer need to try to fit matches within any of the CMPPA's designated exceptions. For example, prior to the IGEA, an OIG could conduct a match to support research or statistical projects without triggering the CMPPA's requirements only if the resulting data was not used to make any decisions concerning the rights, benefits, or privileges of specific individuals. However, now, an OIG can conduct such matches *and* use the results to make decisions concerning the rights, benefits or privileges of specific individuals without triggering the CMPPA's requirements.

OIGs should note that the CMPPA Exemption applies not only to matches performed by OIGs, but also to matches performed by agencies *in coordination with OIGs* in connection with an audit, investigation, inspection, evaluation, or other review. Agencies can therefore engage in matching without following the CMPPA's requirements if the matches are conducted in coordination with an OIG for OIG purposes.

Potential Considerations Prior to Engaging in Matching

Although the CMPPA Exemption means that OIGs do not have to comply with the CMPPA's requirements before engaging in matching, when conducting an audit, investigation, inspection, evaluation, or other review authorized under the IG Act, all other aspects of the Privacy Act still apply, and there may be other applicable laws, rules, and regulations to consider. As such, we recommend that OIGs review applicable OMB guidance.[5] Furthermore, OIGs should make sure that they use this new authority in a responsible manner. Below are a few considerations that OIGs may wish to take into account prior to engaging in matching activities. These are not intended to be an exhaustive list of potential considerations.

- Consider the intended purpose of the proposed matching activity.
    - Does the proposed matching activity further the mission of the OIG to promote economy and efficiency in the administration of, or to prevent and detect fraud and abuse in, the agency's programs and operations?
    - Is the proposed matching activity related to an audit, investigation, inspection, evaluation, or other authorized review?
    - How broad is the scope of the proposed matching activity? Is it reasonably tailored to capture the necessary data?

- Consider engaging in preliminary planning to assess the feasibility of the proposed matching activity.
    - What Federal or State agency currently has the data required to perform the match?

[5] *See, e.g.*, OMB Memoranda 01-05, *Guidance on Inter-Agency Sharing of Personal Data-Protecting Personal Privacy* (Dec. 20, 2000); OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* (Dec. 23, 2016).

- What legal authority can the OIG use to obtain that data? (See the Obtaining Data to Match section for more information)
- What technical capabilities are required to conduct the match? Is any specific software required?

- For a data source OIG, consider whether an exception to the Privacy Act's consent requirements allows the OIG to disclose its information to another OIG (or agency) for the contemplated data comparisons.
  - For disclosures made pursuant to the "law enforcement request" exception, does the information request meet the Privacy Act's requirements at 5 U.S.C. § 552a(b)(7) and applicable Privacy Act regulations?
  - For disclosures made pursuant to the "routine uses" exception, does the source OIG's Systems of Records Notice (SORN) include a routine use permitting a disclosure to the recipient OIG, agency, or non-Federal agency for the stated purpose(s) of the data comparison?

- For a recipient OIG, consider, in consultation with counsel, applicable legal requirements and OMB guidance regarding the ownership, control, and custody of source OIG information and new information created and maintained by the recipient OIG or agency.
  - Does the recipient OIG have appropriate management, operation, and technical security controls in place to adequately safeguard the information being shared with it? (See the Using and Disclosing Data section for more information.)

- Consider, in consultation with counsel, applicable legal restrictions on access to and use of the source information and the newly created information, including restrictions on disclosure.
  - Does the Privacy Act or another law restrict any contemplated redisclosures of data obtained for or as a result of matching activities?
  - Is the data to be matched classified or otherwise restricted for security reasons?
  - Are there any other applicable statutory restrictions or prohibitions on accessing, using, or disclosing the data to be used in the matching activity?
  - Does the recipient OIG, agency, or non-Federal agency to whom data disclosure is contemplated have appropriate management, operation, and technical security controls in place to adequately safeguard the information being shared with it? (See the Using and Disclosing Data section for more information.)

OIGs may wish to set up formal internal approval processes before engaging in matching. For example, an OIG could require relevant component heads, counsel, and the IG or Deputy IG to approve data matches before it engages in matching activities. For OIGs that elect to establish a formal internal approval process, Appendix A contains a sample template data match proposal to use.

Obtaining Data to Use in Data Comparison Activities

While the effect of the IGEA's CMPPA Exemption is to allow OIGs to engage in matching activities without entering into CMAs or complying with other requirements and restrictions in the CMPPA, the CMPPA Exemption does not provide OIGs with any new authority to obtain data. OIGs must therefore rely on their existing authority to obtain data, as well as the additional authority granted by other sections of the IGEA. OIGs should consult with their offices of legal counsel for further clarification and guidance.

In general, how an OIG approaches obtaining data will depend on whether that data is owned by the OIG's agency, another Federal agency, or a State or local agency.[6]

Data Owned by the OIG's Parent Agency

With respect to data owned by the OIG's parent agency, the OIG may obtain that data using its general authority under the IG Act, section 6(a)(1), which authorizes OIGs to have timely access to data available to their agency that relate to agency programs and operations for purposes of carrying out their official responsibilities, unless access is otherwise specifically limited by Congress, such as for Federal grand jury materials. Such intra-agency disclosures are permitted without written consent under the Privacy Act's "need to know" exception.[7] Accordingly, no DUA is necessary when obtaining records from an OIG's parent agency.

Data Owned by Another Federal Agency

With respect to data owned by another Federal agency, an OIG should first determine, in consultation with its office of legal counsel, which applicable statutory, regulatory, or other authorities require that agency to turn over data.[8] In the absence of other authorities, an OIG may

[6] OIGs may also obtain data from private, non-governmental entities to use in data comparisons. In general, such entities are not subject to the Privacy Act. Additionally, the CMPPA does not require CMAs in order to obtain data from non-governmental entities. Thus, the IGEA's CMPPA Exemption did not have any effect on OIGs' obtaining data from non-governmental entities and comparing it with Federal systems of records.

[7] *See* 5 U.S.C. § 552a(b)(1).

