

Centralizing Access to Data to Prevent Improper Payments: A Discussion of the Do Not Pay Data System

February 9, 2026

Congressional Research Service

<https://crsreports.congress.gov>

R48850



R48850

February 9, 2026

Natalie R. Ortiz
Analyst in Government
Organization and
Management

Centralizing Access to Data to Prevent Improper Payments: A Discussion of the Do Not Pay Data System

Improper payments can result from government agencies making errors and mistakes during the payment process, including failing to detect fraud. The result is payments that should not have been made and a diversion of public monies. Curbing improper payments is often of interest to policymakers because reducing improper payments may net savings or offset additional spending. In general, policymakers and a variety of other stakeholders believe that improper payments are largely preventable.

Data access issues are among the root causes of improper payments. In cases where data access issues are a root cause, policymakers and others believe that if the data were accessible or the access issue were otherwise corrected, then improper payments would be prevented. Some of the policies enacted by Congress to curb improper payments are intended to make it easier for agencies to access and use data.

The Payment Integrity Information Act of 2019 (PIIA) codifies the Do Not Pay Initiative, which enables agencies to access and use certain databases to verify payment eligibility prior to awarding or releasing any federal funds. In practice, the Do Not Pay (DNP) system provides agencies with centralized access to the databases agencies may use under the PIIA, and agencies are required to review payments for eligibility using the DNP system. The Bureau of the Fiscal Service within the Department of the Treasury operates the DNP system with assistance from certain Federal Reserve Banks. The Government Accountability Office (GAO) states that the DNP system is a “key resource for preventing improper payments” and that preventative activities are generally the most cost-efficient use of agency resources.

The DNP system relies on data matching. The presumption behind the use of the DNP system is that if an agency discovers that it is slated to make a payment to an entity (e.g., a person) that matches to information in a database that is part of the DNP system, then the agency will further examine whether that entity is in fact eligible to receive such payment. The DNP system itself does not automatically stop a payment transaction from occurring. Matching an intended payment recipient to a DNP system database does not necessarily mean that the payment recipient is in fact ineligible to receive a payment. Certain policies can inform an agency’s decisionmaking around the issuance of certain types of payments and financial awards if a match in the DNP system occurs.

Use of the DNP system, including data matching, occurs within the compliance framework established by the Privacy Act of 1974, which governs how a federal agency may disclose information that identifies an individual to another federal agency. Executive Order (E.O.) 14249, *Protecting America’s Bank Account Against Fraud, Waste, and Abuse*, issued in March 2025, directs executive branch agencies to complete certain administrative processes specified by the Privacy Act to ensure that agencies can disclose information (e.g., Social Security numbers and names) on intended payment recipients to the Treasury Department for the purpose of using the DNP system. The executive order presumes that by reducing administrative barriers to the sharing of payment recipient information with the DNP system, more agencies will use the DNP system, which will presumably increase the detection of improper payments. In August 2025, the Office of Management and Budget stated that the DNP system, “to date, has failed as a tool for comprehensive screening for improper payments to protect against waste, fraud, and abuse.”

While the PIIA mandates agencies to review certain databases before disbursing payments, not all agencies report using the DNP system, and a proportion of those agencies that do use the system indicate that it is not effective in reducing improper payments for them. The DNP system does not necessarily contain all information that is needed by an agency to verify eligibility for a particular type of payment, such as a loan, and the DNP system may be one of several data systems used to establish eligibility. The costs and benefits of integrating use of the DNP system into payment processing workflows, which are largely automated, may vary by agency and by program.

Contents

The Costs of Improper Payments	1
Preventing Improper Payments	2
Data Access as a Root Cause of Improper Payments	3
Issues Accessing Certain Types of Data	4
Multiple Access Issues	6
Using Data to Prevent Improper Payments: History and Context for the Do Not Pay System	7
Data Matching to Detect Improper Payments	7
The “Do Not Pay List”: Origins of the Do Not Pay System	8
Improper Payments Elimination and Recovery Improvement Act of 2012	9
The Payment Integrity Information Act of 2019	11
Overview of Do Not Pay System Operations	12
Assumptions Behind the Operations of the Do Not Pay System and the Role of Data Matching	13
Accessible Databases	14
Services to Agencies	16
Portal	16
Data Analytics Services	18
Funding Sources and Costs to Operate	21
Information Technology	21
Federal Reserve Banks	22
Compliance with the Privacy Act	23
Sourcing Databases for the Do Not Pay System	24
Using the Do Not Pay System as a Paying Agency	25
Data Matching	26
Waiving Computer Matching Agreements Under the Payment Integrity Information Act	28
Effect of Data Matches on Payments	31
Payment Authorities and Roles	32
Due Process Under the Computer Matching and Privacy Protection Act	33
Prompt Payment Act	34
Relevance to Payment Eligibility	35
Risk Appetite	35
Payment Integration and Timing of a Match	36
Adjudicating Matches from Payment Integration	37
Discussion	38
Assessing the Role of the Do Not Pay System in Preventing Improper Payments	38
Measuring Government-wide Improper Payments Prevented	39
Agency Reporting on Improper Payments Prevented	41
Addressing the Usefulness of Data Accessible Through the Do Not Pay System	42
Meeting Data Needs	43
The Authority of the Office of Management and Budget Director to Designate Databases as Part of the Do Not Pay Initiative	44
Assessing the Cost-Effectiveness of Data Matching Using the Do Not Pay System to Agencies	47

Cost-Benefit Analyses.....	47
Data Quality in Cost-Benefit Analyses	48
Conclusion.....	50

Figures

Figure 1. The Federal Payment Process	3
Figure 2. Overpayments Caused by Data Access Issues, FY2021-FY2024.....	4
Figure 3. Do Not Pay Initiative Databases and the Do Not Pay System	14
Figure 4. Process to Onboard an Agency to the Do Not Pay System.....	18
Figure 5. Process to Develop Data Analytics Projects	20
Figure 6. Costs to Operate the Do Not Pay System, FY2012-FY2025	22

Tables

Table 1. Data Types Associated with Overpayments for FY2024.....	5
------------------------------------------------------------------	---

Table A-1. Databases Included in the Do Not Pay Initiative and Part of the Do Not Pay System	52
-------------------------------------------------------------------------------------------------------	----

Appendixes

Appendix. Do Not Pay Initiative Databases.....	52
------------------------------------------------	----

Contacts

Author Information.....	57
-------------------------	----

The Costs of Improper Payments

Improper payments are generally caused by errors and mistakes made by agencies during the payment process. Agencies have reported an estimated \$2.8 trillion in total improper payments between FY2003 and FY2024.¹ Improper payments in FY2024 account for nearly \$162 billion of this total amount (about 6%).²

A large share of improper payments are classified as *overpayments*. An overpayment is a specific type of improper payment that results in monetary losses to the federal government.³ When an overpayment occurs, the improper amount is the difference between the amount that is due to the recipient and the amount that was actually paid.⁴ Overpayments include duplicate payments and full payment amounts if no payment was in fact owed (e.g., because the recipient was ineligible for any portion of the payment up to the full amount). Overpayments can also include cases where an agency makes a payment based upon incorrect information it has received.⁵

Unintentional overpayments are considered accidental in nature, including those that might arise from an agency not having the most up-to-date information for payment processing purposes.⁶ For example, an agency might not have access to the most up-to-date income data for a program applicant, but the application otherwise appears correct based on all of the eligibility verification the agency is able to perform. As a result, the agency issues a payment only to learn later that the income information was out of date, which may have altered the determination of payment eligibility or the payment amount.⁷

Overpayments can typify the concept of *pay-and-chase* when a payment is issued and then found to be improper after the fact, such that recovery would require “chasing” this overpayment. In this way, pay-and-chase is a reactive approach to managing improper payments. GAO describes the recovery of improper payments under a pay-and-chase approach as difficult and expensive.⁸ Overpayments may or may not be recouped by an agency.⁹ Under statute, agencies are given some discretion in determining whether to recover overpayments, as it might not always be cost-

¹ Government Accountability Office (GAO), *Improper Payments: Information on Agencies' Fiscal Year 2024 Estimates*, GAO-25-107753, March 11, 2025, <https://www.gao.gov/products/gao-25-107753>.

² GAO, *Improper Payments: Information on Agencies' Fiscal Year 2024 Estimates*.

³ In addition to overpayments, other types of improper payments include *underpayments* and *technically improper payments*. These other types of improper payments do not result in monetary loss to the government. Underpayments result in a payment recipient not receiving the full amount of funds to which they were entitled. Technically improper payments are payments made in the right amount to the right recipient, but where the payment process did not follow applicable statutory or regulatory requirements. See Office of Management and Budget (OMB), *Transmittal of Appendix C to OMB Circular A-123, Requirements for Payment Integrity Improvement*, M-21-19, March 5, 2025, pp. 9-10, <https://www.whitehouse.gov/wp-content/uploads/2021/03/M-21-19.pdf>.

⁴ OMB, *Transmittal of Appendix C*, M-21-19, p. 68.

⁵ GAO, *Improper Payments and Fraud: How They Are Related but Different*, GAO-24-106608, December 7, 2023, p. 3, <https://www.gao.gov/assets/d24106608.pdf>.

⁶ In contrast to unintentional overpayments, intentional overpayments include cases of fraud, but only after the payment amount has been determined fraudulent by a court or through an adjudication process, and overpayments that occur on purpose (e.g., the agency knowingly issues a payment to an ineligible recipient). See OMB, *Transmittal of Appendix C*, M-21-19, pp. 9-10.

⁷ OMB, *Transmittal of Appendix C*, M-21-19, p. 10.

⁸ GAO, *A Framework for Managing Improper Payments in Emergency Assistance Programs*, GAO-23-105876, July 23, 2023, p. 22, <https://www.gao.gov/assets/gao-23-105876.pdf>.

⁹ OMB, *Transmittal of Appendix C*, M-21-19, pp. 34-36.

effective.¹⁰ Overpayments can cost an agency more money than the original value of the improper amount paid because the costs to recover overpayments require additional resources that can exceed the original payment's value, further underscoring how improper payments result in monetary losses to the government.

Preventing Improper Payments

Preventing improper payments in the first place—that is, before any payment is disbursed—appeals to policymakers because prevention is viewed as cost-effective and has the potential to avoid losses in the context of government costs and spending more generally.¹¹ Policymakers, the Government Accountability Office (GAO), federal inspectors general, and other federal and nonfederal stakeholders largely believe that improper payments are mostly preventable and that agencies can do more using internal processes to reduce the occurrence of improper payments.¹²

Effective policies and processes internal to an agency may prevent and minimize further the risk of making improper payments. A concept that could inform these agency policies and internal processes is *payment integrity*, which is defined by the Office of Management and Budget (OMB) as the process of ensuring that a payment is proper. Payment integrity is considered by OMB to be a concept core to federal financial management and a fundamental component of any agency's overall mission.¹³

One way to prevent improper payments, including overpayments, could be to address their causes. As discussed in greater detail below, OMB believes that data access issues are a cause of improper payments. Thus, the process of ensuring a payment is proper may depend in part on the agency's access to data to verify payment eligibility.

Some of the policies enacted by Congress to curb improper payments are intended to increase access to and use of data that are believed to assist in payment integrity processes and the prevention of improper payments. In general, these data might verify some aspect of payment eligibility—for example, being delinquent on paying back a federal loan might bar eligibility for other types of federal loans and thus the payments that occur under these other loan programs.

This report discusses the role that data access plays in payment integrity and in causing and curbing improper payments. One policy that Congress has enacted to increase data access and use of data to prevent improper payments is the Payment Integrity Information Act of 2019 (PIIA).¹⁴ The PIIA requires agencies to use the Do Not Pay (DNP) system to verify payment eligibility prior to payment disbursement.¹⁵ The DNP system provides agencies with centralized access to certain databases, most of which originate from within the federal government. The assumption is that access to these databases enables agencies to then use data matching to determine whether an intended payment recipient matches to the data accessible through the DNP system (e.g., the social security number [SSN] of an individual who is scheduled to receive an entitlement

¹⁰ 31 U.S.C. §3552(i) requires an agency to conduct recovery audits of “each program and activity of the executive agency that expends \$1,000,000 or more annually *if conducting the audits would be cost effective*” (emphasis added by CRS). For OMB's guidance to agencies on determining the cost-effectiveness of using a recovery audit, see OMB, *Transmittal of Appendix C*, M-21-19, p. 36.

¹¹ OMB, *Transmittal of Appendix C*, M-21-19, p. 28.

¹² For a more general overview of some of the issues and challenges in preventing improper payments, see CRS Report R48296, *Improper Payments: Ongoing Challenges and Recent Legislative Proposals*, by Garrett Hatch.

¹³ OMB, *Transmittal of Appendix C*, M-21-19, p. 29; see p. 68 for definition.

¹⁴ P.L. 116-117.

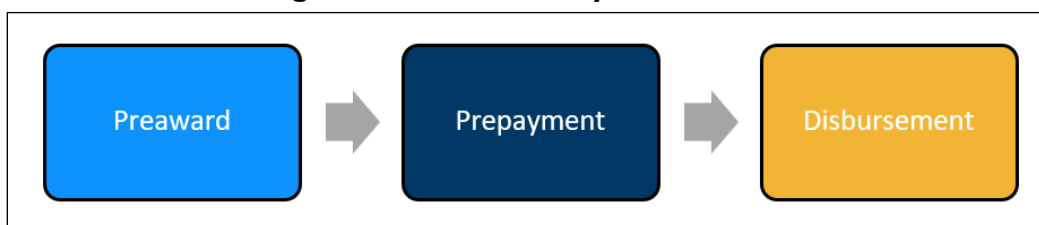
¹⁵ 31 U.S.C. §3354.

payment matches an SSN contained within a DNP system database of deceased individuals). Data matches are presumed to be a possible signal as to payment eligibility. As this report discusses, not all matches are sufficient to render a payment improper nor are all matches indicative of an improper payment.

Data Access as a Root Cause of Improper Payments

According to OMB, data access issues are some of the “root causes” of improper payments.¹⁶ OMB characterizes a root cause as “something that would directly lead to an improper payment, and if corrected, would prevent the improper payment.”¹⁷ Root causes appear somewhere in an agency’s payment process (**Figure 1**), and OMB states that it is important to determine where they arise in the process to ultimately prevent future improper payments.¹⁸

Figure 1. The Federal Payment Process



Source: CRS, based on OMB, *Appendix C to Circular A-123* (Memorandum M-21-19), p. 69, and the “payment lifecycle” from the Bureau of the Fiscal Service (<https://fiscal.treasury.gov/dnp/>).

Data access issues that lead to improper payments are categorized in three ways by OMB:¹⁹

- **The failure to access existing data**, where human error results in not accessing the appropriate data to determine payment eligibility even though the data is accessible to the agency (e.g., when a database with contractor performance data is accessible to the agency, but the agency does not review the database to verify that a contractor has at least satisfactory regulatory compliance ratings prior to awarding a contract).
- **The inability to access existing data**, where the data to determine payment eligibility exists but the agency is unable to access it for some reason (e.g., statute specifically limits the entities that can use or the purposes for which a federal database can be used, such as the National Directory of New Hires).²⁰
- **The absence of available data**, where the data to determine payment eligibility is known to not exist (e.g., in a situation where eligibility is determined in part by

¹⁶ Aside from data access issues, OMB states that other root causes of improper payments include (1) failing to meet statutory or regulatory requirements, which leads to *technically improper payments* (see footnote 3) and (2) being unable to determine whether a payment is proper or improper because of insufficient or missing documentation. In the latter case, OMB anticipates that an agency will eventually determine whether these payments are proper or improper, but that an agency should report such payments as unknown until such determination is made. See OMB, *Transmittal of Appendix C*, M-21-19, pp. 22-24.

¹⁷ OMB, *Transmittal of Appendix C*, M-21-19, p. 22.

¹⁸ OMB, *Transmittal of Appendix C*, M-21-19, p. 26.

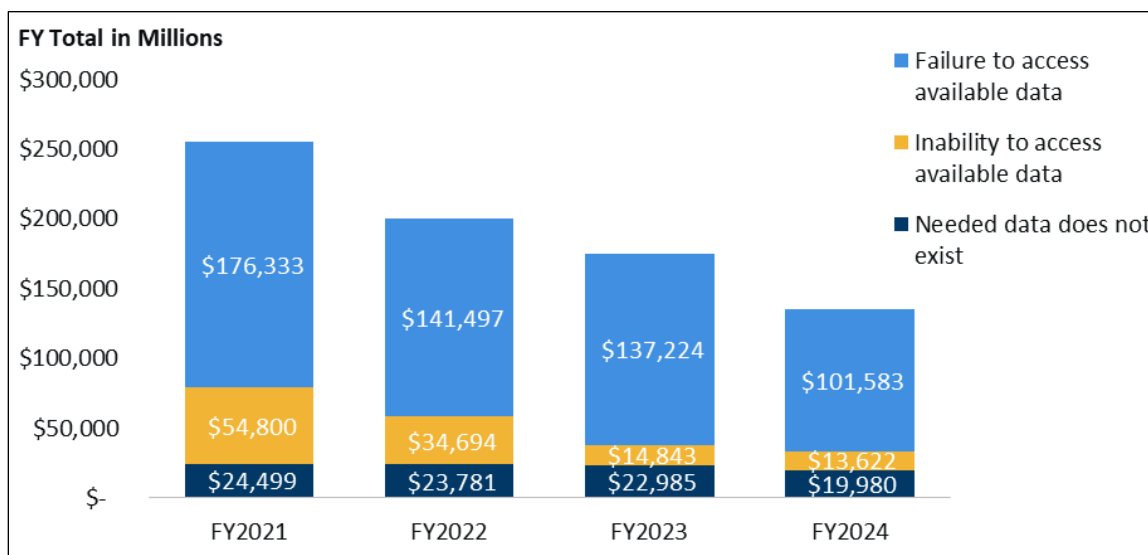
¹⁹ OMB, *Transmittal of Appendix C*, M-21-19, p. 23.

²⁰ For more information on the National Directory of New Hires (NDNH) and how use of the NDNH is restricted by statute to certain entities for certain purposes, see CRS Report RS22889, *The National Directory of New Hires: An Overview*, by Jessica Tollestrup.

the amount per a year child lives with a parent, there is no known database to verify that number).

These three data access issues contributed to agencies reporting an estimated total of \$765.8 billion in improper payments—and, more specifically, in overpayments—between FY2021 and FY2024 (**Figure 2**).²¹ In particular, agencies reported that \$556.6 billion of this—or approximately 73%—was disbursed because of a failure to access existing data.

Figure 2. Overpayments Caused by Data Access Issues, FY2021-FY2024



Source: CRS analysis of the 2024 improper payments dataset on PaymentAccuracy.gov, <https://www.paymentaccuracy.gov/>.

Issues Accessing Certain Types of Data

Agencies have different data needs, requiring access to different types of data as part of their own processes to determine payment eligibility. When a data access issue is identified by an agency as a reason for improper payments, agencies receive guidance from OMB on identifying and reporting the type of data causing such payments.²²

Issues with accessing some types of data result in a larger share of government-wide overpayments compared to others (see **Table 1**). For example, agencies reported that issues with accessing contractor or provider status data resulted in \$232 billion in total overpayments in FY2024. In comparison, issues accessing death data resulted in \$1.5 billion in overpayments during the same fiscal year.

In some cases, agency reporting of improper payments information enables a closer examination of what types of data are associated with a specific data access issue. Some federal programs reported overpayments that are specifically due to an inability to access a specific type of existing data or due to a specific type of data not being known to exist. For example, in FY2024, the Federal Communications Commission (FCC) reported approximately \$21 million in overpayments because of the inability of the Universal Service Fund's (USF's) Schools and

²¹ CRS analysis of the FY2024 improper payments dataset available on PaymentAccuracy.gov, <https://www.paymentaccuracy.gov/>. See also **Figure 2**.

²² OMB, *Transmittal of Appendix C*, M-21-19, pp. 26-27.

Libraries Program to access financial-type data.²³ The FCC reported an additional \$46 million in overpayments under the USF's Lifeline Program due to data on other sources of benefits not existing.

Table I. Data Types Associated with Overpayments for FY2024

Cause Categories Identified by Agencies

Data Type as a Cause of Improper Payments	Total Overpayments (in millions)^a
Contractor or provider status (e.g., contractor performance; eligible to receive federal contracts; eligible to provide medical services)	\$232,139
Medical status (e.g., diagnostic proof) ^b	\$81,717
Financial (e.g., total value of assets; credit history; amount of debt; net worth; tax exemption status)	\$80,235
Employment (e.g., whether the recipient or beneficiary is able to work, available to work, actively seeking work, employed, separated from employment, or registered for employment services) ^c	\$68,886
Residency (e.g., living arrangement; state residency)	\$42,413
Benefits from other sources (e.g., receiving benefits from another federal agency, state, or other source)	\$41,778
Identity (e.g., verification that a person is who they say they are)	\$31,596
Marital status (e.g., divorced; widowed)	\$11,228
Education (e.g., the length of time enrolled; location of the educational institution; accreditation status of educational institution; enrollment status)	\$8,634
Dependency (e.g., is the adoptive parent; stepparent as parent; child relationship to the recipient; dependent of a person; foster child; emancipated)	\$7,953
Citizenship (e.g., legal authorization to remain in the United States according to federal immigration laws; proof of citizenship; any criteria that supports lawful residency status)	\$3,991
Affiliation (e.g., agricultural in nature; business organization; affected by a disaster; ethnicity; employment within a particular organization; faith-based)	\$3,220
Address or location (e.g., of a structure within a specific area; temporary place of residence; place of birth)	\$2,435
Household size (e.g., family members in a household unit; total number of people occupying a housing unit)	\$2,298
Death (e.g., date of death)	\$1,509
Age (e.g., date of birth)	\$586

²³ CRS analysis of the FY2024 improper payments dataset available on [PaymentAccuracy.gov](https://www.paymentaccuracy.gov). For more information on this program, see CRS Report R47621, *The Universal Service Fund and Related FCC Broadband Programs: Overview and Considerations for Congress*, by Patricia Moloney Figliola.

