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

March 5, 2021

M-21-19

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Robert Fairweather
Acting Director

SUBJECT: Transmittal of Appendix C to OMB Circular A-123, Requirements for Payment Integrity Improvement

This Administration will continue to make payment integrity a top priority, focusing on reducing improper payments and protecting taxpayer money a top priority. This includes balancing payment integrity risks and controls to ensure funding is serving its intended purpose. By focusing on taking appropriate actions at the front end to prevent improper payments from being made while also acknowledging the need to balance payment integrity risk and controls, this guidance presents a payment integrity framework that will transform the way agencies improve payment integrity.

One of the priorities in this guidance is reducing administrative burden to allow agencies to focus on preventing improper payments and ensuring taxpayer money is serving its intended purpose. Requirements for payment integrity should not negatively affect program mission, agency efforts to advance equity, efficiency, customer experience, or the overall operations of the agency; therefore, this guidance aims to ensure that federal agencies focus on identifying, assessing, prioritizing, and responding to payment integrity risks to prevent improper payments in the most appropriate manner.

The goal of this revised version of OMB Circular A-123's Appendix C is to transform the payment integrity compliance framework and create a more comprehensive and meaningful set of requirements to allow agencies to spend less time complying with low-value activities and more time researching the underlying causes of improper payments, balancing payment integrity risks and controls, and building the capacity to help prevent future improper payments.

Appendix C to OMB Circular A-123 (which was last updated in June 2018 as OMB Memorandum M-18-20) is hereby modified. Unless otherwise noted in the guidance, the requirements found in Appendix C are effective starting in Fiscal Year 2021.

Please contact Heather Pajak (hpajak@omb.eop.gov) in OMB's Office of Federal Financial Management with any questions regarding this guidance.

Attachment

APPENDIX C

Requirements for Payment Integrity Improvement

Contents

Introduction

Appendix C to OMB Circular A-123 (which was last updated in June 2018 as OMB Memorandum M-18-20, *Requirements for Payment Integrity Improvement*) is hereby modified. Unless otherwise noted, the requirements found in this guidance are effective for Fiscal Year (FY) 2021. This guidance implements the requirements from the Payment Integrity Information Act of 2019 (PIIA).

Throughout the Appendix, the terms "Must" and "Will" denote a requirement that management will comply in all cases. "Should" indicates a presumptively mandatory requirement except in circumstances where the requirement is not relevant for the Agency. "May" or "Could" indicate best practices that may be adopted at the discretion of management. The appendix to this circular contains important terms and definitions. The Agency should consult the terms and definitions in the appendix in conjunction with the main body of this circular for a full understanding of the guidance. Members of the Executive Branch of the Federal Government should consult the Payment Integrity Question and Answer Collection forum if they have questions about this guidance.

Overview

The following paragraphs of this section provide a cursory overview of some of the key Appendix C concepts and requirements. The agency is responsible for consulting the statute, this guidance, and other guidance to both determine applicability of requirements and execute/apply them accordingly. In addition, the agency is responsible for maintaining documentation of fulfilling requirements in this guidance.

Definitions and Abbreviations– Terminology used in Appendix C to Circular A-123 is defined in Appendix 1A and should be consulted in conjunction with the main body of this circular for full understanding and implementation of the guidance. Use of abbreviations is defined in Appendix 1B. (See Sections VIII and IX of this guidance)

Phase 1 and Phase 2 – All programs with annual outlays over $10,000,000 will fall into one of two possible classifications: Phase 1 or Phase 2. Programs that are not likely have an annual amount of improper payments (IP) plus an annual unknown payments (UP) above the statutory threshold (which is either (1) both 1.5 percent of program outlays and $10,000,000 of all program payments made during the FY or (2) $100,000,000) are referred to as being in 'Phase 1'. If a program in Phase 1 determines that it is likely to annually make IPs plus UPs above the statutory threshold then the program will move into 'Phase 2' the following year. Once in Phase 2 a program will have additional requirements such as reporting an annual IP and UP estimate. (See Section II of this guidance)

Types of Payments – All program outlays will fall in one of three possible categories: proper payment; IP; or UP. If a program is in Phase 2 it will need to identify whether the IP is a monetary loss type IP or whether the IP is a non-monetary loss type IP. Programs reporting in Phase 2 will also need to identify their UPs. (See Section I of this guidance)

Improper Payment Risk Assessments – Each program with annual outlays over $10,000,000 must conduct an IP risk assessment at least once every three years to

determine whether the program is likely to have IPs above the statutory threshold. Programs that are not likely to have IPs above the statutory threshold are referred to as being in 'Phase 1'. (See Section II.A of this guidance)

Reporting an Improper Payment Estimate – If the results of a program's IP Risk assessment determine that the total annual IPs PLUS the unknown payments (UP) for the program are likely to be above the statutory threshold, the program will report an IP estimate and a UP estimate in the FY following the FY in which the determination was made. Programs that report IP and UP estimates are referred to as being in 'Phase 2'. (See Section II.B of this guidance)

Causes –Determining the point in the payment process where the payment turned from 'proper' to 'improper' is important when identifying the root cause of the IP and the UP. All programs reporting in Phase 2 will be required to determine the root cause of each IP and each UP and report accordingly. (See Section III of this guidance)

Prevention - To be effective, programs should prioritize efforts toward preventing IPs and UPs from occurring so that they can avoid operating in a "pay-and-chase" environment. All programs should have a structured and systematic approach to recognizing where the potential for IPs and UPs can arise and subsequently addressing the risk, as appropriate. (See Section IV of this guidance)

Payment Integrity Risk Management: The Enterprise Risk Management framework can be used to assist in the identification and management of payment integrity risks for the agency. A significant risk in managing IP risk is the potential that agencies may make investments in risk controls that negatively affect program mission, efficiency, customer experience or the overall operations of the agency. By including an evaluation of payment integrity risk in the Agency Risk Profile, agencies will identify, assess, prioritize, and respond to payment integrity risks and implement control activities to mitigate identified material payment integrity risks. (See Section IV.A of this guidance)

Corrective Action Plan – All programs in Phase 2 that are reporting estimates above the statutory threshold must have a Corrective Action Plan. The Corrective Action Plan is a combination of both mitigation strategies and corrective actions aimed at reducing the likelihood of an IP and/or a UP occurring during the payment process. (See Section IV.B of this guidance)

Tolerable Rate - All programs in Phase 2 should be mindful of the extent to which applying further payment controls would undercut the program's mission or resource management. The tolerable rate of a program should be established by the Agency's senior management, taking into consideration thresholds in PIIA that are used to help identify programs that are likely to be susceptible to IPs. (See Section IV.F of this guidance)

Overpayment Identification – Examples of overpayment identification methods Agencies use include but are not limited to reviews, audits, data analytics, reports, and reconciliations. Each agency must determine the most cost-effective method for their particular circumstance. (See Section V.A of this guidance)

Overpayment Recovery – All programs with overpayments must have a Recovery Audits and Activities Program regardless of which Phase they are operating in. However, a recovery audit should only be a part of the Recovery Audits and Activities Program if it is cost-effective. (See Section V.B of this guidance)

Compliance – Every year, each agency Inspector General (IG) reviews relevant IP and UP reporting and records pertaining to the programs within an agency to determine whether the agency complies with PIIA and OMB guidance. (See Section VI of this guidance)

Non-Compliance Actions – Each year than an IG determines a program is non-compliant, the agency has specific actions that must be taken. The agency actions required will depend on the number of consecutive years the program has been non-compliant. (See Section VI.D of this guidance)

Reporting - At a minimum, there are reporting requirements that apply to all agencies with programs in Phase 1 as well as those with programs in Phase 2. (See Section VII of this guidance)

High-Priority Programs - To be a High-Priority program, a program must be reporting in Phase 2 AND report IPs resulting in monetary loss in excess of $100,000,000 annually. In addition to the reporting that all programs in Phase 2 must complete, High-Priority programs must provide quarterly Payment Integrity Scorecard reporting on www.paymentaccuracy.gov. (See Section VII.B of this guidance)

I. Payment Types

For purposes of PIIA implementation, all program outlays will fall in one of three possible payment type categories: proper payment; IP; or UP. At a high level, a payment is 'proper' if it was made to the right recipient for the right amount, a payment is 'improper' if it was made in an incorrect amount or to the wrong recipient, and for instances where an agency is unable to determine whether the payment falls into the proper or improper category that payment should be considered an 'unknown' payment. Programs should use reasonableness when deciding which of the three buckets a payment falls into.

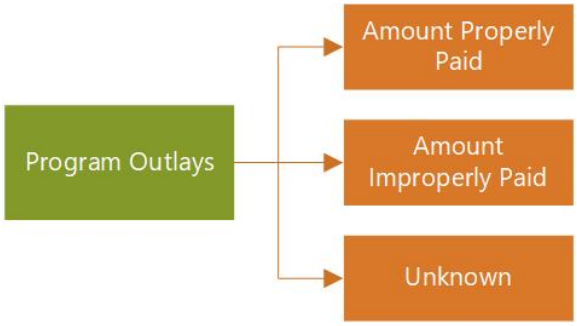

Figure 1 Payment Type Categories

A. Types of Improper Payments

All IPs will fall into one of two categories: (1) IPs resulting in a monetary loss or (2) IPs that do not result in a monetary loss. The monetary loss IPs have an overpayment amount that, in theory, should/could be recovered whereas the non-monetary loss IPs do not have any associated transfer of Federal funds that were in excess and therefore cannot be recovered.

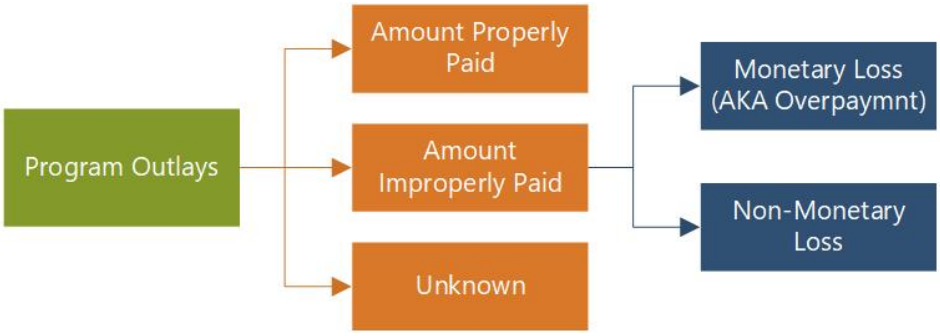

Figure 2. Improper Payment Type Categories

1. Monetary Loss Improper Payments

Although working to reduce all IPs is important goal, the prevention of IPs resulting in a monetary loss should be the highest priority. Both unintentional and intentional IPs that result in a monetary loss jeopardize agency missions by diverting resources from their intended purpose. The nuance between the two is that IPs that are intentional are fraudulent.

a) *Intentional vs. Unintentional Monetary Loss IP*

Monetary loss IPs, fall into two distinct categories, those which are intentional and those which are unintentional. Intentional monetary loss IPs are more commonly referred to as financial fraud and are overpayments that occur on purpose. Unintentional monetary loss IPs are overpayments that are accidental in nature because at the time of the payment the program is

unaware that the payment is an overpayment and the recipient has also not purposefully falsified information for gain.

It is important to note that agencies will only be able to classify their monetary loss IPs as intentional monetary loss IPs after the amount is determined to be fraudulent through the adjudication process. While agencies should track and report their intentional monetary loss IPs, the IP sampling and estimation methodology plans (S&EMP) used for purposes of reporting the UPs and the IPs does not need to be designed as a measure of financial fraud.

Table 1 provides examples of intentional and unintentional monetary loss IPs. Table 1 provides non-exhaustive examples of intentional and unintentional monetary loss IPs.

Intentional Monetary Loss IP	Agency has access to the most up to date income for the applicant and identifies an inaccuracy on the application. Agency decides to issue payment anyway because they feel sorry for the applicant, even though the agency has confirmed that the applicant does not qualify for the payment.
Intentional Monetary Loss IP	Applicant intentionally understates income on application so that they will qualify for a benefit.
Unintentional Monetary Loss IP	Agency does not have access to the most up to date income data for the recipient and the application appears correct based on all of the pre-payment eligibility verification the agency is able to perform so the agency issues payment to recipient.
Unintentional Monetary Loss IP	Applicant does not understand the instructions on the application and provides individual income instead of household income.

Table 1. Examples of Intentional and Unintentional Monetary Loss Improper Payments

b) ***Financial Fraud***

All financial fraud is an intentional monetary loss IP. However, the deceptive nature of financial fraud can make it difficult to quantify because, just as with all IPs, it will appear to fall into the proper payment bucket until it is exposed.

2. Non-Monetary Loss Improper Payments

There are two types of non-monetary loss IPs; underpayments and technically IPs. An underpayment represents instances where a recipient did not receive the funds that they were entitled and a technically IP represents instances where the recipient received funds they were entitled. If a payment was made to the right recipient for the right amount but the payment process failed to follow all applicable statute and regulation there is no amount that needs to be recovered, however, because the payment failed to adhere to all applicable statutes and regulations during the payment process the payment itself is considered a technically IP.

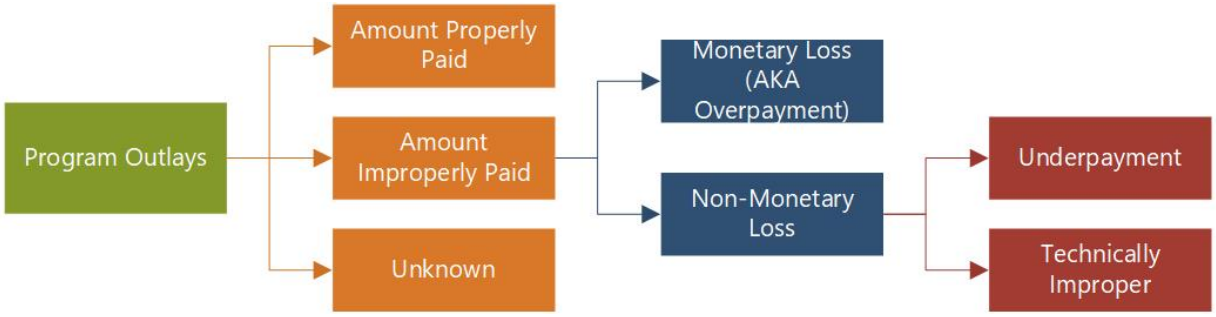

Figure 3. Non-Monetary Loss Improper Payment Type Categories

a) ***Reviewing the Necessity of Statute and Regulation for Technically Improper Payments***

A technically IP is a payment to the right recipient for the right amount and therefore does not result in the need for the program to recover funds due to overpayment. What makes this type of payment technically IP rather than a proper payment is that the payment process of a technically IP failed to follow applicable statute or regulation. For example, paying the right recipient the right amount despite failing to obtain all evidence required under regulation prior to payment or despite failing to obtain a statutorily required signature in a contract prior to payment are both technically IPs. While both of these situations warrant a review of internal controls, neither the regulatory requirement to obtain evidence nor the statutory requirement to obtain a signature proved necessary for the program ensure the payment was made to the right recipient for the right amount.

When a payment is a technically IP, it is important for the program to review whether the specific statute or regulation that was not followed is in fact necessary to ensure the payment is paid to the right recipient for the right amount. When reviewing statutory and regulatory requirements for payments, programs should identify requirements that are imposing additional burdensome requirements that are not necessary to ensure the payment is made to the right recipient for the right amount. If a program identified statutory or regulatory requirements that are causing an otherwise proper payments to be a technically IP, the program should report these barriers or other statutory objectives in the accompanying materials to their annual financial statement.

It is important to note that failing to obtain documentation that is not required by statute or regulation is not a technically IP if the payment was made to the right recipient for the right amount. The important nuance of the technically IP is that the specific requirement that was not followed in the payment process is one that is required by statute or regulation. A failure to follow a requirement in the payment process that is not a requirement in place because of a statute or regulation should not be considered an IP if the payment was made to the right recipient for the correct amount. When this situation occurs, an agency should evaluate whether that additional internal control is in fact necessary to ensure the payment is paid to the right recipient for the right amount.

B. Unknown Payments

If a program cannot discern whether a payment is proper or improper, the payment is considered an UP. If a program is still conducting research or going through the review of a payment at the time that the program must finish their sampling and report its results, the payment will be considered an UP for reporting purposes that year. This is done so that the program would not unintentionally over or under report the payment type results. An UP will eventually be determined to be proper or improper but because the program does not know whether it is proper or improper at the time of their review, they must call it an UP for purposes of this guidance. Programs may be required to report the review results of their UPs in future reporting years as the results become available. Agencies should not cushion their reporting timeframe specifically for the purpose of allowing the agency additional time to verify whether an UP is proper or improper.

1. Treatment of different types of payments in Phase 1 vs Phase 2

When a program is in phase 1 and assessing whether the program is likely to have IPs above the statutory threshold, UPs and IPs are both considered types of payments that contribute to the likelihood that a program could have IPs above the statutory threshold. Therefore, in phase 1, the program is considered likely to make IPs above the statutory threshold when the sum of the UPs and the IPs exceeds the statutory threshold. When a program is in phase 2, the UPs will be accounted for but should be reported separately from the estimate of the monetary loss and non-monetary loss IPs. The UP estimate will be considered and added to the IP estimate for purposes of compliance and for purposes of determining whether the program is above the statutory threshold.

C. Identifying the Correct Type of Payment

To efficiently prevent IPs and UPs, it is first important to properly understand the payment type. There are three main types of payments which collectively degrade the payment integrity of the agency: Monetary Loss IPs, Non-Monetary Loss IPs, and UPs. Correctly identifying the type of payment will aide in being able to effectively prevent that type of payment from occurring in the future. The decision tree below is meant to provide a cursory overview for determining the payment type.

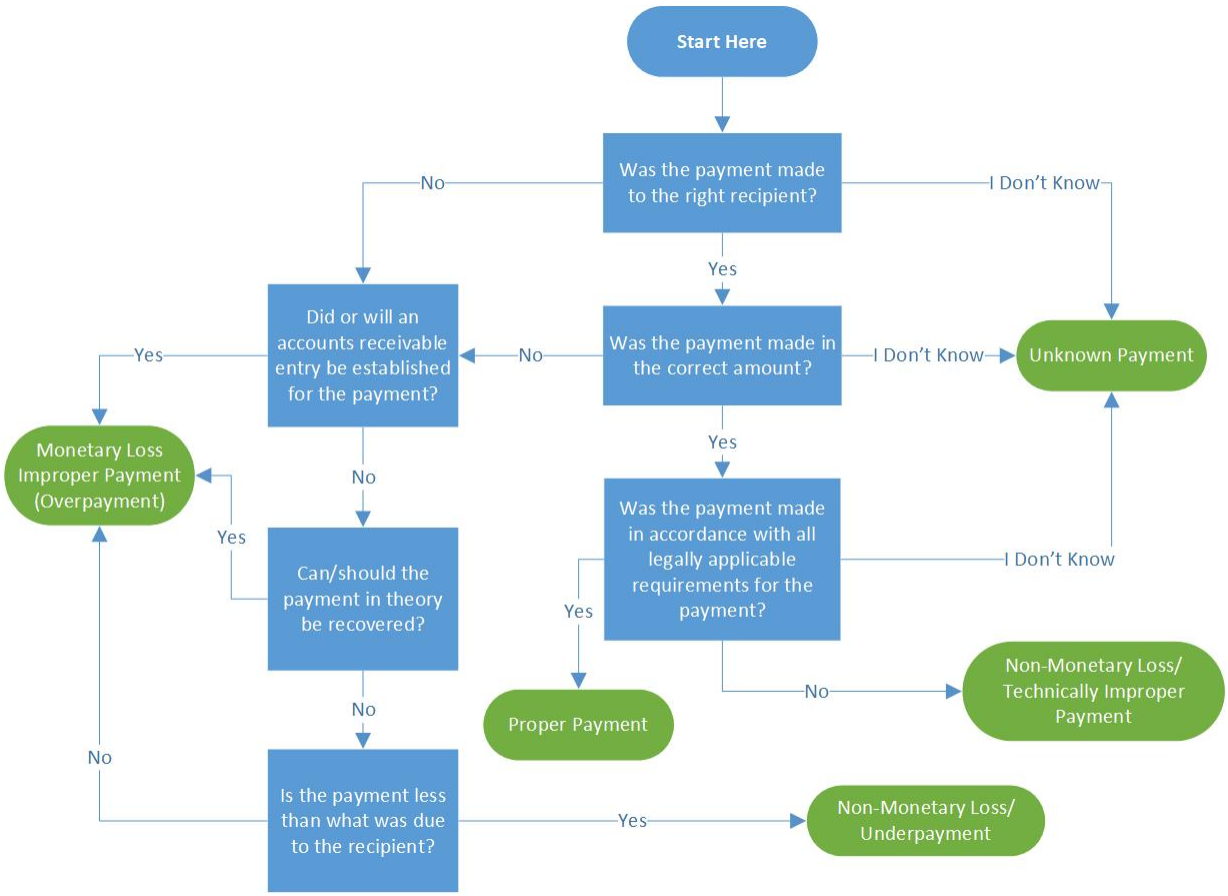

Figure 4. Decision Tree for Determining Payment Type

II. Phases of Assessments

The following 'Phases' require varying degrees of effort; each program is responsible for determining which of the 'Phases' it falls into. All programs with annual outlays greater than $10,000,000 will fall into either phase 1 or phase 2.