[8] For example, in some cases OIGs may be able to rely upon the authority of executive orders of the President, memorandums of understanding between federal agencies, or federal agency charter language to obtain information.

rely on sections 6(a)(3) and 6(c)(1) of the IG Act to request and receive the necessary information and to seek assistance from that agency.[9] Although the contemplated data comparison activities are now exempt from CMPPA-required matching agreements, we recommend that OIGs at least consider applicable OMB guidance on inter-agency information sharing, such as OMB Memoranda 01-05, "Guidance on Inter-Agency Sharing of Personal Data—Protecting Personal Privacy," before engaging in the comparisons. OIGs are not required, pursuant to the CMPPA Exemption, to enter into CMAs or any other written agreement for data comparison activities; one of the purposes of the IGEA was to free OIGs from having to enter into such agreements. Nevertheless, some OIGs may find it helpful, at their discretion, to document the basis for the data exchange and the safeguards that are in place in a written agreement. Appendix C contains a template Data Use Agreement (DUA) for those OIGs that may wish to enter into written agreements, and Appendix B contains a general guide on drafting a DUA. OIG components should consult with their respective offices of legal counsel to ensure that any DUA documents transmitted externally (to other Federal or non-Federal agencies) contain appropriate markings, such as identifying if the DUA contains law enforcement sensitive or controlled unclassified information. Counsel should also be consulted and review DUAs in advance of any external disclosure to ensure law enforcement techniques or information are not inappropriately included in a DUA.

In general, the requesting OIG should strongly consider going through the data source agency's OIG to obtain the data. If the source agency's OIG has an authorized purpose for requesting data under the IG Act, such as for a joint fraud detection or prevention effort, then obtaining the data through that OIG may be appropriate. That disclosure is still contingent on an available Privacy Act exception though, such as for routine uses or law enforcement requests. The OIG from the source agency may also be in a position to provide useful guidance on the feasibility, and potential usefulness, of obtaining the data being sought, and may provide other suitable options. Additionally, obtaining data through the source agency's OIG may enhance current and future collaborative fraud detection and prevention efforts.

Data Owned by a State or Local Agency

With respect to data owned by a State or local agency, an OIG should first determine, in consultation with its office of legal counsel, whether there are any applicable statutory, regulatory,

[9] IG Act Section 6(a)(3) authorizes OIGs to request necessary information or assistance from Federal, State, or local agencies, to carry out IG duties and responsibilities. Section 6(c)(1) requires Federal agencies upon an OIG request for information or assistance under Section 6(a)(3) to furnish information or assistance, insofar as furnishing such information or assistance is practicable and not in contravention of any existing statutory restriction or regulation. If, in the judgment of an OIG, information requested pursuant to Section 6(a)(3) is not provided or unreasonably refused, the OIG is required to report the circumstances to the head of the establishment without delay. See IG Act Section 6(c)(2).

or other avenues for requiring that agency to turn over that data, such as an IG subpoena. In instances where State or local law may prohibit or restrict disclosure, OIGs should determine whether there are any applicable Federal laws that preempt the conflicting State or local laws.

If not issuing a legal demand, OIGs may rely on section 6(a)(3) of the IG Act to request the necessary information and assistance from the State or local agency. A recipient OIG should ensure that its applicable SORN allows for creation and maintenance of the new information generated by the data comparison activities.

Appendix C contains a template DUA that OIGs can use when working with State entities, if the parties so choose, and Appendix B contains a general guide on drafting a DUA.

Using and Disclosing Data

Privacy Act Restrictions on Disclosure

The Privacy Act prohibits agencies from disclosing "records"[10] in a "system of records"[11] to any person or agency unless either the person to whom the records pertain provides written consent to the disclosure or a statutory exception applies.[12] One exception, commonly referred to as the "law enforcement request exception," allows disclosure without written consent to an agency for a "civil or criminal law enforcement activity" upon a valid request from the head of the agency.[13] Another exception allows disclosure without written consent, if the disclosure is for a "routine use."[14] The Privacy Act states that "'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."[15] The

[10] "[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4).

[11] "[T]he term 'system of records' means 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[.]" 5 U.S.C. § 552a(a)(5).

[12] *See* 5 U.S.C. § 552a(b).

[13] *See* 5 U.S.C. § 552a(b)(7).

[14] *See* 5 U.S.C. § 552a(b)(3).

[15] 5 U.S.C. § 552a(a)(7). In the OMB Privacy Act Guidelines, OMB explains that "[t]he term 'routine use' was introduced to recognize the practical limitations of restricting use of information to explicit and expressed purposes for which it was collected. It recognizes that there are corollary purposes 'compatible with the purpose for which [the information] was collected' that are appropriate and necessary for the efficient conduct of government and in the best interest

Privacy Act further requires that agencies publish in the Federal Register each system of records that the agency maintains and the routine uses of the system of records.[16]

When disclosing information as part of a data comparison for civil or criminal law enforcement purposes, OIGs may be able to rely on the Privacy Act "law enforcement request exception."[17] However, when OIGs wish to conduct data comparisons for other purposes, such as audits or evaluations, OIGs will not be able to rely upon the "law enforcement request exception" as authority for disclosure. In such circumstances, OIGs should rely on the "routine use" exception, if applicable. In order to use the "routine use" exception, the applicable SORN must include a routine use that allows for the particular disclosure. Although other routine uses may cover the disclosure of most data, now that an OIG's data comparison activities are no longer subject to the CMPPA's unique disclosure mechanism, OIGs may wish to consider publishing a routine use specifically identifying data matching to ensure their ability to disclose protected information for a data comparison purpose is permitted. Likewise, OIGs may wish to consider encouraging their parent agencies to add language to their SORNs to encompass data matching that permits their parent agencies to disclose records upon another OIG's request for a match.

Routine Use Language

Below is sample "routine use" language for OIGs and their data comparison activities and for parent agencies and their OIG-coordinated data comparison activities:

> In addition to those disclosures generally permitted under subsection (b) of the Privacy Act of 1974, 5 U.S.C. 552a(b), [OIG or agency] may disclose records routinely to:
>
> For OIGs:
>
> (1) Compare such records to records in other Federal agencies' systems of records or to non-Federal records.
>
> For agencies:
>
> (2) Compare such records to other agencies' systems of records or to non-Federal records, in coordination with an OIG in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the IG Act.

---

of both the individual and the public." *U.S. Office of Management and Budget's Privacy Act Guidelines*, 40 Fed. Reg. 28948, 28953 (July 9, 1975).

[16] 5 U.S.C. § 552a(e)(4).

[17] Some regulations may restrict disclosure even if an OIG can claim that the Privacy Act's law enforcement exception applies. OIGs should review all applicable regulations in conjunction with the Privacy Act to ensure disclosures are permitted.