Data Type as a Cause of Improper Payments	Total Overpayments (in millions) ^a
Military status (e.g., military discharge status; military service status; service connection)	\$571
Incarceration status (e.g., is in a jail or prison)	\$326

Source: Information on data types, including examples, is from OMB, *Circular A-123 Appendix C*. Overpayments information is from CRS analysis of FY2024 improper payments dataset available on PaymentAccuracy.gov, <https://www.paymentaccuracy.gov/>.

Notes: Agencies may receive more information on data types from OMB during OMB's annual data call for PaymentAccuracy.gov. All agencies are instructed to provide OMB with data related to the agency's identification of overpayments as part of the annual data call.

- a. The "Total Overpayments" column does not sum to the total amount of overpayments caused by a data access issue, as reported in **Figure 2**, as some agencies did not provide any information on the data types that are associated with the agency's overpayments for the fiscal year. The agencies that reported data access issues as reasons for overpayments, but did not report data types, include the Administration for Children and Families for two programs (Child Care and Development Fund and Head Start Disaster Recovery) and the Centers for Medicare and Medicaid Services for several programs (Children's Health Insurance Program [CHIP], Medicaid, Medicare Advantage Part C, Medicare Fee-for-Service, and Medicare Prescription Drug Benefit [Part D]).
- b. OMB Circular A-123, Appendix C, does not include medical status as a data-related cause category type, but the category is included in the improper payments dataset on PaymentAccuracy.gov. In discussing root causes in Circular A-123, Appendix C, OMB provides a medical-related example for improper payments caused by situations in which there is no database or dataset known to exist.
- c. An example from SSA illustrates some of the complexities involved in understanding the cause of improper payments by a particular data type. In SSA's FY2024 reporting on PaymentAccuracy.gov, SSA states that it relies, in part, on self-reported wages to determine whether a Supplemental Security Income (SSI) program applicant or recipient has earned income below a certain threshold to meet the program's employment eligibility criteria. SSA also reports using data from the Administration for Children and Families (i.e., data from the National Directory of New Hires) and the Internal Revenue Service for this purpose. Whereas some agencies may categorize income data as being a type of financial data, in this case, with the SSA, income data are necessary for the agency's employment-related data needs.

Multiple Access Issues

In practice, multiple data-related access issues could be attributable to improper payments within an agency. For example, an agency can face multiple issues accessing one specific type of data needed. In FY2021, the U.S. Department of Agriculture (USDA) reported \$153 million in total overpayments for the Federal Crop Insurance Program that were due to a combination of (1) failing to access and (2) being unable to access existing affiliation-related data (\$43 million and \$110 million, respectively).²⁴

Equally, an agency may face issues accessing multiple types of data. For example, the Department of Veterans Affairs (VA) reported \$481 million in total overpayments in its pension program for FY2022, of which \$466 million was reportedly due to a failure to access data and another \$15 million due to the inability to access data. The agency's total overpayments in this case are caused by these two data access issues and also associated with accessing multiple types of data, including (1) death data, (2) data on dependents, (3) financial data, (4) military status data, and (5) incarceration status data.

²⁴ CRS analysis of the FY2024 improper payments dataset available on PaymentAccuracy.gov. For more information on this program, see CRS In Focus IF12201, *Farm Bill Primer: Federal Crop Insurance Program*, by Stephanie Rosch.

Causes of improper payments, including overpayments, can also vary from year to year. Certain data access issues and data types that were reported by an agency one fiscal year might not be reported by it in the next year's reporting.

Using Data to Prevent Improper Payments: History and Context for the Do Not Pay System

That data access issues might be a cause of improper payments follows from decades of legislative and executive activities that have been concerned with increasing the use of data in detecting and preventing improper payments. These historical efforts were part of the lead up to the enactment of the PIIA. As discussed more fully below, the PIIA codified the requirement that executive branch agencies use the DNP system to verify payment eligibility before issuing any payment and established a presumption of access to the databases contained within the system.

The PIIA appears to offer at least a partial policy solution to improper payments that are caused by a failure to access existing data, particularly those data that are presumed to be relevant to preventing improper payments or that are caused by an inability to access existing data because the PIIA establishes a presumption of access. Use of the DNP system by agencies largely relies on data matching, and some of the history surrounding the use of data matching in identifying improper payments is also discussed below.

Data Matching to Detect Improper Payments

In 1986, the Office of Technology Assessment (OTA) published a report that discussed the use of *data matching* to detect fraud, waste, abuse, and improper payments in federal programs at the time.²⁵ Data matching—sometimes also referred to as computer matching—involves comparing data from one file or database with data from another database as a way of verifying the accuracy of the data (e.g., ensuring that the name associated with an SSN used on a federal form is the same as the Social Security Administration (SSA) has recorded it). For example, OTA stated that,

[i]n general, matching is used to detect unreported income, unreported assets, duplicate benefits, incorrect [SSNs], overpayments, ineligible recipients, incongruous entitlements ([Supplemental Security Income] checks mailed to deceased individuals, mothers claiming more children than exist), present addresses of individuals (Parent Locator Service, Student Loan defaulters), and providers billing twice for the same service.²⁶

GAO had previously testified at a Senate hearing in 1982 that data matching was “a relatively low cost method of identifying and reducing erroneous payments.”²⁷ OTA's report, which was written at the request of certain Senate and House committees, was prompted by the increasing availability of information technologies to the federal government, including computerized databases and the ability to share data at a new scale, and the implications of those developments, including possible gains in operational efficiency.²⁸ Data matching became more accessible

²⁵ OTA, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, June 1986, https://digital.library.unt.edu/ark:/67531/metadc97397/m2/1/high_res_d/1001676451.pdf.

²⁶ OTA, *Federal Government Information Technology*, p. 39.

²⁷ Statement of Acting Director General Accounting Office Wilbur D. Campbell in U.S. Congress, Senate Committee on Governmental Affairs Subcommittee on Oversight of Government Management, *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs*, hearings, 97th Cong., 2nd sess., December 16, 1982, p. 176.

²⁸ OTA, *Federal Government Information Technology*, p. iii.

because of this evolution in the federal technology landscape and could replace manual processes for comparing information.

The OTA report provided agency examples of data matching, describing actions taken under the Administrations of Presidents Jimmy Carter and Ronald Reagan to use data matching, and presenting various federal laws that authorized data matching in particular scenarios, including for verifying payment eligibility under certain federal programs.²⁹ OTA's report, however, indicated that efforts to use data matching to prevent fraud, waste, abuse, and improper payments were generally performed in isolation across the federal government, such as by safety net benefit programs or by inspectors general.³⁰

The OTA report also discussed the extent to which the Privacy Act of 1974—which provides a government-wide framework for the disclosure and sharing of data that agencies maintain on individuals—contemplated data matching by agencies and whether agencies that used data matching to detect fraud, waste, and abuse were complying with the Privacy Act when disclosing and accessing data for such matching.³¹ Following the publication of the OTA report and other legislative activities, including hearings, Congress would subsequently pass the Computer Matching and Privacy Protection Act of 1988 (CMPPA), which amended the Privacy Act to regulate data matching that is conducted by executive branch agencies to (1) verify the eligibility of recipients for payments made under federal benefit programs and (2) to recover payments made under such programs.³² The role of the Privacy Act, including the CMPPA, in DNP system operations is discussed later in this report.³³

The “Do Not Pay List”: Origins of the Do Not Pay System

A number of legislative and executive branch actions in the early 2000s continued to bring attention to the use of data matching to prevent improper payments. Following from the Federal Improper Payments Information Act of 2002,³⁴ the 2009 executive order (E.O.) titled “Reducing Improper Payments” (E.O. 13520),³⁵ and the 2010 presidential memorandum titled “Finding and Recapturing Improper Payments,”³⁶ President Barack Obama directed executive branch agencies to enhance payment accuracy through the use of the “Do Not Pay List.”³⁷

The “Do Not Pay List” was intended to operate as a network of certain federal databases “with relevant information on eligibility” that were to be “[thoroughly] reviewed” before the release of federal funds:

²⁹ OTA, *Federal Government Information Technology*, pp. 37-63.

³⁰ OTA, *Federal Government Information Technology*, pp. 43-46.

³¹ OTA, *Federal Government Information Technology*, pp. 37-38. The Privacy Act of 1974 (P.L. 93-579), as amended, is codified at 5 U.S.C. §552a.

³² P.L. 100-503; 5 U.S.C. §552a(a)(8)(A)(i).

³³ See the section titled, “Compliance with the Privacy Act.”

³⁴ P.L. 107-300.

³⁵ Executive Order 13520 of November 20, 2009, “Reducing Improper Payments,” 74 *Federal Register* 62201, November 25, 2009, <https://www.federalregister.gov/documents/2009/11/25/E9-28493/reducing-improper-payments>.

³⁶ White House, “Finding and Recapturing Improper Payments,” presidential memorandum of March 10, 2010, 75 *Federal Register* 12119, March 15, 2010, <https://www.federalregister.gov/documents/2010/03/15/2010-5685/finding-and-recapturing-improper-payments>.

³⁷ White House, “Enhancing Payment Accuracy Through a ‘Do Not Pay List,’” presidential memorandum of June 18, 2010, 75 *Federal Register* 35953, June 23, 2010, <https://www.federalregister.gov/documents/2010/06/23/2010-15412/enhancing-payment-accuracy-through-a-do-not-pay-list>.

In those cases where data available to agencies clearly shows that a potential recipient of a Federal payment is ineligible for it, subsequent payment to that recipient is unacceptable. We must ensure that such payments are not made.

Agencies maintain many databases containing information on a recipient's eligibility to receive Federal benefits payments or Federal awards, such as grants and contracts. By checking these databases before making payments or awards, agencies can identify ineligible recipients and prevent certain improper payments from being made in the first place.³⁸

Subsequent to the presidential memorandum on the Do Not Pay List, OMB published a memorandum on some of the benefits of data sharing between federal agencies, including the role of data sharing in supporting the implementation of the Do Not Pay List.³⁹ In separate reporting, OMB claimed that use of the Do Not Pay List would help agencies realize administrative gains and minimize the risk of disbursing federal funds to ineligible recipients of federal awards or payments.⁴⁰ OMB made additional claims about the potential benefits of automating data matching between an agency's intended payment recipients and data from the network of databases established under the presidential memorandum, suggesting that such automation could decrease the time to verify eligibility for a payment by 50%.⁴¹

In its FY2012 budget request, the Treasury Department sought \$10 million to “[e]xpand the Do Not Pay Portal and increase analytical capabilities to detect fraud patterns and reduce improper payments,” noting that the department would assume maintenance of VerifyPayment.gov to serve as a “one-stop-shop” to support the operations of the Do Not Pay List.⁴² The Consolidated Appropriations Act, 2012, authorized the amount requested to reduce improper payments.⁴³

Improper Payments Elimination and Recovery Improvement Act of 2012

The Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA 2012) established the statutory authority for the operations of the DNP system, as this report uses the term.⁴⁴ The act codified the requirement that agencies review, at a minimum, the databases that had been specified in President Obama's 2010 presidential memorandum and permitted the OMB Director to designate other databases for agencies to review prior to disbursing any federal payment.⁴⁵ IPERIA 2012 referred to the collective use of these databases as the “Do Not Pay

³⁸ White House, “Enhancing Payment Accuracy Through a ‘Do Not Pay List,’” p. 1.

³⁹ Memorandum from Jeffrey D. Zients, Deputy Director for Management, and Cass R. Sunstein, Administrator of the Office of Information and Regulatory Affairs, OMB, to heads of executive departments and agencies, “Sharing Data While Protecting Privacy,” November 3, 2010, p. 2, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2011/m11-02.pdf.

⁴⁰ OMB, *Report to Congress on the Benefits of the President's E-Government Initiatives Fiscal Year 2011*, p. 34, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/assets/egov_docs/FY11_EGov_Benefits_Report.pdf.

⁴¹ OMB, *Report to Congress on the Benefits of the President's E-Government Initiatives Fiscal Year 2012*, p. 42, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/assets/egov_docs/fy12_egov_benefits_report.pdf.

⁴² U.S. Department of the Treasury, *FY 2012 Congressional Justification*, pp. BPD-7-BPD-78, <https://home.treasury.gov/system/files/266/CJ-FY2012-Complete-508.pdf#page=244>. See also page 6 of the Departmental Summary (<https://home.treasury.gov/system/files/266/CJ-FY2012-Complete-508.pdf#page=7>).

⁴³ P.L. 112-74 Division C Title I (125 Stat. 886).

⁴⁴ P.L. 112-248 §5 (126 Stat. 2392).

⁴⁵ P.L. 112-248 §5(a-b).

Initiative” (DNPI).⁴⁶ Furthermore, the act established a presumption of access to these DNPI databases by agencies for the purposes of identifying and preventing improper payments.⁴⁷

IPERIA 2012 did not refer to the Do Not Pay List or to any name that had been used by OMB or the Treasury Department following implementation of President Obama’s 2010 presidential memorandum. Instead, IPERIA 2012 authorized the establishment of an “initial working system” for the prepayment and pre-award review of the DNPI databases and for the investigation of “fraud and systemic improper payments detections through analytic technologies and other techniques, which may include commercial database use or access.”⁴⁸

In an August 2013 memorandum implementing the IPERIA 2012 provisions for using the DNPI databases in prepayment procedures, OMB referred to the “Treasury’s Working System” as meaning the “functions performed by the Department of the Treasury that are authorized by section 5 of [IPERIA 2012].”⁴⁹ (See **text box** for a list of the various names used for the DNP system over time.)

Identifying the Do Not Pay System by Name Over Time

The Do Not Pay (DNP) system—as this report uses the term—has been identified by different names over time, beginning with the “Do Not Pay List” in a 2010 presidential memorandum.⁵⁰ These different names are used in various documents that have been submitted to Congress, including in budget requests from the Department of the Treasury and in reports from the Office of Management and Budget (OMB) that were mandated by the E-Government Act of 2002 (P.L. 107-347). Executive branch agencies may also refer to their use of the DNP system by these different names in various reports they are mandated to produce, including their annual financial reporting.⁵¹ These names include, but are not necessarily limited to, the following (in alphabetical order):

- Do Not Pay
- Do Not Pay Business Center
- Do Not Pay Initiative
- Do Not Pay List
- Do Not Pay Portal or Do Not Pay Online Portal
- Do Not Pay System
- Do Not Pay Working System
- GOVerify Business Center
- Treasury’s Working System
- verifypayment.gov

Executive Order 14249, issued in March 2025 by President Trump, refers to the DNP system as the “Do Not Pay Working System.” An August 2025 memorandum from OMB with guidance on implementation of the executive order states, “For purposes of this guidance, the Do Not Pay Working System is the same as the Initial Working System identified in 31 U.S.C. § 3354(c). It includes Treasury’s system of records for Do Not Pay.”⁵²

⁴⁶ P.L. 112-248 §5(b)(1).

⁴⁷ P.L. 112-248 §5(b)(3).

⁴⁸ P.L. 112-248 §5(d).

⁴⁹ Memorandum from Sylvia M. Burwell, Director, OMB, to heads of executive departments and agencies, “Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative, August 16, 2013, p. 6, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2013/m-13-20.pdf.

⁵⁰ White House, “Enhancing Payment Accuracy Through a ‘Do Not Pay List.’”

⁵¹ For example, see reporting requirements described in OMB, *Transmittal of Appendix C*, M-21-19, p. 56.

⁵² OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, August 20, 2025, p. 1 (footnote 2), <https://www.whitehouse.gov/wp-content/uploads/2025/08/M-25-32-Preventing-Improper-Payments-and-Protecting-Privacy-Through-Do-Not-Pay.pdf>.

In the lead up to consideration of IPERIA 2012, a Senate Committee received testimony from the head of the Office of Federal Financial Management (OFFM) within OMB on implementation of the Do Not Pay List, including the role of data access in reducing improper payments:

During the course of this work, we are discovering that increasing agency access to relevant data sources as well as driving efficiencies in the current process for inter-agency data sharing may improve improper payment outcomes.⁵³

At the same hearing, the committee also heard from the Treasury Department on the perceived advantages of data access for not only reducing improper payments but as an alternative to other approaches to managing improper payments:

If agencies have access to accurate and timely data on death, employment status, income levels, incarceration and residents of dependent children as well as information on whether or not applicants are already receiving benefits and whether applicants are suspended or disbarred from doing business with the Federal Government, the number of improper or erroneous payments could be drastically reduced.

Rather than trying to reduce improper payments using only an expensive, and in many cases unsuccessful, pay-and-chase fund recovery model, we will work with agencies to help validate payment data before the payments are made. Our goal is to get accurate data in the hand of agencies early in the decisionmaking process for payment and also prior to making contract awards.⁵⁴

The Payment Integrity Information Act of 2019

IPERIA 2012 was repealed by the PIIA in March 2020.⁵⁵ However, the PIIA preserved some aspects of IPERIA 2012, including the requirement in IPERIA 2012 that agencies review DNPI databases to verify payment eligibility prior to the disbursement or awarding of federal funds, and it maintained the authority of the OMB Director to designate additional databases for such review.⁵⁶ Under the PIIA, as it was with IPERIA 2012, use of these databases continues to be identified as the DNPI.⁵⁷ These databases are discussed in greater detail in a later section of the report (see “Accessible Databases”).⁵⁸

The PIIA also directed the working system established under IPERIA 2012 to continue to be in operation and required that each executive branch agency review all of the agency’s payments and awards through that system.⁵⁹

The PIIA does not specifically authorize the Treasury Department to operate the DNP system. Instead, the Treasury Department’s role is based on OMB’s decisionmaking, first to support the

⁵³ Prepared testimony of OMB Controller Daniel I. Werfel in U.S. Congress, Senate Committee on Homeland Security and Government Affairs Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, *Assessing Efforts to Eliminate Improper Payments*, 112th Cong., 1st sess., May 11, 2011, p. 48, <https://www.govinfo.gov/content/pkg/CHRG-112shrg67640/pdf/CHRG-112shrg67640.pdf>.

⁵⁴ Statement of Department of Treasury Assistant Fiscal Secretary Richard Gregg in U.S. Congress, Senate Committee on Homeland Security and Government Affairs Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, *Assessing Efforts to Eliminate Improper Payments*, 112th Cong., 1st sess., May 11, 2011, p. 9, <https://www.govinfo.gov/content/pkg/CHRG-112shrg67640/pdf/CHRG-112shrg67640.pdf>.

⁵⁵ IPERIA is repealed in P.L. 116-117 §3(a)(3) (134 Stat. 133).

⁵⁶ 31 U.S.C. §3354(b)(1).

⁵⁷ 31 U.S.C. §3354(b)(1).

⁵⁸ More information on these databases is also contained in **Table A-1**.

⁵⁹ 31 U.S.C. §3354(c).

implementation of a Do Not Pay List under the 2010 presidential memorandum and then to implement the initial working system provisions of IPERIA 2012.⁶⁰ IPERIA 2012 specified only that the system “may be located within an appropriate agency.”⁶¹ The PIIA refers to “the head of the agency operating the Working System” for authorities that are then exercised in practice by the Treasury Department given its role in operating the DNP system.⁶²

Overview of Do Not Pay System Operations

The DNP system is operated by the Bureau of the Fiscal Service (the Fiscal Service), a statutory component within the Treasury Department.⁶³ Within the Fiscal Service, the management of the DNP system is located within the Office of Payment Integrity (OPI).⁶⁴ Funding and costs to operate it are discussed below (see “Funding Sources and Costs to Operate”).

As the PIIA mandates the review of all payments by executive branch agencies through the DNP system, users of the DNP system include payment-making agencies, agencies that provide financial management services (e.g., payment services) to multiple agencies through the federal shared service model, as well as entities from the federal oversight community, like inspectors general.⁶⁵ The PIIA also permits access to, but does not mandate the use of, the DNPI databases by the judicial and legislative branches of the federal government.⁶⁶

Additionally, the PIIA provides access to and use of the DNPI databases to state governments that administer federally funded programs, including access by any state’s contractor, agent of the state, or auditor or program that is responsible for reducing improper payments in federally funded, state-administered programs.⁶⁷ The Treasury Department states that the PIIA gives “DNP the authority to work directly with state agencies that manage federally funded state administered

⁶⁰ IPERIA 2012 instructed the OMB Director to “establish a working system for prepayment and preaward review that includes the Do Not Pay Initiative” (i.e., the DNPI databases) (see §5(d); 126 Stat. 2394).

⁶¹ P.L. 112-248 §5(d)(2)(A).

⁶² This reference is made in 31 U.S.C. §3354(a)(3)(B)(i).

⁶³ 31 U.S.C. §306.

⁶⁴ In summer 2022, the Fiscal Service announced that it was merging two separate offices that were involved in DNP system operations—the Do Not Pay Business Center and the Payment Integrity Center of Excellence—into a single Office of Payment Integrity (OPI). In summer 2025, some electronic material and documentation from the Fiscal Service that contains information on DNP system operations suggests that the DNP system is part of the Treasury Department’s “Fraud Prevention and Financial Integrity (FPFI) Office.” As of December 2025, there is a Treasury Department website for an Office of Payment Integrity with which the DNP system is associated (<https://paymentintegrity.treasury.gov/paymentintegrity/about/>).

⁶⁵ As to users from the oversight community, see as an example a discussion from the Pandemic Response Accountability Committee (PRAC), which is part of the Council of the Inspectors General on Integrity and Efficiency (CIGIE), on their use of data from the DNP system to identify certain Small Business Administration (SBA) loans that were applied for using questionable SSNs (<https://pandemicoversight.gov/media/file/do-not-pay-fraud-report-follow-5-11-2023pdf>). Examples of federal shared service providers (FSSPs) in financial management include the Administrative Resource Center (located within the Treasury Department) and the Interior Business Center (located within the Department of the Interior). Additionally, shared service providers in grants management may also process payments, such as the Payment Management System (located within the Department of Health and Human Services). The shared service model is described in OMB Memorandum 19-16, which also establishes operational processes for the model (see <https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-16.pdf>).

⁶⁶ 31 U.S.C. §3354(b)(3)(C).