A. Phase 1: Identify Susceptible Programs and Activities with an IP Risk Assessment

Agencies should assess all programs with annual outlays greater than $10,000,000 for IP risk at least once every three years. The purpose of an IP risk assessment is to determine whether the total annual IPs PLUS the UPs for a program are collectively likely to be above or below the statutory threshold for the given year.

If the assessment determines that it is likely that the program's IPs plus the program's UPs are above the statutory threshold then, the following year the program should produce a statistically valid estimate of the programs IPs and UPs. If the IP risk assessment demonstrates that the program is not likely to make IPs and UPs above the statutory threshold, then the program will not produce a statistically valid estimate in the following year and instead will conduct another IP risk assessment in three years.

1. Structure of an IP Risk Assessment

IP risk assessments may be qualitative or quantitative in nature. The agency should develop an IP risk assessment methodology that is appropriate to ensure that the result of the IP risk assessment reasonably supports whether the program is or is not susceptible to significant IPs (i.e. likely to have IPs plus Ups that are above or below the statutory threshold).

Additionally, agencies should be mindful that, when evaluating compliance, the Inspector General (IG) will evaluate and take into account the adequacy of the IP risk assessment and the IP risk assessment methodology used. Their compliance evaluation will include whether the audits, examinations, and legal actions of the OIG indicate a higher risk of IPs or actual IPs that were not included in the IP risk assessments. With that in mind, when developing an IP risk assessment methodology, agencies are encouraged to review the results of audits, examinations and legal actions of the OIG and take into account whether they impact the risk of IPs in the program. OMB does not need to approve a program's IP risk assessment methodology prior to implementation, however, the agency should be able to make the methodology available upon request in the case that OMB wishes to conduct a review.

a) *Factors that may impact the level of IPs and UPs within a program and could be considered (if applicable) when conducting a qualitative IP risk assessment.*

When conducting a qualitative assessment for risk of IPs and UPs, the agency should ensure that proper consideration has been given to relevant factors that would help prove that the program is likely to be above or below the statutory threshold. Examples of factors that could be considered when conducting a qualitative IP risk assessment include but are not limited to:

(1) whether the program reviewed is new to the agency;
(2) the complexity of the program reviewed;
(3) the volume of payments made through the program reviewed;
(4) whether payments or payment eligibility decisions are made outside of the agency, such as by a State or local government;
(5) recent major changes in program funding, authorities, practices, or procedures;
(6) the level, experience, and quality of training for personnel responsible for making program eligibility determinations or certifying that payments are accurate;
(7) significant deficiencies in the audit report or other relevant management findings of the agency that might hinder accurate payment certification;
(8) similarities (a combination of outlays, mission, payment process, etc.) to other programs that have reported IP and UP estimates or been deemed susceptible to significant IPs;
(9) the accuracy and reliability of IP and UP estimates previously reported for the program, or other indicator of potential susceptibility to IPs and UPs identified by the OIG of the executive agency, the Government Accountability Office, other audits performed by or on behalf of the Federal, State, or local government, disclosures by the executive agency, or any other means;
(10) whether the program lacks information or data systems to confirm eligibility or provide for other payment integrity needs; and
(11) the risk of fraud as assessed by the agency under the Standards for Internal Control in the Federal Government published by the Government Accountability Office (commonly known as the 'Green Book').

The risk factors above are provided as examples only, it is the agency's responsibility to determine the risk factors and the associated scoring or risk factor weighting methodology that should be considered for each individual program and risk.

2. **Frequency of an IP Risk Assessment**

Programs with annual outlays above $10,000,000, must conduct an IP risk assessment **at least once every three years** UNLESS the program moves to Phase 2 and is reporting IPs plus UPs above the statutory threshold. A program should not operate in both Phases at once, meaning, if a program is operating in Phase 2, and reporting an annual IP estimate, the program should not also be spending resources to conduct an IP risk assessment during that same year. To the extent possible, data used for conducting an IP risk assessment in a given program should coincide with the FY being reported (for example, the IP risk assessment reported in the FY 2021 Annual Data Call would be based on data from FY 2021 (October 2020 through September 2021).

a) ***Conducting an off-cycle IP risk assessment***

If a program that is on a three-year IP risk assessment cycle experiences a significant change in legislation and/or a significant increase in its funding level, agencies may need to reassess the program's risk susceptibility during the next annual cycle, even if it is less than three years from the last IP risk assessment. Examples of events that may trigger an off-cycle risk assessment include but are not limited to, national disasters, national emergencies, or a change to program structure that increases payment integrity risk. The agency will determine whether the factor is significant enough to cause the program to become likely to make IPs and UPs that would collectively be above the statutory threshold.

b) ***IP risk assessments in newly established programs***

For newly established programs, an IP risk assessment should be completed after the first 12 months of the program even if the first 12 months do not coincide with the FY. After the first IP risk assessment is conducted, agencies have discretion to adjust the 12-month IP risk assessment time frame so that the IP risk assessment is appropriately aligned or staggered with other agency programs on a three-year IP risk assessment cycle.

c) ***Timing for the IP risk assessment when a program's annual outlays move above the $10,000,000 threshold***

A program whose outlays fluctuate above and below the $10,000,000 threshold over time will not necessarily perform an IP risk assessment every three years. The decision tree provided in Figure 5 below can be used by a program to determine the timing and frequency of an IP risk assessment. A program that fluctuates above and below the $10,000,000 threshold may not be required to complete an IP risk assessment exactly on the three year mark if the annual outlays fall below the $10,000,000 threshold the year that the program is 'due' for assessment. In Figure 5 the program is assumed to be 'due' for an IP risk assessment in Year 1, however, if the outlays for the program in Year 1 are below the $10,000,000 threshold, the program does not need to perform an IP risk assessment in Year 1. However, if the outlays for the program are above the $10,000,000 threshold in Year 1, the IP risk assessment is required because programs with annual outlays greater than $10,000,000 must conduct an IP risk assessment at least once every three years and this particular program was originally 'due' in Year 1. Note that some programs may need to wait until the entire 12-month period has concluded for outlays to be greater than $10,000,000. If this occurs, it is reasonable to assume that the program may actually conduct the IP risk assessment during Year 2, however, to the extent possible, data used for conducting an IP risk assessment in a given program should coincide with the FY being reported, therefore the outlays that the program will be assessing will be those from Year 2.

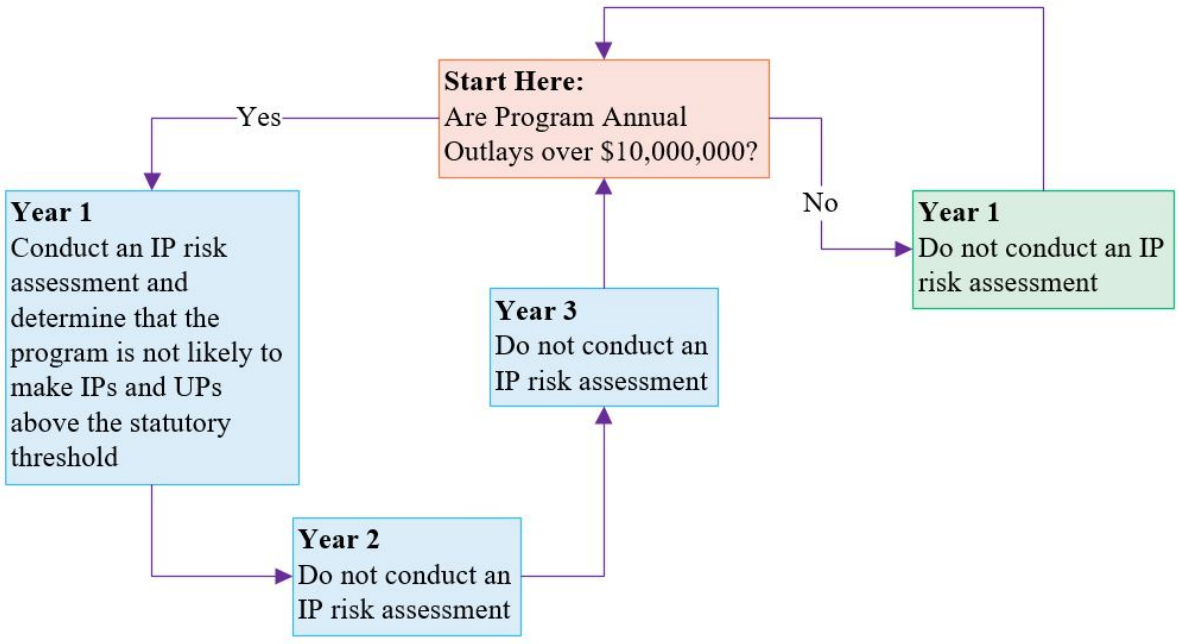

Figure 5. Example of IP Risk Assessment Timing

3. Programs Deemed Susceptible to Significant IPs Outside of the Normal IP Risk Assessment Process

OMB may determine on a case-by-case basis that certain programs may still be subject to the annual IP reporting requirements. If this occurs, OMB will notify the program.

B. Phase 2: Report IP Estimates for Identified Susceptible Programs with a Statistically Valid Sampling and Estimation Methodology Plan

Programs reporting IPs for the first time and programs revising their current IP Sampling and Estimation Methodology Plan (S&EMP) should conform to the process and content described in this guidance.

1. Purpose of an IP Estimate

The main purpose of an IP estimate is to reflect the annual estimated known IPs made by the program. When developing the S&EMP, errors identified for one payment should never exceed the amount of the payment. It is important to note that the S&EMP should have a mechanism for identifying, accounting for, and estimating the annual UPs and the annual IPs separately.

2. Suggested Content of a Sampling and Estimation Methodology Plan

The head of each agency is ultimately responsible for producing a statistically valid estimate of the IPs and UPs made under the program that is in Phase 2. Each agency has the responsibility of designing and documenting a program's S&EMP with the mindfulness that during their annual compliance review, their OIG will take into account the accuracy of the IP and UP estimates and whether the S&EMP used is adequate and appropriate given program characteristics. The program will be responsible for producing an IP and UP estimate that is accurate and appropriate given program characteristics and it will be the OIG's responsibility to evaluate whether the explanation provided by the program and the S&EMP without point estimates and confidence intervals around those estimates warrants compliance during the annual OIG compliance review. For purposes of this guidance, S&EMPs will be considered statistically valid if they produce point estimates and confidence intervals around those estimates. Agencies must work with their statistician to determine the appropriate confidence interval given program characteristics, available resources, and whether the estimate is reliable. If a program is unable to develop a S&EMP that produces a point estimate and confidence interval around the estimate then it must include in their S&EMP a detailed explanation as to why it is not possible.

3. Reporting Timeframe

To the extent possible, data used for estimating IPs and UPs in a given program should coincide with the FY being reported (for example, the estimate reported in the FY 2021 Annual Data Call would be based on data from FY 2021 (October 2020 through September 2021). The 12-month timeframe represented in the reported estimate should be documented in the S&EMP submission. For consistency purposes, the agency should continue using the same timeframe (i.e. October through September) for subsequent reporting years, unless a different timeframe needs to be used. If the timeframe needs to change for subsequent reporting years then the agency should resubmit their S&EMP and accompanying checklist with certification with the updated 12-month timeframe.

4. **Sampling and Estimation Methodology Plan Checklist**

A S&EMP checklist must accompany all S&EMPs submitted to OMB. The most current version of the S&EMP checklist is located on the Payment Integrity Information Act Required Submissions to OMB Max Page.

Each submitted S&EMP checklist must be signed by an agency official stating that the S&EMP will produce a statistically valid estimate. The certification should be signed by an agency official of the agency's choosing (e.g., this could be the Chief Financial Officer, his/her Deputy, a program official, etc.). The signed S&EMP checklist will serve as evidence that the agency believes the S&EMP is statistically valid. Agencies are encouraged to provide their secure Max link to their OIG so the OIG is able to review this documentation during their annual compliance review.

5. **Sampling and Estimation Methodology Plan Submission to OMB**

When an agency has completed their S&EMP, it must submit the S&EMP and a completed S&EMP checklist in pdf format to OMB by uploading one package containing both the S&EMP and the S&EMP checklist via the Sampling and Estimation Methodologies folder located within the agency secure Max page under the Payment Integrity Information Act Required Submissions to OMB Max Page. The package must be received no later than June 30 of the FY for which the estimate is being produced (e.g., the sampling methodology to be used for the FY 2021 reporting cycle must be submitted by June 30, 2021).

6. **Frequency of Submitting a Sampling and Estimation Methodology Plan and Reporting an Estimate**

Programs in Phase 2 will report a statistically valid estimate of IPs and UPs on an annual basis. Once a program has submitted a S&EMP to OMB, under this guidance or under a previous version of Circular A-123, Appendix C, the program does not need to resubmit a S&EMP - unless an update to the plan is warranted. Programs choosing to continue to utilize a S&EMP prepared under a previous version of Circular A-123, Appendix C must ensure that the S&EMP has been uploaded via the Sampling and Estimation Methodologies folder located within the agency secure Max page under the Payment Integrity Information Act Required Submissions to OMB Max Page.

a) ***When to Update a Sampling and Estimation Methodology Plan***

Programs using a S&EMP submitted under this guidance or under a previous version of Circular A-123, Appendix C should consider updating their S&EMP if the program is impacted by any significant legislative, funding, structural, or guidance changes. A S&EMP that is being updated should include some language explaining why the S&EMP is changing and how the S&EMP is different from the one previously submitted.

7. **OMB Receipt of S&EMP**

It is important to note that OMB will not be issuing a formal approval to the agency for the statistically valid S&EMP as it is the agency's responsibility to produce a statistically valid S&EMP and load it to the appropriate Max site. The time stamp on the Max site will serve as documentation and evidence of the submission date. Once the agency has loaded the statistically valid S&EMP and accompanying checklist package to their Max site the agency may begin to execute the S&EMP.

C. Moving Between Phases

1. Statutory Threshold and Phase Determination

The statutory threshold is determined by statute. Programs are considered to be above the statutory threshold if they are reporting an annual IP and UP estimate that is either above $10,000,000 and 1.5% of the program's total annual outlays or above $100,000,000 regardless of the associated percentage of the program's total annual outlays that the estimated IP and UP amount represents. The Table 2 below illustrates when a program would be considered to be above or below the statutory threshold based on the combination of their annual IP and UP rate and dollar amount.

		IP and UP Rate			
		0.50%	1%	1.6%	2%
IP and UP Dollar Amount	$9,000,000	Below the Statutory Threshold	Below the Statutory Threshold	Below the Statutory Threshold	Below the Statutory Threshold
	$11,000,000	Below the Statutory Threshold	Below the Statutory Threshold	Above the Statutory Threshold	Above the Statutory Threshold
	$99,000,000	Below the Statutory Threshold	Above the Statutory Threshold	Above the Statutory Threshold	Above the Statutory Threshold
	$101,000,000	Above the Statutory Threshold	Above the Statutory Threshold	Above the Statutory Threshold	Above the Statutory Threshold

Table 2. Statutory Threshold Determination Based on Dollar Amount and Rate

2. Phase 1 to Phase 2

When an agency determines through IP risk assessment that the total annual IPs PLUS the UPs for the program are likely to be above the statutory threshold, the program will report an IP and UP estimate in the FY following the FY in which the risk assessment determination was made.

3. Phase 2 to Phase 1

When a program is in Phase 2, then it will stay in Phase 2 and report an IP and UP estimate annually until the reported estimate is below the statutory threshold. If a program is in Phase 2, has established a baseline, and reports an IP and UP estimate that is below the statutory threshold it will automatically move back into Phase 1 the following FY unless the OIG issued a non-compliance finding for the program in the previous year and the finding demonstrated that the program IP and UPs estimate was inaccurate and inappropriate given the program characteristics. The demonstration in the OIG compliance report, must include, at a minimum, a revised statistically valid IP and UP estimate that is accurate and appropriate and also adheres to this guidance.

When a program moves from Phase 2 to Phase 1, the program will treat the result in the Phase 2 year as the first year in the IP risk assessment cycle. Figure 6 below provides an illustration of when a program will move between the two Phases.

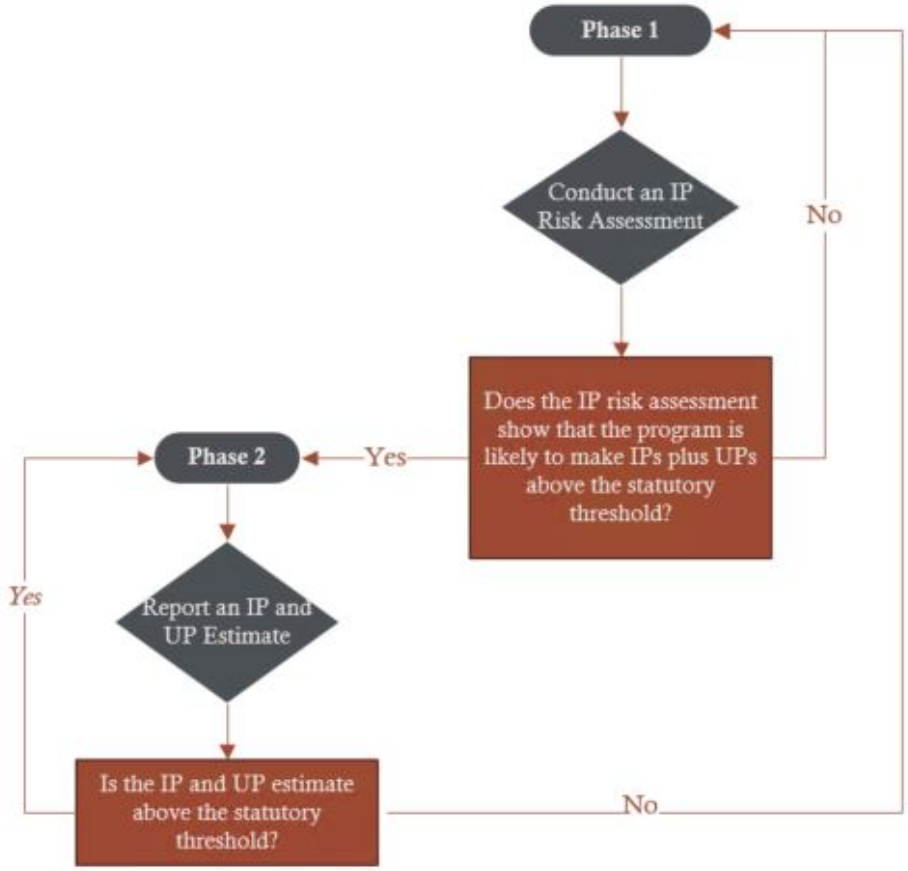

Figure 6. Moving Between Phase 1 and Phase 2

4. **Example of Moving Between the Phases**

Figure 7, below, provides an illustration of moving back and forth between Phase 1 and Phase 2 over multiple years. In Figure 7, it is assumed that Year A represents the first year of a brand new program. Each new year is indicated with a different letter. For example, if Year A is the first year of the program, Year B could represent the 2nd year of the program if the annual outlays were over $10,000,000 and Year G could represent the 2nd year of the program if the annual outlays were not over $10,000,000.