OIG Privacy Reviews

Under the recently updated OMB Circular A-108, which provides agencies with guidance on implementing various Privacy Act requirements, OIGs should review their current systems of records (SORs) and SORNs to determine whether updates are necessary to accommodate any contemplated data comparison activities or if there are any records maintained in de facto systems of records but without the requisite SORNs. As a reminder, OIGs do not need to issue SORNs for any OIG-maintained records that are covered by a government-wide SOR (such as ethics program records in an Office of Government Ethics SOR) or agency-specific SOR, as those records must be maintained consistently in accordance with SORN-specific requirements. Below are examples of OIG SORNs:

- FHFA OIG: https://www.gpo.gov/fdsys/pkg/FR-2011-03-02/pdf/2011-4624.pdf
- HUD OIG: https://www.federalregister.gov/documents/2010/12/29/2010-32769/office-of-inspector-general-privacy-act-of-1974-notification-of-the-office-of-inspector-general
- HHS OIG: https://www.hhs.gov/foia/privacy/sorns/09900100/index.html

Keeping Records of Matching Activities

Each OIG is responsible for ensuring that its data comparison records are accounted for under the Privacy Act, 5 U.S.C. § 552a(c), and that they are retained and destroyed in accordance with applicable requirements under the Federal Records Act, implementing regulations, NARA General Records Schedules, and agency and OIG-specific records retention requirements. Separate from these requirements, such records may be useful for a variety of OIG purposes, such as project planning, reporting to Congress as necessary on the OIG's activities, and for sharing with other OIGs and CIGIE to the extent permitted by law.

Appendix A: Data Match Proposal Template

Data Comparison (Match) of (insert description of records) Records to (insert description of records) Records

DMP (insert name of OIG) OIG # XX-XX

(Establish a numbering convention that allows for simple tracking of the number of OIG component DMPs for each fiscal year. For example, (XXX) OIG OA # 17-01, which would signify the specified (XXX) OIG's Office of Audit's first DMP in fiscal year 2017.)

I. Purpose

(Provide a high-level description of what the data match will do. This section should also explain the concept and the usefulness of the match, and sufficient details to describe the purpose. All other information in other sections of the underlying data use agreement (DUA) must support and agree with the purpose described in this section.)

II. Responsible OIG Component/Contacts

(Identify the OIG component that will be responsible for the data match and identify and provide contact information for the individual(s) within that component who will be responsible for conducting the data match).

III. Legal Authority

(Cite the appropriate laws and sections that permit the data exchange and computerized comparison of information, such as applicable IG Act provisions, and any disclosure exceptions, including routine uses or the law enforcement exception under the Privacy Act that permit any disclosures contemplated. See below and template DUA—Appendix C—for sample language.)

1. The IG Act, 5 U.S.C. App. 3 § 6(a)(3), explicitly grants each Inspector General the authority "to request such information or assistance as may be necessary for carrying out the duties and responsibilities provided by this Act from any Federal, State, or local governmental agency or unit thereof."

2. The IG Act, 5 U.S.C. App. 3 § 6(a)(9), explicitly grants each Inspector General "the authority to the extent and in such amounts as may be provided in advance by appropriations Acts, to enter into contracts and other arrangements for audits, studies, analyses, and other services with public agencies and with private persons, and to make such payments as may be necessary to carry out the provisions of this Act."

3. The IG Act, 5 U.S.C. App. 3 § 6(j)(2), exempts (XXX) OIG from the computer matching

provisions of the Privacy Act. (XXX) OIG or an agency in coordination with (XXX) OIG may therefore conduct a computerized comparison of two or more automated Federal systems of records, or a computerized comparison of a Federal system of records with other records or non-Federal records in conducting an audit, investigation, inspection, evaluation, or other review authorized under the IG Act.

4. The IG Act grants each Inspector General the duty and responsibility to (1) provide policy direction for the programs and operations of the establishment; (2) conduct, supervise, and coordinate audits and investigations relating to the programs and operations of the establishment; and (3) recommend policies for, and conduct, supervise, or coordinate other activities carried out or financed by such establishment for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, its programs and operations. 5 U.S.C. App. 3 §§ 4(a)(1) and (3).

5. The IG Act, 5 U.S.C. App. 3 §§ 6(a)(1), (2), authorizes (XXX) OIG:

> (1)(A) to have timely access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials available to the applicable establishment that relate to the programs and operations with respect to which the (XXX) OIG has responsibilities under the IG Act;
>
> > (B) to have access under subparagraph (A) above, notwithstanding any other provision of law, except pursuant to any provision of law enacted by Congress that expressly-
> >
> > > (i) refers to the Inspector General; and
> > >
> > > (ii) limits the right of access of the Inspector General; and
> >
> > (C) except as provided in subsection (i), with regard to Federal grand jury materials protected from disclosure pursuant to rule 6(e) of the Federal Rules of Criminal Procedure, to have timely access to such information if the Attorney General grants the request in accordance with subsection (h);
>
> (2) to make such investigations and reports relating to the administration of the programs and operations of the applicable establishment as are, in the judgment of the Inspector General, necessary or desirable;

6. (XXX) OIG's routine uses under the Privacy permit the following that are relevant to the proposed matching activity:

> (List disclosing OIG's applicable routine uses or any other applicable exceptions that allow disclosure under the Privacy Act).

IV. Proposed Data Match

(Describe the data matching operation in detail and explain how the data match will function, including such items as files to be matched, past history of similar matching, and estimate of the number of records.)

V. Justification and Anticipated Results

A. Justification

(Describe what the responsible component within your OIG is trying to accomplish with the match and why the data match will assist in that effort.)

B. Anticipated Results

(Describe the results expected from the data match and what actions your OIG may take as a result of the match (e.g. pursue criminal prosecution, seek civil monetary penalties, refer to the agency for administrative action/ suspension or termination of benefits, recovery of overpayments, reclamation, etc.). If results are determinable, describe expected results, such as how many individuals will be impacted and any determinable estimate of any savings.)

This DMP is:

□ Approved
□ Denied
□ More information required: _____

_____ _____
Signature of Component Head Date

_____
Title of Component Head

This DMP is:

□ Approved
□ Denied
□ More information required: _____

_____ _____
Signature of Final Authorizing Official Date

_____
Title of Final Authorizing Official

Appendix B: Data Use Agreement Preparation Guide

The below guidance is not binding on any Inspector General Office (IG Office). This guidance also does not represent the official legal interpretation of CIGIE or its members regarding implementation of Section 6(j)(2) of the IG Act, related provisions of the IG Act, or other laws, regulations, and implementing guidance. Each IG Office should make its own independent assessment of how to apply the new computerized data matching exemption. Because the legal parameters are not identical across the IG community, IG Offices should consult with their respective offices of legal counsel and/or legislative committees for additional clarification or to discuss any outstanding issues, as necessary.