⁶⁷ 31 U.S.C. §3354(b)(3)(C).

programs such as, but not limited to: Medicaid, Supplemental Nutrition Assistance Program (SNAP), and Unemployment Insurance.”⁶⁸

Assumptions Behind the Operations of the Do Not Pay System and the Role of Data Matching

Use of the DNP system by a paying agency largely relies on data matching to enable comparisons of information, usually by using an identifier as the basis for a match (e.g., a person’s name or their SSN). The assumption behind use of the DNP system is that if a paying agency matches an intended payment recipient to information in one of the system’s databases (e.g., the intended payment recipient’s name matches to a name in a DNPI database), or if there are discrepancies in the information the paying agency has compared to information in one of the DNP system’s databases (e.g., information concerning an entity’s eligibility to be awarded a federal contract or subcontract), then the transaction would be subject to additional scrutiny by the paying agency. In other words, it is assumed that a data match is indicating something to the paying agency about the intended payment recipient’s eligibility (or ineligibility) for a federal award or payment that warrants investigation by the agency before it is issued. The concept of these operations is illustrated in **Figure 3**.

For example, one of the databases available through the DNP system is the General Service Administration’s (GSA’s) exclusion records, which identify those entities (i.e., persons or organizations) from GSA’s System for Award Management (SAM) that are ineligible to receive federal contracts and certain types of federal assistance because of debarment or suspension.⁶⁹ The presumption is that if an award or a payment is going to be issued to an entity that appears to be debarred or suspended based on a match to the exclusion records available through the DNP system, then the paying agency would further examine whether that entity is in fact eligible to receive federal funds.

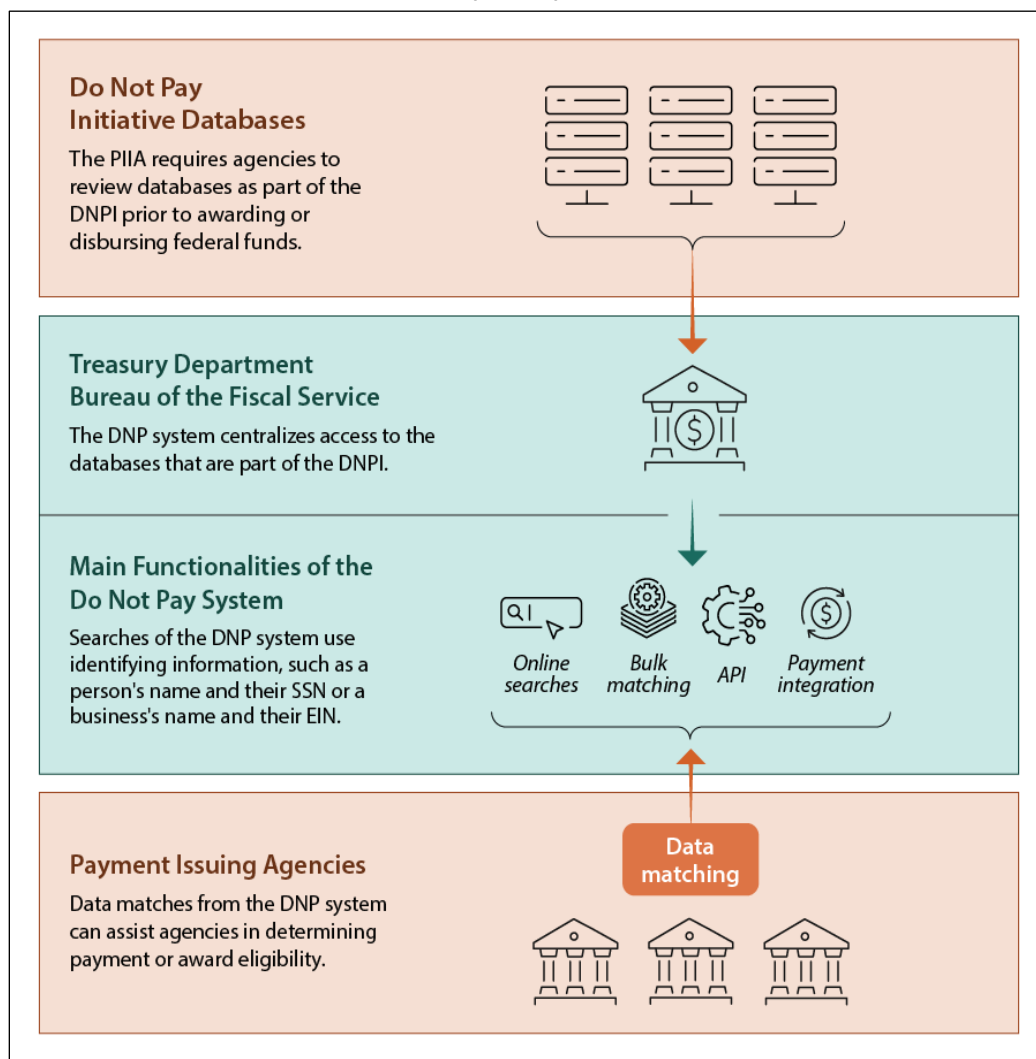
The prepayment and pre-award review of DNPI databases that occurs through the DNP system are for the purposes of determining payment eligibility and specifically to prevent improper payments before the release of any federal funds. As discussed later in this report, matches in the DNP system do not automatically stop a payment transaction from occurring, and a match does not necessarily mean an entity is ineligible to receive any payment (see “Effect of Data Matches on Payments”).

⁶⁸ Bureau of the Fiscal Service, “Fact Sheet—Do Not Pay Portal,” May 2025, <https://fiscal.treasury.gov/files/dnp/DoNotPayFactSheet.pdf>. The precise scope of federally funded, state-administered programs is not defined by the PIIA.

⁶⁹ For more information on these exclusions in the System for Award Management (SAM), see 2 C.F.R. §180 Subpart E. These exclusion records may be known by their former name, the Excluded Parties List System, as noted in 31 U.S.C. §3354(a)(2)(B).

Figure 3. Do Not Pay Initiative Databases and the Do Not Pay System

Concept of Operations



Source: CRS.

Accessible Databases

The PIIA instructs agencies to review, at a minimum, certain databases to determine payment eligibility. The six named databases are⁷⁰

- the death records maintained by the Commissioner of Social Security;⁷¹
- information regarding incarcerated individuals maintained by the Commissioner of Social Security under Sections 202(x) and 1611(e) of the Social Security Act;⁷²

⁷⁰ 31 U.S.C. §3354(b)(1)(A).

⁷¹ For more information and background on these records, see CRS Report R46640, *The Social Security Administration's Death Data: In Brief*, by Paul S. Davies.

⁷² Codified at 42 U.S.C. §402(x) and 42 U.S.C. §1382(e), respectively. In practice, this information is part of the Social (continued...)

- the System for Award Management (SAM) exclusion records maintained by the General Services Administration (GSA);
- the Debt Check Database of the Department of the Treasury, which is associated with the Treasury Offset Program (TOP);
- the Credit Alert System (also referred to as the Credit Alert Interactive Voice Response System [CAIVRS]) of the Department of Housing and Urban Development (HUD); and
- the list of excluded individuals and entities from the Office of Inspector General (IG) of the Department of Health and Human Services (HHS).

Additionally, the PIIA authorizes the OMB Director to designate other databases as part of the DNPI, with consideration to be given to “any database that substantially assists in preventing improper payments.” When making such designations, the director is first to provide public notice and an opportunity for comment.⁷³ Because the PIIA effectively continued “the working system” established under IPERIA 2012, and IPERIA 2012 also permitted database designations by the OMB Director, some DNPI database designations predate the PIIA.⁷⁴

In a 2013 memorandum, OMB stated that it would consider when making such designations

- statutory or other limitations on the use and sharing of specific data;
- privacy restrictions and risks associated with specific data;
- the likelihood that the data will strengthen program integrity across programs and agencies;
- the benefits of streamlining access to the data through the central DNPI;
- the costs associated with expanding or centralizing access to data, including modifications needed to system interfaces or other capabilities in order to make data accessible; and, as appropriate,
- other policy and stakeholder considerations.⁷⁵

The use of other data is also named in the PIIA as being pertinent to preventing improper payments, but the PIIA does not necessarily deem these data as DNPI databases. This includes information on the death of individuals from the Department of Defense (DOD), the Department of State (DOS), the Department of Veterans Affairs (VA), and the Office of Personnel Management (OPM).⁷⁶

The PIIA directs DOD and DOS to “promptly and on a regular basis” make such death information available to each agency that the OMB Director determines has a need for receiving

Security Administration’s (SSA’s) Prisoner Update Processing System (PUPS). For more information on what information SSA maintains as it relates to incarceration, see SSA, Program Operations Manual System (POMS) “GN 02607.890 Requests for Prisoner Record Changes, Updates, or Deletions to the Prisoner Update Processing Systems (PUPS),” February 28, 2024, <https://secure.ssa.gov/poms.Nsf/Lnx/0202607890>.

⁷³ 31 U.S.C. §3354(b)(2)(B).

⁷⁴ See §5(b)(2) (126 Stat. 2393).

⁷⁵ OMB, *Protecting Privacy While Reducing Improper Payments with the Do Not Pay Initiative*, memorandum to the heads of executive departments and agencies, M-13-20, August 16, 2013, p. 8, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2013/m-13-20.pdf.

⁷⁶ 31 U.S.C. §3356(a), referencing section 7(a) of IPERIA (), which was added by §3(2) (129 Stat. 2226).

and using such information.⁷⁷ These data from DOD and DOS are, in turn, listed as among the databases accessible through the DNP system.⁷⁸

In contrast, the PIIA instructs the VA Secretary and OPM Director “to facilitate the centralized access of death data for the use of reducing improper payments” and permits them to “identify additional Federal sources of death data and direct the data owner to provide that data to [one] or more executive agencies for that purpose.”⁷⁹ These data from OPM and the VA are not listed among the databases accessible through the DNP system.

Table A-1 (in the **Appendix**) provides details on the databases that are available through the DNP system, including whether such databases are required by statute or have been designated by the OMB Director. Additionally, **Table A-1** includes those databases that are designated by the OMB Director as part of the DNPI according to *Federal Register* notices, but that do not appear in a list from the Fiscal Service on what is accessible through the DNP system.⁸⁰ It is unclear if agencies access these particular databases that are part of the DNPI using other methods or if there are plans to eventually integrate these databases into the DNP system to centralize access to them.

Services to Agencies

The DNP system provides paying agencies with services that are intended to prevent improper payments. These services include (1) a searchable portal, where agencies can query the various DNPI databases that make up the DNP system, and (2) data analytics, where an agency can provide its payment data to the Fiscal Service for analysis (hereinafter referred to as data analytics services [DAS]). These DAS projects largely rely upon analyses using data from DNPI databases.

Portal

The DNP system’s portal enables agencies to search the DNP system’s constituent databases. An agency can conduct this search using one or more of the portal’s functionalities, including one-time searches and automated matching. The functionality determines when any matching information is available to an agency (e.g., real time, next business day). These functionalities include the following:

- **Online search**, where an agency can enter an intended payment recipient’s identifying information into a user interface to see if there is a match against any of those DNP system databases for which the agency is approved to access. These searches are generally conducted pre-award or prepayment and matches are available immediately.⁸¹
- **Bulk matching**, where the agency electronically sends one or more payment files that include information on intended payment recipients for a particular time frame (e.g., all payments that are scheduled to be disbursed in a month for a certain program) to be matched against approved DNP system databases. Bulk

⁷⁷ 31 U.S.C. §3356(a).

⁷⁸ Bureau of the Fiscal Service, “What Can I Search?” July 14, 2025, <https://fiscal.treasury.gov/dnp/search.html>.

⁷⁹ 31 U.S.C. §3356(b)(2).

⁸⁰ Bureau of the Fiscal Service, “What Can I Search,” <https://fiscal.treasury.gov/dnp/search.html>. Databases listed on this website As of July 14, 2025

⁸¹ Bureau of the Fiscal Service, “Do Not Pay Portal Initial Questions Guide,” July 2025, p. 15, <https://fiscal.treasury.gov/files/dnp/dnp-initial-questions-form.pdf>.

matching is generally conducted prepayment or pre-award.⁸² The timing of the bulk matching process is sensitive to the internal processes of the paying agency. With bulk matching, any matches are available to the agency the next day, and an agency's prepayment process may, for example, be weeks long. Thus, a payment could be disbursed weeks after the bulk matching results were reviewed by the agency. Results from batch matching may be more useful to an agency at a certain point of time—for example, at the time of payment—given the total length of time an agency takes to process a payment.⁸³

- **Continuous monitoring**, where the agency electronically sends a file on some cadence (e.g., biweekly) with information on recipients of recurring types of payments (e.g., all vendors that are scheduled to receive a payment on a monthly basis) to be matched against approved databases. Matches from this file are available to an agency in either of two scenarios: when information in the file changes (e.g., because a new vendor has been added to the agency file that is then matched to a DNP system database), or when there has been a change within one of the approved DNP system databases (e.g., a match is found when one was not previously made).⁸⁴
- **Application Programming Interface (API)**, where an agency searches those DNP system databases for which it has approval by querying an API, which may integrate results from the portal's search function within an agency's internal processes.⁸⁵ Matches could be available to an agency in real time upon a query of the API, but availability could also depend on how the data from the query is integrated into the agency's related workflows and processes.

To gain access to the portal, an agency initiates what the Fiscal Service calls an “onboarding process.”⁸⁶ This process is depicted in **Figure 4**. The Fiscal Service notes that the time frame for moving through the onboarding process is “contingent on several factors, including agency involvement and responsiveness, [the Fiscal Service's] legal review, availability and capacity of agency development resources, and internal onboarding and development workloads.”⁸⁷

⁸² Bureau of the Fiscal Service, “Do Not Pay Portal Batch Matching and Continuous Monitoring Implementation Guide,” June 2025, p. 5, <https://fiscal.treasury.gov/files/dnp/batch-common-implementation-guide.pdf>.

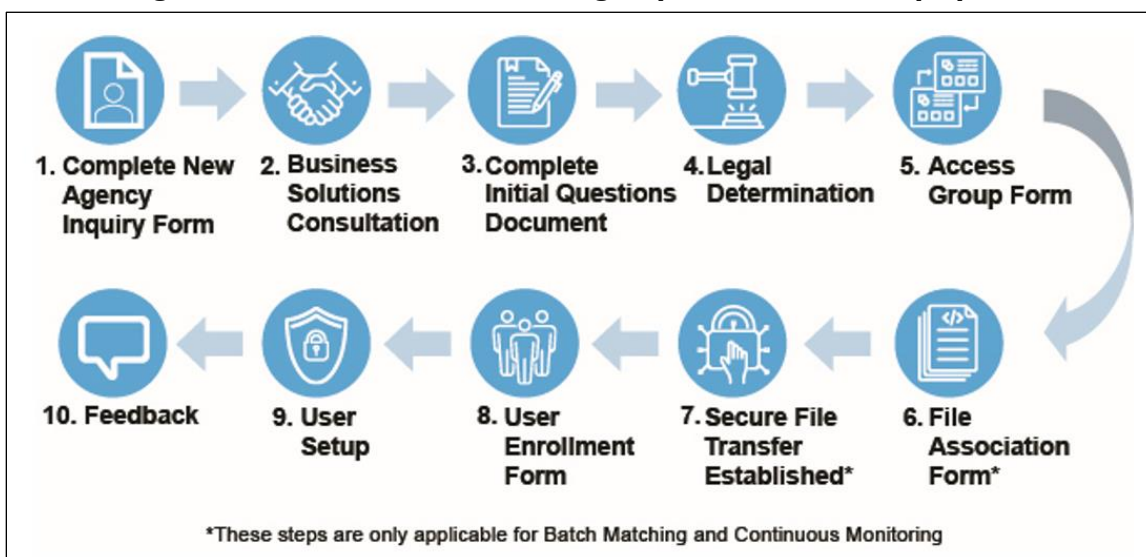
⁸³ Bureau of the Fiscal Service, “Do Not Pay Portal Batch Matching,” p. 7.

⁸⁴ Bureau of the Fiscal Service, “Do Not Pay Portal Batch Matching,” pp. 4-5.

⁸⁵ Bureau of the Fiscal Service, “Using the Do Not Pay Portal,” <https://fiscal.treasury.gov/dnp/using-the-dnp-portal.html>.

⁸⁶ See Bureau of the Fiscal Service, “Do Not Pay Portal Onboarding Guide,” June 2025, <https://fiscal.treasury.gov/files/dnp/onboarding-guide.pdf>.

⁸⁷ Bureau of the Fiscal Service, “Do Not Pay Portal Onboarding Guide,” p. 4.

Figure 4. Process to Onboard an Agency to the Do Not Pay System

Source: Bureau of the Fiscal Service, “Interested in Onboarding to the DNP Portal,” <https://fiscal.treasury.gov/dnp/getting-started.html>.

As part of the onboarding process to gain access to the DNP portal, an agency identifies which DNP system databases it is interested in using.⁸⁸ This suggests that access to all databases may not be necessary for an agency or a program (e.g., the data are irrelevant for payment eligibility determinations) or that access may not be permitted in some cases. For example, for certain databases, agencies must identify whether their use aligns with certain specified purposes. Before permission is granted, the Fiscal Service conducts a legal review that includes the paying agency’s stated basis for accessing specific databases for the specific portal functionalities that were described above.⁸⁹

Data Analytics Services

DNP system operations include providing agencies with data analytic services (DAS). DAS are tied to the DNP system’s legislative history, where IPERIA 2012 described “the working system” as including “investigation activities for fraud and systemic improper payments detection through analytic technologies and other techniques, which may include commercial database use or access.”⁹⁰ The Fiscal Service began offering these services in 2014.⁹¹

DAS projects can include assessments of a paying agency’s data quality and business processes, as well as projects that produce various types of payment risk and confidence scoring, including, for example, identifying payments most at risk of being disbursed to deceased recipients.⁹²

⁸⁸ For more information, see Bureau of the Fiscal Service, “Do Not Pay Portal Initial Questions Guide,” pp. 9-14.

⁸⁹ Bureau of the Fiscal Service, “Do Not Pay Portal Onboarding Guide,” p. 10.

⁹⁰ §5(d)(2)(c) (126 Stat. 2394).

⁹¹ Treasury Department Office of Inspector General, *Performance Metric Policy Needed for the Fiscal Service Do Not Pay Business Center’s Data Analytics Services*, OIG-20-025, January 28, 2020, p. 7, <https://www.govinfo.gov/content/pkg/GOVPUB-T72-PURL-gpo173147/pdf/GOVPUB-T72-PURL-gpo173147.pdf>.

⁹² For example, see Bureau of the Fiscal Service, “Death Record Confidence Scoring Tool,” July 31, 2025, <https://fiscal.treasury.gov/files/dnp/dnp-drc-scoring-tool-guide.pdf>.

The Fiscal Service also conducts analyses of what it calls “cross-government data.” These analyses reuse data the Fiscal Service has collected through its government-wide role in the federal payment process to identify payments that might be at risk of being improper.⁹³ For example, because the Treasury Department, through the Fiscal Service, disburses the majority of agencies’ payments and does so using electronic transfers of funds (ETFs; e.g., direct deposits) through the automated clearinghouse (ACH) network, the Fiscal Service has data related to payment processing from financial institutions (e.g., banks). Information that may be received from a financial institution can include when an account holder at the institution is deceased, particularly in cases involving recurring federal payments made under entitlement programs and annuities pursuant to federal regulations governing the federal government’s participation in the ACH.⁹⁴ In turn, the Fiscal Service can use this data in analyses to identify payments made across all federal agencies and programs where a recipient has been identified as deceased by a financial institution.⁹⁵ According to the Fiscal Service, it is also able to identify through cross-government data analyses those individuals who receive payments from more than one federal program.⁹⁶

The Fiscal Service works with an agency to develop a specific DAS project and establishes specific roles and responsibilities for it and the agency.⁹⁷ The process these projects are expected to follow and the distribution of responsibilities between the Fiscal Service and paying agencies is illustrated in **Figure 5**.

⁹³ Bureau of the Fiscal Service, “Do Not Pay Analytics Services,” May 30, 2025, <https://fiscal.treasury.gov/dnp/analytics.html>.

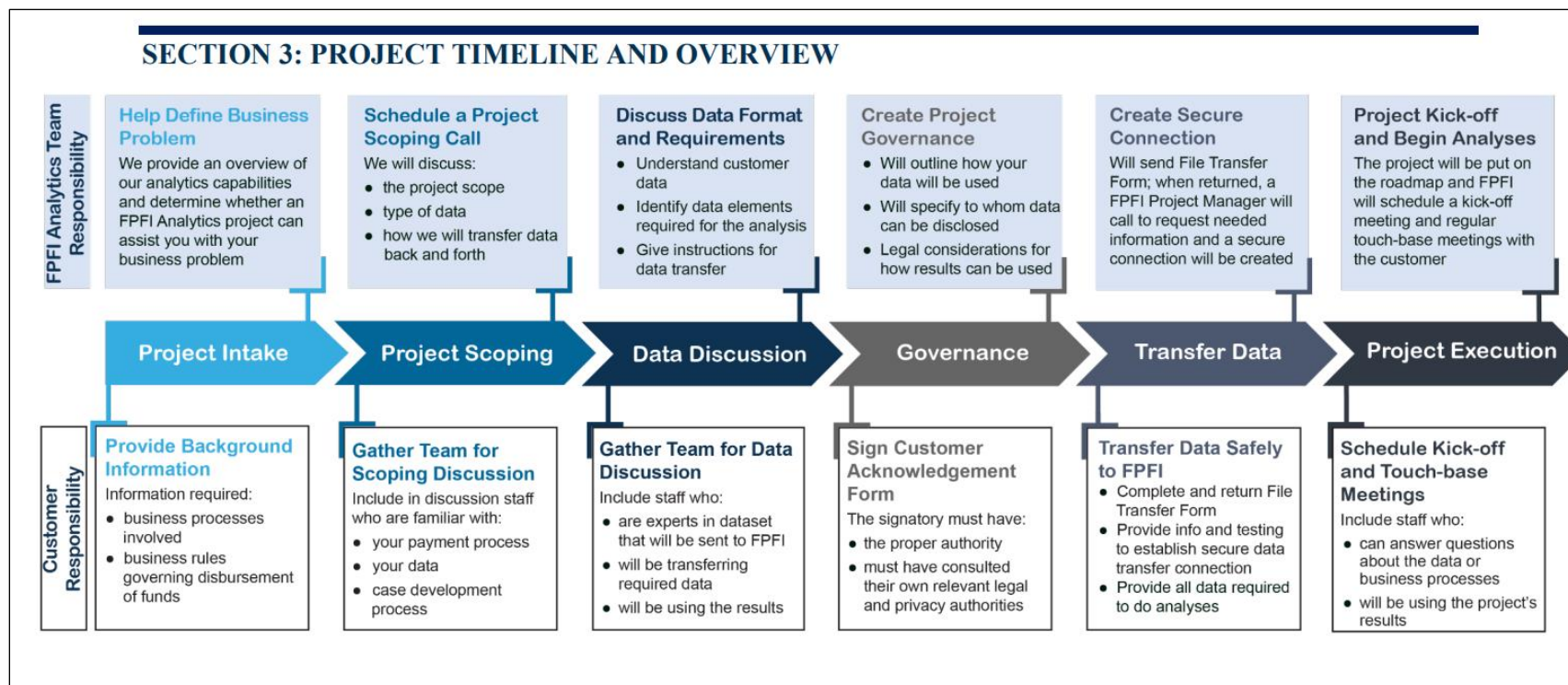
⁹⁴ 31 C.F.R. §210.10. The standard for a financial institution is actual or constructive knowledge of death, which means that it “received information, by whatever means” of the death or incapacity of a recipient or beneficiary and “has had a reasonable opportunity to act on such information or that [the financial institution] would have learned of the death or incapacity if it had followed commercially reasonable business practices” (31 C.F.R. §210.2(b)). See also Bureau of the Fiscal Service, *A Guide to Federal Government ACH Payments*, Chapter 5 (Reclamations), June 2023, pp. 5–4–5–5, <https://tfx.treasury.gov/media/60015/download?inline>.