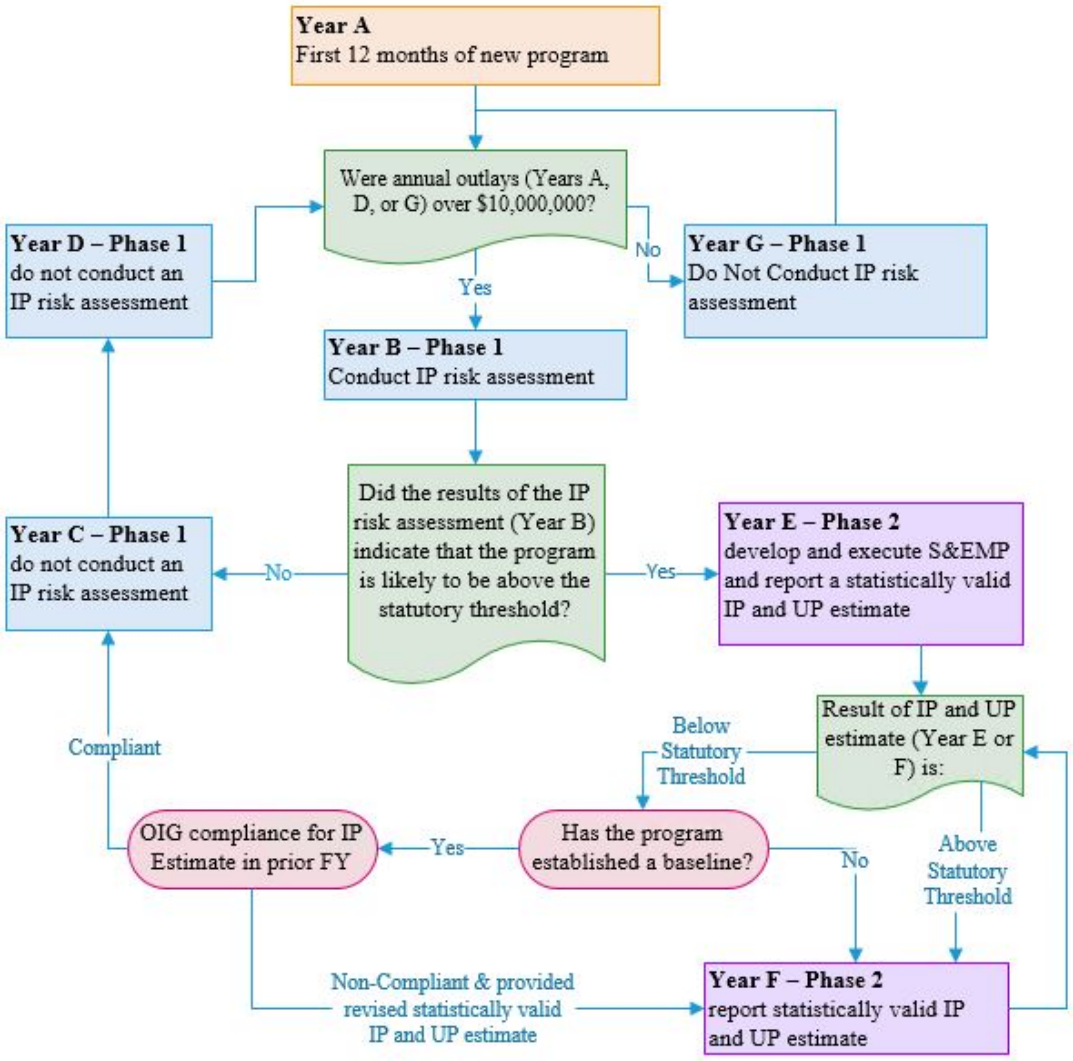

Figure 7. Example of Moving Between Phase 1 and Phase 2

III. Causes

A. Identifying the Root Cause of the Improper Payment

To effectively prevent an IP or a UP from occurring, agencies must properly identify the reasons their programs are at risk of IPs. Agencies should ensure they have identified a true root cause of an IP or a UP as it is critical to understand the true root cause of a problem in order to formulate effective corrective actions. The root cause is the core issue that sets in motion the entire cause-and-effect reaction that ultimately leads to the IP of the UP. Identifying the root cause requires the program to continue asking 'why did this occur?' until the root cause is identified. It is important to continue asking 'why' the condition occurred, noting the answer, and then asking why for each answer over and over until the 'root' cause is identified. Often, the reason for a problem is only a symptom of the real cause and by using a series of logical 'why' questions over and over programs can ensure they are not only focusing on the symptoms of the problem. Programs that are reporting an IP and UP estimate should be able to identify the root causes of the IP and the UP.

A root cause is something that would directly lead to an improper payment, and if corrected, would prevent the improper payment

B. Cause Category

The cause categories in Table 3 are provided as a starting point for each program to use when identifying their root cause. To identify the true root cause, it is likely that the program will need to continue to ask 'why' for each of the categories provided. Examples of cause categories are provided below, however, agencies should consult the OMB Annual Data Call guidance for the most up-to-date listing of cause categories each year. Each program should distribute its total IP and UP estimate (which is based on dollars, as opposed to number of occurrences) across the cause categories provided by OMB.

Cause Category	Definition	Examples include but are not limited to…
Statutory Requirements of Program Were Not Met	An exception in that a payment made to an otherwise qualified recipient for the right amount but the payment process failed to meet all regulatory and/or statutory requirements. All Technically IPs will fall into this cause category.	when a vendor is paid the contracted amount for services provided; however, the person authorizing the services did not have the legal authority needed from the contracting officer to authorize the services, or, when a vendor is paid the correct amount for services provided but the contract the agency used to secure the services did not meet all of the requirements in the Federal Acquisition Regulation.
Unable to Determine whether Proper or Improper	A payment that could be either proper or improper but the agency is unable to determine whether the payment was proper or improper as a result of insufficient or lack of documentation. All UPs will fall into this cause category.	when an agency is required to verify income prior to issuing a payment to a beneficiary and a beneficiary's case file lacks updated income information or pay stubs and the agency has no other way of verifying whether a change in income has occurred since the last time they issued a benefit. The beneficiary may still be qualified to receive benefits, but they might have also had an increase or decrease in income affecting their eligibility for the program. Therefore, because the reviewer does not have the information needed (updated income) during the time of the review, it is unknown whether an overpayment or underpayment has been made.
Data/Information Needed Does Not Exist	A situation in which there is no known database, dataset or location currently in existence that contains the data/information needed to validate the payment accuracy prior to making the payment.	when a recipient's eligibility is dependent on the length of time a child spent with their guardian – no database or dataset is currently in existence containing this type of information; when a medical provider fails to provide proof of a broken leg (required by statute or regulation) to support a claim –no database or location is currently in existence containing x-rays or any other type of information that can confirm a leg is actually broken.
Inability to Access Data/Information	A situation in which the data or information needed to validate payment accuracy exists but the agency or entity making the payment does not have access to it.	when a statutory constraint prevents a program from being able to access information that would help prevent IPs (for example, not confirming a recipient's earnings or work status through existing databases due to statutory constraints, or, a beneficiary failing to provide an agency with information on earnings, and the agency does not have access to databases containing the earnings information).
Failure to Access Data/Information	IPs are attributed to human errors to access the appropriate data/information to determine whether or not a beneficiary or recipient should be receiving a payment, even though such data/information exists and is accessible to the agency or entity making the payment.	when agency with access to the death master file fails to verify eligibility prior to approving entitlements; when an entity has access to the information that would verify a beneficiaries household income and the entity making the payment does not check that information prior to payment.

Table 3. Cause Category Definition and Examples

The first two cause categories in Table 3, Statutory Requirements of Program Were Not Met and Unable to Determine Whether Proper or Improper, are directly linked to the IP type. The next three cause categories, Data/Information Needed Does Not Exist, Inability to Access

Data/Information, and Failure to Access Data/Information, are used to classify the data/information that could have prevented the IP.

C. Using the Cause Category to Identify the Root Cause and Corrective Action

These purpose of these cause categories is twofold. First, they help the program identify the correct path for the 'why' questions which will help determine the root cause, and second, they help the program identify an effective direction for the mitigation strategy or corrective action. Table 4 provides an example of a 'why' question that programs can begin with as they drill down to the true root cause of the IP and also illustrations of how the corrective action approach may differ depending on the cause category.

Cause Category	To identify the root cause for IP amounts places into this category, the program could begin by asking:	Possible Corrective Action Direction
Statutory requirements of program were not met	*"Why weren't we able to follow the statutory/regulatory requirement?"*	Request statutory requirement removal or adjustment to align with payment integrity need
Unable to determine whether proper or improper	*"Why didn't we have the documentation needed to determine whether the payment was proper or improper?"*	Training on which documentation must be submitted, automate application process to prevent incomplete documentation
Failure to Access Data/Information	*"Why didn't we access the data/information?"*	Training on how to review the information, automate the payment process requirements to enable data access
Data/Information Needed Does Not Exist	*"Why doesn't the data/information exist?"*	Create central location for information, adjust program requirements to omit the requirement for the information
Inability to Access Data/Information	*"Why can't we access the data/information?"*	Request statutory change to allow the program to access the information

Table 4. Cause Category Link to Root Cause and Corrective Action

D. Choosing the Correct Cause Category

Figure 8 can be used to help a program identify the most appropriate cause category.

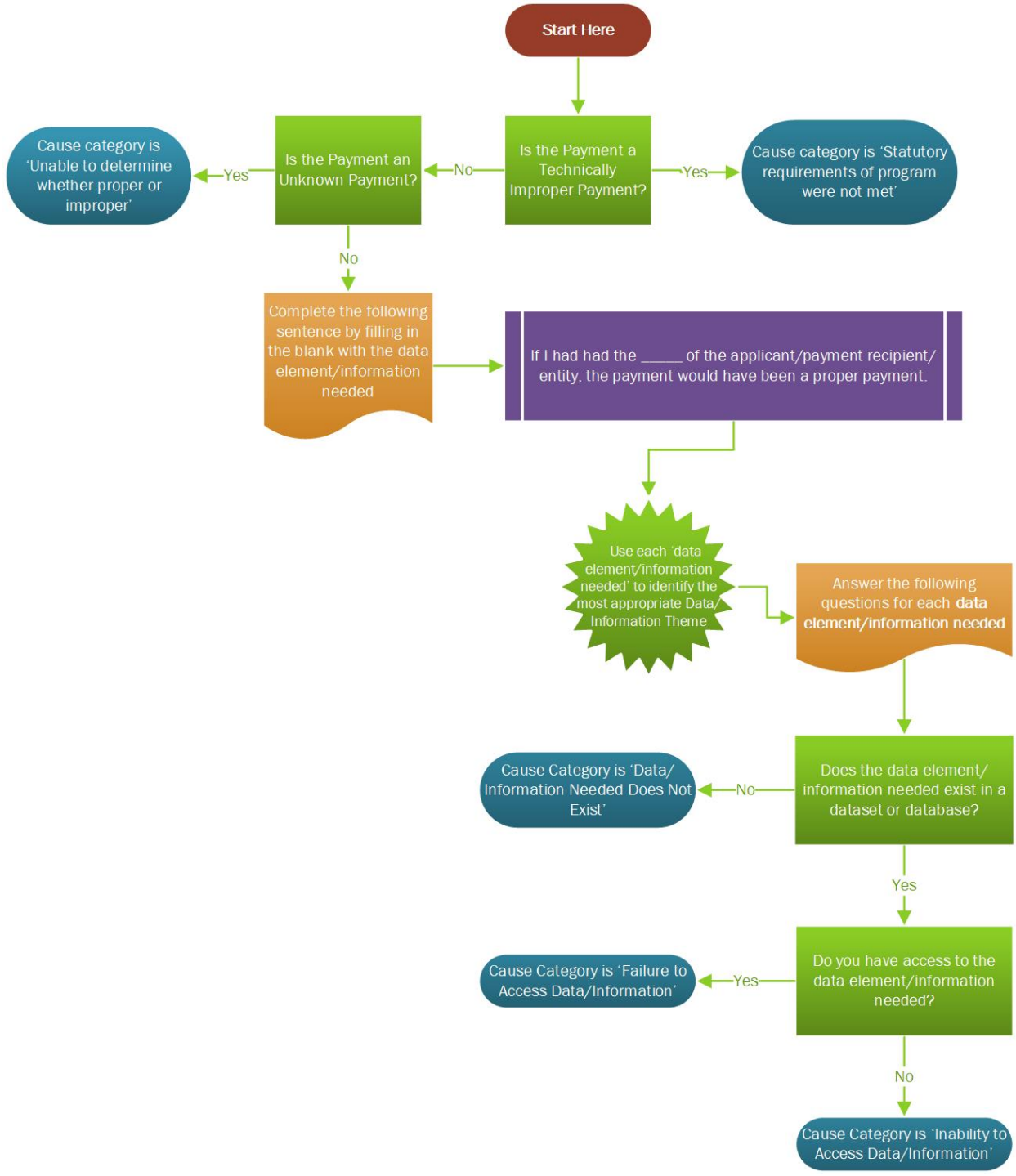

Figure 8. Decision Tree for Determining the Cause Category of the Improper Payment

After the cause category is identified, a program should ask enough 'why' questions until it has reached the point in the payment process in which the payment changed from proper to improper. When identifying the root cause of the IP of the UP a common mistake is the failure to look deep enough for the true root cause of the IP or the UP. A program will know that they have asked enough 'why' questions and reached the root cause if the elimination of the cause will prevent the error from occurring again.

E. Data/Information Theme

When a data/information-related cause category is selected as a reason for IPs in the OMB Annual Data Call, agencies will also identify the theme of the data element/information criteria needed. This is best accomplished by completing the sentence in Figure 8 to narrow down to the data/information theme. Examples of data/information themes are provided below in Table 5, however, agencies should consult the OMB Annual Data Call for the most up-to-date listing of data/information themes each year.

Data/Information Theme	Definition	Possible criteria that could fall into this category include but are not limited to…
Address/Location	Information regarding where the applicant/recipient lived, owned property, or was physically present in a specific location	living arrangement/location or place of residency, place of birth, location or property, or temporary housing.
Affiliation	Criteria that require the applicant/recipient as being attached or connected to a type of group, organization, or particular attribute.	agricultural in nature, business organization, affected by a disaster, ethnicity, employment within a particular organization, or faith based.
Age	The biological age of the recipient/beneficiary.	date of birth or biological age.
Citizenship	Recognized as a United States citizen through birth or naturalization, or as a lawfully present non-citizen in the United States.	legal authorization to remain in the United States according to Federal immigration laws or any other criteria that supports or identifies citizenship.
Contractor or Provider Status	Status or standing of contractor or provider.	contractor Performance, recipient eligibility to receive Federal contracts, recipient eligibility to receive payments due to U.S. sanctions against targeted foreign countries, or recipient eligibility to provide medical services.
Deceased	Date of death of recipient/beneficiary.	date of death or proof of death.
Dependency	Describes who the recipient/beneficiary relies on as a primary source of support.	biological or adoptive mother or father, stepparent if considered to be the parent, child relationship to the recipient, dependent, foster child, or independent.
Education Related	The education level or enrollment status of the recipient/beneficiary.	the length the recipient/beneficiary has been enrolled, the location of institution, the number of family members of the recipient/beneficiary enrolled in college, accreditation of educational institution, status of academic progress, degree earned by recipient or beneficiary, grade level of the recipient/beneficiary, or undergraduate/graduate enrollment status of recipient/beneficiary.
Employment	The employment status of the recipient/beneficiary.	whether the recipient/beneficiary is able to work, available to work, actively seeking work, employed, separated from employment, or registered for employment service.
Financial	The financial position or status of a beneficiary, recipient, applicant, or their family.	total worth of assets, credit history, amount of debt, net worth, or tax emption status.
Household size	Number of family members in a household.	family of householder living in the housing using or total number of people occupying a housing unit.
Identity	Able to establish that some is uniquely who they claim to be.	valid social security number.
Marital Status	A person's state of being single, married, separated, divorced, or widowed.	divorced, married, separated, widowed, or single.
Military Status	The condition of being, or having been in the uniformed services.	military discharge status, military service status, selective service status, or service connection.
Prisoner Status	Eligibility for benefits or payment based on prisoner status.	felon or prisoner.
***Receiving Benefits from Other Sources*:**	Beneficiary or recipient is receiving benefits from an additional source.	receiving benefits from another Federal agency or state, or from other sources.
Residency	Status of Recipient's living location or arrangement.	living arrangement or state residency.

Table 5. Data/Information Theme Definitions and Criteria

IV. Prevention

To be effective, programs should not operate in a "pay-and-chase" model and instead, should prioritize efforts toward preventing IPs and UPs from occurring. The reason for this is not only to avoid the IP and the UP but also to avoid expending resources to try and recover the overpayment. All programs reporting an IP estimate plus an UP estimate exceeding the statutory thresholds must put in place and annually report on their corrective action plan to prevent and reduce the IP and UP amounts.

A. Payment Integrity Risks

1. Payment Integrity Risk Identification

All programs should have a structured and systematic approach to recognizing where the potential for IPs and UPs can arise. The identification of payment integrity risks should be a continuous process to ensure new or changing risks are not overlooked. The IP Risk Assessment described in Phase 1 and the S&EMP described in Phase 2 are tools that can help a program understand the points within the payment process that may be vulnerable to IPs and UPs.

When identifying payment integrity risks within a program it is important to determine and understand the inherent vulnerabilities that a program faces based on the types of payments the program makes and how the payment process is structured. For example, an agency that primarily makes payments to non-Federal entities, such as a benefit-paying agency, has a higher risk for making IPs than an agency that rarely pays non-Federal entities.

Programs should consider the causes of IPs and UPs and the likelihood of their occurrence in their process of identifying and monitoring payment integrity risks to the program. Isolating the components of the payment process can be an effective way to identify payment integrity risks. The use of data analytics to identify trends, patterns, anomalies, and exceptions within data to identify indicators of IPs is an example of an effective means of identifying payment integrity risks.

2. Controls to Manage Payment Integrity Risk

Agencies have the responsibility to respond to identified payment integrity risks and prevent IPs from occurring. Agencies should also minimize the amount of UPs that occur because the inability to ascertain whether payments are proper or improper represents lost credibility in program management over ensuring payment integrity. Programs must proactively manage their payment integrity risk in order to prevent IPs and UPs. In combatting payment integrity risk, it is important to assess the agency's controls and the control environment.

a) *Internal Control Standards Application to Payment Integrity*

Robust internal control processes should lead to fewer IPs and fewer UPs. Establishing and maintaining effective internal controls—including an internal control system that prevents IPs and UPs from being made and promptly detects and recovers any IPs that are made—should be a priority. It is important to note that the five standards and attributes (Control Environment, Risk Assessment, Control Activities, Information and Communications, and Monitoring) should be applied to the specific facts and circumstances of the various agency operations and programs. In other words, agencies are not expected to address each attribute listed below. Agencies should use the attributes listed as a guide in evaluating each of the five standards, and should consider other attributes that may be applicable to its particular circumstances.

In addition, management has discretion in determining the breadth and depth of the scope of assessing internal control over IPs and UPs. These standards and attributes can be implemented to fit the circumstances, conditions, and risks relevant to the situation of each agency.

3. **Enterprise Risk Management for Payment Integrity**

The Enterprise Risk Management framework, introduced in OMB Circular A-123, can be used to assist in the identification and management of payment integrity risks for the agency. Ensuring the integrity of Federal payments is fundamental to the core mission for agencies. A significant risk in managing IP risk is the potential that agencies may make investments in risk controls that negatively affect program mission, efficiency, customer experience or the overall operations of the agency. Agency senior management is required to manage the payment integrity risk to an agency achieving its strategic, operations, reporting, or compliance objectives. Figure 9 highlights examples of how payment integrity risk cuts across an agency's strategic, operations, reporting and compliance objectives.