Data Use Agreement (DUA) Elements:

I. Title/Parties, Summary Description, and Identifying Number

A. Title/Parties to the DUA

State as part of the name of the DUA the names of the parties providing and receiving data through the DUA (e.g., Data Use Agreement Between Social Security Administration Office of the Inspector General and U.S. Department of Health and Human Services).

B. Identifying Number

Establish a numbering convention that allows for simple tracking of the number of OIG component DUAs for each fiscal year. For example, SSA OIG OA # 17-01 would signify SSA OIG's Office of Audit's first DUA in fiscal year 2017.

C. Summary Description

Use a DUA summary that best summarizes the intended match of data (e.g., Data match of (insert description of source agency/entity records) records to (insert description of recipient agency/entity records) records to identify for investigation/review (amend as appropriate) potentially ineligible (describe program/activity) beneficiaries/recipients, related fraud perpetrators, and improper payments, and pursue/refer matters for appropriate civil, criminal, and/or administrative action).

II. Purpose, Responsible Component, and Legal Authority

A. Purpose and Responsible Component

Provide a high-level description of what the data match will do. This section should explain the concept and the usefulness of the data comparison/match. It should describe which agency or agencies will "take action" (e.g. investigate, pursue criminal prosecution, civil monetary penalties, refer match results to its establishment for administrative action/suspension or termination of benefits, recovery of overpayments, or reclamation, and/or identify internal control weaknesses, needed program improvements, questioned costs and funds for better use, etc.) and the results expected from the data match. This section should also contain sufficient details to describe the purpose. All other information in other sections of the agreement must support and agree with the purpose described in this section. State which component within your OIG is responsible for this DUA.

B. Legal Authority

Cite the appropriate laws and sections that permit the data exchange and computerized comparison of information, such as applicable IG Act provisions (see sample DUA template for examples of authorities), and routine uses under the Privacy Act that permit any disclosures contemplated.

III. Operation of the Data Match

Describe the data matching operation in detail and explain how the data match will function. It should discuss the responsibilities of each of the parties to the DUA, including which agency or office will disclose its information (i.e., who will send a finder file with data elements and/or identifiers for the recipient agency to match against its records), what information will be disclosed (e.g., what data elements will be provided from what system of records of the disclosing agency), in what format will data be remitted (e.g., electronically, hard copy, etc.), and how the systems exchange(s) and related matching will operate (e.g., recipient agency will match the disclosing agency's finder file/data against what system of record(s) of the recipient agency, and what will be provided in return), the frequency of the exchange(s) (i.e., yearly, monthly, daily, or on a one-time basis, etc.), the time frame to complete activities (e.g., 30 months), and what agency or office takes action (i.e., the results of the match will be used by (insert name of OIG conducting the data comparison/match) to do what).

Discuss the record selection criteria (attribute values) that will be used for the matching. For example, an SSN may be used to identify the individual, but a date range or other selection criteria may be necessary to limit the volume of records received and to restrict the query to only those records that are necessary for the investigation/audit.

IV. Justification and Anticipated Results

A. Justification

Describe what the parties are trying to accomplish with the data comparison and why this data comparison/match will assist in that effort.

B. Anticipated Results

If results are determinable, describe expected results, such as how many individuals will be impacted, an estimate of any savings, and anticipated program improvements.

V. Description of Records to be Matched/Systems of Records

A. Recipient Agency/OIG:

Cite the *specific* system of records to be used in the comparison/match, including all system of record identifying information.

B. Source/Other Agency/Entity:

The *specific* system of records should be cited, if one is identifiable, including all designations. If the other agency/entity has requested routine use and/or publication information, require the same information from them. If State records are involved, they may not have systems of records or notices like Federal systems of records. State records should be described in as much detail as possible.

C. Number of Records Involved:

Provide the total number of records in the system of records to be used in the match or an approximation of the total if the total is not determinable. If an entire database is not being matched/compared, provide the number of records involved in each database included in the comparison/match. Describe the database(s) expected to be used and any identifiable subsets of data expected to be accessed.

D. Data Elements Used in the Comparison/Match:

Specifically identify each data element in both the recipient OIG's finder file and the reply (results of data comparison) file. This section can be referenced as an Exhibit.

A determination should be made whether a data dictionary or data base schema (both "metadata") should be requested from the system owners. This metadata (i.e., data about data), if required, should be requested early in the process to assist in the development of a clear and concise data request. An analysis of what data is necessary should be completed before the DUA is signed.

VI. Retention and Destruction of Identifiable Records

Explain the records retention expectations, such as records resulting from the match are to be retained for the purposes of the data match, investigative follow up, ultimate action, and as necessary to comply with applicable records retention laws, guidelines, and peer and internal quality reviews, etc. Explain the procedures for the timely destruction of the records after completion of the data comparison, if applicable.

VII. Security Procedures

State the responsibilities of the respective parties in the event of a breach or suspected breach of the information (loss reporting and breach notification).

Describe how both agencies/entities (including States) will ensure the administrative, physical and technical security of the information, including limiting access to individuals with appropriate clearance.

State that policies and procedures will be adopted to ensure compliance with the DUA. Specify permission for onsite inspections to ensure applicable compliance requirements are met.

VIII. Records Usage, Duplication, and Re-disclosure Restrictions

Describe the specifics of how each data exchange agency (including States) will use, and not use, the data. This section also governs whether and how records may be duplicated. Generally, OIGs should not permit other agencies to re-disclose OIGs' data unless required by law. OIGs should usually require other agencies, including States, to obtain OIGs' written permission before re-disclosing any information. Data disclosed, and obtained, should be used only for the purposes set forth in the DUA, and a clause should specify such limitations. Any uses beyond those set forth in the DUA should require a separate DUA setting forth those uses.

IX. Reimbursement

Agencies are generally entitled to be paid for services rendered unless there is legal authority to the contrary or an arrangement in place that benefits/furthers the mission of both agencies. Describe the reimbursement agreement, if any, for the matching activity, or provide a clear statement that reimbursement is not contemplated, and an explanation why the agency is not being reimbursed for the exchange of data. The section should include specific language to substantiate the mutually beneficial arrangement as such arrangements will be specifically quantifiable, and the financial advantages to the OIG may be intangible.

X. Integration Clause

Insert provision stating that this agreement constitutes the entire agreement of the parties with respect to its subject matter and supersedes previous drafts or other oral or written discussions of this agreement. (Recipient OIG) and (source agency/entity) have made no representations,

warranties, or promises outside of this agreement. This agreement takes precedence over any other documents that may be in conflict with it.