⁹⁵ For more information, see the discussion and description provided by OMB in the *Federal Register* notice that proposes to designate the Treasury Department’s Death Notification Entries (DNE) as part of the DNPI (“Proposed Designation of Databases to the Do Not Pay Working System,”⁸⁹ *Federal Register* 18689, August 29, 2024, <https://www.federalregister.gov/documents/2024/08/29/2024-18689/proposed-designation-of-databases-to-the-do-not-pay-working-system>).

⁹⁶ Bureau of the Fiscal Service, “Do Not Pay Analytics Services,” May 30, 2025, <https://fiscal.treasury.gov/dnp/analytics.html>.

⁹⁷ For more information on the process, see Bureau of the Fiscal Service, “Do Not Pay Analytics Project Implementation Guide,” June 2025, pp. 6–13, <https://fiscal.treasury.gov/files/dnp/dnp-analytics-implementation-guide.pdf>.

Figure 5. Process to Develop Data Analytics Projects



Source: Bureau of the Fiscal Service, “Analytics Project Implementation Guide,” June 2025, p. 6, <https://fiscal.treasury.gov/files/dnp/dnp-analytics-implementation-guide.pdf>.

Funding Sources and Costs to Operate

The Fiscal Service does not use a fee-based or cost-recovery model to provide the services available through the DNP system, and it is publicized as being a “no cost resource” for federal agencies and for federally funded, state-administered programs. The Fiscal Service funds the DNP system through annual appropriations to its salaries and expenses account, further allocating such appropriations for budget activities related to payments (disbursements).⁹⁸ Additionally, as discussed below, the Fiscal Service relies on certain Federal Reserve Banks (FRBs) to support the operations of the DNP system, which is funded through a separate account.

Figure 6 illustrates the distribution of the costs to operate the DNP system by funding source for FY2012 to FY2025. A majority of the system’s operational costs are associated with FRB reimbursements, suggesting that FRBs play a large role in enabling the DNP system.

Information Technology

The DNP system is considered by the Fiscal Service as a *major information technology (IT) investment* for the purposes of the Information Technology Management Reform Act of 1996, as amended, which requires agencies to use a capital planning and investment control (CPIC) process.⁹⁹ A major IT investment is defined by OMB as one that requires special management attention for particular reasons, including because of its importance to the mission or function to the government; because of significant program or policy implications; because of its high executive visibility; or by agency definition according to the agency’s CPIC process.¹⁰⁰

As a result of the major IT investment designation, the Fiscal Service provides some detailed information about the DNP system’s operational costs, including operations and maintenance (O&M) costs (i.e., those costs for operating and maintaining the system) and development, modernization, and enhancement (DME) costs (e.g., those costs to modify the existing system to significantly improve capabilities or performance).¹⁰¹ Since 2013, the Fiscal Service has included these IT costs in what the agency calls a “summary of capital investments,” which is published annually as part of the Treasury Department’s budget request.¹⁰² This capital investments summary provides financial information for the prior, current, and forthcoming fiscal year. In addition, the Fiscal Service provides reporting on the DNP system as part of a “capital investment plan,” which includes more technical information about the system and its development relative to the cost information contained within the capital investment summary.¹⁰³

⁹⁸ In its FY2026 congressional budget justification and budget-in-brief (BIB), the Treasury Department uses the term “disbursements” whereas the budget activity had been referred to as “payments” in the budget documents for previous fiscal years. From FY2014 to FY2016, the Fiscal Service categorized the DNP system as its own budget activity and separate from budget resources for payments.

⁹⁹ 40 U.S.C. §11302.

¹⁰⁰ OMB, *Management and Oversight of Federal Information Technology*, memorandum for heads of executive departments and agencies, M-15-14, June 10, 2015, p. 18, <https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf>.

¹⁰¹ For more information on the IT budgeting process, see CRS Report R46877, *Federal Information Technology (IT) Budgeting Process in the Executive Branch: An Overview*, by Dominick A. Fiorentino.

¹⁰² These summaries can be found for FY2026 and prior years at <https://home.treasury.gov/about/budget-financial-reporting-planning-and-performance/budget-requestannual-performance-plan-and-reports/summary-of-capital-investments>.

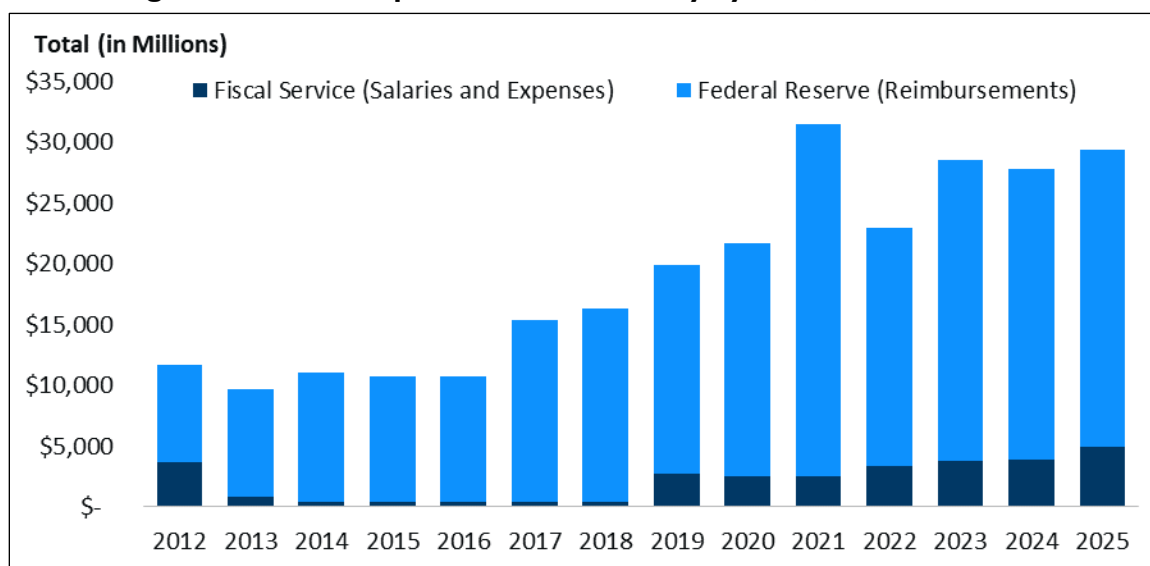
¹⁰³ A capital investment plan for FY2026 is not available as of the date of this report. For FY2026, the Treasury Department has posted only summaries of capital investments for its component agencies.

Federal Reserve Banks

Certain FRBs support the operations of the DNP system in their capacity as *fiscal agents* supporting the Treasury Department.¹⁰⁴ Since 2011, the Kansas City FRB and the St. Louis FRB have played a role in developing and operating the DNP system and enabling it to provide its intended services to federal agencies.¹⁰⁵ The Fiscal Service reimburses FRBs for the role they play as fiscal agents through an appropriations account Congress established specifically for such purpose.¹⁰⁶ The total amount of the reimbursements to FRBs for the DNP system are included in the Fiscal Service’s annual “summary of capital investments,” as mentioned above.

As part of its annual report to Congress, the Board of Governors of the Federal Reserve System may provide some reporting on the activities of FRBs that are related to the DNP system. In some years, for example, the report provides some detail on how supporting the DNP system contributes to year-to-year changes in the total expenses of FRBs to provide fiscal agent services to the Treasury Department for payment-related activities. In its calendar year 2021 report, the Federal Reserve Board stated that the DNP system was one of three payment programs that contributed to a 20% increase from the previous year in the banks’ fiscal agent expenses for payment-related services provided to the Treasury Department.¹⁰⁷

Figure 6. Costs to Operate the Do Not Pay System, FY2012-FY2025



Source: CRS analysis of Treasury Department summaries of capital investments for the Fiscal Service for FY2014 to FY2026. Summaries and capital investment plans are available at <https://home.treasury.gov/about/budget-financial-reporting-planning-and-performance/budget-requestannual-performance-plan-and-reports/summary-of-capital-investments>.

Notes: For the Fiscal Service and FRBs, costs include those categorized as operations and maintenance (O&M) and as development, modernization, and enhancement costs (DME). For the Fiscal Service, O&M and DME costs are reported as being associated with its “Salaries and Expenses” (S&E) account and include full-time equivalent

¹⁰⁴ See 12 U.S.C. §391.

¹⁰⁵ Treasury Department Office of Inspector General, *Performance Metric Policy Needed for the Fiscal Service Do Not Pay Business Center’s Data Analytics Services*, OIG-20-025, January 28, 2020, p. 27, <https://www.govinfo.gov/content/pkg/GOVPUB-T72-PURL-gpo173147/pdf/GOVPUB-T72-PURL-gpo173147.pdf>.

¹⁰⁶ 12 U.S.C. §391a.

¹⁰⁷ Board of Governors of the Federal Reserve System, *108th Annual Report of the Board of Governors of the Federal Reserve System* p. 67, <https://www.federalreserve.gov/publications/files/2021-annual-report.pdf>.

(FTE) and non-FTE costs. For FRBs, the Fiscal Service reports costs as being associated with the “Federal Reserve Bank Reimbursement Fund” and no further breakdown is provided. FY2025 data are based on estimated obligations reported by the Treasury Department in its FY2026 summary of capital investments; for all other fiscal years, data are reported actuals or estimated actuals.

Compliance with the Privacy Act

The Privacy Act of 1974 governs how agencies may disclose data, information, or other types of *records* about an individual.¹⁰⁸ The Privacy Act generally bars an agency from sharing records that are contained in a *system of records* with another agency—referred to in the act as a disclosure of information—without an individual’s written consent unless an exception applies.¹⁰⁹ *Systems of records* refer to records that have been grouped together (e.g., a database) and that permit a record from within that group to be retrieved using some identifier for the individual whom the data concerns (e.g., searchable by a Social Security number [SSN]).¹¹⁰

One of the Privacy Act’s exceptions—that is, when a disclosure by an agency is permissible without consent—is for a *routine use*.¹¹¹ Under the Privacy Act, a routine use means an agency may disclose data to another agency for “use of such record for a purpose that is compatible with the purpose for which the record was collected.”¹¹²

Additionally, an amendment to the Privacy Act—called the Computer Matching and Privacy Protection of 1988 (CMPPA)—establishes rules for the comparison and matching of data on individuals in certain circumstances, including for the purpose of determining eligibility for payments under a federal benefit program.¹¹³ Historically, the Privacy Act’s routine use exception has been viewed as the mechanism under which data matching—particularly in the prevention and reduction of improper payments and fraud, waste, and abuse more generally—has occurred.¹¹⁴ An August 2025 memorandum from the OMB Director to agencies reaffirmed the use of the routine use exception as a way to accomplish the type of data disclosure that is needed in the context of the DNP system.¹¹⁵

Use of the DNP system implicates the Privacy Act and its amendments in a number of ways. The Privacy Act bears upon the sourcing of databases that make up the DNP system, in a paying agency’s use of the DNP system, and in the data matching that occurs by using the DNP system. In both cases—(1) where an agency is the source of a DNP system database and (2) where an agency is accessing and reviewing those databases—these data disclosures by federal agencies operate within the framework established by the Privacy Act. As discussed below, disclosures in

¹⁰⁸ The Privacy Act defines *records* to mean “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)). For more information on the Privacy Act generally, see CRS Report R47863, *The Privacy Act of 1974: Overview and Issues for Congress*, by Meghan M. Stuessy.

¹⁰⁹ 5 U.S.C. §552a(b).

¹¹⁰ 5 U.S.C. §552a(a)(5).

¹¹¹ 5 U.S.C. §552a(b)(3).

¹¹² 5 U.S.C. §552a(a)(7).

¹¹³ P.L. 100-503. For a short overview of what the CMPPA requires, see CRS In Focus IF12053, *Federal Data Integration and Individual Rights: The Computer Matching and Privacy Protection Act*, by Natalie R. Ortiz.

¹¹⁴ See discussion of this history in Appendix A of CRS Report R47325, *Computer Matching and Privacy Protection Act: Data Integration and Individual Rights*, by Natalie R. Ortiz.

¹¹⁵ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, pp. 1-3 of Appendix I: Routine Use for Do Not Pay.

both cases have typically been categorized by the relevant agency as routine uses of data. Sometimes, however, there are specific restrictions in statute that prevent access and use of data in the context of the DNP system, regardless of the Privacy Act's routine use exception and the PIIA's mandates. For example, the Internal Revenue Service (IRS) abides by the requirements of Section 6103 of the *Internal Revenue Code* that tax returns and tax return information—which include information on income and assets, for example—are confidential unless disclosure is expressly authorized in statute.¹¹⁶

Routine uses are published by agencies in the *Federal Register* as part of a *system of records notice* (SORN). SORNs are required to identify each routine use of data from systems of records.¹¹⁷ For the purposes of the DNP system, a system of records can be referring to (1) one of the databases that make up the DNP system, (2) data or a dataset from a paying agency that concerns its intended payment recipients, and (3) the DNP system itself, as maintained by the Fiscal Service.

Sourcing Databases for the Do Not Pay System

As shown in **Table A-1** (in the **Appendix**), the databases in the DNP system are largely sourced from federal agencies, with a number of different federal agencies providing such databases. The agencies that source data to the Fiscal Service for the purposes of the DNP system disclose these data within the bounds of their statutory authorities.

Even though the PIIA names certain databases for agencies to review and permits the OMB Director to designate a database as part of the DNPI, such naming and designations do not necessarily mean that the data can be provided to the DNP system. For example, the death data that the Commissioner of Social Security receives from states is governed by Section 205(r) of the Social Security Act, which includes a paragraph that explicitly restricts disclosures of such death records except as provided for in the section.¹¹⁸ In 2023, an amendment to Section 205(r) of the Social Security Act took effect that temporarily permits disclosure of state-provided death data to “the agency operating the Do Not Pay working system.”¹¹⁹ Absent this amendment, the governing statute had been interpreted by SSA as restricting the Commissioner of Social Security from disclosing the death records obtained from states and therefore in tension with the language in the PIIA that agencies review, as appropriate, “the death records maintained by the Commissioner of Social Security.”¹²⁰

OMB also notes that its designation is not sufficient to allow an agency to disclose data to the Fiscal Service for the purposes of the DNP system, that the agency must have such disclosure authority, and that such designation is subject to the determination of such authority by the agency.¹²¹

¹¹⁶ 26 U.S.C. §6103. For further discussion of this confidentiality requirement, see CRS Report R48323, *Disclosure of Federal Tax Return Information to Congressional Committees*, by Justin C. Chung.

¹¹⁷ 5 U.S.C. §552a(e)(4)(D).

¹¹⁸ 42 U.S.C. §405(r)(6).

¹¹⁹ The amendment was made by P.L. 116-260 Title VIII §801 (134 Stat. 3201), which was signed into law on December 27, 2020. The amendment to Section 205(r) of the Social Security Act (42 U.S.C. §405(r)) took effect three years after enactment of (i.e., December 27, 2023). The amendment to the statute is set to expire three years following its effective date (i.e., December 27, 2026).

¹²⁰ Social Security Advisory Board, *Social Security and the Death Master File*, June 2019, pp. 1-2, <https://s3-us-gov-west-1.amazonaws.com/cg-778536a2-e58c-44f1-9173-29749804ec54/uploads/2019/06/2019-DMF-v10-2019-06-17-Accessible.pdf>.

¹²¹ OMB, *Protecting Privacy*, M-13-20, p. 9.

If there is no specific restriction in statute, then a routine use under the Privacy Act is one mechanism that permits an agency to disclose data, including as a database searchable through the DNP system. For example, in the case of the “debt check database”—which is a subset of records maintained by the Treasury Department for the purposes of debt collection and is specifically named in the PIIA as a database to review under the DNPI—the Fiscal Service describes how use of the database through the DNP system is dependent upon and limited to the legal authorities that govern the data.¹²² This includes the authority that enables the Treasury Department to disclose the data for a routine use that it has identified pursuant to the Privacy Act. Only certain uses of the debt check database through the DNP system are compatible with these routine uses. Agencies that seek access of the debt check database through the DNP system indicate during the onboarding process whether their use of the data is consistent with those stated routine uses.¹²³ The routine uses identified by the Treasury Department for their debt collection records include, but are not limited to, disclosures that are to

A Federal or State agency, its employees, agents (including contractors of its agents) or contractors; (b) fiscal or financial agent designated by the Fiscal Service or other Department of the Treasury bureau or office, including employees, agents or contractors of such agent; or (c) contractor of the Fiscal Service, for the purpose of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state in a state-administered, Federally funded program; disclosure may be made to conduct computerized comparisons for this purpose.¹²⁴

While it may appear that this routine use could be blanket authority to enable access to the debt check database in the DNP system, the Fiscal Service restricts access to federal agencies only and does not appear to facilitate the use of the database by state governments that use the DNP system.¹²⁵

Using the Do Not Pay System as a Paying Agency

A routine use is also relevant to agencies that review those DNP system databases for which they have approval. Use of the DNP system necessitates a disclosure of information from the paying agency to the Fiscal Service. The onboarding process includes identifying the routine use that authorizes the paying agency to make this disclosure.¹²⁶

The language used in SORNs to identify routine use disclosures for the purposes of searching the DNP system has typically varied by agency. In August 2025, the OMB Director provided standardized language for agencies to use in their SORNs for routine use disclosures:

To the U.S. Department of the Treasury when disclosure of the information is relevant to review payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state (meaning a state of the United States, the District of Columbia, a territory or possession of the United States, or a federally recognized Indian tribe) in a state-administered, federally funded program.¹²⁷

¹²² Bureau of the Fiscal Service, “Do Not Pay Portal Initial Questions Guide,” pp. 20-21.

¹²³ Bureau of the Fiscal Service, “Initial Questions Guide,” p. 12.

¹²⁴ Bureau of the Fiscal Service, “Privacy Act of 1974; System of Records,” 85 *Federal Register* 11776, February 27, 2020, <https://www.federalregister.gov/d/2020-03969/p-519>.

¹²⁵ Bureau of the Fiscal Service, “Initial Questions Guide,” p. 19.

¹²⁶ Bureau of the Fiscal Service, “Do Not Pay Portal Initial Questions Guide,” p. 8.

¹²⁷ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 2 of Appendix I.

In its August 2025 memorandum, OMB indicated that agencies are expected to conform the language in any existing routine use to the standardized language provided.¹²⁸ For example, in June 2024, the Department of Housing and Urban Development (HUD) published a routine use in the *Federal Register* for disclosures from a particular system of records that would presumably need to be modified in accordance with the OMB memorandum:

To the US Department of Treasury through a computer matching program interface between [Computerized Homes Underwriting Management System] and Treasury’s Do Not Pay (DNP) system for the purposes of preventing and recovering improper payments and to verify borrower eligibility to participate in [the Federal Housing Administration’s] mortgage insurance programs per the [PIIA].¹²⁹

The standardized routine use language would also be used by an agency when it identifies or establishes a new system of records with “information whose disclosure to Treasury would be relevant and necessary for identifying, preventing, or recouping improper payments by reviewing payment and award eligibility through the Do Not Pay Working System.”¹³⁰

OMB’s August 2025 memorandum stems from E.O. 14249, *Protecting America’s Bank Account Against Fraud, Waste, and Abuse*, which was issued by President Donald Trump in March 2025.¹³¹ Among other directives, the E.O. instructs all agency heads to review and modify as necessary the agency’s SORNs to

include a “routine use” that allows for the disclosure of records to the Treasury Department for the purposes of identifying, preventing, or recouping fraud and improper payments, to the extent permissible by law.¹³²

Data Matching

Using the DNP system as a paying agency means that it has to disclose information that identifies an intended payment recipient. That identifying information is used to locate a possible match, if one exists, to data from a DNP system database. This identifying information—in either a DNP database or from the paying agency—could include an individual’s first name and last name, an entity’s name (e.g., a legal business name), and an identification number, such as an SSN, individual taxpayer identification number (ITIN), or employer identification number (EIN).

The DNP system allows these identifiers to be used alone in some cases (e.g., a lookup in the portal using online search that uses only SSN) or in combination with each other (e.g., the SSN plus first name and last name). Whether such identifiers are combined or how they are combined can determine the precision of the match. For example, the Fiscal Service advises agencies to use three identifiers together for the most accurate matches when using the portal’s online search

¹²⁸ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 2 of Appendix I.

¹²⁹ HUD, “Privacy Act of 1974; System of Records,” 89 *Federal Register* 47978, June 4, 2024, <https://www.federalregister.gov/d/2024-12178/p-45>.

¹³⁰ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 1 of Appendix I.

¹³¹ Executive Order 14249 of March 25, 2025 “Protecting America’s Bank Account Against Fraud, Waste, and Abuse,” 90 *Federal Register* 14011, March 28, 2025, <https://www.federalregister.gov/documents/2025/03/28/2025-05524/protecting-americas-bank-account-against-fraud-waste-and-abuse>.