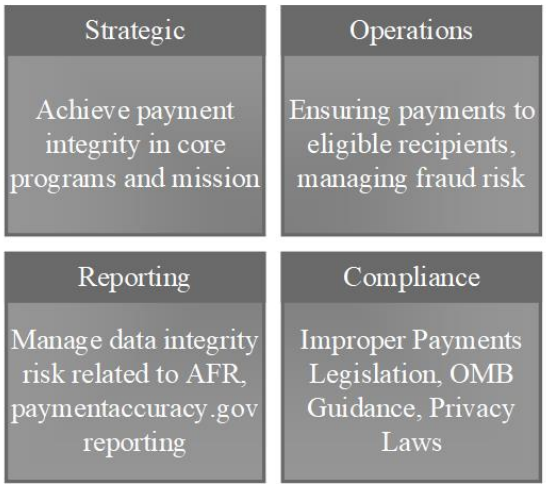

Figure 9. Interaction between Payment Integrity Risks and Agency Objectives

The Agency's Risk Profile, as required by OMB Circular No. A-123, should include an evaluation of payment integrity risks. To effectively manage payment integrity risk, agency senior management must perform an assessment in which they identify and evaluate the potential payment integrity risks the agency faces, analyze the potential likelihood and impact of those risks, and finally, prioritize the risks. The payment integrity risks should be prioritized based on the results of the assessment and the program's tolerable IP rate. When prioritizing payment integrity risks it is important to consider the extent to which control activities currently in place mitigate the likelihood and impact of risks and whether the remaining risk after considering those control activities result in the program exceeding their tolerable IP rate.

When performing the assessment, the ERM model, should be used to identify, assess, prioritize, and respond to payment integrity risks. Once results of this assessment have been finalized, agency senior management should escalate significant payment integrity risks to the agency designated risk official for inclusion in the Risk Profile. When considering root causes, mitigation activities, and corrective action plans for payment integrity risks, senior agency officials should work with the designated risk official to take an enterprise approach to better identify whether similar challenges exist across other parts of the enterprise and to identify most effective mitigation and corrective action.

B. Mitigation Strategies and Corrective Actions

Identifying the cause(s) of IPs and UPs and the point within the payment process where the transaction turned from 'proper' to 'improper' (or 'unknown') will allow the agency to clearly identify the specific payment integrity risks. Distinguishing between what constitutes a root cause that created an error versus an internal control problem that did not catch an error is critical when developing mitigation strategies and corrective actions to address IPs and UPs. Once the program has gained insight into their payment integrity risks and the root causes of their IPs and UPs the program can take action to develop and implement effective IP mitigation strategies and corrective actions which will collectively form the corrective action plan.

A corrective action plan should be proportional to the severity of the associated amount and rate of the root cause. For example, agencies should develop and implement mitigation strategies or corrective actions that cost less than the IP or UP amount they are designed to prevent. Acknowledging any barriers that prevent the program from further reducing the IP level in a particular area are necessary both in terms of identifying and achieving the program's tolerable rate and also in terms of ensuring the program is operating in a financially responsible manner. For example, if the statutory construct of the program is such that it increases the risk for IPs, a program may determine that accepting that increased risk is necessary to ensure the program achieves its mission.

When developing responses to mitigate the likelihood and impact of payment integrity risks, agencies should consider whether they want to accept the risk that the IP or the UP will occur, completely avoid the possibility of the IP or the UP occurring, reduce the likelihood that the IP or the UP will occur, share the risk that the IP or the UP will occur with others, or use some combination of the responses mentioned.

Additionally, agencies should be mindful of burden when developing internal controls to serve as IP or UP mitigation strategies during the payment process so that the efficiency of the payment process is not compromised. For example, when establishing documentation requirements for payments, agencies should ensure that all documentation requirements are necessary and should refrain from imposing additional burdensome documentation requirements that are not needed to validate the eligibility of the payment recipient.

C. Measuring the Effectiveness of a Corrective Action Plan

When developing mitigation strategies and corrective actions, agencies should identify annual benchmarks that can be used to demonstrate the progress of the corrective action plan implementation as well as the impact on IP and UP prevention. An effective corrective action will eliminate the root cause of the IP or the UP and prevent it from reoccurring, and effective mitigation strategy will minimize the likelihood of an IP or the UP occurring or reduce the impact of the IP or the UP.

To measure the overall effectiveness of a corrective action plan on an annual basis, agencies should monitor and measure the effectiveness and progress of each individual mitigation strategy and corrective action on a continuous basis. Effective mitigation strategies and corrective actions should have some nexus to the root cause. Collectively, the results will inform whether the overall corrective action plan is effective, whether the annual benchmark is met, and also provide insight to which components of the plan may need to be modified or refined to improve effectiveness.

D. Modifying Corrective Action Plans

The result(s) of the Corrective Action Plan effectiveness measurement should inform whether a modification to an underlying component of a program corrective action plan is needed. As a program payment process incorporates and perfects the execution of mitigation strategies and corrective actions it is likely that the existing mitigation strategies and corrective action can be intensified or expanded, resulting in a high-impact, high return-on-investment in terms of reduced or prevented IPs and UPs. Agencies should make necessary refinements to a corrective action plan when the original intent of the corrective actions and mitigation strategies within the corrective action plan are failing to achieve their intended purpose and result.

E. The Do Not Pay Initiative

The DNP Initiative (Initiative) includes multiple resources across the Federal Government designed to help agencies determine eligibility to confirm that the right recipient obtains the right payment amount. Each agency has access to and should use the Initiative to verify payment eligibility for the purposes of identifying and preventing IPs. Each agency shall thoroughly review prepayment and pre-award procedures and ensure available databases with relevant information are checked to determine eligibility and prevent IPs and UPs before the release of any Federal funds.

Each State and any contractor, subcontractor, or agent of a State, including a State auditor or State program are responsible for reducing IPs and UPs of a Federally funded State-administered program. shall have access to, and use of, the Initiative for the purpose of verifying payment eligibility.

1. The Treasury Working System

Under the Initiative, the Department of the Treasury (Treasury) operates the Initial Working System (the "Treasury Working System") to conduct a thorough review of databases and help verify eligibility and prevent IPs and UPs prior to the release of Federal funds. The Treasury Working System consists of six databases enumerated in the PIIA, as well as any additional databases designated by the Director of OMB or a designee. All agencies are required to use the Treasury Working System to support their payment process. At a minimum and before issuing any payment or award, each agency shall review as appropriate the databases within the Treasury Working System to verify eligibility of the payment.

2. Other Databases

In addition to the databases comprising the Treasury Working System, the Director of OMB (or a designee) may designate other databases that substantially assist in preventing IPs and UPs for inclusion in the Initiative. This may include the designation of additional working systems operated by other agencies. Before issuing any payment or award, each agency shall also review as appropriate the databases designated by the Director or a designee for inclusion in the Initiative that are outside of the Treasury Working System, to verify eligibility of the payment.

3. Designating Additional Databases for Inclusion in the Initiative

To become part of the Initiative or to suggest additional databases (either commercial or Government) for use in the Initiative, agencies must submit their request to Treasury, Bureau of Fiscal Service. OMB-established procedures and criteria will be followed to determine whether databases are designated into the Treasury Working System or included in the Initiative outside of the Treasury Working System.

4. **Agency Review of Data/Information Needs**

At a minimum, agencies should annually review their data/information themes under the following cause categories, 'Data Needed Does Not Exist', 'Inability to Access Data', and 'Failure to Access Data', and provide additional database suggestions to the Treasury Working System. If the agency does not know of a database that contains the criteria they need to validate the eligibility of the payment, the agency should consult the Treasury Working System to determine whether such a database exists and could be incorporated into the payment process of the agency or piloted to determine value under the Treasury Working System's pilot authority.

5. **Computer Matching Agreements Under the Initiative**

Generally speaking, agencies may enter into Computer Matching Agreements (CMAs) with other agencies that allow ongoing matching, which includes automated matching, in order to assist in the detection and prevention of IPs. In the context of the Initiative, when they meet applicable criteria, agencies may be able to operate matching programs that assist in the detection and prevention of IPs under procedures that vary from standard matching programs.

a) ***Waiving Requirements for Computer Matching Agreements***

Agencies may seek from Treasury a waiver of the CMA requirements under 5 U.S.C § 552a(o) in any case or class of cases for computer matching activities that involve a working system and that are conducted under the Initiative for the purposes of identifying and preventing IPs and UPs. A waiver will allow the implementation of a computer matching program without a CMA between the source agency and the recipient agency or non-Federal agency, provided there is sufficient authority, and any disclosure by a Federal agency is limited to only such information as is necessary and is made pursuant to a valid routine use or otherwise permitted by the Privacy Act. In the absence of an affirmative written waiver by Treasury, agencies must continue to comply with law and policy governing CMAs. Furthermore, a waiver of the CMA requirements under 5 U.S.C. § 552a(o) does not affect the due process rights of an individual under 5 U.S.C. § 552a(p). Even when granted a waiver of the CMA requirements, agencies must continue to comply with law and policy concerning due process in a matching program.

To request a CMA waiver for matching programs, agencies must send a CMA Waiver Request to Treasury. CMA Waiver Requests will be handled and evaluated by Treasury based on procedures and criteria established by OMB.

b) ***Modified Computer Matching Agreements***

Matching programs using databases that are part of the Initiative and do not involve a working system or otherwise do not obtain a waiver of the CMA requirements under 5 U.S.C § 552a(o) are subject to certain modified procedures established in the PIIA governing matching programs. The procedures apply to agreements that have the purpose of assisting in the detection and prevention of IPs.

(1)Data Integrity Board Review

Not later than 60 days after the date on which a proposal for a CMA for a matching program with the purpose of assisting in the detection and prevention of IPs and UPs has been presented to a Data Integrity Board (DIB) for consideration, the DIB shall respond to the proposal.

(2)Extension
A CMA for a matching program with the purpose of assisting in the detection and prevention of IPs and UPs will have a termination date of less than three years. During the 3-month period ending on the date on which the agreement is scheduled to terminate, the agreement may be renewed by the agencies entering the agreement for not more than 3 additional years.

(3)Multiple Agencies
A CMA for a matching program with the purpose of assisting in the detection and prevention of IPs and UPs may involve multiple agencies.

(4)Savings Estimate
An agency justification, under 5 U.S.C. § 552a(o)(1)(B), for a matching program with the purpose of assisting in the detection and prevention of IPs and UPs is not required to contain a specific estimate of any savings under the CMA.

F. Identifying and Achieving a Tolerable IP Rate

In the context of Enterprise Risk Management and the management of payment integrity risk, agency senior management should identify their Risk Appetite for Payment Integrity risk in relation to accomplishing strategic objectives and while considering reputational risks that can impact trust in the agency. Agency senior management must acknowledge that while every action has risk, their job is to mitigate risk without jeopardizing the mission. With this Risk Appetite in mind, agency leaders can set Risk Tolerance bands for IPs and UPs for each program. Agency senior management should balance payment integrity risk with controls to identify, achieve, and maintain a tolerable IP and UP rate for a program. Identifying IPs and UPs that are unavoidable and beyond the agency's ability to reduce to the statutory threshold, is an important component in identifying and achieving a tolerable IP and UP rate. When determining the tolerable IP and UP rate of IPs and UPs, the agency senior management may consider, among other things, the blanket thresholds included in PIIA that are used to initially help identify programs that are likely to be susceptible to significant IPs plus UPs. However, the tolerable IP and UP rate for a program may be either above or below this blanket threshold. It is up to agency senior management to determine how low a program IP and UP rate can be without disproportionally increasing another risk. For example, a program's tolerable IP and UP rate may be 7.5% if the agency senior management determines that additional controls to lower the rate below 7.5% would significantly alter the program mission or represent an inefficient use of taxpayer funds to operate the program (i.e. spending $2 to prevent a $1 of IPs).

G. Tolerable IP and UP Rate vs. IP and UP Reduction Target Rate

If a program's tolerable IP and UP rate is above the statutory threshold, then the IP and UP reduction target will eventually be set to equal that tolerable IP and UP rate. When a program establishes an IP and UP reduction target, it is only for the following FY, as such if a program needs multiple years to achieve a tolerable IP and UP rate it may take multiple years for the program to establish an IP and UP reduction target that is equal to the tolerable IP and UP rate. For compliance purposes, programs reporting an IP and UP estimate that is above the statutory threshold are only required to establish and publish an IP and UP reduction target for the following year. However, if the IP and UP reduction target is greater than the tolerable IP and

UP rate, and a program needs multiple years to achieve their tolerable IP and UP rate, programs should establish a plan(s) for achieving both rates.

H. Examples of Prevention Strategies

Prevention of IPs requires a multi-pronged approach that is continually evolving. For example, a program will often have multiple mitigation strategies and corrective actions in place to prevent IPs and UPs from occurring and it can take extraordinary patience and thought to develop prevention capabilities that are both cost-effective and successful. Table 6 below highlights examples of some of the common IP and UP mitigation strategies and corrective actions currently being used by agencies to prevent IPs and UPs.

IP Mitigation Strategies and Corrective Actions	Example
Automation	Automated interface between financial system and the system for award management; converting payments to electronic methods
Behavioral/Psychological Influence	Changing the way options are ordered or presented helps reduce cognitive burden and enable individuals to make better choices
Training	Refresher sessions; external trainings; mandatory annual trainings; prior authorization
Internal Process or Policy Change	Starting quality reviews; new pre-check list; policy update cycles
Cross Enterprise Sharing	Workgroups; playbooks; cross-agency best practice sharing; pilots; data sharing
Audits	Frequent reconciliations; access restrictions; passwords; exception reports
Predictive Analytics	Automatically rejecting a payment when the existence of a number of known IP characteristics are present.

Table 6. Improper Payment Mitigation Strategies and Corrective Actions

V. Identification and Recovery of Overpayments

It is important to remember that recoveries can only be made on actual monetary loss IPs, also referred to as overpayments that are determined recoverable and not on the statistical projections used to estimate the annual IP amount for a program. Non-Monetary loss type IPs are unable to be recovered because no cash disbursement was made to the wrong recipient in the wrong amount. Monetary loss type IPs have recovery potential. The recovery potential of an UP cannot be determined until the executive agency concludes whether the payment is a proper payment, a non-monetary loss type IP, or a monetary loss type IP.

A. Overpayment Identification

While it is preferable that agencies focus efforts toward preventing the overpayment from occurring, it is important for agencies to have cost effective means to both identify and recover the overpayment if it does occur. Agencies use a variety of policies and activities to identify and recover overpayments. The examples that follow are not meant to provide an exhaustive list of overpayment identification methods, rather they are meant to help agencies strengthen their payment process. Each agency must determine the most cost-effective method for their particular circumstance.

1. **Reviews**

Reviews are a mechanism agencies use to assist with identification of overpayments across the Federal Government. This includes but is not limited to activities such as IP risk assessments

conducted under PIIA, agency post-payment reviews, Budget Execution Monthly Reviews, Dormant Account Reviews; Monitoring Debt collection software to track recovery of overpayments; SF-50 vs. SF52 validation, and S&EMP conducted under PIIA.

2. **Audits**

The use of audits is also another common mechanism that helps identify overpayments. Examples include but are not limited to performance of post-award audits, recovery auditing techniques such as data matching with Federal, State, and local databases, audit reports, GAO audits, OIG audits, and the results of the agency audit resolution and follow-up process.

3. **Data Analytics**

Using data analytics to identify overpayments is not only beneficial for identifying overpayments after they have occurred, but it establishing a robust data analytics effort can move an agency from a "pay-and-chase" approach to a predictive approach allowing the agency to identify potential IPs or UPs before they even occur. There are wide range of analytics techniques available such as rule-based, anomaly detection, predictive analytics, network/link analytics, or text analytics. Examples of analytics approaches used to identify overpayments include but are not limited to using data analytics to monitor and detect misuse in ongoing complex contracts, to monitor and detect misuse in Government purchase cards, for identifying above average payments to a vendor, for identification of duplicate payments, or to identify exceeded purchase orders.

4. **Reports**

Reports can also be helpful for identifying overpayments. While reports are in a 'pay-and-chase' status, programs can often use the reports to help identify weaknesses in internal controls that, if strengthened, could prevent future overpayments from occurring. Examples of such reports include but are not limited to GAO reports, reports from the public such as new media, or self-reported errors.

5. **Reconciliations**

Reconciliations are a common accounting mechanism which have the benefit of helping identify overpayments. Examples include but are not limited to conducting contract reconciliations by comparing invoices, receiving reports, and payments as well as verifying the terms of the contract have been met and are properly recorded, performing reporting and accounting outlays reconciliations, service provider payroll disbursement reconciliations, general ledger gross pay file reconciliation, or reconciling employee data with the accounting and disbursing systems. When overpayments are identified through reconciliation programs should review their internal controls and determine whether additional mitigation strategies should be established to prevent the overpayments from occurring in the future.

B. Recovery Audits and Activities Program

Agencies should conduct their recovery audits and activities program in a manner that will ensure the greatest financial benefit for the Government. The methods to identify and recover overpayments must be cost-effective regardless of whether the recovery audits and activities program utilizes a recovery audit or other mechanisms to identify and recover overpayments. Each agency will determine the most cost-effective combination of recovery activities and recovery audits as part of their Recovery Audits and Activities Program.

1. **Cost-Effectiveness of Using a Recovery Audit**

All programs that expend $1,000,000 or more annually should be considered for recovery audits, however, agencies are only required to conduct recovery audits if conducting the audits would be cost-effective.

Agencies may exclude payments from certain programs from recovery audit activities if the agency determines that recovery audits are not a cost-effective method for identifying and recapturing overpayments or if other mechanisms to identify and recapture overpayments are already in place. Common mechanisms used to identify overpayments outside of a recovery audit include: statistical samples and IP risk assessments, agency post-payment reviews, prior payment recapture audits, Office of Inspector General (OIG) reviews, Government Accountability Office reports, self-reported errors, reports from the public, audit reports, and the results of the agency audit resolution and follow-up process.

2. **Determining Cost-Effectiveness of Using a Recovery Audit**

When determining the cost-effectiveness of a recovery audit, an agency should assess the likelihood that the expected recoveries will be greater than the costs incurred to identify and recover the overpayments. When assessing the cost-effectiveness of the overpayment identification, agencies should consider whether their current business practices that make up their Recovery Activities (e.g., Single Audit reports; self-reported overpayments, statistical samples conducted under PIIA, agency post-payment reviews, etc.) provide an efficient and effective means for the identification of overpayments. Agencies must be mindful of the costs incurred to identify and recover overpayments and should consider whether there is value in leveraging their internal controls to build their Recovery Activities and Audits Program. Tracking the identification of overpayments and subsequent recovery efforts and evaluating the mechanisms used to do is important for operating a cost-effective Recovery Audits and Activities Program.

Agencies should consider whether laws or regulations allow recovery; whether the recipient of the overpayment is likely to have resources to repay overpayments from non-Federal funds; and how expensive attempts to recover some or all of the overpayments will be. Agencies are encouraged to pilot limited scope recovery audits in areas deemed of highest risk (e.g., based on PIIA IP risk assessments or estimation process) to assess the likelihood of cost-effective recovery audits on a larger scale.

Recovery audits are generally most efficient and effective where there is a central electronic database (e.g., a database that contains information on transactions and eligibility information) and sophisticated software that can be used to perform matches and analysis to identify the significant overpayments (e.g., duplicate payments) that are recoverable at a low cost per overpayment.

If an agency determines that it would be unable to conduct a cost-effective recovery audit for certain programs, the analysis will need to be repeated only if circumstances change within the program that might make a recovery audit cost-effective.

3. **Implementation of a Recovery Audit**

If an agency determines that a recovery audit would be cost-effective, the recovery audit should be implemented in a manner designed to ensure the greatest financial benefit to the Federal Government. The agency shall give priority to the most recent payments and to payments made

in any program reporting an IP estimate above the statutory threshold. Agencies may conduct the recovery audit directly, by using other departments and agencies of the United States, or by procuring performance of recovery audits by private sector sources by contract, subject to the availability of appropriations, or by any combination thereof.

a) ***Using a Contract for Recovery Audit***

(1)Recovery Audit Contractor May:
If an agency chooses to conduct a recovery audit by contract, the agency may authorize the contractor to notify entities, including individuals, of potential overpayments made to those entities; respond to questions concerning potential overpayments; and take other administrative actions with respect to an overpayment claim made or to be made by the agency.