XI. Duration, Modification and Termination of the Agreement

The DUA should contain a finite time period/duration. Define the period in which an agreement will remain in effect and any renewal terms. The DUA should remain in effect for a reasonable duration necessary to accomplishment the intended data match. In addition, describe how modifications may be made to the agreement. For example, modifications may be made if all parties agree in writing. State how termination can occur. For example, either party may unilaterally terminate this agreement with 90 days' prior written notice to the other party or immediate termination may occur with the mutual written consent of all parties.

XII. Dispute Resolution

Explain how disputes under the agreement will be resolved (e.g., in accordance with instructions provided in the Treasury Financial Manual (TFM) Volume I, Part 2, Chapter 4700, Appendix 10, *Intragovernmental Transaction Guide*).

XIII. Persons to Contact

For the practical purpose of conducting the match, parties to the agreement should list the names and contact information, including telephone, facsimile, and/or email, of persons who are responsible for conducting the data comparison.

OIG contacts are:	**Other Agency/Entity contacts are:**
(Enter name, title, address, and telephone number).	(Enter name, title, address, and telephone number).
Program Information:	Program Information:
Systems Operations:	Systems Operations:
Information Exchange & Matching Staff:	Information Exchange & Matching Staff:

Note: Under FISMA, each system subject to FISMA should have an Information System Security Manager (ISSM) and an Information System Security Officer (ISSO). Where applicable, consideration should be given to whether such contacts should be listed here.

XIV. Authorized Officials/Signatures

The DUA must be executed by the appropriate officials in the agencies/entities with authority to give it effect. For example, OIGs should designate who has the authority to execute DUAs, such as the Inspector General or Deputy Inspector General. The other agency/entity should provide a similar official to sign.

Appendix C: Data Use Agreement Template

The below sample DUA template is not a binding template format for any Inspector General Office (IG Office). This sample template also does not represent the official legal position of CIGIE or its members regarding the DUA format to use to when implementing Section 6(j)(2) of the IG Act, related provisions of the IG Act, or other laws, regulations, and implementing guidance. Each IG Office should make its own independent assessment of how to apply the new computerized data matching exemption, and what format and content is appropriate for a DUA with other entities. Because the legal parameters are not identical across the IG community, and each match is different, IG Offices should consult with their respective offices of legal counsel, and, if necessary, legislative committees for further clarification or to discuss any outstanding issues.

Data Use Agreement Between (Insert name of OIG seeking to match) (XXX OIG) and (Insert name of entity with whom you are seeking match) (XXX)

(XXX) OIG OI DUA # 17-01

I. SUMMARY DESCRIPTION

Data match of (insert name of agency whose records are being matched) (XXX) (describe records, e.g., Title II (TII) disability records) to (insert name of agency with whom you are intending to match records) (XXX) (describe records) records, to identify and investigate potentially ineligible TII disability beneficiaries, fraud perpetrators, and improper payments, and pursue/refer matters for appropriate civil, criminal, and/or administrative action.

II. PURPOSE AND RESPONSIBLE COMPONENT

This Data Use Agreement (DUA) establishes the terms, conditions, and safeguards under which the (insert OIG name) OIG will disclose the records of (XXX insert agency/entity name) (insert description of records – e.g., TII disability beneficiaries) in (XXX) OIG's system of records to (insert recipient), Office of (insert name) Programs, for a periodic computerized comparison to (describe recipient records) records. (XXX) OIG will use the results of the comparison to assist in the detection and prevention of fraud, waste and abuse in (XXX's - insert agency/entity name) (insert program name) program and related improper

payments by (1) identifying and investigating (insert name of program) beneficiaries and others that potentially should have reported (insert program name) payments for offset against (insert name of benefits) benefits, (2) pursuing appropriate civil, and criminal action, and (3) referring matters to (XXX) for (XXX) administrative action, where appropriate.

The (XXX) OIG component responsible for this agreement and its contents is the (XXX) OIG Office of Investigations (OI).

III. LEGAL AUTHORITY

A. (XXX) OIG enters into this DUA pursuant to the authority granted by the Inspector General Act of 1978 (IG Act), as amended. The IG Act, 5 U.S.C. App. 3 § 6(a) (3), explicitly grants each Inspector General the authority "to request such information or assistance as may be necessary for carrying out the duties and responsibilities provided by this Act from any Federal, State, or local governmental agency or unit thereof."

B. The IG Act, 5 U.S.C. App. 3 § 6(a) (9), explicitly grants each Inspector General with "the authority to the extent and in such amounts as may be provided in advance by appropriations Acts, to enter into contracts and other arrangements for audits, studies, analyses, and other services with public agencies and with private persons, and to make such payments as may be necessary to carry out the provisions of this Act."

C. The IG Act, 5 U.S.C. App. 3 § 6(j)(2), exempts (XXX) OIG from the computer matching provisions of the Privacy Act, by excluding a computerized comparison of two or more automated Federal systems of records, or a computerized comparison of a Federal system of records with other records or non-Federal records, performed by an Inspector General or by an agency in coordination with an Inspector General in conducting an audit, investigation, inspection, evaluation, or other review authorized under the IG Act from the Privacy Act definition of a matching program.

D. The IG Act grants each Inspector General with the duty and responsibility to provide policy direction for and to conduct, supervise, and coordinate audits and investigations relating to the programs and operations of the establishment within which it is established, and to recommend policies for, and to conduct, supervise, or coordinate other activities carried out or financed by such establishment for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, its programs and operations. 5 U.S.C. App. 3 §§ 4(a)(1), 4(a)(3).

E. The IG Act, 5 U.S.C. App. 3 §§ 6(a)(1), (2), authorizes (XXX) OIG:

(1)

(A) to have timely access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials available to the applicable establishment which relate to the programs and operations with respect to which the (XXX) OIG Inspector General has responsibilities under the IG Act;

(B) to have access under subparagraph (A) above, notwithstanding any other provision of law, except pursuant to any provision of law enacted by Congress that expressly-

(i) refers to the Inspector General; and

(ii) limits the right of access of the Inspector General; and

(C) except as provided in subsection (i), with regard to Federal grand jury materials protected from disclosure pursuant to rule 6(e) of the Federal Rules of Criminal Procedure, to have timely access to such information if the Attorney General grants the request in accordance with subsection (h);

(2) to make such investigations and reports relating to the administration of the programs and operations of the applicable establishment as are, in the judgment of the Inspector General, necessary or desirable;

F. (insert name of disclosing OIG/agency) (OIG – remove OIG, as necessary, if the routine use cited is an agency's disclosure authority)'s routine uses under the Privacy Act for its (insert citation of SORN, and applicable routine uses contained in that SORN), permit the following, among other, routine uses of the information from this (XXX) OIG systems of records:

1. Information from this system of records may be disclosed to any other federal agency or any foreign, state, or local government agency responsible for enforcing, investigating, or prosecuting violations of administrative, civil, or criminal law or regulation where that information is relevant to an enforcement proceeding, investigation, or prosecution within the agency's jurisdiction. (routine use a.)