¹³² Executive Order 14249 of March 25, 2025 “Protecting America’s Bank Account Against Fraud, Waste, and Abuse,” 90 *Federal Register* 14011, March 28, 2025, <https://www.federalregister.gov/d/2025-05524/p-11>.

functionality; the Fiscal Service notes that using first and last name only in bulk matching will result in a less conclusive match than when combined with an identifier like SSN or ITIN.¹³³

Using the DNP system can trigger the CMPPA. As introduced earlier, the CMPPA amended the Privacy Act and is implemented within the Privacy Act’s statutory framework. Where data matching using the DNP system may first involve a disclosure of records as governed by the Privacy Act, the subsequent performance of that data matching may be governed by the CMPPA.

The CMPPA establishes procedural requirements for *matching programs*. Matching programs are computerized comparisons of data that are for the purpose of establishing or verifying the eligibility of applicants, beneficiaries, recipients, participants, or providers of services under a *federal benefit program*.¹³⁴ Matching programs are defined to also include data comparisons that use the personnel or payroll records of federal employees, members of the uniformed services, and individuals entitled to any retirement program, including survivor benefits.¹³⁵ For the purposes of the CMPAA, a federal benefit program is any program funded by the federal government—including those administered by state governments or any other agents—that provides cash or assistance in the form of payments, grants, loans, or loan guarantees to individuals.¹³⁶ In addition to applying to federal agencies that act as *recipient* and *source* agencies within matching programs, the CMPPA’s requirements extend to matching programs that are between a federal agency and a state or local government.¹³⁷

The Fiscal Service classifies some DNP system databases as “restricted,” whereas others are classified as “public.” The Fiscal Service states that it labels a database as restricted because it contains personally identifiable information (PII) and that the use of these databases with such information may require compliance with the CMPPA, including the execution of a computer matching agreement (CMA).¹³⁸

The CMPPA does not apply to cases of data comparisons that do not involve a system of records (as defined by the Privacy Act), which in turn establishes the scope of the CMPPA’s applicability to the operations of the DNP system. As identified in **Table A-1**, the DNP system does make use of some commercially sourced databases that may not be considered a system of records as

¹³³ Bureau of the Fiscal Service, “Understanding the DNP Portal Matching Logic,” <https://fiscal.treasury.gov/files/dnp/dnp-portal-matching-logic.pdf>.

¹³⁴ 5 U.S.C. §552a(a)(8)(A)(i)(I). In addition to including verifications of eligibility, matching programs also include comparisons for the purpose of recouping payments or delinquent debts under such *federal benefit programs*.

¹³⁵ 5 U.S.C. §552a(a)(8)(A)(ii).

¹³⁶ 5 U.S.C. §552a(a)(12).

¹³⁷ The definition of matching programs includes comparisons of *systems of records* with non-federal records (5 U.S.C. §552a(a)(8)(A)). “Non-federal records” is not defined by the CMPAA. Instead, the CMPPA defines the parties to a matching program. A *recipient agency* is “any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program (5 U.S.C. §552a(a)(9)). A *source agency* is defined as “any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program” (5 U.S.C. §552a(a)(11)). The CMPPA also defines *non-federal agency* as “any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program” (5 U.S.C. §552a(a)(10)), which implies that a non-federal agency can be a recipient agency.

¹³⁸ Bureau of the Fiscal Service, “Do Not Pay Privacy Program,” May 30, 2025, <https://fiscal.treasury.gov/dnp/privacy-program.html>. Neither the Privacy Act of 1974 nor the CMPPA defines or uses the term “PII.” OMB defines PII in Circular A-130, *Managing Information as a Strategic Resource* (see Appendix II of Circular A-130, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf). OMB noted that the appendix does not extend or interpret the Privacy Act (p. Appendix II-1)).

defined by the Privacy Act.¹³⁹ In *Federal Register* notices published by OMB to designate a database as part of the DNPI, OMB notes when such designated databases are not considered systems of records.¹⁴⁰ Accordingly, the Privacy Act in general, and the CMPPA in particular, might not always be applicable to the use of the DNP system.¹⁴¹

Waiving Computer Matching Agreements Under the Payment Integrity Information Act

The PIIA contemplates the CMPPA's requirement for CMAs. CMAs are to contain certain information about matching programs. This information includes but is not limited to (1) the procedures related to verifying the information that is produced in a matching program and (2) information from assessments that have been made as to the accuracy of the data used in a matching program.¹⁴² OMB characterizes the requirement for CMAs as “[helping] to ensure that the matching program is conducted in a manner that ensures accountability, due process, information quality, data minimization, security, and transparency.”¹⁴³

The PIIA allows the Treasury Department, as the agency operating the DNP system, in consultation with OMB, to waive the CMPPA's CMA requirement in “any case or class of cases for computer matching activities conducted under [the DNPI].”¹⁴⁴ In other words, agencies that use the DNP system for the purposes covered by the CMPPA (e.g., verifying eligibility for payments under federal benefit programs) are generally subject to the CMPPA's statutory requirements, unless a waiver from the Treasury Department applies.¹⁴⁵

Recent Developments: OMB Guidance to Implement E.O. 14249 and Waiving Computer Matching Agreements

E.O. 14249, which was briefly discussed above, directs the Treasury Department Secretary to minimize administrative barriers to agencies' access and use of data to prevent fraud and

¹³⁹ The use of commercial databases may be more nuanced in practice. OMB reminds agencies “that information in commercial databases used in the [DNPI] 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” (OMB, *Protecting Privacy*, M-13-20, p. 14).

¹⁴⁰ See, for example, “Considerations for Designating AVS and DNE” in OMB, “Proposed Designation of Databases to the Do Not Pay System,” 89 *Federal Register* 70208, August 29, 2024, <https://www.federalregister.gov/documents/2024/08/29/2024-18689/proposed-designation-of-databases-to-the-do-not-pay-working-system>. In this *Federal Register* notice, OMB states for Account Verification Service (AVS) that “Fiscal Service has determined that AVS does not by itself meet the definition of a system of records under the Privacy Act of 1974 (Privacy Act), as amended, which is codified at 5 U.S.C. 552a(a)(5).” Of Death Notification Entries (DNE), OMB states that “DNEs pertain to deceased persons. The beneficiary/recipient in the DNE is identified as deceased by the originator of the DNE, and, therefore, the DNE data maintained by Fiscal Service would not be covered by the Privacy Act.” OMB also notes that the Privacy Act and CMPPA do not apply in certain circumstances (see OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 1 of Appendix II).

¹⁴¹ In addition to the discussion in footnote 137 on what constitutes a *source* and *recipient* agency in a matching program, see also the discussion on issues involving how agencies interpret the scope of the CMPPA on pp. 12-13 in CRS Report R47325, *Computer Matching and Privacy Protection Act: Data Integration and Individual Rights*, by Natalie R. Ortiz. See also GAO's discussion on issues involving the interpretation of the CMPPA to the DNP system in *Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation*, GAO-14-44, October 2014, pp. 16-17, <https://www.gao.gov/assets/d1444.pdf>.

¹⁴² 5 U.S.C. §552a(o).

¹⁴³ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, Appendix II p. 1.

¹⁴⁴ 31 U.S.C. §3354(b)(3)(B)(i).

¹⁴⁵ OMB, *Transmittal of Appendix C*, M-21-19, p. 32.

improper payments by exercising the CMA waiver authority granted to the Treasury Department in the PIIA for the purposes of the DNPI.¹⁴⁶ An August 2025 memorandum from OMB that was issued in response to this executive order establishes requirements to govern these waivers.¹⁴⁷

In its memorandum, OMB states that waivers of the CMPPA's CMA requirement will be granted for the class of matching programs that meet all four of the following circumstances:

- i. The only purposes of the matching program are identifying and preventing improper payments and conducting any related recovery activities by verifying through Do Not Pay prepayment or pre-award eligibility.
- ii. The matching program involves one or more databases contained in Do Not Pay during the period in which the waiver is in effect.
- iii. The matching program involves either:
 1. one payment-certifying agency's system(s) of records that maintain(s) information relevant and necessary for verifying payment or award eligibility and related recovery activities; or
 2. a state, or agency thereof, responsible for reducing improper payments of a state-administered, federally funded program.
- iv. The matching program involves verifying prepayment or pre-award eligibility in one or more of the eligible object classes ... or any other object classes specified by Treasury, in consultation with OMB.¹⁴⁸

¹⁴⁶ Executive Order 14249 of March 25, 2025 "Protecting America's Bank Account Against Fraud, Waste, and Abuse," 90 *Federal Register* 14011, March 28, 2025, <https://www.federalregister.gov/d/2025-05524/p-10>.

¹⁴⁷ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, Appendix II.

¹⁴⁸ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 2 of Appendix II.

The fourth criterion uses a concept—*object classes*—from the federal budget, which is the subject of OMB Circular A-11. Circular A-11 describes *object classes* as categories from a federal classification system that correspond to types and definitions for obligations incurred by the federal government.¹⁴⁹ Object classes that are eligible for a CMA waiver include those from four of the five major object classes: personnel compensation and benefits, contractual services and supplies, asset acquisition, and grants and fixed charges.¹⁵⁰ Major object classes are divided into smaller classes.¹⁵¹ The **text box** lists the object classes eligible for a waiver according to the OMB memorandum.¹⁵²

OMB specifically excludes some object classes from being eligible for the CMA waiver.¹⁵³ For example, verifications through the DNP system of *personnel compensation*, which is defined in Circular A-11 as “compensation directly related to duties performed for the government by Federal civilian employees, military personnel, and non-Federal personnel,” are not eligible for the CMA waiver.¹⁵⁴

Object Classes Eligible for a Computer Matching Agreement Waiver

As discussed in the Office of Management and Budget’s (OMB’s) memorandum *Preventing Improper Payments and Protecting Privacy Through Do Not Pay* (M-25-32), whether a specific matching program that uses the Do Not Pay (DNP) system is eligible for a waiver of the computer matching agreement (CMA) otherwise required by the Computer Matching and Privacy Protection Act of 1988 (CMPPA) depends on certain criteria, including whether the payments to be verified are for certain object classes. The Payment Integrity Information Act of 2019 (PIIA) authorizes the Secretary of the Department of the Treasury to waive the requirement for a CMA for any case or class of cases, in consultation with OMB. OMB identifies the object classes that are eligible for the waiver when the other criteria are also met.

Personnel compensation and benefits

- Civilian personnel benefits
- Military personnel benefits
- Benefits for former personnel

Grants and fixed charges

- Grants, subsidies, and contributions
- Insurance claims and indemnities
- Refunds

Acquisition of assets

- Equipment
- Land and structures
- Investments and loans

Contractual services and supplies

- Advisory and assistance services
- Other services from non-federal sources
- Other goods and services from federal sources
- Operation and maintenance of facilities
- Research and development contracts
- Medical care operation and maintenance of equipment
- Subsistence and support of persons
- Supplies and materials

A CMA would thus be necessary in those circumstances where use of the DNP system is to determine the eligibility of payments that correspond to the ineligible object classes identified by OMB. A CMA would also be needed in cases where the other criteria for a waiver are not met.

If use of the DNP system, however, meets the criteria for a waiver, then that matching program could proceed for four years without a CMA, at which point the waiver may be continued as

¹⁴⁹ OMB, *Preparation, Submission, and Execution of the Budget*, Circular A-11, July 2024, pp. 1-2 of “Section 83—Object Classification (Schedule O),” <https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf#page=241>.

¹⁵⁰ The fifth major object class is “other.”

¹⁵¹ OMB, *Preparation, Submission, and Execution of the Budget*, Circular A-11, p. 4 of Section 83—Object Classification.

¹⁵² OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 3 of Appendix II.

¹⁵³ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 3 of Appendix II.

¹⁵⁴ See definition for *personnel compensation* in OMB, *Preparation, Submission, and Execution of the Budget*, Circular A-11, p. 4 of Section 83.

determined by the Treasury Department in consultation with OMB.¹⁵⁵ According to a *Federal Register* notice, on September 3, 2025, the Treasury Department Secretary authorized the issuance of four-year waivers for those classes of matching programs (i.e., uses of the DNP system) defined as eligible in OMB’s memorandum.¹⁵⁶ On September 10, 2025, the Fiscal Service published in the *Federal Register* an intent to issue these waivers, which would be effective through September 10, 2029.¹⁵⁷ The notice did not provide any information on the agencies or programs that would be covered by the waiver.

Where E.O. 14249 might have intended the exercise of the PIIA’s CMA waiver authority to reduce administrative barriers to using the DNP system, OMB states that a paying agency must still meet other administrative and statutory requirements when a waiver is applicable, including¹⁵⁸

- entering into a data sharing agreement with the Treasury Department that contains certain information, some of which would also be in a CMA (e.g., procedures for verifying information produced in the matching program);¹⁵⁹
- reporting the matching program to OMB and certain congressional committees, which is required by the CMPPA;¹⁶⁰
- providing public notice of the matching program, as required by the CMPPA;¹⁶¹
- conducting annual, role-based training on applicable Privacy Act requirements for any agency official involved in the matching program; and
- complying with any other Privacy Act or CMPPA requirement (e.g., providing an individual with notice of match findings and an opportunity to contest such findings).¹⁶²

Effect of Data Matches on Payments

Data matches in the DNP system do not necessarily stop a payment from being disbursed. The PIIA includes a stipulation for use of DNPI databases that provides for payments:

Payment otherwise required.—When using the Do Not Pay Initiative, an executive agency shall recognize that there may be circumstances under 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 Do Not Pay Initiative.¹⁶³

¹⁵⁵ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 3 of Appendix II.

¹⁵⁶ Bureau of the Fiscal Service, “Notice of Intent to Issue a Four-Year Waiver from the Requirements of Computer Matching Agreements for Do Not Pay,” 90 *Federal Register* 43729, September 10, 2025, <https://www.federalregister.gov/documents/2025/09/10/2025-17382/waiver-of-computer-matching-agreements-for-do-not-pay>.

¹⁵⁷ Bureau of the Fiscal Service, “Notice of Intent to Issue a Four-Year Waiver.”

¹⁵⁸ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, pp. 4-5 of Appendix II.

¹⁵⁹ 5 U.S.C. §552a(o)(1)(E).

¹⁶⁰ 5 U.S.C. §552a(r). See also OMB, *Federal Agency Responsibility for Review, Reporting, and Publication under the Privacy Act*, Circular A-108, December 23, 2016, pp. 20-23, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf#page=20.

¹⁶¹ 5 U.S.C. §552a(e)(12). See also OMB, Circular A-108, pp. 18-19.

¹⁶² 5 U.S.C. §552a(p)(1)(B).

¹⁶³ 31 U.S.C. §3354(b)(4).

Additionally, the Fiscal Service states that the DNP system does not instruct agencies on what to do if a data match is found. Instead, the Fiscal Service indicates that it provides information

to assist agencies in determining payment eligibility based on the agency’s internal policies and business processes. While DNP will not tell an agency whether or not to make a payment, it may help them identify anomalies and potential problems.¹⁶⁴

Thus, while use of the DNP system is sometimes characterized as a way to avoid a reactive, “pay-and-chase” approach to improper payments, representing the system in this way may oversimplify the circumstances and payment laws that agencies take into account. A data match using the DNP system does not in and of itself mean that the associated payment would necessarily be improper.

As further discussed below, agencies may contextualize data matches from the DNP system in terms of the type of payment the match concerns. Particular types of payments may be subject to specific conditions on their disbursement. Certain policies can inform an agency’s decisionmaking around benefit program payments, entitlement payments, financial awards, and vendor or contractor payments.

Additionally, other factors related to agency management may also play into how decisions are made about payments that are associated with data matches from the DNP system. For example, an agency’s internal policies, including those that consider *risk appetite* and the potential cost inefficiencies of investigating payments that may be improper, may also have an effect on whether a data match is alone sufficient to stop the disbursement of federal funds.

Finally, data matches that are produced from *payment integration*—a process undertaken by the Treasury Department at the time of payment that leverages its government-wide role in disbursing federal funds—further highlights the role of agency decisionmaking in determining whether a data match from the DNP system is associated with a proper or improper payment.

Payment Authorities and Roles

Within the federal payment process, the Treasury Department is required

to disburse money only as provided by a voucher certified by (A) the head of the executive agency concerned; or (B) an officer or employee of the executive agency having written authorization from the head of the agency to certify vouchers.¹⁶⁵

Certifying officials, in contrast, are responsible for the information submitted to the Treasury Department, the computation and correctness of amounts to be paid, and “the legality of the proposed payment under the appropriation or fund involved.”¹⁶⁶

In other words, while the Treasury Department is vested with the authority to make a payment on behalf of agencies, that payment is transacted as directed by the agency official who has

¹⁶⁴ Bureau of the Fiscal Service, “Frequently Asked Questions,” “Using Do Not Pay,” “Will DNP tell me what to do if a match is found?” July 3, 2025, <https://fiscal.treasury.gov/dnp/faqs.html>.

¹⁶⁵ 31 U.S.C. §3325(a). The term voucher in statute reflects processes, which were largely manual, as they were at the time.

¹⁶⁶ 31 U.S.C. §3528(a).

authorized the payment.¹⁶⁷ That certifying official who authorizes payment is thus accountable for the payment,¹⁶⁸ and statute acknowledges the differences in accountability.¹⁶⁹

As GAO has noted, payment certification, which might also be called payment authorization, has generally been a process that is separate from payment approval. Payment approvals are more administrative in nature, such as approving a contract or deeming an applicant qualified for a loan:

Agency officials authorized to perform administrative approvals are generally required to follow agency policies and procedures as opposed to statutory requirements and Treasury regulations followed by certifying officers.¹⁷⁰

Still, GAO states that the responsibilities of certifying officials generally extend to most aspects of payment transactions and that these officials have more responsibility than those performing administrative approvals.

GAO has also observed the role that technology has played in modifying payment process:

Under traditional payment processes, certifying officers reviewed all invoices they authorized for payment. Although the certifying officers are primarily responsible for payments authorized, the volume of transactions, the geographic dispersion of activities, and the emphasis on prompt payment make it virtually impossible for these individuals to review all invoices before authorizing payment. Consequently, in fulfilling their responsibilities, these officers must rely on the systems, internal controls, and personnel that process the transactions. As a result, payment process oversight has generally shifted from individual transaction reviews to reviews of internal control over systems that process the transactions.¹⁷¹

Due Process Under the Computer Matching and Privacy Protection Act

As introduced above, the CMPPA imposes certain procedural requirements on agencies that conduct or participate in matching programs. One of these procedural requirements concerns due process.¹⁷² As some uses of the DNP system constitute a matching program, the CMPPA's due process requirements are relevant to the effect of a data match on whether a payment is disbursed. According to OMB's guidance to agencies on the implementation of the PIIA's requirements,

¹⁶⁷ See discussion in section D ("Illegal or Improper Payment") of chapter 9 ("Liability and Relief of Accountable Officers") in GAO, Office of the General Counsel (OGC), *Principles of Federal Appropriations Law*, volume II, 3rd ed., GAO-06-382SP, February 2006, p. 75 of chapter 9 (9–75), <https://www.gao.gov/assets/2019-11/202819.pdf#page=429>.

¹⁶⁸ 31 U.S.C. §3528(a)(4) addresses liability for certifying officials and 31 U.S.C. §3325(a)(3) addresses accountability for the "correctness of computations on a voucher." See discussion in GAO OGC, *Principles of Appropriations Law*, about the liability of certifying officials for improper payment in the context of automated payment systems: "The increased use of automated payment systems has changed the way certifying officers must operate.... Thus, in considering requests for relief under an automated payment system where verification of individual transactions is impossible as a practical matter, the basic question will be the reasonableness of the certifying officer's reliance on the system to continually produce legal and accurate payments" (pp. 9–79–9–80).

¹⁶⁹ 31 U.S.C. §3325(a)(3).

¹⁷⁰ GAO, *Streamlining the Payment Process While Maintaining Effective Internal Control*, GAO/AIMD-21.3.2, May 2000, p. 6 footnote 1, <https://www.gao.gov/assets/aimd-21.3.2.pdf>.

¹⁷¹ GAO, *Streamlining the Payment Process*, p. 10.

¹⁷² 5 U.S.C. §552a(p).

even if the CMPPA's CMA requirement is waived for certain uses of the DNP system, "agencies must continue to comply with law and policy concerning due process in a matching program."¹⁷³

The CMPPA's due process provision is specifically intended to protect any individual whose data is used in a matching program.¹⁷⁴ Under the CMPPA, before suspending, terminating, reducing, or making a final denial of any financial assistance or payment to an individual under a *federal benefit program* (as defined by the CMPPA), or before taking any other adverse action against such individual, agencies are instructed to provide the individual with due process. This includes verifying the data match through investigation and confirmation, and providing the individual with notice of the finding and the opportunity to contest the finding.¹⁷⁵

The CMPPA provides that an individual will have 30 days to respond to the notice and contest the finding, unless there is a regulation or statute that covers such notice and contest processes for the relevant paying program.¹⁷⁶ Thus, an agency's procedures for due process may result in the disbursement of a payment despite a data match because, for example, the data match could not be verified or because it was successfully contested. Furthermore, at least some programs operate under governing laws and related regulations that permit payments to be issued while individuals exercise their due process rights.¹⁷⁷

Prompt Payment Act

Despite a data match in the DNP system, an agency may disburse a payment in some situations involving federal contracts because of the obligations that are created under such contracts. Specifically, the Federal Acquisition Regulation (FAR) establishes certain policies and requirements that agencies must meet in their contracting activities, including those concerning payments under such contracts.¹⁷⁸ The FAR implements the Prompt Payment Act, which directs agencies to pay procurement-related invoices to vendors or contractors within 30 days of receipt and to pay interest to contractors if such payments are made late.¹⁷⁹

Depending on an agency's processes, these 30 days may occur before an agency can determine whether a data match generated by the DNP system is relevant to the contract. Generally, an agency may avoid interest penalties when delaying a payment to a contractor when there is a disagreement about the payment amount, contract compliance, or the amount temporarily withheld or retained by an agency in accordance with the terms of the contract.¹⁸⁰ Absent a

¹⁷³ OMB, *Transmittal of Appendix C*, M-21-19, p. 32. See also OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 4 of Appendix II: "Any agency making use of this waiver must still comply with all other applicable requirements of the Privacy Act. For example, a waiver of the matching agreement requirement under 5 U.S.C. § 552a(o) does not affect the requirement at 5 U.S.C. § 552a(p)(1)(A) for the agency to independently verify information produced by the matching program, or the requirement at 5 U.S.C. § 552a(p)(1)(B) for the agency to provide an individual with notice containing a statement of the agency's findings and informing the individual of the opportunity to contest such findings."