(2)Recovery Audit Contractor May Not:
In addition to provisions that describe the scope of recovery audits (and any other provisions required by law, regulation, or agency policy), any contract with a private sector firm for recovery audit services should include provisions that prohibit the recovery audit contractor from:

a. Having the authority to make a final determination relating to whether any overpayment occurred or whether to compromise, settle, or terminate an overpayment claim;
b. Requiring production of any records or information by the agency's contractors. Only duly authorized employees of the agency can compel the production of information or records from the agency's contractors, in accordance with applicable contract terms and agency regulations;
c. Using or sharing sensitive financial information with any individual or organization, whether associated with the Federal Government or not, that has not been officially released for use by the general public, except for an authorized purpose of fulfilling the payment recapture audit contract; and
d. Disclosing any information that identifies an individual, or reasonably can be used to identify an individual, for any purpose other than as authorized for fulfilling its responsibilities under the payment recapture audit contract.

(3)Specific Required Actions for Contractor and Agency

Required Actions for the Contractor	Required Response from the Agency
notify the agency of any overpayments identified pertaining to the agency	take prompt and appropriate action to collect overpayments
provide to the agency periodic reports on conditions giving rise to overpayments identified	take prompt and appropriate action to address the recommendations
provide any recommendations on how to mitigate the conditions giving rise to overpayments	
notify the agency of any overpayments identified pertaining to any other agency that are beyond the scope of the contract	take prompt and appropriate action to forward to other agencies any information that applies to that agency
report to the agency credible evidence of fraudulent overpayments or vulnerabilities to fraudulent overpayments	take prompt and appropriate action to address the vulnerabilities to fraudulent overpayments
conduct appropriate training of personnel of the contractor on identification of fraudulent and non-fraudulent overpayments	

Table 7. Recovery Audit Requirements for the Agency and the Contractor

Agencies should require contractors to become familiar with the agency's specific policies and procedures and may allow recovery audit contractors to establish a presence on, or visit, the property, premises, or offices of any subject of recovery audits.

b) ***Contingency Contract With a Private Sector Contractor***

With respect to contracts with private sector contractors performing recovery audits, agencies may utilize a number of options, including a contingency contract with a private sector contractor, to conduct recovery audit services.

However, certain types of payments recovered may not be available to pay the recovery audit costs (for instance, amounts recovered due to interim IPs made under ongoing contracts if these amounts are still needed to make subsequent payments under the contract or amounts recovered from closed accounts). Therefore, agencies would need to establish other funding arrangements (such as through appropriations) when making payments to private sector payment recapture audit contractors in such cases where recoveries cannot be used to pay contingency fee contracts.

4. **Collection of Overpayments**

The actual collection activity may be carried out by Federal agencies or non-Federal entities expending Federal awards, as appropriate. However, agencies or non-Federal entities may use another private sector entity, such as a private collection agency, to perform this function, if this practice is permitted by statute. A recovery audit contractor may not perform the collection activity, unless it meets the definition of a private collection agency, and the agency involved has statutory authority to utilize private collection agencies. Agencies should ensure that applicable laws and regulations governing collection of amounts owed to the Federal Government are followed.

5. **Rules for disposition of overpayments recovered with a Recovery Audit**

The agency will determine the distribution of overpayments recovered with a recovery audit in accordance with the disposition requirements below:

a) ***Overpayments Collected under Recovery Audit from Expired Discretionary Treasury Appropriation Fund Symbols (TAFSs) Containing Funds Appropriated after July 22, 2010***
If the overpayment has been collected from an expired discretionary Treasury Appropriation Fund Symbol (TAFS) containing funds appropriated after July 22, 2010, then the agency head must first reimburse the actual expenses incurred by the agency in the administration of the Recovery Audits and Activities program. After they have reimbursed for actual expenses, the agency head may distribute up to a select percentage among a Financial Management Improvement Program, the Original Purpose; and/or to Inspector General Activities. Finally, the remaining amount should either be deposited in the Treasury or reverted depending on the specific type of TAFS.

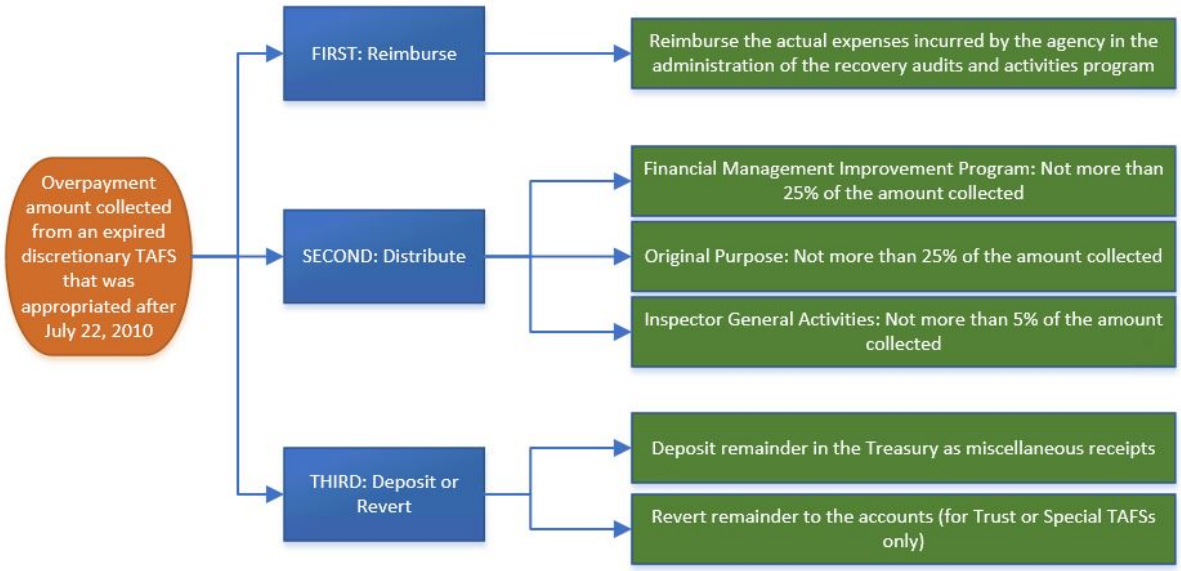

Figure 10. Disposition of Overpayment collected from an expired discretionary TAFS that was appropriated after July 22, 2010

(1)Using overpayment collections for a Financial Management Improvement Program
Not more than 25 percent of the amounts collected may be used for a Financial Management Improvement Program. If the recovered overpayments are used for a Financial Management Improvement Program, this funding may be credited, if applicable, for the purpose of the Financial Management Improvement Program by the agency head to any agency appropriations (i.e., TAFS) that are available for obligation at the time of collection. These funds should be used to supplement and not supplant any other amounts available for the Financial Management Improvement Program, and should remain available until expended. Such funds can go to non-Federal entities such as State and local governments if the agency determines that is the best disposition of the funds to support its Financial Management Improvement Program.

(2)Using overpayment collections for their Original Purpose
Not more than 25 percent of the amounts collected may be used for the original purpose. This funding should be credited to the appropriation (i.e., TAFS), if any, available for obligation at the time of collection for the same general purposes as the appropriation (i.e., TAFS) from

which the overpayment was made, and must remain available for the same period of availability and purposes as the appropriation (i.e., TAFS) to which credited.

(a) Using Trust or Special (i.e., TAFS) overpayment collections for their Original Purpose

If the appropriation from which an overpayment was made has expired, and the recovered overpayments are made from a trust or special TAFS, the funds shall revert to that account.

(b) Using Non-Trust of Non-Special (i.e., TAFS) overpayment collections for their Original Purpose

If the appropriation from which an overpayment was made has expired and the recovered overpayments are NOT from a trust or special fund account, the funds are newly available for the same time period as the funds were originally available for obligation. If the funds have been recovered more than five FYs from the last FY in which the funds were available for obligation, then the recovered overpayments shall be deposited into the Treasury as miscellaneous receipts.

(3)Using overpayment collections for Inspector General Activities

Not more than five percent of the amounts collected by an agency through recovery audits shall be available to the OIG of that agency for the OIG to carry out PIIA requirements; or any other activities of the OIG relating to investigating IPs or auditing internal controls associated with payments. The funding shall remain available for the same period and purposes as the appropriation (i.e., TAFS) to which credited.

(4)Remaining Overpayment Collections

Amounts collected that are not used (1) To reimburse the actual expenses incurred by the agency in the administration of the program, (2) To carry out the Financial Management Improvement Program, (3) For the Original Purpose, or (4) For OIG Activities, shall be deposited in the Treasury as miscellaneous receipts, except that in the case of recoveries of overpayments that are made from trust or special TAFS, those amounts shall revert to those TAFS.

b) ***Overpayments Collected under Recovery Audit from Unexpired Discretionary TAFSs, Expired Discretionary TAFSs Appropriated before July 22, 2010, or from Mandatory TAFSs***

If the overpayment has been collected from an unexpired discretionary TAFS, an expired discretionary TAFS that was appropriated before July 22, 2010, or from a mandatory TAFS then the agency head must credit the TAFS from which the overpayment was made and the amount must be available for the purpose of the TAFS and to reimburse the actual expenses incurred by the agency in the administration of the program.

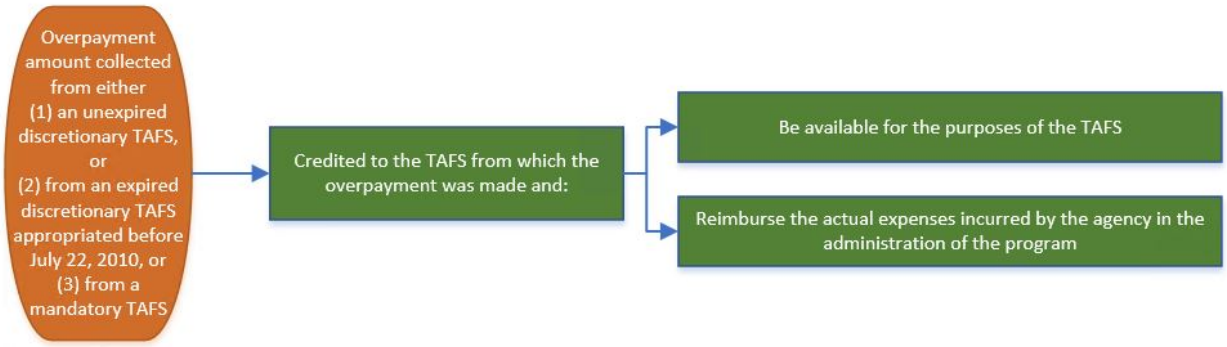

Figure 11. Disposition of Overpayment collected from either (1) an unexpired discretionary TAFS, or (2) from an expired discretionary TAFS appropriated before July 22, 2010, or (3) from a mandatory TAFS

c) ***Overpayments Collected under Recovery Audit from Closed TAFSs***

If the overpayment is collected from a closed TAFS, the budgetary resources are cancelled and the amount is deposited in the Treasury as miscellaneous receipts.

Figure 12. Disposition of Overpayment collected from a closed TAFS

d) ***Example of the Disposition of Overpayments Recovered through a Recovery Audit***
Figure 13 provides a decision tree that can be used to help with the proper disposition of overpayments recovered through recovery audits.

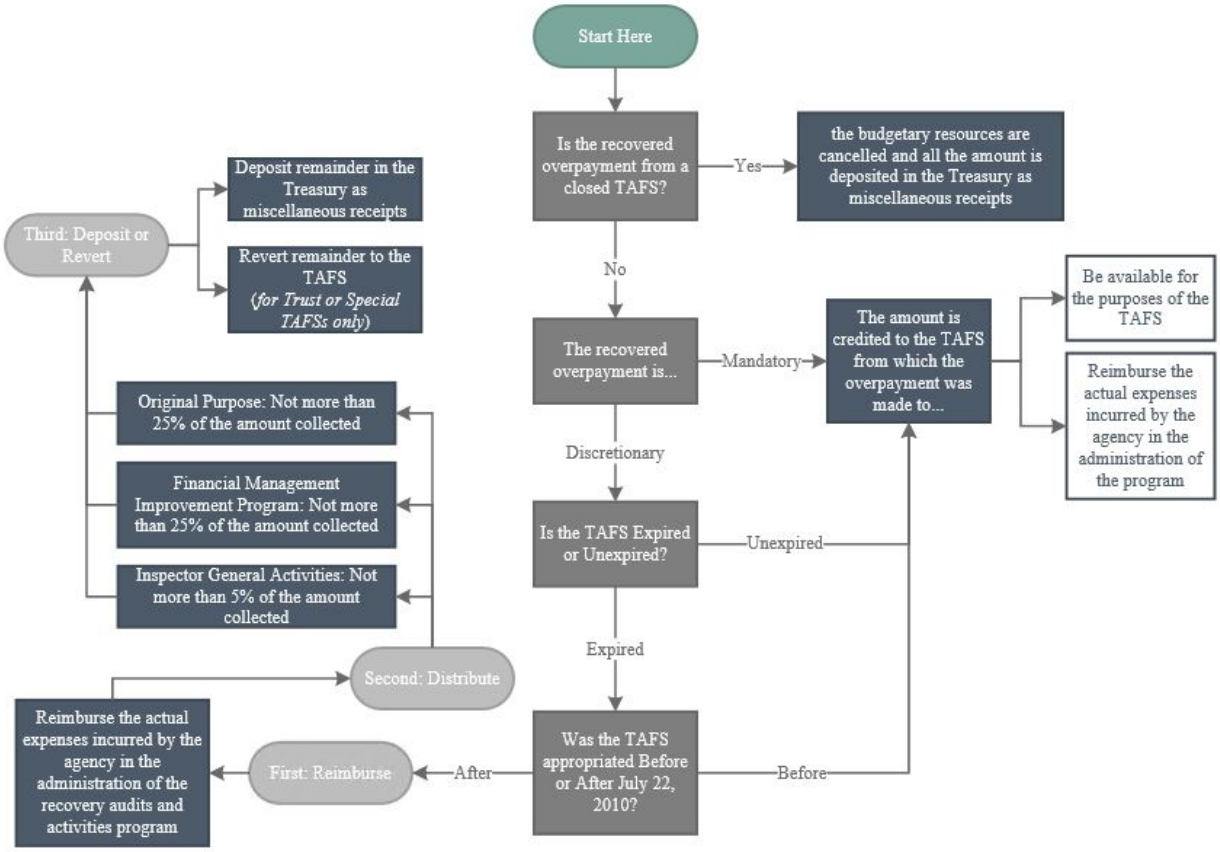

Figure 13. Decision Tree for Disposition of Overpayments Recovered through a Recovery Audit

VI. Compliance

Each FY, the agency is responsible for ensuring it has met the requirements to achieve compliance with PIIA and the OIG is responsible for evaluating the agency to determine whether the agency is compliant with PIIA. The IG is responsible for submitting a report on that determination. The OIG review of the accompanying materials to the FY2021 annual financial statement will be considered year 1 of a PIIA compliance review and all programs will consider the resulting OIG compliance report to be year 1 of the report for the purpose of implementing Section VI.D of this guidance.

A. Achieving and Evaluating Compliance (Agency and OIG Responsibilities)

If a program does not meet one or more of the following requirements then it is not compliant under PIIA. An agency is considered to be not compliance under PIIA if it has one or more programs that are found non-compliant with PIIA.

1a. Published Payment Integrity information with the annual financial statement

To achieve compliance the agency must publish any applicable payment integrity information in its annual financial statement in accordance with payment integrity guidance provided in OMB Circular A136. In addition, the agency must publish any applicable payment integrity information required in the accompanying materials to the annual financial statement in accordance with applicable guidance. The most common accompanying materials to the annual financial statement are the payment integrity information published on paymentaccuracy.gov. This information is provided by the agency to OMB through the Annual Data Call and is then subsequently published on paymentaccuracy.gov.

The OIG should evaluate whether the agency has followed applicable requirements related to the formulation and inclusion of the payment integrity information in the annual financial statement and in the accompanying materials to the annual financial statement. In addition to consulting this guidance document, the OIG should consult the following documents, at a minimum, to determine and evaluate the applicable requirements for their agency: OMB Circular A-136, OMB Annual Data Call Instructions, OMB Payment Integrity Question and Answer Platform, and the CIGIE guidance required under PIIA.

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program regarding the specific actions and steps the program must take to achieve compliance with this criterion.

1b. Posted the annual financial statement and accompanying materials on the agency website

To achieve compliance the agency must include a link to paymentaccuracy.gov within its annual financial statement to any accompanying materials to the annual financial statement required under guidance from OMB and then publish their annual financial statement on their agency website.

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program and/or other part of the agency regarding the specific actions and steps the program must take to achieve compliance with this criterion.

2a. Conducted IP risk assessments for each program with annual outlays greater than $10,000,000 at least once in the last three years

To achieve compliance the agency must conduct an IP risk assessment at least once every three years, for each program with annual outlays greater than $10,000,000 to determine whether the program is likely to make IPs plus UPs that would be in total above the statutory threshold. The agency is responsible for ensuring that all programs with annual outlays greater than $10,000,000 have been assessed at least once every three years.

The OIG should evaluate whether the agency has conducted IP risk assessments for each program with annual outlays greater than $10,000,000 at least once in the last three years. When assessing the timing and rotation piece of this criterion, the OIG should take into account factors such as, the specific IP risk assessment timing requirements when there are new programs, whether the program in question has been fluctuating back and forth above and below $10,000,000 in annual outlays, and whether the program is already in Phase 2 and is no longer required to conduct a separate IP risk assessment once every three years.

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program and/or other part of the agency regarding the specific actions and steps the program must to take achieve compliance with this criterion.

2b. Adequately concluded whether the program is likely to make IPs and UPs above or below the statutory threshold

To achieve compliance the agency must ensure that the IP risk assessment methodology used adequately concludes whether the program is likely to make IPs plus UPs above or below the statutory threshold.

The OIG should evaluate and take into account the adequacy of the program IP risk assessment when determining program compliance. The OIG should review the IP risk assessment methodology of the agency, including whether the audits, examinations, and legal actions of the OIG indicate a higher risk of IPs or actual IPs that were not included in the IP risk assessments. After evaluating the program's assessment of the level of IP risk the OIG should determine whether the IP risk assessment adequately concludes whether the program is likely to make IPs and UPs above or below the statutory threshold. The OIG is not required to recreate every step of the IP risk assessment, but rather to ensure that the IP risk assessment methodology employed by the agency adequately concludes whether the program is likely to make IPs and UPs above or below the statutory threshold.

If the OIG determines that the IP risk assessment incorrectly identified whether the program is likely to make IPs and UPs above or below the statutory threshold the OIG should provide recommended changes the program should make to their IP risk assessment methodology to achieve the alternate conclusion.