2. Information from this system of records may be disclosed to (1) the Department of Justice in connection with requests for legal advice and in connection with actual or potential criminal prosecutions or civil litigation

pertaining to the Office of Inspector General, and (2) a Federal or State grand jury, a Federal or State court, administrative tribunal, opposing counsel, or witnesses in the course of civil or criminal proceedings pertaining to the Office of Inspector General. (routine use b.)

3. Information from this system of records may be disclosed to the Department of Justice, to a judicial or administrative tribunal, opposing counsel, and witnesses, in the course of proceedings involving (XXX), an (XXX) employee (where the matter pertains to the employee's official duties), or the United States, or any agency thereof where the litigation is likely to affect [XXX], or [XXX] is a party or has an interest in the litigation and the use of the information is relevant and necessary to the litigation. (routine use k.)

4. Information from this system of records may be disclosed to third party contacts, including public and private organizations, in order to obtain information relevant and necessary to the investigation of potential violations in (XXX) programs and operations, or where disclosure would enable the ((XXX) OIG to identify violations in (XXX) programs or operations or otherwise assist the OIG in pursuing on-going investigations. (routine use m.)

G. (XXX) OIG's Privacy Act routine uses for its (insert citation of SORN, and list below applicable routine uses contained in that SORN), permit the following, among other, routine uses of information from this (XXX) OIG system of records:

1. In the event that this system of records maintained by this Agency to carry out its functions, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, foreign, state, or local, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto where such responsibility rests outside of OIG. (routine use (1))

2. Disclosures may be made to federal, state, or local agencies where disclosure is necessary in order to obtain records relevant and necessary to a civil or administrative investigation of the Office of Inspector General. (routine use (2))

3. Disclosures may be made to third party contacts where the party contacted may have information needed to establish or verify information relevant and necessary to a civil or administrative investigation by the OIG or in

preparation for proceedings pursuant to section 1128A of the Social Security Act, and "Civil Money Penalties". (routine use (5))

4. Disclosures may be made to federal, state, and local agencies, or to other entities administrating federally funded programs where necessary to take action based on an OIG investigation or audit, which identifies individuals not entitled to program benefits or individuals delinquent on loan payments under federally funded programs. (routine use (6))

(Insert any other applicable Privacy Act disclosure exceptions)

IV. OPERATION OF THE DATA MATCH/RESPONSIBILITIES OF THE PARTIES

A. (XXX's – Insert Other Agency/Entity Name) Responsibilities

Example 1:

1. (*insert name of recipient agency/entity*) will receive (*insert frequency of match, if occurring more than once*) from (*XXX*) OIG an Excel spreadsheet of beneficiaries with the following columns (attributes):

    i. name;

    ii. date of birth;

    iii. social security number;

    iv. date of award (if multiple awards); and

    v. award amount.

2. (*insert recipient agency/entity name*) will identify (*insert program name*) payment activity in the (*insert system name*) system for the beneficiaries listed in the (*XXX*) OIG Excel spreadsheet *XXX* using the beneficiaries' social security numbers and payment dates. The date range for the payment activity starts on *DD/MM/YYYY* and ends on *DD/MM/YYYY*. This date range may change on subsequent matching requests/updates.

3. (insert recipient agency/entity name) will provide (XXX) OIG (source agency/OIG) an Excel spreadsheet with the original attributes (columns) used in the search, plus the following columns resulting from the query against the (Insert system name) system. The spreadsheet should contain the following columns (attributes):

    i. name;

ii. date of birth;

iii. social security number (e.g., SSN's should be in the 000-00-0000 format);

iv. date of award (if multiple awards);

v. award amount; and

vi. residence location.

Example 2:

1. (insert recipient agency/entity name) will receive (insert frequency of match, if occurring more than once) from (XXX) OIG electronic (XXX) beneficiary (specify type, e.g., Excel) spreadsheets with names, dates of birth, Social Security number, and award amount.

2. (insert recipient agency/entity name) will match the (XXX) OIG (specify type, e.g., Excel) spreadsheet data against its (Insert system name) system to identify (insert program name) payment activity for the listed (insert program name) beneficiaries for the period specified by (insert name of OI/OA Division seeking information).

3. (insert recipient agency/entity name) will provide (XXX) OIG (source agency/OIG) a listing of (insert program name) beneficiaries that match its payment activity file along with any pertinent residence location information, for the period specified by (XXX) OIG.

Example 3:

A. On a monthly basis, (source agency/entity) will disclose (program/activity name) payment data to (XXX) from the (XXX) system of records (SOR) published as XXXX (XXXXXXXXXX and XXXXXX Records).

B. The component responsible for this disclosure on behalf of (source agency/entity) is XXXX Services.

B. <u>(XXX) OIG Responsibilities</u>

Example 1:

(XXX) OIG Office of Investigations (OI) Responsibilities

1. (XXX/insert Division name) will identify from the (XXX) record a list of (XX) beneficiaries with addresses listed in certain counties/cities in the United States.

2. (XXX) will prepare a spreadsheet of the (XX) beneficiaries with addresses listed in certain counties/cities of the United States.

3. (XXX) will send the spreadsheet to (XXX insert data source agency that will respond to data provided by OIG) with a request for (describe records being sought) information for a specified period.

4. (XXX) will refer all match data received from (XXX) to OI Field Divisions for appropriate investigative follow-up.

5. OI Field Divisions will refer the names of (XX) beneficiaries who received (XXXX) payments that should have been offset against (XXX) payments to (insert agency name) so (XX) benefits can be reduced, suspended or terminated pursuant to (insert agency name) policy, and, if applicable, administrative action.

6. OI Field Divisions will refer to authorities for criminal prosecution and civil action those residents of the United States who received and converted to their own use any improperly paid benefits, as appropriate.