¹⁷⁴ 5 U.S.C. § 552a(p)(1).

¹⁷⁵ 5 U.S.C. § 552a(p)(1)(A-B).

¹⁷⁶ 5 U.S.C. § 552a(p)(1)(C).

¹⁷⁷ For example, in the case of the state administration of the federal Supplemental Nutrition Assistance Program (SNAP), 7 U.S.C. § 2020(e)(10) and regulations at 7 C.F.R. § 273.15(k) directs states to continue benefits when a household requests a hearing in a timely manner after receiving notice of a reduction or termination of its benefits.

¹⁷⁸ For more information on the FAR, see CRS Report R42826, *The Federal Acquisition Regulation (FAR): Answers to Frequently Asked Questions*, by David H. Carpenter, Matthew D. Trout, and Dominick A. Fiorentino.

¹⁷⁹ P.L. 97-177, as amended; codified as amended at 31 U.S.C. §§ 3901-3907. See also 5 C.F.R. § 1315 and 48 C.F.R. § 32.9.

¹⁸⁰ 48 C.F.R. § 32.907(d).

permissible delay, a payment may be issued to a contractor to avoid the accrual of interest, interest payments, and, if a contractor requests it, an additional penalty for late payment.¹⁸¹ Additionally, as discussed below, an agency considers whether a match from the DNP system is relevant to a contractor's eligibility for a payment.

Relevance to Payment Eligibility

A data match from the DNP system may have no bearing on a recipient's eligibility for a specific payment. For example, as noted at the beginning of this report, the DNP system includes the debarment and suspension records (also known as exclusion records) from the GSA's System for Award Management (SAM).¹⁸² It is possible for an agency to match a contractor that is due a payment to these exclusion records and still issue a payment to the contractor. Specifically, the FAR permits agencies to continue contracts—including continuing to issue payments under such contracts—to contractors that had existing contracts at the time they were debarred, suspended, proposed for debarment, or agreed to be excluded, unless the head of the paying agency intervenes.¹⁸³

Furthermore, an individual debarred, suspended, or otherwise excluded under the federal debarment and suspension system in their business capacity (e.g., as a contractor) is not necessarily prohibited from receiving other types of federal payments. While procurement and nonprocurement debarment and suspension decisions have reciprocal effects, the effect of procurement-related debarment or suspension on nonprocurement eligibility extends only to payments from *covered transactions* (e.g., loans, loan guarantees, cooperative agreements, subsidies, and grants).¹⁸⁴ Thus, a data match to the SAM exclusion records contained within the DNP system would not necessarily preclude an individual's eligibility for certain payments that are not covered transactions—including, for example, an entitlement or benefit payment in their non-business capacity, such as a Social Security retirement payment, or a salary paid due to federal employment.¹⁸⁵

Matches to a DNP system database can also be used to confirm eligibility in the positive in some cases. For example, the DNP system contains some information from the IRS on the tax status of organizations, including those with a 501(c)(3) exemption and those that have had their exemption status automatically revoked. Some grant programs use this tax status as a condition of eligibility, which could be confirmed through the DNP system, if the entity does not also match the automatic revocation data.¹⁸⁶

Risk Appetite

There is also the possibility that an agency will disburse a payment even when a data match in the DNP system is thought to preclude eligibility for the receipt of federal funds. For instance, some improper payments may be considered tolerable by agency management within the agency's

¹⁸¹ 48 C.F.R. §32.907(c).

¹⁸² See "Assumptions Behind the Operations of the Do Not Pay System and the Role of Data Matching."

¹⁸³ 48 C.F.R. §9.405-1(a)(1).

¹⁸⁴ 2 CFR §180.210 provides for which nonprocurement transactions are *covered transactions*.

¹⁸⁵ 2 CFR §108.2015 provides for nonprocurement transactions that are not *covered transactions*.

¹⁸⁶ Bureau of the Fiscal Service, "IRS Tax Exempt Organization Search," <https://fiscal.treasury.gov/files/dnp/irs-teos-qrc.pdf>.

enterprise risk management (ERM) and internal control framework.¹⁸⁷ OMB states that an agency's senior management determines the agency's *risk appetite* under this framework. In this case, risk appetite is how much risk to payment integrity the agency is willing to accept in pursuit of its mission and strategic objectives, while also considering tradeoffs. An agency may tolerate some improper payments because to stop them, for example, would introduce cost inefficiencies or seriously affect the operations of the agency's program, or for some other reason identified by senior management.¹⁸⁸ Thus, the cost of agency staff time to validate information from a data match in the DNP system, in addition to recovery costs, may cost more than the overpayment (e.g., spending \$2 to save \$1 in improper payments).¹⁸⁹

Risk is also an explicit part of the decisionmaking process in the awarding of financial assistance. Agencies that award financial assistance are directed to assess the risk posed by applicants.¹⁹⁰ In identifying risks, agencies are directed to review the DNP system for eligibility and financial integrity information.¹⁹¹ Agencies are granted discretion to make federal awards to applicants if the information from the DNP system is either not relevant or the agency can appropriately mitigate any associated risks by imposing certain conditions on the award.¹⁹²

Payment Integration and Timing of a Match

A data match in the DNP system might also occur too late in the payment process. Specifically, payments disbursed by the Treasury Department are matched at the time of payment to SSA's "Full" Death Master File (DMF-Full) database, which is temporarily accessible through the DNP system.¹⁹³ Matching at this time is referred to as *payment integration*.

Payment integration uses the payment file submitted by an agency through Payment Automation Manager (PAM), which is a software application that is used government-wide to disburse almost all federal funds, particularly payments issued in bulk, including those made under federal benefit programs, tax refunds, and federal salaries.¹⁹⁴

¹⁸⁷ OMB, *Transmittal of Appendix C*, M-21-19, p. 33. See additional discussion for identifying a program's tolerable improper payment rate in U.S. Chief Financial Officers Council, *Optimizing Payment Integrity Activities: A Guide for Identifying a Program's Tolerable Improper Payment Rate*, October 2021, https://www.cfo.gov/assets/files/TolerableRateGuide_final.pdf.

¹⁸⁸ OMB, *Transmittal of Appendix C*, M-21-19, p. 33.

¹⁸⁹ See discussion on using cost-benefit analyses to determine whether reducing improper payment rates through the implementation of a corrective action plan is practical and desirable in CFO Council, *Optimizing Payment Integrity Activities*, pp. 23-33. A corrective action plan includes mitigation strategies and corrective actions to prevent future improper payment and is generally intended to address root causes (see OMB, *Transmittal of Appendix C*, M-21-19, p. 30).

¹⁹⁰ 2 C.F.R. §200.206.

¹⁹¹ 2 C.F.R. §200.206(a)(1).

¹⁹² 2 C.F.R. 200.206(a)(2).

¹⁹³ The DMF-Full is considered to be the most complete compiling of death records maintained by SSA because it includes deaths reported to SSA by state vital records offices. See footnote 119 for discussion on why the inclusion of DMF-Full in the DNP system is temporary. For additional background on the DMF-Full, see CRS Report R46640, *The Social Security Administration's Death Data: In Brief*, by Paul S. Davies. Documentation from the Fiscal Service indicates that payment integration will use only the DMF-Full beginning in July 2025. Prior to July 2025, the Fiscal Service was matching against other databases from the DNP system that contain information on persons identified as deceased, including from the Defense Department, State Department, and commercial sources.

¹⁹⁴ Bureau of the Fiscal Service, "Using the DNP Portal," "Payment Integration," <https://fiscal.treasury.gov/dnp/using-the-dnp-portal.html>. The Treasury Department uses several systems to intake payment information from agencies as part of the payment processes it manages. These systems are discussed in the context of policies concerning payments (continued...)

Because payment integration is at the time of payment, and paying agencies ultimately authorize the disbursement of payments through certification, the payment is likely to be disbursed as certified by the paying agency, despite the potential for a data match in the DNP system.¹⁹⁵

According to some documentation from the Fiscal Service, it appears that an agency can request to enable an automatic stop on a payment when there is a data match that meets specific criteria at the time of payment integration.¹⁹⁶ The Fiscal Service emphasizes in its documentation that the DNP system does not itself stop the payment because of a data match. Instead, the paying agency has created a process that enables PAM to stop the transaction. The Office of Personnel Management (OPM) is noted by the Fiscal Service to be an agency that stops a payment because of a “conclusive match” during payment integration.¹⁹⁷

Adjudicating Matches from Payment Integration

Data matches from payment integration are available to agencies to review within the DNP system’s web-based portal. As such, these matches are accessible to those agencies that use the DNP system’s portal function and submit payments for processing through PAM.¹⁹⁸

Matches that are found during payment integration are to be *adjudicated* by the paying agency.¹⁹⁹ Adjudication includes (1) verifying the match to determine whether the payment is proper or improper and then (2) recording the determination of whether a payment is proper or improper within the DNP system’s portal.²⁰⁰ If not adjudicated as improper, a match—and the associated payment—could be adjudicated as proper because of an agency’s business requirements, business processes, or business rules or because the match is a false positive.²⁰¹ For example, in its FY2024 reporting on PaymentAccuracy.gov, the Department of Defense said of its data matches that

[r]esearch has determined that the majority of these match results are false positives (e.g., a vendor’s [ITIN] is matched to a deceased individual’s [SSN], and the payment is

disbursed by the Treasury Department in Treasury Financial Manual (TFM) Chapter 3000 “Requirements for Scheduling Payments Disbursed by the Bureau of the Fiscal Service,” <https://tfx.treasury.gov/tfm/volume1/part4a/chapter-3000-requirements-scheduling-payments-disbursed-bureau-fiscal-service>.

¹⁹⁵ For additional discussion of certification, see Treasury Department, TFM 3085, “Certification of Payments to Treasury,” <https://tfx.treasury.gov/tfm/volume1/part4a/chapter-3000-requirements-scheduling-payments-disbursed-bureau-fiscal-service>.

¹⁹⁶ Bureau of the Fiscal Service, “Payment Adjudication Do Not Pay Portal Quick Reference Card,” p. 3, <https://fiscal.treasury.gov/files/dnp/qrc-payment-adjudication.pdf>.

¹⁹⁷ Bureau of the Fiscal Service, “Adjudication Summary Report Do Not Pay Portal Quick Reference Card,” p. 2, <https://fiscal.treasury.gov/files/dnp/qrc-adjudication-summary-report.pdf>.

¹⁹⁸ Bureau of the Fiscal Service, “Payment Activity Report Do Not Pay Portal Quick Reference Card,” <https://fiscal.treasury.gov/files/dnp/qrc-payment-activity-report.pdf>. While the Treasury Department disburses most federal payments, there are other “non-Treasury Disbursement Officers” (NTDOs) (see 31 U.S.C. §3321(c) for agencies with statutory disbursement authority). NTDOs are subject, however, to requirements in TFM Chapter 4000 “Requirements for Non-Treasury Disbursing Officers (NTDOs),” <https://tfx.treasury.gov/tfm/volume1/part4a/chapter-4000-requirements-non-treasury-disbursing-officers-ntdos>. E.O. 14249 seeks to reduce the number of NTDOs.

¹⁹⁹ Only certain users of the portal can adjudicate a payment on behalf of an agency in the DNP system. Each user is assigned a specific type of role within a hierarchy. Where a role is placed within that hierarchy determines what information can be accessed within the DNP system and what activities can be performed. The agency using the DNP system determines the roles its staff will assume. No role within the hierarchy—and therefore within an agency—is able to perform all activities that are possible within the DNP system. For more information on user roles and responsibilities see Treasury Department Bureau of the Fiscal Service, “User Roles and Responsibility Do Not Pay Portal Quick Reference Card,” <https://fiscal.treasury.gov/files/dnp/qrc-roles-and-responsibilities.pdf>.

²⁰⁰ Bureau of the Fiscal Service, “Payment Adjudication.”

²⁰¹ Bureau of the Fiscal Service, “Payment Adjudication.”

erroneously flagged). The remaining matches are almost always deemed proper based on established business rules related to contracts terms and vendor performance (as payments cannot be stopped to vendors who performed properly under contractual agreements). The Department has historically adjudicated and deemed proper all potential improper payments identified using the DNP Portal.²⁰²

Discussion

Centralizing access to certain databases is intended to prevent improper payments under the PIIA. There are reasons, as discussed above, for why a data match in a centralized system of databases might not indicate a payment is improper. Some data matches, however, might be such an indication. In the case of the DNP system, an agency may consider a number of factors when determining what to do with a data match, or the agency may be required to take certain steps such as independent verification; agencies may differ in what factors are considered.

Congress, GAO, and the White House have often shown interest in the potential efficiency and effectiveness of centralizing data access as a way to prevent improper payments. This interest is evidenced through legislation that requires use of a centralized data system, the designation of additional databases available through such a system, executive mandates to reduce administrative barriers that might prevent the use of such a system, and the institutionalizing of practices and activities that incorporate the use of such a system within agency management and financial management frameworks.

A number of issues are raised by the operations of the DNP system and its role in preventing improper payments. These issues include (1) the availability and completeness of information on the effectiveness of the DNP system; (2) the usefulness of the databases that are accessible through the DNP system for preventing improper payments; and (3) the cost-effectiveness of data matching for agencies using the DNP system. Each of these issues is discussed in what follows, along with corresponding policy considerations and options.

Assessing the Role of the Do Not Pay System in Preventing Improper Payments

Congress may be challenged to ascertain the effectiveness of the DNP system, and the use of DNPI databases more generally, in reducing improper payments. There are some reasons for this, including that not all agencies use the DNP system, despite the PIIA's mandate and the presumption of access to the data within. The Department of Transportation (DOT) inspector general (IG), for example, reported in November 2023 that the DOT did not use the DNP system as required by the PIIA.²⁰³ Specifically, the DOT IG found that DOT policy does not define when and how to use the DNP system nor does the department have documented procedures for verifying a payment recipient's eligibility through the DNP system. Similarly, the SBA IG reported that the SBA did not review some of the databases that are required under the PIIA,

²⁰² PaymentAccuracy.gov, Annual Improper Payments Dashboard, "DOD FY 2024 Supplemental Payment Integrity Information," https://tableau.d2d.gsa.gov/views/AnnualPaymentIntegrityReportDraft_09302022/SupplementalPaymentIntegrityInformation?%3Aembed=y&%3AisGuestRedirectFromVizportal=y.

²⁰³ Department of Transportation Office of the Inspector General, *DOT's Policies and DNP Portal Use Are Not Sufficient to Comply with the DNP Initiative*, November 20, 2023, p. 3, https://www.oig.dot.gov/sites/default/files/DOT%20Do%20Not%20Pay_Final%20Audit%20Report_11.20.2023.pdf.

resulting in over \$145 million in SBA loans and grants being disbursed to entities that were listed in DNP system databases.²⁰⁴

Given that not all agencies use the DNP system, government-wide estimates of improper payments are only partially relevant to understanding the results produced by the DNP system. One assumption that may arise in response to this is that getting more agencies to use the DNP system might result in some decrease in improper payments. The magnitude of a change in improper payments, however, is hard to estimate because it might presume that the DNP system works for all agencies effectively and similarly. For FY2024, 62 agencies, including the 24 so-called “CFO Act agencies,” provided data on PaymentAccuracy.gov.²⁰⁵ Of these 62 agencies, 48 reported using the DNP system and 15 of these agency-users (31%) reported that the DNP system was not effective in preventing improper payments for them.

As discussed below, reporting from the Treasury Department and from agencies on the DNP system is one reason it is difficult to parse its role in preventing improper payments. Performance measures, such as improper payments prevented, that have been used by the Treasury Department for the DNP system have changed over the past several fiscal years, making it challenging to draw conclusions about the effectiveness of the system over time.

Measuring Government-wide Improper Payments Prevented

The Treasury Department provides some annual reporting on the DNP system’s performance as part of its congressional budget justification, which includes the performance plan required by the Government Performance and Results Act of 1993 (GPRA), as amended.²⁰⁶ Various performance measures for the DNP system have been used from year to year.

For example, as part of its FY2022 budget justification, the Fiscal Service reported identifying 22,800 improper payments at a value of \$43.5 million in FY2020.²⁰⁷ In its FY2024 justification, the Fiscal Service indicated that it was discontinuing use of these two performance measures (i.e., number and value) for FY2023 and FY2024.²⁰⁸ Instead, the Fiscal Service specified that it would be using new performance measurements: (1) *potential* improper payments identified, stopped, or recovered and (2) percentage of payments screened by Do Not Pay. However, in its FY2025 budget justification, percentage of payments screened by Do Not Pay was identified as being discontinued (after being identified as new in the previous fiscal year’s document), and no data was provided for that performance measure.²⁰⁹

²⁰⁴ Small Business Administration Office of the Inspector General, *Evaluation of COVID-19 Economic Injury Disaster Loan Applicants on the U.S. Department of the Treasury’s Do Not Pay List*, pp. 7-8, <https://www.sba.gov/sites/default/files/2024-06/SBA%20OIG%20Report%2024-18.pdf#page=14>.

²⁰⁵ PaymentAccuracy.gov, Annual Improper Payments Dashboard, “Supplemental Information,” https://tableau.d2d.gsa.gov/views/AnnualPaymentIntegrityReportDraft_09302022/SupplementalPaymentIntegrityInformation.

²⁰⁶ Requirements for the content of congressional budget justification materials are addressed in OMB Circular A-11: *Preparation, Submission, and Execution of the Budget* (July 2024; see <https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf>, p. 4 of Section 22—Communications with the Congress and the Public and Clearance Requirements). GPRA (P.L. 103-62) was amended by the GPRA Modernization Act of 2010 (P.L. 111-352).

²⁰⁷ Treasury Department, *U.S. Department of the Treasury FY 2022 Budget in Brief*, May 29, 2021, p. 76 (“Performance Highlights”), <https://home.treasury.gov/system/files/266/FY-2022-BIB.pdf>.

²⁰⁸ Treasury Department, *U.S. Department of the Treasury FY 2024 Budget in Brief*, March 9, 2023, p. 82 (“Performance Highlights”), <https://home.treasury.gov/system/files/266/FY-2024-Budget-in-Brief.pdf>.

²⁰⁹ Treasury Department, *U.S. Department of the Treasury FY 2025 Budget in Brief*, March 4, 2024, p. 76 (“Performance Highlights”), <https://home.treasury.gov/system/files/266/FY-2025-Budget-in-Brief-Combined.pdf>.

Other informal reporting from the Fiscal Service states that \$652.7 million in improper payments was “prevented and/or recovered” government-wide in FY2023.²¹⁰ The total is the combination of several activities, including but not limited to \$97.1 million in payments prevented through the use of cross-government data and \$45.8 million in payments prevented or confirmed as improper in the DNP system. While the Fiscal Service appears to have discontinued using the value of improper payments as an annual performance measure, it does seem capable of tracking it in some manner.

It is unclear how performance of the DNP system, as measured by the count of *potential* improper payments identified, takes into account false positive matches and payments that are ultimately adjudicated as proper by paying agencies. Additionally, it is unclear how the Treasury Department’s reporting, especially that associated with the budget process and financial reporting, reflects total system use, including that by (1) executive branch agencies, (2) federal agencies from the judicial and legislative branches of the federal government, and (3) federally funded, state-administered programs.

It is also unclear the extent to which the reporting reflects the totality of the system’s operations, including the various portal functionalities and DAS. In January 2020, before the PIIA became law, the Treasury Department IG issued a report on the need for the Fiscal Service to develop performance metrics for DAS projects undertaken by the Fiscal Service as part of the DNP system’s operations. The report stated that

[w]ithout performance metrics that include the measurement of the actual impact of DAS projects on agencies’ efforts to prevent improper payments, Fiscal Service cannot fully measure if DAS are meeting the [Do Not Pay] Business Center’s objectives. In addition, we found that Fiscal Service had not established a formal policy for the development, implementation, and periodic review of performance metrics for DAS.²¹¹

Policy Considerations

For FY2026, the Treasury Department is seeking for the Fiscal Service an additional \$48.8 million for payment integrity that will “fully leverage Do Not Pay.”²¹² When appropriating funding for this request or others in future fiscal years, Congress could consider whether to use appropriations report language to address how the performance of the DNP system is measured and reported.²¹³ The Treasury Department stated that it would update key performance indicators for FY2026 to FY2030 to be consistent with a strategic plan for the same time frame.²¹⁴ Such updating may include the performance measures used by the department for the DNP system.²¹⁵ Congress could also amend the PIIA to account for additional reporting by the Treasury Department.

Congress could also consider conducting oversight of how the Fiscal Service measures the performance of the DNP system against the system’s intended role in preventing improper

²¹⁰ Treasury Department, Fiscal Service, Office of Payment Integrity, “Payment Integrity Journal,” winter 2024, <https://fiscal.treasury.gov/files/dnp/payment-integrity-journal-winter-2024.pdf>.

²¹¹ Treasury Department OIG, *Performance Metric Policy Needed*, p. 2.

²¹² Treasury Department, *Bureau of the Fiscal Service*, budget-in-brief, FY2026, p. 4, <https://home.treasury.gov/system/files/266/12.-Fiscal-FY-2026-BIB.pdf>.

²¹³ For more information, see “Legislative Reports” in CRS Report R46899, *Regular Appropriations Acts: Selected Statutory Interpretation Issues*, by Sean Stiff.

²¹⁴ Agency strategic plans are required by 5 U.S.C. §306.

²¹⁵ Treasury Department, *FY 2026 Executive Summary*, FY 2026 congressional justification, p. 12, <https://home.treasury.gov/system/files/266/01.-FY-2026-Treasury-Executive-Summary.pdf>.

payments. Congress may seek to have the Treasury IG investigate the Fiscal Service’s methodology for measuring the performance of the DNP system, including the extent to which measures using *potential* improper payments as the unit of analysis are (1) representing data matches using only the portal’s functionalities (e.g., online search, batch matching); (2) considering other analyses, such as DAS projects; (3) accounting for false positive data matches; and (4) being adjusted for proper payment adjudications by agencies within the portal.