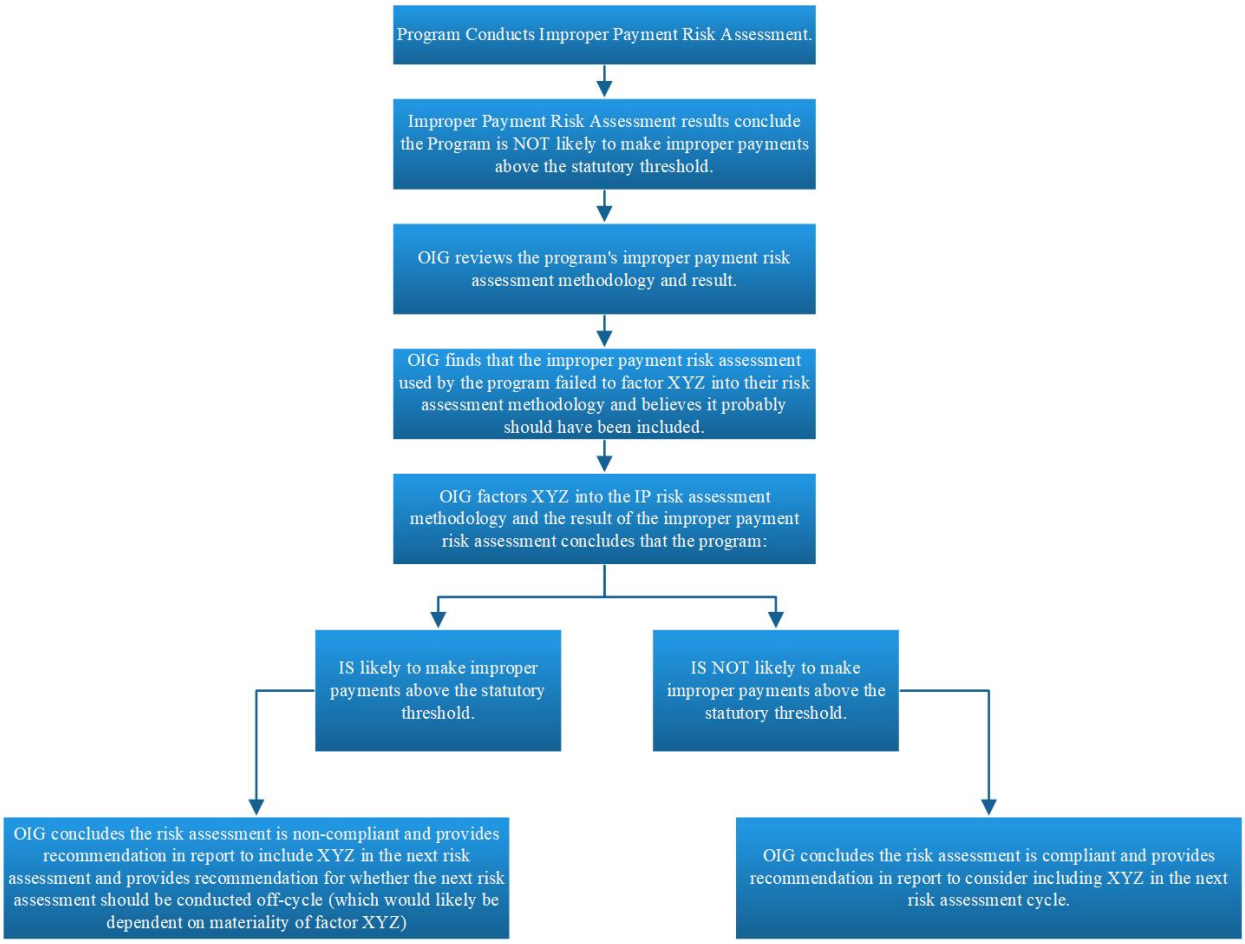

Figure 14. Example of OIG Compliance Evaluation of a Program's IP Risk Assessment

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program regarding the specific actions and steps the program must to take achieve compliance with this criterion.

3. **Published IP and UP estimates for programs susceptible to significant IPs and UPs in the accompanying materials to the annual financial statement**

To achieve compliance the program should submit a S&EMP to OMB in the FY after the FY that the program was deemed likely to be susceptible to IPs and UPs and subsequently publish an IP and UP estimate. If the IP and UP estimate is above the statutory threshold then the program should continue publishing an IP and UP estimate for that program in the following FY. Agencies should ensure that the program IP and UP estimate is accurate and that the S&EMP used is appropriate given program characteristics.

The OIG should evaluate and take into account the adequacy of the S&EMP when determining program compliance. The OIG should review the accuracy of the IP and UP estimate and whether the S&EMP used is appropriate given program characteristics. The OIG is not required to recreate every step of the S&EMP, but rather to ensure that the S&EMP employed by the agency produced an IP and UP estimate that was representative of the program's annual IPs and UPs.

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program and/or other part of the agency regarding the specific actions and steps the program must take to achieve compliance with this criterion.

4. **Published corrective action plans for each program for which an estimate above the statutory threshold was published in the accompanying materials to the annual financial statement**

Each program reporting an IP plus an UP estimate that is above the statutory threshold must publish corrective action plans in the accompanying materials to the annual financial statement. The program is responsible for ensuring that the root causes are properly identified and that the corrective action plans are effective and adequately address the root causes of IPs and UPs. The program should be able to demonstrate that it has properly identified the cause(s) of IPs and UPs, the point within the payment process where the transaction turned from 'proper' to 'improper', and that the mitigation strategies and corrective actions it has developed and implemented to address the causes are effective.

In addition, the agency is responsible for effectively implementing and prioritizing the programmatic corrective action plans within the agency to prevent the largest amount of IPs. The agency should be able to demonstrate that its programmatic corrective action plans are effectively implemented and how they are prioritized within the agency. Finally, the agency should be able to demonstrate how the corrective actions are preventing and reducing IPs.

When determining compliance, the OIG should first evaluate the root cause and eligibility classification and determine whether the program has correctly identified the causes of IPs and UPs. The OIG should also review the oversight and/or financial controls used by the program to identify and prevent IPs and UPs.

When reviewing the corrective action plans for compliance, the OIG should evaluate and take into account whether the corrective action plans:

1. are focused on the true causes of IPs and UPs;
2. are adequately addressing those causes;
3. are effective;
4. are effectively implemented;
5. are prioritized within the agency; and
6. are reducing IPs.

If an agency and OIG agree a program has reached a tolerable IP and UP rate, then the OIG should evaluate and take into account whether the corrective action plans will maintain the tolerable IP and UP rate for the program.

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program regarding the specific actions and steps the program must take to achieve compliance with this criterion.

5a. Published an IP and UP reduction target for each program for which an estimate above the statutory threshold was published in the accompanying materials to the annual financial statement

If a program's reported IP estimate plus the UP estimate is above the statutory threshold, the program is required to establish and publish an IP and UP reduction target for the following FY in the accompanying materials to the annual financial statement. In general, reduction targets will likely be lower than the current year (CY) IP estimate plus the UP estimate unless the program has reached its tolerable IP and UP rate. If a program has reached its tolerable IP and UP rate, the reduction target will be identical to the CY IP and UP estimate. If a program establishes a reduction target that does not decrease (e.g., a target that is constant or increasing), the program should be able to clearly explain the reason(s) for establishing such a target.

A program should ensure that their IP and UP reduction target is the appropriate balance of aggressive and realistic given the program characteristics. In establishing a reduction target with and aggressive and realistic balance, a program should consider available resources to ensure that the established reduction target does not result in the need for the agency to spend more preventing the IP or the UP than the actual IP or the UP itself. In establishing an aggressive and realistic reduction target the program should also consider existing program characteristics to ensure that achieving the established target is not something outside of the agency's control. An aggressive and realistic target may be equal to the CY IP and UP estimate if the program has achieved its tolerable IP rate. An aggressive and realistic may be lower than the CY IP and UP estimate if the program is still able to deploy resources effectively to increase the amount of IPs the program prevents on an annual basis.

OMB does not expect the program to publish a reduction target until a baseline has been established and reported. If the program's reported IP estimate plus the UP estimate is below the statutory threshold the program is not required to establish and publish a reduction target for the next FY.

When determining compliance the OIG should take into account whether the program was required to establish a reduction target based on their reported IP and UP estimate. If the program was required to do so, the OIG should determine whether the program published a reduction target that was appropriately aggressive and realistic given the program characteristics.

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program and/or other part of the agency regarding the specific actions and steps the program must take to achieve compliance with this criterion.

5b. Demonstrated improvements to payment integrity or reached a tolerable IP and UP rate

If the program reported an IP and UP estimate above the statutory threshold in the prior year and the CY, and the program has not yet achieved its tolerable IP and UP rate, the program is responsible for demonstrating improvements. The program should ensure that it undertakes new actions during the year to improve their payment integrity. For corrective actions taking several years to implement, new action includes forward progress on the milestones needed to fully implement the corrective action plan. The program will be responsible for demonstrating improvements in their payment integrity each year following a year that the program reports an IP and UP estimate above the statutory threshold, therefore, programs should be mindful of new

actions taken each year to continue to improve their payment integrity until the program has achieved a tolerable IP and UP rate. While improvements that bring the IP estimate to a tolerable IP rate are what programs should strive for, achieving compliance is not contingent upon the magnitude of the improvement(s). Examples of improvements could include but are not limited to:

1. reducing the IP and UP estimate,
2. meeting the set reduction target,
3. enhancing or expanding sampling and estimation methods (examples could include but are not limited to including a new portion of the population in the S&EMP or tightening a confidence interval),
4. developing or implementing new mitigation strategies (examples could include but are not limited to exploring how behavioral insights or automation could prevent IPs and UPs in the program),
5. determining the tolerable IP and UP rate (examples could include but are not limited to conducting a cost benefit analysis to help determine the usefulness of increasing preventative measures),
6. expanding or enhancing corrective action plans (examples could include but are not limited to piloting promising aspects from a corrective action plan with a new population), or
7. moving from low value to high value payment integrity related work (examples could include but are not limited to reviewing internal agency payment controls and eliminating those which are not necessary to ensure the payment is proper in accordance with PIIA).

If a program cannot demonstrate that it took new actions during the year to improve payment integrity, the program should be prepared to demonstrate that it has achieved their tolerable IP and UP rate and are taking actions to maintain the rate.

When evaluating whether a program has demonstrated improvement, the OIG should consider whether the program has taken any new action within the past year to improve payment integrity. If the program cannot demonstrate that new actions have been taken then the OIG should consider whether the program has achieved a tolerable IP and UP rate and is taking actions to maintain the tolerable IP and UP rate.

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program regarding the specific actions and steps the program must take to achieve compliance with this criterion.

5c. Developed a plan to meet the IP and UP reduction target

If the program reported an IP and UP estimate above the statutory threshold in the CY, and established an IP and UP reduction target for the following FY, the program is responsible for developing a plan to meet the reduction target established. The program should maintain and update the plan to meet the IP and UP reduction target as needed to ensure that the program will be able to demonstrate improvements in payment integrity that occurred over the course of the FY.

Failing to meet a reduction target does not equate to non-compliance, however, if this occurs, the program should revisit their methodology for establishing the IP and UP reduction target to ensure that the next reduction target is an appropriate balance of aggressive and realistic and the

program should revisit and if needed revise their plan to meet the IP and UP reduction target as well. The plan to meet the IP and UP reduction target will likely be similar to, or even a subpart of, the corrective action plan, however, the plan to meet the IP and UP reduction target is specifically focused on the actions the program will take during the following year to meet the IP and UP reduction target they have established for the following FY.

When evaluating whether a program has demonstrated improvement, the OIG should consider whether the program has a plan to meet the IP and UP reduction target they have established for the following FY. If an agency and OIG agree a program has reached a tolerable IP and UP rate, then OIG should consider whether the program has a plan to maintain the tolerable IP and UP rate.

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program and/or other part of the agency regarding the specific actions and steps the program must take to achieve compliance with this criterion.

6. **Reported an IP and UP estimate of less than 10% for each program for which an estimate was published in the accompanying materials to the annual financial statement**

If the program reported an IP and UP estimate above 10% for the FY, the program will be non-compliant. If a program reports an IP and UP estimate above 10% for multiple consecutive FYs, the program should seriously consider whether additional actions can be taken to reduce the rate or whether the program may have achieved its tolerable IP and UP rate.

When evaluating whether a program has reported an IP and UP estimate of less than 10% for each program, the OIG should take into consideration the point estimate for the program. If the IP and UP estimate is greater than or equal to 10%, the OIG should take into consideration whether the program has demonstrated that it has achieved a tolerable IP and UP rate when evaluating this criterion and when providing recommendations to achieve compliance.

If the OIG determines that a program is non-compliant for this particular criterion then the final OIG report must provide concrete recommendations to the program and/or other part of the agency regarding the specific actions and steps the program must take to achieve compliance with this criterion. To help the program provide essential information in their non-compliance reports, if the action(s) and steps needed to become compliant are not cost-effective or require a statutory or regulatory change that significantly interferes with program statutory purpose, then the OIG should state the funding and/or statutory or regulatory changes needed and then explain why they are infeasible.

B. Procedures for Compliance Determinations

In accordance with PIIA, OIGs should consult guidance issued by CIGIE for specific procedures regarding how they should determine compliance. In particular, OIGs should consult guidance issued by CIGIE for their procedures for evaluating:

1. the IP risk assessment methodology of the program, including whether the audits, examinations, and legal actions of the OIG indicate a higher risk of IPs or actual IPs were not included in the IP risk assessments;
2. the accuracy of the IP and UP estimates and whether the S&EMP used is appropriate given program characteristics;

3. the corrective action plans for the program and whether they are adequate and focused on the true causes of IPs;
4. whether the actions taken to implement the corrective action plans are reducing IPs and UPs;
5. whether the corrective action plans for the program are effectively implemented;
6. whether the corrective action plans for all programs are effectively prioritized within the agency;
7. the adequacy of agency and program corrective action plans to address the causes of IPs;
8. the agency and program efforts to prevent and reduce IPs and UPs; and
9. whether an agency has published an annual financial statement.

In addition, the OIGs must consult guidance issued by CIGIE for the procedures they should follow to identify and make any recommendations for actions the program and/or other part of the agency could take to further improve the prevention and reduction of IPs and UPs.

C. Requirements for the OIG Compliance Report

After each agency OIG has reviewed the payment integrity reporting in the agency's annual financial statement, and accompanying materials to the annual financial statement, to determine if the agency is in compliance under PIIA, it is required to prepare a report.

1. PIIA OIG Compliance Report Due Date

The review typically begins when the annual financial statement and the accompanying materials to the annual financial statement are published, which typically occurs in mid-November. The OIG compliance report should be published within 180 days after the day the publication date for the Annual Financial Statement of the Agency and the Accompanying Materials to the Annual Financial Statement of the Agency, whichever is later. If the 180th day falls on a weekend, the review, determination, and report should be completed by the next business day.

2. PIIA OIG Compliance Report Recipients

The OIG should publish their final PIIA Compliance report on the public central website designated by the Council of the Inspectors General on Integrity and Efficiency. Once the report has been published, a link to the report should be electronically provided to the following:

1. The head of the agency;
2. The Committee on Homeland Security and Governmental Affairs of the Senate;
3. The Committee on Oversight and Reform of the House of Representatives;
4. The appropriate authorizing and appropriations committees of Congress;
5. The Comptroller General of the United States; and
6. The Controller of the Office of Management and Budget
    a. *Submission of PIIA OIG Compliance Reports to OMB*: To submit a report to the Controller of the OMB the OIG should upload the link to their final report to the Payment Integrity Information Act Required Submissions to OMB page on the Max community.

The OIG may also share a pdf of the report with the recipients above. To reduce waste and unnecessary burden, the OIG should refrain from physically printing and mailing the final report or any associated material (i.e. cover letters) to the recipients above.

3. **Agency Efforts to Prevent and Reduce IPs and UPs**

The final compliance report must also include an evaluation of agency efforts to prevent and reduce IPs and UPs. This overall evaluation of agency efforts to prevent and reduce IPs and UPs is a requirement for all OIG reports regardless of whether the agency being evaluated has programs reporting estimates above the statutory threshold. This evaluation is also in addition to any evaluation of an individual program's compliance with the specific criterion in Section VI.A of this guidance.

In addition, for each agency program reporting an estimate above the statutory threshold, the OIG must include recommendation(s) for action(s) to further improve prevention and reduction of IPs and UPs within the program. The OIG will engage with the program and/or other part of the agency regarding the specific corrective action recommendations to ensure appropriate and effective corrective action recommendations are made. The OIG should not recommend any actions which would adversely impact the compliance with the criterion in Sections VI.A or VI.B of this guidance.

If the program reported an IP and UP estimate above the statutory threshold, and the OIG is unable to provide concrete recommendations for actions to further improve the prevention and reduction of IPs and UPs in a program, then the OIG must state whether it believes that the program has reached a tolerable IP and UP rate.

4. **Recommendations for Improvement vs. Recommendations for Compliance**

OMB relies on the judgement of the OIG to determine whether the evidence in the review constitutes a noncompliance determination with a recommendation for compliance or, alternatively, constitutes a compliance determination with a recommendation for improvement.

A recommendation for compliance is required each time an OIG determines a program fails to comply with a particular criterion. For example, if an OIG determines that a program has not developed a corrective action plan for a program reporting an IP and UP estimate above the statutory threshold, the OIG is required to include at least one recommendation for a corresponding action that, if taken by the program, would result in achieving compliance with the Published Corrective Action Plans criterion.

A recommendation for improvement should be considered any time an OIG identifies an action that if taken would improve the program as it relates to a specific evaluation criterion, however, overall the OIG determines that the program itself is compliant with the criterion. For example, an OIG may identify a way for one of the mitigation strategies within the corrective action plan of a program to be implemented more effectively. This factor, in isolation, likely does not constitute a noncompliance determination for the Published Corrective Action Plans criterion, but the OIG should still include this recommended action in their final report so the program can improve the effectiveness of corrective action plan implementation.

5. **Compliance Status Table and Summary**

The report should contain a high-level summary toward the beginning of the report that (a) clearly states the agency's overall compliance status (i.e., compliant or non-compliant) and (b) indicates which of the requirements the agency complied with and which requirements the agency did not comply with.

In addition, to improve consistency across reporting format, each report must include the following program level Table at the beginning of the report:

Program Name	Published payment integrity information with the annual financial statement	Posted the annual financial statement and accompanying materials on the agency website	Conducted IP risk assessments for each program with annual outlays greater than $10,000,000 at least once in the last three years	Adequately concluded whether the program is likely to make IPs and UPs above or below the statutory threshold	Published IP and UP estimates for programs susceptible to significant IPs in the accompanying materials to the annual financial statement	Published corrective action plans for each program for which an estimate above the statutory threshold was published in the accompanying materials to the annual financial statement	Published IP and UP reduction target for each program for which an estimate above the statutory threshold was published in the accompanying materials to the annual financial statement	Has demonstrated improvements to payment integrity or reached a tolerable IP and UP rate	Has developed a plan to meet the IP and UP reduction target	Reported an IP and UP estimate of less than 10% for each program for which an estimate was published in the accompanying materials to the annual financial statement
Program A										
Program B										
Program C										
Program D										
Program E										

Table 8. PIIA Compliance Reporting Table

This table should include the criteria assessed by the agency OIG as well as the name of each program assessed. Within the table, each agency OIG should indicate, for each criteria, whether the program was compliant or non-compliant. For instances where a particular criterion does not apply (such as instances where the program is only in Phase 1) the agency OIG may place NA. If the final table includes more than 30 programs, the OIG may elect to include the entire table in an appendix to the report for readability of the report. If the entire table is included in an appendix, the OIG should still include a table containing non-compliant programs only at the beginning of the report. Table 8 is provided as an example of a compliance reporting table.

D. Agency Responsibility When a Program is Non-Compliant

When the OIG determines that a program is non-compliant for the FY, the agency must complete the appropriate action below.

1. **Each year of non-compliance**
   a. For each program that is non-compliant the agency will provide information, describing the actions that the agency will take to come into compliance in the OMB Annual Data Call. This information will be published on paymentaccuracy.gov and serve as the plan that agencies are required to submit to the appropriate authorizing and appropriations committees of Congress including:
      i. measurable milestones to be accomplished in order to achieve compliance for each program;

ii. the designation of a senior agency official who shall be accountable for the progress of the executive agency in coming into compliance for each program; and

iii. the establishment of an accountability mechanism, such as a performance agreement, with appropriate incentives and consequences tied to the success of the senior agency official in leading the efforts of the agency to come into compliance for each program.

2. **2nd consecutive year of non-compliance**

   a. For programs that are not compliant for **two consecutive fiscal years,** the agency shall propose to the Director of OMB in its next Budget submission, additional program integrity proposals that would help the program come into compliance. This process will unfold as part of the annual development of the President's Budget. In the Budget submission the agency must describe how each proposal would help the program come into compliance.

   b. If the Director of OMB determines that additional funding would help the program become compliant, the agency shall obligate an amount of additional funding determined by the Director of OMB to intensify compliance efforts. When providing additional funding for compliance efforts, the agency should:

      i. Exercise reprogramming or transfer authority to provide additional funding to meet the level determined by the Director of OMB; and

      ii. Submit a request to Congress for additional reprogramming or transfer authority if additional funding is needed to meet the full level of funding determined by the Director of OMB.