Example 2:

(XXX) OIG Office of Investigations (OI) Responsibilities

1. (XXX) OIG will match (XXX)'s data with data in XXXXXXXXXXXX (XXXX), XX-XXXX, to determine XXXXXXXXXXXXXXXXXXXXXXXXX.

2. (XXX) OIG will use (XXX)'s data to XXXXXXXXXXXXXXXXX.

3. (XXX) OIG will use (XXXX)'s data to determine XXXXXXXXXXXXXX.

4. (XXX) OIG will use (XXX)'s data to identify potential XXXX XXXXXX and will use the information to XXXXXXXXXXXXXXXXXXXXXXXXX.

C. Organization(s) to Process Cases

(XXX) OIG, OI

D. Timeframe to Complete Computer Operation(s)

Approximately 30 months

E. Timeframe to Complete Case Processing

Approximately 30 months.

F. Organization to Complete Management Information/Data Collection Sheet, Analysis, and Study Report or Other Reports, If Applicable

(XXX) OIG OI

V. JUSTIFICATION AND ANTICIPATED RESULTS

A. Reason or Basis for Proposal

1. The purpose of this DUA for (XXX) OIG is to assist in the detection and prevention of improper payments and related fraud and abuse in (XXX)'s (XXXX) program.

2. (XXX) OIG will use the information derived from this match to assist in the detection and prevention of improper payments by (1) identifying (XXX) beneficiaries that received (XXXX) payment who should have offset these payments against (XXX) payments, (2) referring information to (XXX) to have overpayments posted on (XXX)'s records due to ineligibility, and suspension or termination of benefits, and (3) pursuing appropriate civil and criminal action.

3. The (XXX) is the most viable (or only) source of (XXXX) payment information to: (1) identify and assess (XXX) beneficiaries that received (XXXX) payments, which should have been reported to (XXX) so they could be offset against (XXXX) payments, (2) facilitate referring information to (XXX) to have overpayments posted on (XXX)'s records due to ineligibility, and suspension or termination of benefits, and (3) pursue appropriate civil, criminal and administrative action. This match is believed to be the most efficient and comprehensive method of collecting and comparing information to carry out the provisions of the IG Act as it relates to the detection and prevention of improper payments and related fraud, waste and abuse pertaining to (XXX) program eligibility for individuals not reporting (XXXX) payments to (XXX) so (XXX) benefits can be appropriately offset, and assessment of the (insert agency name)'s related administration of the (XXX) program.

B. Improve Program Integrity

Program integrity will be improved through suspension and/or termination of benefits to those not entitled to receive them, recovery of overpayments to the extent feasible, and deterrent impact from civil, criminal and administrative actions. (XXX) OIG expects (XXX) to realize substantial cost savings in the (XXX) program and expects that the match under this agreement will detect and prevent improper payments and related fraud, waste and abuse in the (XXX) program. If (XXX) OIG identifies any deficiencies in or lack of internal accounting or administrative controls, or inefficiencies or ineffectiveness in program operations during our computer matching activities, we expect that improvements in such controls, inefficiencies or ineffectiveness will be realized through the implementation of our recommendations for corrective action.

C. Implement Program Improvement

(XXX) OIG believes this match may encourage (XXX – insert agency name) to periodically obtain XXX information to assess eligibility and reduce improper payments, and deter fraud.

VI. RECIPIENT AGENCY/(XXX) OIG

A. Name of System

The relevant System of Records Notices are (insert applicable systems below in place of samples):

1. (list applicable agency and OIG SORNS)

2. Criminal Investigative Files of the Inspector General, (XXX/OIG (system number OIG-001) published in the Federal Register (XX Fed. Reg. XXXXX, April xx, xxxx), incorporating by reference (XXX) system of records number XX-XX-XXXX entitled Criminal Investigative Files of the Inspector General*, (XXX)*/OS/OIG (XX Fed. Reg. XXXXX, Nov. 2, XXXX).

3. Civil and Administrative Investigative Files of the Inspector General, (XXX)/OIG (system number OIG-002) published in the Federal Register (XX) Fed. Reg. XXXXX, April XX, XXXX), incorporating by reference (XXX) system of records number XX-XX-XXXX entitled Civil and Administrative Investigative Files of the Inspector General, (XXX)/OS/OIG (XX Fed. Reg. XXXXX, Sept. XX, XXXX).

B. Size of System Universe

The (insert name of record) Record file will contain approximately (insert number of records) records of individuals.

C. Record Fields/Elements to be Used

The data elements included in the match file are (insert applicable data elements):

1. Social Security number (SSN);

2. Name;

3. Date of birth;

4. Award Amount;

5. XXXXX.

VII. SOURCE AGENCY

A. Name of System

(Insert system name)

B. Size of System Universe

(Insert size of universe)

C. Number of Finder File Records in Match Universe

(Insert number of finder file records)

D. Records Fields/Elements to be Used by/Provided to (XXX) OIG

(Insert field/elements)

VIII. PROCEDURES FOR RETENTION AND TIMELY DESTRUCTION OF IDENTIFIABLE RECORDS

(XXX) OIG and (XXX) will retain the electronic files received from each other only for the period required for any processing related to the data match contemplated under this agreement and then will destroy all such data by electronic purging. (XXX) OIG will retain data only to the extent that it is required to retain the information to meet evidentiary requirements, quality control, peer review, or records retention requirements. If such retention is warranted, (XXX) OIG will retire the retained records in accordance with applicable Federal Records Retention Schedules (44 U.S.C. § 3303a). (XXX) OIG will not create permanent files or a separate system comprised solely of the data (XXX) provides to (XXX) OIG.

IX. SECURITY PROCEDURES

(XXX) OIG and (XXX – insert data source agency name) will comply with the applicable requirements of the Federal Information Security Management Act (FISMA), 44 U.S.C. Chapter 35, Subchapter II, as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); related Office of Management and Budget (OMB) circulars and memoranda, such as Circular A-130, Managing Information as a Strategic Resource (July 28, 2016), and Memorandum M-06-16, Protection of Sensitive Agency Information (June 23, 2006); National Institute of Standards and Technology (NIST) directives; and the Federal Acquisition Regulations, including any applicable amendments published after the effective date of this agreement. These laws, directives, and regulations include requirements for safeguarding Federal information systems and personally identifiable information (PII) used in Federal agency business processes, as well as related reporting requirements. Both agencies recognize and will implement the laws, regulations, NIST standards, and OMB directives including those published subsequent to the effective date of this agreement.