The Fiscal Service, however, is not necessarily the sole source of information on the effect of the DNP system on preventing improper payments, at least where government-wide totals might be concerned. For example, in its FY2024 annual report, the St. Louis FRB reported that it identified \$2.82 billion in improper and stopped payments in its role as a fiscal agent supporting the operations of the DNP system.²¹⁶ Like the measures used by the Fiscal Service, it is unclear how the St. Louis FRB calculates “improper and stopped payments.” According to the January 2020 Treasury Department IG report, the St. Louis FRB has a distinct role in providing the DNP system’s DAS functionality.²¹⁷ As such, the total reported improper payments identified may be derived from those ad hoc projects versus from agencies using the DNP system’s portal functionalities in the course of routine payment processes. Congress may consider whether the FRBs involved in the operations of the DNP system could supplement the Fiscal Service’s reporting.

Agency Reporting on Improper Payments Prevented

Congress could also look to paying agencies to report on the effect of the DNP system in preventing improper payments. Under the PIIA, OMB is charged with evaluating whether use of the DNPI databases has reduced improper payments.²¹⁸ OMB accomplishes this in part by imposing reporting requirements on agencies. That agency reporting, while available in annual financial reporting and on PaymentAccuracy.gov, varies widely in details that concern the DNP system.²¹⁹ Outside of OMB’s requirement under the PIIA to report on use of DNPI databases, there is no standalone statutory reporting requirement for agencies that is related to their use of the DNP system.

For example, in its FY2024 financial report, the Department of Health and Human Services (HHS) reported that the Centers for Medicare and Medicaid Services (CMS) screened 1 billion payments valued at \$429.3 billion through the DNP system’s portal and prevented 363,386 payments valued at \$2.6 billion because of such screening.²²⁰ According to PaymentAccuracy.gov for FY2024, the Department of Homeland Security (DHS) reported that 3.8 million disbursed payments valued at \$45.6 billion were subject to comparison with data from certain DNP system databases through payment integration.²²¹ DHS stated that less than 1% of these payments matched to a DNP database and required investigation and adjudication. These examples from

²¹⁶ Federal Reserve Bank of St. Louis, “Our People, Our Work” (2024 annual report), <https://www.stlouisfed.org/annual-report/2024/our-people-our-work>.

²¹⁷ Treasury Department OIG, *Performance Metric Policy Needed*, p. 7.

²¹⁸ 31 U.S.C. §3354(b)(5)(A).

²¹⁹ See reporting requirements in OMB, *Transmittal of Appendix C*, M-21-19, p. 55.

²²⁰ HHS, *Fiscal Year 2024 Agency Financial Report*, November 14, 2024, p. 197, <https://www.hhs.gov/sites/default/files/fy-2024-hhs-agency-financial-report.pdf>.

²²¹ PaymentAccuracy.gov, Annual Improper Payments Dashboard, “DHS FY 2024 Supplemental Payment Integrity Information,” https://tableau.d2d.gsa.gov/views/AnnualPaymentIntegrityReportDraft_09302022/SupplementalPaymentIntegrityInformation.

HHS and DHS suggest that at least some agencies may be positioned to report more specifically on the payments that are reviewed using the DNP system.

Additionally, while agency IGs may occasionally issue reports on an agency's use of the DNP system (see DOT and SBA examples above), these reports are generally the exception and not the rule. IGs are obligated to report on their agency's *compliance* with the PIIA as the term is specifically defined.²²² *Compliance* under the PIIA does not specifically include the PIIA's requirements for agencies to use the DNPI databases or to review payments using the DNP system.²²³

Policy Considerations

Requiring agency-level reporting on certain DNP system outputs and outcomes may be challenging to implement. According to what some agencies have reported on PaymentAccuracy.gov in FY2024, part of the challenge in measuring the effect of the DNP system is due to the system's design. For example, the Department of Energy stated in its reporting that because the DNP system is designed to be a proactive solution to preventing improper payments, counting the number of improper payments prevented or quantifying the dollar amount of improper payments prevented through the use of the DNP system would be a cost that outweighs the benefit of such use.²²⁴ OMB has previously suggested that measuring and reporting improper payments may lead to "a heavy" administrative burden.²²⁵

At the same time, it should not necessarily be viewed as problematic if an agency observes few matches of its intended payment recipients to the DNP system's databases or if an agency fails to realize a substantive reduction in improper payments. Instead, for example, an agency may see this as verifying the internal controls they have to ensure a recipient's eligibility for a payment.²²⁶ Thus, the number of matches—a possible indicator of potential improper payments—may be challenging to interpret across the board.

Addressing the Usefulness of Data Accessible Through the Do Not Pay System

While the DNP system provides agencies with access to data, the data accessible through the DNP system may be of limited use to agencies given the wide range of information that is pertinent to determinations of payment eligibility. The DNP system does not necessarily provide access to all types of eligibility-related information an agency may need to review or consider when determining eligibility. For example, as observed in **Table 1**, agencies identify issues accessing certain financial status data—including but not limited to data related to assets owned

²²² 31 U.S.C. §3353.

²²³ See definition at 31 U.S.C. §3351(2). See also "Noncompliance with PIIA" in CRS Report R48296, *Improper Payments: Ongoing Challenges and Recent Legislative Proposals*, by Garrett Hatch.

²²⁴ PaymentAccuracy.gov, Annual Improper Payments Dashboard, "DOE FY 2024 Supplemental Payment Integrity Information," https://tableau.d2d.gsa.gov/views/AnnualPaymentIntegrityReportDraft_09302022/SupplementalPaymentIntegrityInformation.

²²⁵ OMB, *Transmittal of Appendix C to OMB Circular A-123, Requirements for Payment Integrity Improvement*, M-18-20, June 26, 2018, p. 24, <https://bidenwhitehouse.archives.gov/wp-content/uploads/2018/06/M-18-20.pdf>. This memorandum (M-18-20) was revised by M-21-19 following enactment of the PIIA.

²²⁶ This is an example from the Department of Transportation as reported by the agency on PaymentAccuracy.gov, Annual Improper Payments Dashboard, "DOT FY 2024 Supplemental Payment Integrity Information," https://tableau.d2d.gsa.gov/views/AnnualPaymentIntegrityReportDraft_09302022/SupplementalPaymentIntegrityInformation.

or to credit history—as one of the top causes of overpayments. While the DNP system contains some debt-related databases (e.g., the debt check database from the Treasury Offset Program [TOP] and the Credit Alert Interactive Voice Response System [CAIVRS]), that specific type of financial data may be insufficient or irrelevant for what is needed to establish payment eligibility on the basis of a particular aspect of financial status.

Meeting Data Needs

While data access issues are viewed as a root cause of improper payments, what specific data need to be accessed in the process of determining payment eligibility is a consideration for federal programs. For some federal programs, specific data systems or data sources have to be reviewed or consulted, and use of the DNP may be one additional database system to integrate into that review process. Increasing the number of databases to review, however, does not necessarily mean the same thing as providing access to the specific data agencies need to review to determine payment eligibility.

For example, GAO reported that state governments use 34 data sources to verify income or assets for six federally funded, state-administered programs, including databases from federal, state, and commercial sources.²²⁷ The number of data sources needed is due to (1) the challenge of obtaining access to data; (2) the resource-intensiveness of obtaining access; and, (3) given such access challenges and resource intensity, the tradeoffs among data sources in comprehensiveness, timeliness, and other measures of accuracy needed for income verification purposes.²²⁸ These data-related tradeoffs, as GAO has reported, may affect program integrity and program efficiencies.

GAO has also reported that some federal agencies use commercial sources of data for program integrity activities, despite the availability of federal data, because the federal agencies that could source data cannot provide the level of service and investment in data needed.²²⁹ These data services include collecting, maintaining, and verifying data and providing the infrastructure to support such services, including related information technologies. Additionally, agencies consider a number of data quality features when deciding what data to use in association with their program integrity activities, including the accuracy of the data, the data's timeliness, the completeness of the data, and the technical aspects of using and processing the data within an agency's operating environment, including its information technology systems.²³⁰

Policy Considerations

To address potential limitations in the data accessible via the DNP system, and increase access to those data needed to prevent improper payments, Congress could consider naming additional databases as part of the DNPI. In some years, the Treasury Department has proposed legislation that would, in effect, make certain databases accessible through the DNP system. For example, in its FY2024 congressional budget justification, the department sought legislation that would permit the Fiscal Service to provide access to the National Directory of New Hires (NDNH) via the DNP system to those agencies that are authorized under the Social Security Act to use NDNH

²²⁷ GAO, *Federal Low-Income Programs: Use of Data to Verify Eligibility Varies Among Selected Programs and Opportunities Exist to Promote Additional Use*, GAO-21-183, February 2021, p. 13, <https://www.gao.gov/assets/d21183.pdf>.

²²⁸ GAO, *Federal Low-Income Programs*, pp. 34-37.

²²⁹ GAO, *Program Integrity: Views on the Use of Commercial Data Services to Help Identify Fraud and Improper Payments*, GAO-16-624, June 2016, p. 9, <https://www.gao.gov/assets/gao-16-624.pdf>.

²³⁰ GAO, *Program Integrity*, pp. 11-20.

data.²³¹ A second legislative proposal for FY2024 called for an amendment to the Fair Credit Reporting Act (FCRA) that would authorize the DNP system to use data aggregators, such as credit reporting agencies, for income and residency data.²³²

Congress might also consider addressing specific statutory barriers that prevent the Fiscal Service from making certain data accessible to payment-issuing agencies through the DNP system. For example, some members of Congress have introduced legislation that would make the DMF-Full permanently accessible to the Treasury Department and thus to agencies via the DNP system.²³³ GAO has also made this recommendation about the DMF-Full.²³⁴ As presented in **Table 1**, issues accessing death data do result in overpayments, as reported by agencies, though to a lesser extent than other data types. When debating on whether to statutorily designate certain databases for use as a DNPI database, policymakers may consider the extent to which that database addresses the data needs of agencies.

Similarly, when Congress considers legislation that would in essence establish an eligibility verification data system, it may consider to what extent these new systems (1) address the data needs of agencies, (2) interface with the DNP system, or (3) are designed to account for some of the issues that have been reported on in terms of data accuracy, data timeliness, and data completeness for eligibility determinations.²³⁵ While data access may be necessary to prevent improper payments, some data may not meet the needs of agencies. Conversely, Congress may also give further consideration to the availability—or absence—of data when requiring that payment eligibility be based on some criteria that will need to be verified.

The Authority of the Office of Management and Budget Director to Designate Databases as Part of the Do Not Pay Initiative

While additional databases for the DNPI and the DNP system could be sourced from federal agencies, some of GAO's reporting suggests that some federal data is not necessarily in a state that facilitates the kind of use needed in program integrity activities, including payment eligibility determinations.²³⁶

Congress arguably realized some of the ways that federal data is imperfect or insufficient for particular agency needs and uses. The commercial use of data within the working system was specifically included in IPERIA 2012 “for fraud and systemic improper payments detection through analytic technologies and other techniques.”²³⁷ The PIIA affords the OMB Director the

²³¹ Treasury Department, *Department of the Treasury Bureau of the Fiscal Service Congressional Budget Justification and Annual Performance Plan and Report FY2024*, p. 10, <https://home.treasury.gov/system/files/266/17.-Fiscal-Service-FY-2024-CJ.pdf>. For more information on NDNH, see CRS Report RS22889, *The National Directory of New Hires: An Overview*, by Jessica Tollestrup, particularly the section titled, “Entities That May Receive NDNH Data.”

²³² FCRA is 15 U.S.C. §§1681 et seq. 15 U.S.C. §1681b prescribes the permissible uses of consumer credit reports, which includes, for example, for use in determinations of eligibility for a benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status (15 U.S.C. §1681b(a)(3)(D)).

²³³ See, for example, S. 269 and H.R. 2716 in the 119th Congress and S. 2492 in the 118th Congress. Refer to the section titled, “Sourcing Databases for the Do Not Pay System,” of this report for a short discussion of the issues related to the DMF-Full.

²³⁴ GAO, *Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated \$233 Billion to \$521 Billion Annually to Fraud, Based on Various Risk Environments*, GAO-24-105833, April 2024, p. 69, <https://www.gao.gov/assets/gao-24-105833.pdf>.

²³⁵ Examples of such systems include those that would be established under S. 1807 and H.R. 1755 in the 119th Congress.

²³⁶ GAO, *Program Integrity*, p. 9.

²³⁷ §5(d)(2)(c).

latitude to designate databases, including commercial databases, as DNPI databases.²³⁸ The exercise of this authority has resulted in the accessibility of additional data, including some commercial databases, through the DNP system.

For example, in June 2025, the OMB Director proposed to designate the use of the Department of Veterans Affairs' (VA's) Benefits Enterprise Platform (BEP) in conjunction with the Public Assistance Reporting Information System (PARIS) via the DNP system.²³⁹ According to the notice, the BEP data

will strengthen program integrity across programs and agencies by facilitating: (A) income verification (a process by which States compare income reported to the State by the client to income the client is actually receiving according to the BEP database) and (B) the coordination of benefits (e.g., between [state-administered] Medicaid and VA benefits).

PARIS is administered by the Administration for Children and Families (ACF), a component of HHS, and it is designed for use by state governments administering federal benefit programs to determine whether program applicants or benefit recipients are receiving benefits in other states.²⁴⁰ PARIS is not technically a DNPI database or part of the DNP system, either by statute or the OMB Director's designation. Instead, there is a memorandum of agreement between ACF and the Fiscal Service that (1) establishes the Fiscal Service as the provider of the interstate data matching that is necessary for the operations of PARIS and (2) forms the basis for a separate matching program between the states that participate in PARIS and the Fiscal Service for the DNP system.²⁴¹ Thus, designation of the BEP to the DNP system expands the data provided to state governments only in the context of their use of PARIS. According to the notice, the BEP data would not be accessible to federal agencies.

The PIIA, however, is not the sole statutory authority that could be exercised by the OMB Director to establish the sharing of a federal database with other federal agencies. The OMB Director has authority under the Paperwork Reduction Act of 1995 (PRA) to direct an agency to make information that the agency has collected available to another agency so long as the disclosure is not inconsistent with applicable law.²⁴² Thus, the director of OMB is positioned to facilitate interagency data access generally, in addition to the more specific purposes of preventing improper payments under the PIIA. Arguably, the OMB Director could use their PRA authorities to facilitate data sharing for the purposes of preventing improper payments, independent of the PIIA.

Policy Considerations

Congress could conduct oversight of how the OMB Director exercises their authority to designate databases for inclusion in the DNPI. The PIIA requires the OMB Director to consider any

²³⁸ 31 U.S.C. §3354(b)(1)(B).

²³⁹ OMB, "Proposed Designation of Database to the Do Not Pay Working System," 90 *Federal Register* 26831, June 24, 2025, <https://www.federalregister.gov/documents/2025/06/24/2025-11557/proposed-designation-of-database-to-the-do-not-pay-working-system>.

²⁴⁰ For more information on PARIS, see Department of Health and Human Services, Administration for Children and Families, "About," <https://acf.gov/paris/about>.

²⁴¹ *Memorandum of Agreement Among the Administration for Children & Families of the U.S. Department of Health & Human Services (HHS) and the U.S. Department of the Treasury, Bureau of the Fiscal Service Regarding Consultation and Information Sharing*, September 2024, https://acf.gov/sites/default/files/documents/paris/2024-ACF-PARIS_DNP-Agreement-signed-website.pdf.

²⁴² 44 U.S.C. §3510.

database that “substantially assists in preventing improper payments.”²⁴³ If it chooses to conduct oversight of how the OMB Director makes such designations of databases, Congress may seek additional information from OMB on how “substantially assists” is determined or demonstrated.

Additionally, in March 2025, President Trump issued E.O. 14243, “Stopping Waste, Fraud, and Abuse by Eliminating Information Silos.”²⁴⁴ The E.O. seeks to eliminate administrative barriers that prevent access to data and interagency data sharing, particularly when such data sharing may assist in efforts to detect overpayments and fraud. Agencies are directed to evaluate their guidance and regulations that govern data access, including their system of records notices (SORNs). As discussed in an earlier section of this report (see “Compliance with the Privacy Act”), these notices specify disclosures under the Privacy Act that are *routine uses*, which may form the basis for agencies to source databases for access via the DNP system and which agencies use to conduct searches of their intended payment recipients through the DNP system.

E.O. 14243 reinforces directions to agencies about amending routine uses in SORNs to accommodate disclosure to the DNP system in E.O. 14249, *Protecting America’s Bank Account Against Fraud, Waste, and Abuse*. In its August 2025 memorandum implementing E.O. 14249, OMB tasks agencies with identifying

which of the agency’s systems of records maintain information about applicants for, or recipients of, federal funds *that agencies use* to make eligibility determination for payments to beneficiaries, award and loan recipients, vendors, contractors, and other payees.²⁴⁵

In previous efforts to designate databases as part of the DNPI, OMB has stated that the agency maintaining a database proposed for designation would have to publish an amended SORN to authorize the disclosures to prevent improper payments and make the database accessible via the DNP system.²⁴⁶ Congress may wish to monitor the extent to which the number of DNPI databases is potentially increasing under these executive orders and whether access to those additional databases is reducing improper payments.

Lastly, policymakers could also use their oversight role to understand if and how agencies access and use the databases that have been designated as part of DNPI by the OMB Director but are not part of the DNP system. In its guidance on implementing the PIIA, OMB directs agencies to review these designated databases “that are outside of the Treasury Working System,” to verify payment eligibility.²⁴⁷ **Table A-1** includes those databases that are designated by the OMB Director as part of the DNPI but are not included in a listing from the Fiscal Service of databases accessible through the DNP system.²⁴⁸

OMB states that it has developed and follows procedures and criteria “to determine whether databases are designated into the Treasury Working System or included in the Initiative outside of the Treasury Working System.”²⁴⁹ In conducting oversight of these specific designations,

²⁴³ 31 U.S.C. §3354(b)(2)(A).

²⁴⁴ Executive Order 13681 of March 20, 2025, “Stopping Waste, Fraud, and Abuse by Eliminating Information Silos,” 90 *Federal Register* 14243, March 25, 2025, <https://www.federalregister.gov/documents/2025/03/25/2025-05214/stopping-waste-fraud-and-abuse-by-eliminating-information-silos>.

²⁴⁵ OMB, *Preventing Improper Payments and Protecting Privacy Through Do Not Pay*, M-25-32, p. 1 of Appendix I.

²⁴⁶ See OMB, “Do Not Pay Data Designation Analysis,” supporting and related material for *Proposed Designation of Databases for Treasury’s Working System under the Do Not Pay Initiative*, docket OMB-2021-0003-0001, January 21, 2021, <https://www.regulations.gov/document/OMB-2021-0003-0001>.

²⁴⁷ OMB, *Transmittal of Appendix C*, M-21-19, p. 31.

²⁴⁸ Bureau of the Fiscal Service, “What Can I Search,” <https://fiscal.treasury.gov/dnp/search.html>. Databases listed on this website as of July 14, 2025.

²⁴⁹ OMB, *Transmittal of Appendix C*, M-21-19, p. 31.

Congress could examine what factors are used to determine whether these designated databases are accessible via the DNP system or not.

Assessing the Cost-Effectiveness of Data Matching Using the Do Not Pay System to Agencies

Use of the DNP system comes with a cost to agencies that can be measured in terms of agency time and resources, including staff and technology. This is because data access via the DNP system is insufficient alone; data matching is needed to use the data that is accessible.

Congress recognized the costs of data matching when it considered and ultimately passed the CMPPA. In a House committee report on the CMPPA, committee members expressed doubt as to whether the practice of data matching had generally been established as cost-effective.²⁵⁰

The CMPPA contains several provisions that point toward Congress's concern of cost-effectiveness, including a requirement that a cost-benefit analysis be performed and be demonstrative of cost savings prior to the approval and start of a matching program.²⁵¹ These analyses are usually conducted as part of a computer matching agreement (CMA) and used to justify a matching program.²⁵²

Cost-Benefit Analyses

When the PIIA granted the Treasury Department the authority to waive the CMPPA's CMA requirement for certain cases of data matching involving use of the DNP system, the act effectively waived the conduct of the cost-benefit analysis that would otherwise be performed as part of the CMA approval process.

OMB's guidance to agencies on implementing the CMPPA suggests that conducting cost-benefit analyses of matching programs is neither about balancing individual protections and rights under the Privacy Act with cost savings, nor is it always the case to presume that any savings should prevail when tradeoffs with individual privacy are considered. Rather such cost-benefit analyses are to ensure sound agency management:

Particularly in a time when competition for scarce resources is especially intense, it is not in the government's interests to engage in matching activities that drain agency resources that could be better spent elsewhere. Agencies should use the [cost-benefit analysis] requirement as an opportunity to reexamine [matching] programs and weed out those that produce only marginal results.²⁵³

When there is no waiver under the PIIA, a CMA for a matching program using the DNP system should generally be accompanied by a cost-benefit analysis. These cost-benefit analyses, however, are not required under statute to contain a specific estimate of any cost savings to justify an agency's use of the DNP system.²⁵⁴ For example, a CMA between CMS and the Fiscal Service for a matching program using DNP system databases to verify the eligibility of providers and

²⁵⁰ U.S. Congress, House Committee on Government Operations, *Computer Matching and Privacy Protection Act of 1988*, report to accompany H.R. 4699, 100th Cong., 2nd sess., July 27, 1988, H.Rept. 100-802, pp. 13-14.

²⁵¹ 5 U.S.C. §552a(u)(4)(A).

²⁵² 5 U.S.C. §552a(o)(1)(B).

²⁵³ OMB, "Privacy Act of 1974; Final Guidance Interpreting the Provisions of, the Computer Matching and Privacy Protection Act of 1988," 54 *Federal Register* 25828, June 19, 1989, <https://www.govinfo.gov/content/pkg/FR-1989-06-19/pdf/FR-1989-06-19.pdf#page=128>.