3. **3rd consecutive year of non-compliance**

   a. For programs that are not compliant for **three consecutive fiscal years,** within 30 days of the determination of non-compliance, the agency will submit to the appropriate authorizing and appropriations committees of Congress, the OMB, and the Comptroller General of the United States a report that includes:

      i. Reauthorization proposals for each (discretionary) program that has not been in compliance for three consecutive years; and/or

      ii. Proposed statutory changes necessary to bring the program that has not been in compliance for three consecutive years into compliance.

   If the agency determines that the two actions above will not bring the program into compliance, then the report must provide:

      iii. A description of the actions that the agency is undertaking to bring the program into compliance and

      iv. A timeline for when the program will achieve compliance based on the actions described.

4. **4th, 5th, 6th, etc. consecutive year of non-compliance**

   a. For programs that are not compliant for **four or more consecutive fiscal years**, within 30 days of the determination of non-compliance, the agency will submit to the appropriate authorizing and appropriations committees of Congress and the OMB, a report that includes:

i. the activities taken to comply with the requirements for 1, 2, 3, 4, or more consecutive years of noncompliance;
ii. a description of any requirements that were fulfilled for 1, 2, 3, 4, or more consecutive years of noncompliance that are still relevant and being pursued as a means to bring the program into compliance and prevent and reduce IPs;
iii. a description of any new corrective actions; and
iv. a timeline for when the program will achieve compliance based on the actions described within the report.

5. **Illustration of Agency Responsibility**

Agency ABC has five programs. Table 9, below, demonstrates the agency responsibility based on the individual compliance results of the five programs.

	Year 1		Year 2		Year 3		Year 4		Year 5	
	Compliance Determination	Years of Non-Compliance	Compliance Determination	Consecutive Years of Non-Compliance	Compliance Determination	Consecutive Years of Non-Compliance	Compliance Determination	Consecutive Years of Non-Compliance	Compliance Determination	Consecutive Years of Non-Compliance
Program A	Compliant	0	Compliant	0	Non-Compliant	1	Non-Compliant	2	Non-Compliant	3
Program B	Compliant	0	Non-Compliant	1	Non-Compliant	2	Compliant	0	Non-Compliant	1
Program C	Non-Compliant	1	Non-Compliant	2	Non-Compliant	3	Non-Compliant	4	Non-Compliant	5
Program D	Compliant	0	Non-Compliant	1	Non-Compliant	2	Non-Compliant	3	Non-Compliant	4
Program E	Non-Compliant	1	Compliant	0	Non-Compliant	1	Compliant	0	Non-Compliant	1
Within 30 Days of Determination	NA		NA		Report for Program C		Report for Programs C & D		Report for Programs A, C, & D	
In Next OMB Annual Data Call	Provide information for Programs C & E		Provide information for Programs B, C & D		Provide information for Programs A, B, C, D, & E		Provide information for Programs, A, C, & D		Provide information for Programs A, B, C, D, & E	
In Next Budget Submission to OMB	NA		Proposal for Program C		Proposal for Programs B & D		Proposal for Program A		NA	

Table 9. Example of Agency Responsibilities When Programs are Non-Compliance

6. **Agency Submission of Non-Compliance Materials to OMB**

To submit a non-compliance report to the OMB, the agency should upload the document to the Payment Integrity Information Act Required Submissions to OMB page on the Max community.

VII. Reporting Requirements

At a minimum, there will be reporting requirements in both OMB Circular A136 and the OMB Annual Data Call that apply to all agencies with programs in Phase 1 as well as those with programs in Phase 2. Agencies should consult those documents in conjunction with this circular to determine the full scope of the reporting requirements for their programs.

A. Reporting Requirements for All agencies

1. AFR or PAR and the OMB Circular A136

Agencies should consult OMB Circular A136 annually to determine which of the Payment Integrity reporting requirements apply to their agency. At a minimum, all agencies with programs in Phase 1 as well as those with programs in Phase 2 will provide a link in their AFR or PAR to paymentaccuracy.gov so the reader can access information about agency IP risk assessments, recoveries, and other agency-wide reporting requirements.

2. Paymentaccuracy.gov and the OMB Annual Data Call

Agencies should consult the Annual Data Call guidance annually to determine which of the reporting requirements apply to their agency. At a minimum, all agencies will provide OMB with data related to the status of their IP risk assessments, their identification and recovery of overpayments, and other agency-wide reporting requirements applicable to agencies with programs in both Phase 1 as well as those with programs in Phase 2.

B. Additional Reporting Requirements for Some Agencies

1. The High Dollar Overpayment and High-Priority Program Report

High-Priority programs must provide select information through a mechanism determined by OMB on a quarterly basis. The collected information will be published quarterly in a Payment Integrity Scorecard on paymentaccuracy.gov. This published information will fulfill the High Dollar Overpayment Reporting Requirements and also the High-Priority Program Reporting Requirements.

a) *IG Review Responsibilities*

Agencies must provide a link to this publication to their agency IG so that the OIG can review. During the review of each Scorecard, the agency IG shall assess the information provided on the Scorecard and determine the extent of IG oversight warranted to prevent monetary loss IPs. In addition, based on the information provided on the Scorecard, the IG may provide the agency head with concrete and actionable recommendations for modifying the agency's plans for actions the agency plans to take to recover monetary loss IPs, as well as any actions the agency intends to take to prevent IPs and UPs from occurring in the future.

b) *When to Report*

A program automatically becomes 'High-Priority' when its annual reported monetary loss IP estimate is greater than or equal to $100,000,000, regardless of the IP and UP rate. A program is not considered to be a High-Priority program when its annual reported monetary loss IP estimate is less than $100,000,000. The point at which a program reports its annual IP and UP estimate is the point at which a program would move in or out of high-priority status. The agency and OIG are responsible for monitoring the annual IP and UP estimate for each of their programs so that they know whether a program is or is not considered High-Priority. Programs will be expected to provide information for the Payment Integrity Scorecard immediately following the

publication of an annual monetary loss IP estimate that is greater than or equal to $100,000,000 and will be expected to continue providing information on a quarterly basis until the program reports an annual monetary loss IP estimate that is less than $100,000,000. The information provided for the Payment Integrity Scorecard will include but is not limited to actions the program has taken or intends to take to prevent IPs and UPs from occurring in the future as well as actions the program plans to take to recover monetary loss IPs. The agency should contact OMB to obtain access to the information collection method.

C. Agency & OIG Action Due Dates and Applicability

At a minimum, agencies should be aware of the following potential requirements in Table 10 below.

Action Required	When	Applicability	Submit To
IP Risk Assessment	Once every 3 years	All programs not in Phase 2 that have annual outlays over $10M	Agency should keep and be prepared to share with OIG during Compliance Review
S&EMP	By June 30 of the first FY for which the estimate is being produced	All programs in Phase 2	Improper Payment Sampling and Estimation Methodologies Page for Agency
Annual Financial Statement of the Agency Reporting	November 15th	Agencies with Programs in Phase 1 and/or Phase 2	Agency should publish on their own website
Annual Data Call	Varies (Typically Mid-October)	Agencies with Programs in Phase 1 and/or Phase 2	Annual Data Call for Paymentaccuracy.gov Page for Agency and/or Additional Location Provided by OMB
OIG Compliance Report	180 days after the day the publication date for the Annual Financial Statement of the Agency and the Accompanying Materials to the Annual Financial Statement of the Agency, whichever is later	All OIGs of Agencies with Programs in Phase 1 and/or Phase 2	Annual OIG PIIA Compliance Determination Reports Page for Agency
All Years of Non-Compliance	The Agency's next Annual Data Call Submission	Agencies with Non-Compliant Programs	Annual Data Call for Paymentaccuracy.gov Page for Agency and/or Additional Location Provided by OMB
2nd Year Non-Compliant	The Agency's next Budget submission after publication of the OIG Compliance Report	Agencies with Programs Non-Compliant for 2 consecutive years	2nd Consecutive Year of Non-Compliance Program Integrity Proposals Page for Agency
3rd Year Non-Compliant	Within 30 days of the publication of the OIG Compliance Report	Agencies with Programs Non-Compliant for 3 consecutive years	3rd Consecutive Year of Non-Compliance Reauthorization and Statutory Proposals Report Page for Agency
4 or More Years Non-Compliant	Within 30 days of the publication of the OIG Compliance Report	Agencies with Programs Non-Compliant for 4 or more consecutive years	4th, 5th, 6th, etc. Consecutive Year of Non-Compliance Report Page for Agency
Recovery Audit Cost-Effectiveness Analysis	Internally as determined by each agency	All Programs in Phase 1 or Phase 2 with more than $1M in annual outlays	No Submission Required. Agencies should maintain the analysis internally
High Dollar Overpayment and High-Priority Program Report	Quarterly	All Programs in Phase 2 with an annual reported monetary loss IP estimate is greater than or equal to $100M	Individual Submission Link Provided to High-Priority Program Provided by OMB
High-Priority Program Meeting	Annually	All Programs in Phase 2 with an annual reported monetary loss IP estimate is greater than or equal to $100M	Agencies with High-Priority Programs must meet with OMB annually to report on actions taken during the preceding year and planned actions to prevent IPs

Table 10. Agency and OIG Reporting Requirements

VIII. Appendix 1A: Definitions for Purposes of this Guidance

For the purposes of this guidance the following terms and definitions are used:

A.

Abuse: Behavior that is deficient or improper when compared with behavior that a prudent person considers reasonable and necessary in operational practice given the facts and circumstances.

Accept the Improper Payment Risk: When no action is taken to respond to the IP risk based on the insignificance of the risk.

Accompanying Materials: Refers to public information in a location separate from the annual financial statement of the agency. The type of information and location may vary by agency but examples could include but are not limited to an errata report, a reference to data on an external website (such as paymentaccuracy.gov), or a reference to a related agency public report to fulfill reporting requirements (such as a reference to a report containing corrective action).

Accuracy: The degree to which the result (i.e. IP estimate, IP risk assessment) conforms to the correct value.

Accurate Improper Payment and Unknown Payment Estimate: Fairly representing the closeness of an IP and UP estimate to a standard or known value.

Action Plan: (*See* Corrective Action Plan)

Actions (Semi-annual or Quarterly): Mitigation strategies which are established to improve the prevention of IPs resulting in monetary loss. Under statute, all High-Priority Programs are required to establish semi-annual or quarterly actions for reducing IPs associated with the high-priority program.

Activity: (*See* Program)

Actual Reduction Target: (*See* IP and UP Reduction Target)

Agency: Means a department, agency, or instrumentality in the executive branch United States Government.

Agency Policies, Procedures, or Documentation Requirements: Requirements that guide the payment process within a program that are developed by the agency, or the entity performing all or part of the payment process on behalf of the agency (i.e. states, local governments, etc.), and conducted in addition to any requirements within the payment process which are mandated by statute or regulation. If an agency is able to discern that the payment was made to the right recipient, for the right amount, and in accordance with applicable regulation and statute, despite failure to comply with all policies, procedures, or documentation requirements surrounding the payment, the payment may be considered proper.

Agency Senior Management: Agency employees serving in key leadership positions just below the top Presidential appointees in the agency. They may be career employees or political appointments and may or may not be members of the Senior Executive Service.

Aggressive and Realistic Reduction Target: A program's projected out year IP and UP rate that they will be working toward achieving in the subsequent FY. An aggressive and realistic reduction target will eventually be equal to the tolerable IP and UP rate for the program, however, if a program is still reporting an IP and UP estimate that is significantly higher than the program's tolerable IP and UP rate, it could take multiple years for the reduction target to equal the tolerable IP and UP rate.

Annual Data Call: In depth payment integrity information provided by the agency to OMB for publication. The data is collected and subsequently published on paymentaccuracy.gov to fulfill multiple statutory reporting requirements in PIIA for both the agency and OMB.

Annual Financial Statement: Formal records of the financial activities during a 12-month consecutive time period. The financial statements are part of the agency financial report.

Annual Financial Statement of the Agency: A report published annually in the form of an Agency Financial Report (AFR) or a Performance and Accountability Report (PAR) that provides financial and performance results that enable the President, Congress, and the American people to assess accomplishments for each FY (October 1st through September 30th).

Annual Improper Payment Estimate: The IP and UP estimate reported in the Annual Data Call and published on paymentaccuracy.gov.

Anomaly Detection Analytics: A data analytics technique used for identification and prevention of IPs and UPs. This type of analytics is focused on investigating aggregate-level transactions, uses "unsupervised modeling" to identify outliers compared to peer groups based on unknown patterns among common and individual fraudsters. This type of analytics technique allows agencies to identify aggregate abnormal patterns across the data that don't conform to established normal behaviors, i.e. outliers.

Audit: A process for assuring an organization's objectives of operational effectiveness, efficiency, reliable financial reporting, and compliance with laws, regulations and policies.

Automation: Automatically controlled operation, process, or system.

Avoid the Improper Payment or Unknown Payment Risk: Action is taken to stop the operational process causing the IP or UP risk.

B.

Baseline: A starting point or the benchmark against which future progress can be assessed or comparisons made. If a program had a 24-month reporting cycle where no significant changes occur in the S&EMP, the program will most likely be considered to have established a baseline.

Behavioral/Psychological Influence: Uses principles from the behavioral sciences such as psychology, neuroscience, and behavioral economics to understand how individuals absorb, process, and react to information and applies this to design practical policies and interventions.

C.

Cause Category: A division of IP or UP causes with shared characteristics.

Compliance: A term used to indicate whether an agency has fulfilled specific statutory requirements. (*See* the Compliance section of this guidance for discussion of requirements).

Computer Matching Activities: Activities conducted pursuant to a matching program.

Computer Matching Agreement: A written agreement between a recipient agency and a source agency (or a non-Federal agency) that is required by the Privacy Act for parties engaging in a matching program. See 5 U.S.C. § 552a(o) as modified by 31 U.S.C. § 3354(d)(1).

Computer Matching Agreement Waiver Request:

A request for waiving the requirements of section 552a(o) under 5 U.S. Code in any case or class of cases for computer matching activities that involve a working system and that are conducted under the Initiative for the purposes of identifying and preventing IPs and UPs.

Computer Matching Program: (*See* Matching Program)

Confidence Interval: The range of values for a given confidence level n into which repeated future samplings are expected to fall n% of the time. For PIIA testing, this is used as the estimate for the IP and UP error rate of the population.

Confirmed Fraud: An IP amount determined to be fraudulent through the adjudication process. Confirmed fraud does not include transactions determined by management to be anomalous or indicative of potential fraud that were referred to the agency's OIG or the Department of Justice, unless the appropriate judicial or adjudicative process has made the determination.

Control Activities: The actions management establishes through policies and procedures to achieve objectives and responds to risks in the internal control system, which includes the entity's information system. In the context of payment integrity, the agency has developed control activities to help management achieve the objective of reducing IPs and UPs by, establishing internal control activities that are responsive to management's objectives to mitigate risks of IPs and UPs (e.g., policies and procedures related to transaction authorization and approvals of program activities), implementing pre-award and pre-payment reviews where detailed criteria are evaluated before funds are expended, utilizing data analytics tools, such as Treasury's Working System, to compare information from different sources to help ensure that payments are appropriate, and performing cost benefit analyses of potential control activities before implementation to help ensure that the cost of those activities to the organization is not greater than the potential benefit of the control.

Control Environment: The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. It is the foundation for an internal control system. It provides the discipline and structure to help an entity achieve its objectives. In the context of payment integrity, the agency has created a control environment that instills a cultural framework of accountability over IPs and UPs by, fostering an atmosphere in which reducing IPs and UPs are a top management priority, providing a cultural framework for managing risk by engaging key stakeholders in the risk management process, increasing accountability and providing leadership in setting and maintaining the agency's ethical code of conduct and laying out defined consequences for violations, clearly defining key areas of authority and responsibility and establishing appropriate lines of reporting within and external to the agency (e.g., program offices or State Governments), and ensuring that personnel involved in developing, maintaining, and implementing control activities have the requisite skills and knowledge, recognizing that staff expertise needs to be frequently updated in evolving areas such as information technology and fraud investigation.

Controls: The systems, policies, procedures, personnel and culture in place within an organization that mitigate the risk of IPs and UPs.

Corrective Action: Action to eliminate the cause of an IP or UP and to prevent recurrence.

Corrective Action Plan: Strategy put in place by a program to prevent and reduce the IP and UP amount. It is responsive to the root causes of the IPs and UPs and proportional to the severity of the associated amount and rate of the root cause. It typically contains multiple mitigation strategies and corrective actions.

Cost Benefit Analysis: A systematic approach to estimating the strengths and weaknesses of alternatives used to determine options which provide the best approach to achieving benefits while preserving savings.

Cost-Effective Payment Recapture Audit Program: (*See* Cost-Effective Recovery Audits and Activities Program)

Cost-Effective Recovery Audits and Activities Program: A recovery audits and activities program in which the benefits (i.e., recovered amounts) exceed the costs (e.g., staff time and resources, or payments for the payment recovery audit contractor) associated with implementing and overseeing the program.

Criteria: (*See* Criterion)

Criterion: The standard that is used for making a decision about something.

Cross Enterprise Sharing: Sharing of documents, processes, and opportunities with intra-agency partners and stakeholder. Potentially managed through federated repositories and a registry to create a longitudinal connection to information used to mitigate IPs and UPs.

D.

Data Element/Information Criteria: Describes the specific characteristic that must be met for being allowed to receive a payment, service, or benefit because you satisfy a certain condition.

Data Integrity Board: The board of senior officials designated by the head of an agency that is responsible for, among other things, reviewing the agency's proposals to conduct or participate in a matching program and conducting an annual review of all matching programs in which the agency has participated. At a minimum, the Data Integrity Board includes the Inspector General of the agency, if any, and the senior official designated by the head of the agency as responsible for implementation of the Privacy Act (i.e., the Senior Agency Official for Privacy). See 5 U.S.C. § 552a(u).

Data Matching: Describes efforts to identify, match, and merge records that correspond to the same entities from several databases or even within one database.

Database: Any collection of data, or information, that is specially organized for rapid search and retrieval by a computer.

Data/Information Needed Does Not Exist: A situation in which there is no known database, dataset or location currently in existence that contains the data/information needed to validate the payment accuracy prior to making the payment.

Data/Information Theme: Describes the subject matter of the Data Element/Information Criteria.

Demonstrating Improvement: Demonstrating improvement could be done through efforts including but not limited to reduction in IP and UP percentage, a decrease in IP and UP dollar amount, an improved method for identifying monetary loss, the implementation of a new mitigation strategy, demonstration of efforts taken to improve prevention of monetary loss, testing payments that had previously been untested but could be, etc.

Determination: Refers to the OIG's conclusion, when published in their annual compliance report, regarding whether a program is compliant or non-complaint.

Disbursement: (*See* Payment)

Discern: To decide or determine.

Do Not Pay: (*See* Treasury Working System)

Do Not Pay Business Center: *(See* Treasury Working System)

Do Not Pay Initiative: The Initiative supports Federal agencies in identifying and preventing IPs. It encompasses multiple resources that are designed to help Federal agencies review payment eligibility for purposes of identifying and preventing IPs and UPs. See the initiative describe in 31 U.S.C. § 3354(b).

Do Not Pay Matching Program: A matching program that is conducted for purposes of the Do Not Pay Initiative and involves at least one of the databases included in the Treasury Working System and/or a database designated for inclusion in the Do Not Pay Initiative by the OMB Director or a designee.

Do Not Pay Portal: A service under the Treasury Working System that agencies can access and use at no cost to check many databases at one time to verify a recipient's eligibility for payment.

Do Not Pay Working System: (*See* Treasury Working System)

Documentation: Material that provides information, evidence, or that serves as a record.

Duplicate Payment: A type of IP in which an identical additional payment for a good or service that has already been paid for.

E.

Eligibility Criteria: (*see* Data Element/Information Criteria)

Eligibility Theme: (See Data/Information Theme)

Enterprise Risk Management: An effective agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impacts of risks as an interrelated portfolio, rather than addressing risks only within silos.