FISMA requirements apply to all Federal contractors, organizations, or entities that possess or use Federal information, or that operate, use, or have access to Federal information systems on behalf of an agency. Both agencies are responsible for oversight and compliance of their contractors and agents.

A. Loss Reporting

If either (XXX) OIG or (XXX) experiences an incident involving the loss or breach of PII provided by (XXX) under the terms of this agreement, (XXX) OIG and (XXX) will follow the incident reporting guidelines issued by OMB. In the event of a reportable incident under OMB guidance involving PII, (XXX) OIG and (XXX) is responsible for following its established procedures, including notification to the proper organizations (e.g., United States Computer Emergency Readiness Team, the agency's privacy office). In addition, (XXX) OIG and (XXX) will notify each other's Systems Security Contact named in this agreement. If (XXX) OIG or (XXX) is unable to speak with each other's Systems Security Contact within one hour, (XXX) OIG and (XXX) will contact the _____at XXX-XXX-XXXX. (Amend, as appropriate, for the loss reporting and the breach notification procedures applicable to each agency).

B. Breach Notification

(XXX) OIG and (XXX – add source agency here and in other subsequent safeguard sections if OIG is disclosing data to a source agency) will follow PII breach notification policies and related procedures issued by OMB. If (XXX) OIG or (XXX) determines that the risk of harm requires notification to affected individuals or other remedies, each entity responsible for the breach OIG will carry out these remedies without cost to the other agency.

C. Administrative Safeguards

(XXX) OIG and (XXX) will restrict access to the data matched and to any data created by the data match to only those authorized employees and officials who need it to perform their official duties in connection with the uses of the data authorized in this agreement. Further, (XXX) OIG and (XXX) will advise all personnel who have access to the data matched and to any data created by the match of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable Federal laws.

D. Physical Safeguards

(XXX) OIG and (XXX) will store the data matched and any data created by the match in an area that is physically and technologically secure from access by unauthorized persons at all times. Only authorized personnel will transport the data matched and any data created by the

match. (XXX) OIG and (XXX) will establish appropriate safeguards for such data, as determined by a risk-based assessment of the circumstances involved.

E. Technical Safeguards

(XXX) OIG (XXX) will process the data matched and any data created by the match under the immediate supervision and control of authorized personnel in a manner that will protect the confidentiality of the data, so that unauthorized persons cannot retrieve any data by computer, remote terminal, or other means. Systems personnel must enter personal identification numbers when accessing data on the agencies' systems. (XXX) OIG and (XXX) will strictly limit authorization to those electronic data areas necessary for the authorized analyst to perform his or her official duties.

F. Application of Policy and Procedures

(XXX) OIG and (XXX) will adopt policies and procedures to ensure that each agency uses the information contained in their respective records or obtained from each other solely as provided in this agreement. (XXX) OIG and (XXX) will comply with these policies and procedures and any subsequent revisions.

X. RECORDS USAGE, DUPLICATION, AND REDISCLOSURE RESTRICTIONS

(XXX) OIG and (XXX – insert other agency name if disclosing information to that agency, so there are reciprocal limitations) will adhere to the following limitations on the use, duplication, and disclosure of the electronic files and data that (XXX) and (XXX) provide each other (tweak as necessary, if only OIG is providing information):

A. Files/data provided under this agreement will be used and accessed only for the purposes described in this agreement.

B. The data provided under this agreement will not be used to extract information concerning individuals therein for any purpose not specified in this agreement.

C. Except for the purposes set forth in this agreement, the files/data provided under this agreement will not be duplicated or disseminated within or outside the agency/entity that received them without the written permission of the source agency. Permission will not be given by the source agency/entity unless the law requires disclosure or the disclosure is essential to the conduct of the purpose of the match under this agreement. For such permission, the recipient agency/entity of the data must specify in writing: (1) what data is requested to be duplicated or disseminated; (2) to whom the data is being duplicated or disseminated; and (3) the reasons that justify such duplication or dissemination.

VIII. REIMBURSEMENT

(INSERT reimbursement arrangement, if applicable)

XIV. INTEGRATION CLAUSE

This agreement constitutes the entire agreement of the parties with respect to its subject matter and supersedes all other data exchange agreements between the parties that pertain to the disclosure of the specified (XXX XXXX) data by (XXX) to (XXX) OIG for the purposes described in this agreement. (XXX) OIG and (XXX) have made no representations, warranties, or promises outside of this agreement. This agreement takes precedence over any other documents that may be in conflict with it.

XV. DURATION, MODIFICATION, AND TERMINATION

A. Effective Date

The effective date of this agreement is XXXXXXXXX.

B. Duration

This agreement will be in effect for a period of XX months, unless renewed or terminated.

C. Renewal

This agreement may be renewed by written agreement of the parties.

D. Modification

The parties may modify this agreement at any time by a written modification, agreed to by both parties.

E. Termination

The parties may terminate this agreement at any time with the consent of both parties. Either party may unilaterally terminate this agreement upon written notice to the other party, in which case the termination shall be effective 90 days after the date of the notice, or at a later date specified in the notice.

XVI. DISPUTE RESOLUTION

Disputes related to this agreement will be resolved in accordance with instructions provided in the Treasury Financial Manual (TFM) Volume I, Part 2, Chapter 4700, Appendix 10, *Intragovernmental Transaction Guide*.

XVII. PERSONS TO CONTACT

A. (XXX) OIG contacts:

Computer System(s)

Name, Title
Division
Office
Address

Telephone:
Fax:
Email:

System(s) Security and Breach Notification

Name, Title
Division
Office
Address

Telephone:
Fax:
Email:

Data Use Agreement

Name, Title
Division
Office
Address

Telephone:
Fax:
Email:

Project Coordinator

Name, Title
Division

Office
Address

Telephone:
Fax:
Email:

B. (XXX) Contacts:

Computer System(s)

Name, Title
Division
Office
Address

Telephone:
Fax:
Email:

System(s) Security and Breach Notification

Name, Title
Division
Office
Address

Telephone:
Fax:
Email:

Data Use Agreement

Name, Title
Division
Office
Address

Telephone:
Fax:

Email:

Project Coordinator

Name, Title
Division
Office
Address

Telephone:
Fax:
Email:

XVIII. SIGNATURES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies/entities to enter into the obligations set forth in this agreement.

(INSERT NAME OF OIG)

_____

(Insert Name)
(Insert Title)
(Insert Agency/Entity Name)
Office of the Inspector General

Date_____

(INSERT NAME OF AGENCY/ENTITY)

_____

(Insert Name)
(Insert Title)
(Insert Agency Name)

Date_____