²⁵⁴ 31 U.S.C. §3354(d)(1)(E). See also OMB, *Transmittal of Appendix C*, M-21-19, p. 33.

suppliers to bill Medicare calculates the costs of the matching program at \$351,430 for three years.²⁵⁵ The majority of these costs are borne by CMS, including costs to adjudicate matches in the DNP system's portal. The CMA notes that

[t]his [cost-benefit analysis] does not quantify amounts of improper payments avoided or recovered to offset the costs of conducting the matching program, so it does not demonstrate that the matching program is likely to be cost effective. However, the parties to this agreement have determined that a matching program is the most efficient, expeditious, and effective means of obtaining and processing the information needed to identify Medicare providers and suppliers who may be ineligible to receive federal payments or awards.²⁵⁶

The CMA provides further information on the cost efficiency of centralizing data access through the DNP system:

[B]enefits are gained through a single matching program using the Treasury's Do Not Pay Working System. These benefits include eliminating the need to manually compare data or execute separate matching agreements with multiple agencies. CMS' costs to detect disqualified providers and suppliers using those alternative methods would be significantly greater than the costs of conducting this matching program.²⁵⁷

While access to centralized data is beneficial for CMS, some agencies indicate that the DNP system duplicates some access to data they already have, such as the exclusion records from GSA's SAM. Thus, within the normal course of an agency's workflow to verify payment eligibility, the DNP system may represent an additional system to use, adding time and thus agency costs for completing administrative processes. In particular, other data systems or data sources used by agencies to determine eligibility may not require the additional steps required by the DNP system, such as the adjudication of data matches.

Some agencies, however, use federal shared service providers (FSSPs) for payment processing and may be indirect users of the DNP system as a result of this arrangement. For these agencies, their costs to be users of the DNP system may be lower, in part because these costs are borne indirectly through the FSSP. Thus, there may be different cost-related considerations for different agencies.

Data Quality in Cost-Benefit Analyses

Another issue that may factor into cost-benefit analyses for agencies is data quality. As noted in a GAO report, data quality is a factor that agencies consider when assessing the data needed for payment eligibility.²⁵⁸ While the GAO report centered on the quality of data from commercial sources, the same considerations about data quality are likely to extend to data from federal sources.

Some agencies report encountering inaccurate data while using the DNP system. For example, in FY2024, of the 48 agencies that use the DNP system and supply information for

²⁵⁵ *Computer Matching Agreement Between Department of Health and Human Services Centers for Medicare and Medicaid Services and U.S. Department of Treasury Bureau of the Fiscal Service for the Do Not Pay Initiative*, HHS computer match no. 2020-04, effective October 13, 2020, p. 21, <https://www.hhs.gov/sites/default/files/cms-irs-do-not-pay-cma-2004-508.pdf>.

²⁵⁶ *Computer Matching Agreement Between CMS and Bureau of the Fiscal Service for the Do Not Pay Initiative*, p. 22.

²⁵⁷ *Computer Matching Agreement Between CMS and Bureau of the Fiscal Service for the Do Not Pay Initiative*, p. 5.

²⁵⁸ GAO, *Program Integrity*, pp. 11-20.

PaymentAccuracy.gov, 19 reported identifying incorrect information at various frequencies, including on daily, weekly, and monthly bases.²⁵⁹

Data quality may appear as an issue in the operations of the DNP system in a number of ways, including false positive matches. It is unclear if the inaccuracies reported by agencies are more likely to be associated with certain databases or if there are discernable patterns in the types of inaccuracies observed by agencies (e.g., an individual taxpayer identification number [ITIN] matches to an SSN).²⁶⁰ The matching logic behind the portal functionality of the DNP system does not differentiate between SSNs, EINs, or ITINs, all of which are nine-digit identifiers, and the Fiscal Service states that it is incumbent on the paying agency to consider whether an identifying number corresponds to an individual or an entity when evaluating a match.²⁶¹ At one time, OMB suggested that false positive matches involving use of the DNP system's payment integration functionality could be burdensome to agencies, which could be a reason for an agency to seek an exception to a requirement to use it.²⁶² Data that is not up to date may be another data quality issue.

Concerns about the quality of the data in the DNP system may be factored into cost calculations by agencies when deciding to use it. In its CMPPA guidance, OMB indicated that data quality carries real costs to agencies:

Record accuracy is important from two standpoints. In the first case, the worse the quality of data, the less likely a matching program will have a cost-beneficial result. In the second case, the Privacy Act requires Federal agencies to maintain records ... in systems of records to a standard of accuracy that will reasonably assure fairness in any determination made on the basis of the record.²⁶³

The characterization of data quality as a cost may be more salient in cases where such data is used in adverse decisionmaking against an individual. Such adverse decisions impose additional costs on agencies in terms of notices (e.g., mail costs), preparing for possible hearings, and other adjudicative processes required under a program. While data quality may be more costly for some agencies because of these additional downstream expenses, it may be less costly for others that do not have such processes.

Policy Considerations

Congress may be satisfied with the way the PIIA requires executive branch agencies to use the DNP system to review all payments for eligibility and how implementation of that mandate has

²⁵⁹ CRS analysis of the information reported for FY2024 on PaymentAccuracy.gov.

²⁶⁰ ITINs and SSNs are both nine-digit identifiers and use the same format of "XXX-XX-XXXX," where each X is a number. The TIN program is administered by the IRS, whereas the assignment of SSNs is managed by SSA. ITINs start with a 9 and the fourth and fifth numbers of the identifier's numerical sequence is within a certain range of possible numbers (for more information, see <https://www.irs.gov/pub/irs-pdf/p4757.pdf>). Since 1996, SSA has not assigned SSNs that start with 9. ITINs expire under certain circumstances, whereas SSNs do not. The DNP system does not validate ITINs or SSNs. EINs use a different format (XX-XXXXXXX) than ITINs and SSNs and can start with a 9 (<https://www.irs.gov/businesses/small-businesses-self-employed/valid-eins>).

²⁶¹ Treasury Department Bureau of the Fiscal Service, "Understanding the DNP Portal Matching Logic," <https://fiscal.treasury.gov/files/dnp/dnp-portal-matching-logic.pdf>.

²⁶² OMB, *Transmittal of Appendix C to OMB Circular A-123, Requirements for Payment Integrity Improvement*, M-18-20, June 26, 2018, p. 62, <https://bidenwhitehouse.archives.gov/wp-content/uploads/2018/06/M-18-20.pdf>. M-18-20 was revised by M-21-19 following the enactment of the PIIA.

²⁶³ OMB, "Privacy Act of 1974; Final Guidance Interpreting the Provisions of, the Computer Matching and Privacy Protection Act of 1988," 54 *Federal Register* 25828, June 19, 1989, <https://www.govinfo.gov/content/pkg/FR-1989-06-19/pdf/FR-1989-06-19.pdf>.

followed. Without consideration to some of Congress's options, the DNP system may continue to prevent some number of improper payments, warranting the continued use of the system under the PIIA as it is. Recent executive orders and the guidance that accompanies their implementation may also factor into the effectiveness of the DNP system in the future. Appropriations, such as those requested by the Treasury Department for FY2026, might also be used to improve the effectiveness of the DNP system to agencies. Still, it might also be possible that some agencies may continue to report that the DNP system is not effective in preventing their improper payments, as noted above.

Congress could consider whether use of the DNP system is an effective way to prevent improper payments for every agency in every case. As discussed at the beginning of this report, the data access issues that lead to improper payments are varied, and multiple issues can work together at times to produce an agency's improper payments. While use of the DNP system is technically characterized by the Fiscal Service as a no-cost resource for agencies, use of the system may not be viewed by an agency as cost-effective. Agencies may assess their costs relative to their data needs and what is accessible through the DNP system when deciding whether and how to use it. Congress may thus consider the extent to which to enforce the PIIA's requirement to review all payments through the DNP system and monitor implementation of E.O. 14249, which directs compliance with the provisions of the PIIA that concern use of the DNP system.

Sometimes, the CMPPA's administrative requirements for CMAs and cost-benefit analyses are perceived as barriers to data access and more specifically to data matching, including for the prevention of improper payments and fraud reduction.²⁶⁴ As such, Congress has reworked how compliance with the CMPPA operates in the context of payment integrity in order to ease that burden. Congress may reconsider if some cost-benefit analyses are informative for agencies in deciding whether or how to use the DNP system. Such analyses may demonstrate different savings and returns to an agency, particularly if information relevant to the operations of the DNP system changes, such as new databases or new functionalities.

Conclusion

The policy contexts in which some centralized data systems may operate can be complex to untangle, partly because of the sheer accumulation of policies that may be relevant and potential conflict or tension among such policies. There is no single policy that governs payment eligibility. Instead, federal payment policies vary in how payment eligibility is determined. This variation challenges the idea that the DNP system might systematically prevent improper payments through payment eligibility verification. Payment eligibility is not solely a function of a data match in the DNP system, but this data matching is foundational to the system's operations and thus its value proposition. Thus, there is somewhat of a disconnect between the intent of the data matching that occurs through the DNP system and the various policy considerations that agencies take stock of when determining payment eligibility. Even if every federal agency, program, and activity were using the DNP system as intended by the PIIA, there remain different laws and regulations governing eligibility for different payments (e.g., contractor payments versus entitlement payments) and thus separate considerations for determining payment eligibility that the DNP system does not necessarily address.

The DNP system itself, at least as it currently operates, does not necessarily assist agencies in sorting through the relevant policy considerations given a data match within the system.

²⁶⁴ GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP, July 2015, p. 7, <https://www.gao.gov/assets/gao-15-593sp.pdf>.

Moreover, in some cases, matches from the DNP system are irrelevant, furthering the idea that the operations of the system are to a certain degree disconnected from payment eligibility policies. But the absence of a data match also does not confer eligibility upon a payment. This is because the DNP system is not an eligibility system per se; agencies often require more information and data from other sources as part of the eligibility determination process.

Anticipating and managing the breadth of policy issues that are relevant to the operations of a centralized data system like the DNP system might be a consideration when Congress authorizes such systems through legislation or enables them through appropriations. There are also practical, implementation-related issues to consider. If a goal of curbing improper payments is to control spending, then one issue to balance is the usefulness of the DNP system to agencies in the payment process. The usefulness of a centralized data system can be measured at least partly in terms of costs and benefits, which may vary from agency to agency or program to program, and which may also vary with the specific ways the system is designed to operate and the specific data that is accessible through the system. Centralized data systems may supplant, supplement, or otherwise operate within the environments, processes, workflows, and decisions an agency has implemented over time to manage compliance with various policies and regulations. Introducing and mandating the use of a new data system can disrupt these existing operations with or without a discernible effect. Congress might seek to address these policy and practical issues when pursuing legislative solutions that rely on centralizing data access within a single system.

Appendix. Do Not Pay Initiative Databases

Table A-1. Databases Included in the Do Not Pay Initiative and Part of the Do Not Pay System

31 U.S.C. §3354(b)(1)

Database	Data Provider	Description of Database	Reason for Inclusion	Accessible via the DNP system ^a
Deceased Data	Commercial (American InfoSource)	Incorporates the public version of the Social Security Administration's (SSA's) Death Master File in addition to information on deceased individuals from obituaries, funeral homes, newspapers, and county court probate records.	Designated ^b	Yes
Death Master File ("DMF-Full")	Social Security Administration (SSA)	Contains records of deaths reported to SSA, including those made by family members, funeral homes, financial institutions, postal authorities, state vital records offices, and other federal agencies.	Statute (31 U.S.C. §3354(a)(2)(A))	Yes ^c
Electronic Verification of Vital Events, Fact of Death (EVVE FOD)	Commercial (National Association for Public Health Statistics and Information Systems)	Facilitates access to vital statistics databases from state governments, providing access to information on deceased individuals from state vital records offices that participate in data sharing.	Designated ^d	Yes
Department of Defense Death Data	Department of Defense	Provides information on confirmed or presumed deaths of active-duty members of the U.S. military and its reserves.	Statute (31 U.S.C. §3356(a))	Yes
Department of State Death Data	Department of State	Contains records of U.S. citizens who are deceased or presumed deceased as reported by U.S. embassies or consulates upon receipt of a foreign death certificate or finding of death by a competent local authority.	Statute (31 U.S.C. §3356(a))	Yes
Automatic Revocation of Exemption List (ARL) (Part of the Tax Exempt Organization Search [TEOS])	Internal Revenue Service (IRS)	Identifies entities that have had their tax-exempt status automatically revoked under the law because they have not filed IRS Form 990 series returns or notices for three consecutive years.	Designated ^b	Yes
Publication 78 (also known as "Select Check" or "Pub 78 Data"; part of the Tax Exempt	IRS	Identifies organizations that can receive tax-deductible charitable contributions, pursuant to requirements that such organizations with gross receipts over \$50,000 file IRS Form 990 once every three years to retain their tax-exempt status.	Designated ^b	Yes

Database	Data Provider	Description of Database	Reason for Inclusion	Accessible via the DNP system ^a
Organization Search [TEOS])				
Form 990-N (also known as “e-Postcard”; part of the Tax Exempt Organization Search [TEOS])	IRS	Identifies organizations that are eligible to file IRS Form 990-N (e-Postcard), which is an annual electronic filing that can be used by small tax-exempt organizations with gross receipts under \$50,000.	Designated ^b	Yes
List of Excluded Individuals and Entities (LEIE)	Department of Health and Human Services (HHS) Office of the Inspector General (OIG)	Identifies individuals and entities currently excluded by the HHS OIG from participation in Medicare, Medicaid, and all other federal health care programs, pursuant to its authorities under the Social Security Act.	Statute (31 U.S.C. §3354(a)(2)(E))	Yes
Specially Designated Nationals List	Treasury Department Office of Foreign Assets Control	Identifies individuals and companies owned by, controlled by, or acting for or on behalf of <i>targeted countries</i> . It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. <i>Specially Designated Nationals</i> (SDNs) have their assets blocked, and U.S. persons, including the government, are generally prohibited from doing business or entering into financial transactions with them.	Designated ^b	Yes
System for Award Management (SAM) Entity Registration Records	General Services Administration (GSA)	Identifies entities that are registered in SAM, pursuant to 2 C.F.R. §25.200(b)(1-2)—which applies to any entity seeking or receiving federal financial assistance—and pursuant to FAR §4.1102—which applies to contractors seeking to be an offeror or quoter.	Designated ^b	Yes
SAM Exclusion Records	GSA	Identifies those persons that an agency has taken action to exclude or disqualify under the nonprocurement or procurement debarment and suspension system.	Statute (31 U.S.C. §3354(a)(2)(B))	Yes
Department of Agriculture (USDA) National Disqualified List	USDA	Identifies providers that are ineligible to receive federal funding to provide meals under the Child and Adult Care Food Program and potentially under other food programs due to a finding of serious deficiency in administration or documentation of the provider’s programs.	Designated ^e	Yes
HHS National Plan & Provider	HHS	Contains information on health care providers and health plans that have been assigned a National Provider Identifier	Designated ^e	Yes

Database	Data Provider	Description of Database	Reason for Inclusion	Accessible via the DNP system ^a
Enumeration System		(NPI), which is unique to a provider, organization, or other <i>covered entity</i> that has applied for an NPI pursuant to federal law and implementing regulations.		
Credit Alert Verification Reporting System (also known as the Credit Alert Interactive Voice Response System [CAIVRS])	Department of Justice (DOJ), Department of Housing and Urban Development, Small Business Administration, USDA, and Department of Veterans Affairs (VA)	Identifies individuals who are delinquent or have defaulted on federal direct or guaranteed loan repayments.	Statute (31 U.S.C. §3354(a)(2)(D))	Yes
Treasury Offset Program (TOP) Debt Check	Treasury Department	Identifies individuals who are delinquent on non-tax debts if allowed by agency statute and regulations and child support obligations as reported by states.	Statute (31 U.S.C. §3354(a)(2)(C))	Yes
Federal Inmate Database (SENTRY)	DOJ BOP	Identifies individuals who are committed by a court to the custody of the Attorney General and housed in a federal prison facility.	Designated ^e	Yes
DNP Adjudication Data	Bureau of the Fiscal Service	Contains information from users of the Do Not Pay system (e.g., federal agencies) on their determinations of whether a payment was adjudicated as proper, improper, or under review, including any comments associated with the determination.	Designated ^e	Yes
Prisoner Updated Processing System (PUPS)	SSA	Contains information reported to SSA by state and local correctional facilities, including jails and prisons, pursuant to agreements that are permitted but not required under Sections 202(x) and 1611(e) of the Social Security Act (42 U.S.C. §§ 402(x) and 1382(e)).	Statute (31 U.S.C. §3354(a)(2)(F))	No
Payments, Claims, and Enhanced Reconciliation (PACER)	Bureau of the Fiscal Service	Contains records of any action taken after a payment has been disbursed, including any offset, disputes, payment reclamation, and returns of funds by a financial institution due to the death of an account holder.	Designated ^e	Yes
Delivery Sequence File	United State Postal Service	Contains validated records for vacant, residential, business, and seasonal addresses.	Designated ^e	No
Federal Audit Clearinghouse	Department of Commerce Census Bureau	Contains the audit records, including indicators for findings of significant vulnerability, completed on organizations	Designated ^e	No

Database	Data Provider	Description of Database	Reason for Inclusion	Accessible via the DNP system ^a
		that spend more than \$750,000 in federal grant funding. ^f		
USASpending	Treasury Department	Contains federal spending data from agencies, pursuant to the requirements of the Digital Accountability and Transparency Act (DATA Act; P.L. 113-101) to make certain information available on USASpending.gov.	Designated ^e	No
American Community Survey (ACS) Annual State and County Data Profiles	Department of Commerce Census Bureau	Contains the publicly available information reported by individuals and households, including their income, receipt of certain federal benefits, veteran status, and employment.	Designated ^e	No
Beneficiary Identification Records Locator Service (BIRLS) ^g	VA	Contains information on veterans of the U.S. military, including their address, whether their service was active duty or within a military reserve component, benefits they are receiving, and whether the veteran is deceased.	Designated ^e	No
Statistics of Income (SOI) Annual Individual Income Tax Zip Code Data	IRS	Contains data from individual income tax returns filed with the IRS that is organized by size of adjusted gross income and aggregated by zip code and by state, including but not limited to the total number of returns, total number of returns claiming a credit, and the total dollar value of the credit.	Designated ^e	No
Electronic Data Gathering, Analysis, and Retrieval (EDGAR) System	Securities and Exchange Commission	Contains information submitted by companies and others pursuant to various laws and regulations that contain reporting requirements, including registration statements and annual and quarterly financial reports.	Designated ^e	No
Death Notification Entries (DNEs)	Bureau of the Fiscal Service	Contains a subset of payment and post-payment data provided by federally funded programs that disburse funds through the Treasury Department, including payees that have been identified by paying agencies. DNEs are sent to financial institutions to support their identification of accounts belonging to decedents and preventing further federal payments to such accounts.	Designated ^h	Yes
Account Verification Services (AVS)	Bureau of the Fiscal Service through a Financial Agent ⁱ	Uses a commercial database source of real-time bank data from a network of banks to validate identity and bank account information, verifying that the bank account owner information matches an agency's intended recipient.	Designated ^h	Yes ⁱ

Database	Data Provider	Description of Database	Reason for Inclusion	Accessible via the DNP system ^a
Benefits Enterprise Platform (BEP)	VA	Contains information on the compensation and pension benefits of veterans of the U.S. military.	Designated ^k	Yes to state governments that also use the Public Assistance Reporting Information Service (PARIS)

Source: The Payment Integrity Information Act (PIIA; P.L. 116-117); Bureau of the Fiscal Service; CRS analysis of *Federal Register* notices published by OMB.

Notes:

- a. According to information available from the Bureau of the Fiscal Service as of July 14, 2025 (<https://fiscal.treasury.gov/dnp/search.html>).
- b. OMB, “Designation of Databases for Treasury’s Working System Under the Do Not Pay Initiative,” 82 Federal Register 55880, November 24, 2017, <https://www.federalregister.gov/documents/2017/11/24/2017-25416/designation-of-databases-for-treasurys-working-system-under-the-do-not-pay-initiative>.
- c. As noted earlier in this report (see footnote 119), the accessibility of the DMF-Full through the DNP system is temporary, as an amendment to Section 205(r) of the Social Security Act (42 U.S.C. §405(r)) that facilitates this access will expire on December 27, 2026. Legislation has been introduced to make accessibility via the DNP system permanent (e.g., S. 269 and H.R. 2716 in the 119th Congress).
- d. OMB, “Designation of Database for Treasury’s Working System Under the Do Not Pay Initiative,” 87 Federal Register 2941, January 19, 2022, <https://www.federalregister.gov/documents/2022/01/19/2022-00889/designation-of-database-for-treasurys-working-system-under-the-do-not-pay-initiative>.
- e. OMB, “Designation of Databases for Treasury’s Working System Under the Do Not Pay Initiative,” 86 Federal Register 26071, May 12, 2021, <https://www.federalregister.gov/documents/2021/05/12/2021-10025/designation-of-databases-for-treasurys-working-system-under-the-do-not-pay-initiative>.
- f. The threshold for such audits was \$750,000 at the time of OMB’s designation. OMB increased the threshold to \$1,000,000 in April 2024. See 2 C.F.R. Part 200 Subpart F (§§200.500-200.51).
- g. BIRLS is included here as it was designated by OMB. Subsequent to OMB’s designation in May 2021, the VA published a Federal Register notice in October 2021 that it was terminating use of BIRLS, that data from BIRLS was migrated to other systems, and that BIRLS data would be associated with a different system of records notice (SORN) (see 86 Federal Register 56761, <https://www.federalregister.gov/documents/2021/10/12/2021-22151/privacy-act-of-1974-system-of-records>).
- h. OMB, “Designation of Databases to the Do Not Pay Working System,” 89 Federal Register 86842, October 31, 2024, <https://www.federalregister.gov/documents/2024/10/31/2024-25234/designation-of-databases-to-the-do-not-pay-working-system>.
- i. Financial agents are financial institutions (e.g., banks) that have been designated by the Treasury Department to provide certain financial services to the federal government. These designations are the subject of 31 C.F.R. §202.
- j. The Bureau of the Fiscal Service has indicated this data will be available beginning in August 2025 but also notes that the date is subject to change (<https://fiscal.treasury.gov/files/dnp/avs-qrc-api.pdf>).
- k. OMB, “Designation of Database to the Do Not Pay Working System,” 90 Federal Register 46417, September 26, 2025, <https://www.federalregister.gov/documents/2025/09/26/2025-18680/designation-of-database-to-the-do-not-pay-working-system>.

Author Information

Natalie R. Ortiz
Analyst in Government Organization and
Management

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.