Estimate: (S*ee* IP and UP estimate)

Estimation Methodology: (*See* Sampling and Estimation Plan)

Executive Agency: (*See* Agency)

F.

Failure to Access Data/Information: IPs are attributed to human errors to access the appropriate data/information to determine whether or not a beneficiary or recipient should be receiving a payment, even though such data/information exists and is accessible to the agency or entity making the payment.

Federal Agency: (*See* Agency)

Federal Financial Assistance: The transfer of anything of value, most often money, from a Federal agency to a non-Federal entity.

Federal Fund: Money that the United States Government makes available for each Federal Agency.

Federal Government: Includes any Federal executive agency, the legislative branch of the United States, and the judicial branch of the United States.

Federally Funded Federally Administered Program: Programs that receive their funding from the Federal Government and are administered, managed, and operated at the Federal level.

Federally Funded State Administered Program: Programs that receive at least part of their funding from the Federal Government, but are administered, managed, and operated at the State or local level (e.g., Medicaid, Unemployment Insurance, Temporary Assistance for Needy Families, Title I Local Educational Agencies, Child and Adult Care Food Program).

Fee: A fixed charge. Fees that may result from an underpayment by an agency are not considered an IP if the fee was paid correctly. These payments are generally separate transactions and may be necessary under certain statutory, contractual, administrative, or other legally applicable requirements.

Financial Fraud: A type of IP resulting in monetary loss which occurred as a result of the recipients' willful misrepresentation for the purposes of obtaining the funds, services, or benefits.

Financial Management Improvement Program: An agency-wide program, conducted by the head of the agency, to address the deficiencies in an agency's internal controls over payments identified during the course of implementing a payment recovery audit, or other agency activities and reviews. The goal of the Financial Management Improvement Program is to mitigate the weakness in the payment process that are causing the monetary loss IPs to occur. The Financial Management Improvement Program should prioritize the prevention of monetary loss IPs over recoveries. The first priority of such a program is to address problems that contribute directly to agency monetary loss IPs. In conducting its financial management improvement programs, the agency head may also seek to reduce errors and waste in programs other than where funds are recovered, as long as the priority remains addressing the problems that contribute directly to the monetary loss IPs of the agency.

Fraud: Obtaining something of value through willful misrepresentation.

Fund: An amount of money established for a particular purpose.

G.

H.

High Dollar Overpayment: The term for overpayments made within high-priority programs.

High Dollar Overpayment Report: A report describing any actions a High-Priority Program has taken or plans to take to recover IPs, as well as any actions the agency intends to take to prevent IPs from occurring in the future.

High-Priority Improper Payments: IPs that occur in High-Priority Programs.

High-Priority Programs: All programs with IPs resulting in monetary loss that exceed $100,000,000 annually. OMB may determine that a program is high-priority for reasons other than exceeding the dollar threshold established above. If this occurs, OMB will notify the agency.

I.

Improper Payment: A payment that was made in an incorrect amount under statutory, contractual, administrative, or other legally applicable requirements. The term improper payment includes; any payment to an ineligible recipient; any payment for an ineligible good or service; any duplicate payment; any payment for a good or service not received, except for those payments where authorized by law; and any payment that does not authorized by law; and any payment that does not account for credit for applicable discounts.

Improper Payment and Unknown Payment Estimate: The IP Estimate PLUS the UP Estimate.

Improper Payment and Unknown Payment Estimate: A statistically valid estimate of the total IPs made annually in a program plus a statistically valid estimate of the total UPs made annually in a program. The collective amount in IPs and UPs divided by the amount in program outlays for a given program in a given FY. It is based on dollars rather than number of occurrences. The IP and UP estimate will be reported as both a percentage and a dollar amount.

Improper Payment and Unknown Payment Rate: The degree of IPs and UPs measured against the outlays.

Improper Payment and Unknown Payment Reduction Target: The estimated IP and UP level the program predicts they will achieve in the following FY. A reduction target may be lower, constant, or higher than the CY IP and UP estimate.

Improper Payment and Unknown Payment Reduction Target Rate: The reduction target IP and UP percentage.

Improper Payment and Unknown Payment Risk: The likelihood that an IP or UP will occur due to vulnerabilities in the payment process.

Improper Payment Error Rate: (*See* IP Rate)

Improper Payment Estimate: A statistically valid estimate of the total IPs made annually in a program. The amount in IPs divided by the amount in program outlays for a given program in a given FY. It is based on dollars rather than number of occurrences. The IP estimate will be reported as both a percentage and a dollar amount.

Improper Payment Percentage: (*See* IP and UP Rate)

Improper Payment Risk Assessment: A systematic process of evaluating the potential IP and UP risk that may be involved in the payment cycle of a program.

Inability to Access Data/Information: A situation in which the data or information needed to validate payment accuracy exists but the agency or entity making the payment does not have access to it.

Ineligible Recipient: An entity that does not meet the stipulated statutory requirements to receive a payment. A payment to an ineligible recipient is an IP.

Information and Communications: The quality information management and personnel communicate and use to support the internal control system. In the context of payment integrity, the agency has effectively used and shared knowledge to manage IPs and UPs by, determining what information is needed by managers to meet and support initiatives aimed at preventing, reducing, and recapturing IPs, ensuring that needed information is provided to managers in an accurate and timely manner, providing managers with timely feedback on applicable performance measures so they can use the information to effectively manage their programs, developing educational programs to assist program participants in understanding program requirements, ensuring that there are adequate means of communicating with, and obtaining information from, external stakeholders that may have a significant impact on IP and UP initiatives, developing working relationships with other organizations to share information and pursue potential instances of waste, fraud and abuse, and making the results of performance reviews widely available to permit independent evaluations of the success of efforts to reduce IPs and UPs.

Inspector General: A person who heads the Office of Inspector General.

Insufficient Documentation: (*See* Insufficient or Lack of Documentation)

Insufficient or Lack of Documentation: A situation in which an agency, or the entity performing all or part of the payment process on behalf of the agency (i.e. states, local governments, etc.), is conducting a review, for the purposes of producing an IP and UP estimate, and is unable to obtain the documentation needed for the reviewer to determine whether the payment was made to the right recipient and/or for the right amount. When this occurs the payment is considered an 'unknown' payment and is not considered an IP for purposes of producing an IP estimate, however it is treated as an IP in the sense that it will be accounted for and reported in conjunction with, but separately from, the IP and UP estimate. If there is sufficient documentation to determine that the payment was made to the right recipient, for the right amount, and in accordance with applicable regulation and statute, despite failure to comply with all

agency policies, procedures, and/or documentation requirements surrounding the payment, the payment may be considered a proper payment.

Intentional Improper Payment: (*See* Financial Fraud)

Interest: A charge for borrowed money generally a percentage of the amount borrowed. Interest that may result from an underpayment by an agency is not considered an IP if the interest was paid correctly. These payments are generally separate transactions and may be necessary under certain statutory, contractual, administrative, or other legally applicable requirements.

Internal Control: Includes the mechanisms, rules, policies, and procedures implemented by an agency to ensure the integrity of financial information as well as the detection and prevention of IPs and UPs. This is often used as an IP and UP mitigation strategy.

Internal Process or Policy Change: Altering or updating a process or policy to prevent or correct error.

J.

K.

Key Performance Indicator Scorecard: (*See* Payment Integrity Scorecard)

Known Improper Payments: This classification of IPs includes the collective estimate of overpayments, underpayments, and technically IPs. This does not include the estimated amount of UPs.

L.

Lacking or Insufficient Documentation: (*See* Insufficient or Lack of Documentation)

Legally Applicable Requirements: Requirements as defined by statute or regulation.

Likely: For purposes of conducting an IP risk assessments "Likely" may be reasonably interpreted as "more likely than not" (i.e., a 50% or greater probability) or as having a "high degree of probability" (e.g., 75% or greater probability). When conducting an IP risk assessment agencies should use a standard that will minimize the risk that agencies are developing, pilot testing and implementing costly estimation programs for programs will not actually have IPs plus UPs exceeding statutory thresholds.

Likely to be: (*See* Likely)

Low Value to High Value Payment Integrity Work: Shifting from low value to high value payment integrity work requires both critical mission achievement and a continuous focus on improving operational efficiency. Time, energy, and resources spent performing repetitive, manual processes, and adhering to unnecessary and obsolete policies, can hinder Agencies' ability to achieve effective payment integrity. Federal agencies can shift time, effort, and/or funding from low to high-value payment integrity work through the elimination of unnecessary requirements, burden reduction, optimization and streamlining, and workload automation.

M.

Margin of Error: An amount that tells you how many percentage points your results may differ from the real population value. This represents the portion of an IP estimate due to random chance within a sample.

Matching Activities: (*See* Computer Matching Activities)

Matching Agreement: (*See* Computer Matching Agreement)

Matching Program: A computerized comparison of records from two or more automated systems of records, or an automated system of records and automated records maintained by a non-Federal agency (or agent thereof). A matching program pertains to either Federal benefit programs or Federal personnel or payroll records. A Federal benefit match is performed for purposes of determining or verifying eligibility for payments under Federal benefit programs, or recouping payments or delinquent debts under Federal benefit programs. A matching program involves not just the matching activity itself, but also the investigative follow-up and ultimate action, if any. See 5 U.S.C. § 552a(a)(8).

Methodology: (*See* Sampling and Estimation Methodology Plan)

Mitigation Strategy: Action designed to reduce or lessen the likelihood or size of an IP or a UP.

Monetary Loss: Monetary loss to the Federal Government is an amount that should not have been paid and in theory should/could be recovered. A Monetary loss type IP is an overpayment.

Monetary Loss Type Improper Payment: (*See* Monetary Loss)

Monitoring: Activities management establishes and operates to assess the quality of performance over time and promptly resolve the findings of audits and other reviews. In the context of payment integrity, the agency has assessed the success of IP initiatives by, adhering to existing laws and OMB guidance to institute a statistical methodology to estimate the level of IPs and UPs being made by the agency's programs, using an internal control assessment methodology that includes testing of control design and operating effectiveness and the evaluation of the significance of internal control deficiencies related to IPs and UPs, establishing program-specific targets for reducing IPs and UPs in programs that measure and report annual IP and UP estimates, assessing the progress of implementation of corrective actions over time and ensuring that the root causes of IP and UP internal control deficiencies are resolved, considering the possibility of engaging contractors that specialize in specific areas where in-house expertise is not available, such as payment recapture audits and fraud detection analytics, remediating identified internal control deficiencies on a timely basis, adjusting control activities, as necessary, based on the results of monitoring activities. The agency should periodically test the controls to ensure they are effective in identifying, preventing, and recapturing IPs, and understanding any statutory or regulatory barriers or other objectives that may limit the agency's corrective actions in reducing IPs and UPs and actions taken by the agency to mitigate the barriers' or other statutory objectives' effects.

N.

Network/Link Analytics: A data analytics technique used to identify and prevent IPs and UPs. This technique can be useful for uncovering organized fraud and associations between fraudsters by using social network analytics, looking at linked patterns for investigation and discovery. For example, an individual may not be suspicious based on their actions alone, yet suspicion may arise when their actions are connected to others through a set of commonalities based on associated attributes, revealing schemes that may have otherwise gone unnoticed.

Non-Federal Entity: A self-sustaining organization, incorporated or unincorporated, that is not an agency or instrumentality of the Federal Government. Non-Federal entities include a State, interstate, Indian tribal, or local government, as well as private organizations.

Non-Federal Fund: Money available that is not from a Federal Fund.

Non-Financial Fraud: A type of fraud which occurs as a result of willful misrepresentation, such as incorrectly stating your weight on a drivers license, where the willful misrepresentation is not for the purposes of obtaining the funds, services, or benefits. For example, non-financial fraud could be a fraud that affects an agency's reputation or national security even if it doesn't lead to major financial loss for your agency.

Non-Monetary Loss: Non-Monetary loss to the Federal Government is either an underpayment or a payment to the right recipient for the correct amount where the payment process fails to follow applicable regulations and/or statutes.

Non-Recovery Audit Recaptures: Recovered overpayments that were identified for recovery through a means other than a Recovery Audit (i.e. statistical samples conducted under PIIA; agency post-payment reviews or audits; OIG reviews; Single Audit reports; self-reported overpayments; or reports from the public).

O.

Office of Inspector General: A term for the oversight division of a Federal agency aimed at preventing inefficient or unlawful operations within their agency.

OMB Annual Data Call: (*See* Annual Data Call)

OMB Payment Integrity Question and Answer Platform: (*See* Payment integrity Question and Answer Platform)

Outlay: (*See* Payment)

Overpayment: A payment in excess of what is due. When an overpayment occurs, the improper amount is the difference between the amount due and the amount of which was actually paid. Overpayments are monetary loss type IPs.

Overpayment Recapture Audit: (*See* Recovery Audit)

P.

Payment: Any transfer of Federal funds *(including a commitment for future transfer, such as cash, securities, loans, loan guarantees, and insurance subsidies)* to any non-Federal person or entity or a Federal employee, that is made by a Federal agency, a Federal contractor, a Federal grantee, or a Governmental or other organization administering a Federal program or activity.

Payment Cycle: A series of events and processing steps that are regularly repeated in the same order prior to a payment being made.

Payment for an Ineligible Good or Service: An IP that includes a payment for any good or service that is rejected under any provision of any contract, grant, lease, cooperative agreement, or other funding mechanism.

Payment Integrity: The process of ensuring that a payment is proper.

Payment Integrity Information Act of 2019: Also known as Public Law No: 116-117, PIIA was signed into law on March 2nd, 2020. In revoking the 2002 Improper Payments Information Act (IPIA), the 2010 Improper Payments Elimination and Recovery Act (IPERA), the 2012 Improper Payments Elimination and Recovery Improvement Act (IPERIA), and the 2015 Fraud Reduction and Data Analytics Act (FRDAA), the PIIA incorporates select provisions from IPIA, IPERA, IPERIA, and FRDAA into a single subchapter in the U.S. Code, while also introducing new aspects into the payment integrity statutory framework. Examples of changes include, but are not limited to Establishing a threshold for IP risk assessments; Allowing for flexibility in select reporting requirement due dates; Clarifying expectations for OIGs annual compliance review; Requiring OMB to report a Government-wide IP and UP rate; and Establishing an Interagency Working Group to Improve Payment Integrity.

Payment Integrity Proposal: A proposal aimed at bolstering Federal payment integrity and public trust in Government by reducing IPs. A proposal can be in the form of either a legislative or administrative reform which if enacted will help prevent IPs and UPs.

Payment Integrity Question and Answer Platform: A platform where OMB provides answers to both agency and OIG questions related to Payment Integrity. The platform is available to all members of the Executive Branch of the Federal Government.

Payment Integrity Risk: The vulnerability that a program faces in the payment process which negatively impacts the likelihood that the IPs and UPs will occur.

Payment Integrity Scorecard: Highlights actions planned and taken to mitigate root causes of IPs within High-Priority programs. They are located on paymentaccuracy.gov and updated by each program on a quarterly basis.

Payment Process: A general term used to refer to the stages that occur from the beginning to the end of the payment lifecycle. For example, the beginning of the process may occur when a potential payment recipient begins to fill out an online application for benefits and the end of the process may occur when the recipient receives the payment from the agency. Or, a payment process may begin when a beneficiary arrives at a facility to receive care and end with the Government paying the facility for the care they provided. The payment process should be wide enough for the program to be able to pinpoint the location within the process that the payment changed from being proper to being improper.

Payment Recapture Audit: (*See* Recovery Audit)

Payment Recapture Audit Contingency Contract: (*See* Recovery Audit Contingency Contract)

Payment Recapture Audit Program: (*See* Recovery Audits and Activities Program)

Payment Recovery: (*See* Recovery)

Paymentaccuracy.gov: A website established to create a centralized location to publish information about IPs. This website includes current and historical information about IPs and UPs made under Federal programs that have been determined to be susceptible to significant IPs and UPs based on assessments of all Government programs, including quarterly scorecards for the Government's high-priority programs. This website also provides a centralized place where the public can report suspected incidents of fraud, waste, and abuse.

Payments to Foreign Governments: Transfer of funds to a foreign government. Payments to foreign governments should be reviewed in the IP risk assessment. They should be included in the review and evaluation.

Phase 1: The first of two stages in the process of review for IP and UP. During this stage an IP risk assessment is conducted at least once every three years to determine whether a program is likely to be susceptible to significant IPs and UPs.

Phase 2: The second of two stages in the process of review for IPs and UPs. During this stage a program will use a statistically valid sampling and estimation methodology to report an annual IP and UP estimate. Phase 2 is not required if the results of Phase 1 indicate that the program is not likely to be susceptible to significant IPs and UPs.

PIIA Target: (*See* IP and UP Reduction Target)

Plan to Meet the IP and UP Reduction Target: Describes the actions the program will take to achieve the IP and UP reduction target in the following FY.

Point (within a payment process): When a payment changes from being proper to being improper.

Point Estimate: A single value given as an estimate of a parameter of a population.

Policy Change or Internal Process: (*See* Internal Process or Policy Change)

Population: A finite or infinite collection of payments under consideration.

Post-Award Audit: refers to a post-award examination of the accounting and financial records of a payment recipient that is performed by an agency official, or an authorized representative of the agency official, pursuant to the audit and records clauses incorporated in the contract or award. A post-award audit is normally performed by an internal or external auditor that serves in an advisory capacity to the agency official. A post-award audit, as distinguished from a recovery audit, is normally performed for the purpose of determining if amounts claimed by the recipient are in compliance with the terms of the award or contract, and with applicable laws and regulations. Such reviews involve the recipient's accounting records, including the internal control systems. A post-award audit may also include a review of other pertinent records (e.g., reviews to determine if a proposal was complete, accurate, and current); and reviews of recipients' systems established for identifying and returning any IPs received under its Federal awards.

Post-Payment Review: A post-payment review is conducted after the payment is made. This type of a review could include the use of data analytics to see trends, develop predictive models, and develop risk scores unique to the program's payments. This review is distinguished from a recovery audit because it is performed for the purpose of reviewing the payments to ensure they are in compliance with relevant policies or to review the payments for the purpose of using data analytics to help prevent future IPs.

Potential Susceptibility to Improper Payments: A risk factor for potential consideration in Phase 1 referencing indicators of IP and UP risk that previous audit reports may have identified and could be valid indicators to consider during the Phase 1 IP risk assessment.

Pre-Payment Review: Analyzing payment data for indicators that a payment is being made in error or is vulnerable to abuse prior to issuing the payment.

Predictive Analytics: A data analytics technique used to prevent IPs and UPs. It uses predictive capabilities to identify unobserved attributes that lead to suspicion of IPs and UPs based on known IPs. Predictive analytics is most effective if it is built after a program evolves through more standard capabilities that are also more cost-effective.

Program Integrity: A foundational concept that seeks to ensure that agencies develop and maintain structures, controls, and processes to safeguard taxpayer resources.

Program Integrity Proposal: (*See* Payment Integrity Proposal)

Program: Includes activities or sets of activities administered by the head of the agency. The term "program" in this guidance implies "program or activity." The agency is authorized to determine the most appropriate grouping of activities to create a "program" for purposes of this guidance. The grouping should be in a manner that most clearly identifies and reports IPs for their agency. When determining how agency activities should be grouped, agencies should not put activities into groupings that may mask significant IP estimates by the large size or scope of a grouping. In addition, agencies should not intentionally group activities in an effort to reduce the size and fall below the statutory thresholds.

Prompt Payment Act Interest Payment: A payment of interest on a delinquent payment required by the Prompt Payment Act. Interest that may result from an underpayment by an agency are not considered an IP if the interest was paid correctly. These payments are generally separate transactions and may be necessary under certain statutory, contractual, administrative, or other legally applicable requirements.

Proper Payment: A payment made to the right recipient for the right amount that has met all program specific legally applicable requirements for the payment.

Psychological/Behavioral Influence: (*See* Behavioral/Psychological Influence)

Published: To report publicly. Typically, this phrase is used in this guidance to reference IP information that is to be placed in the accompanying materials to the annual financial statement.

Q.

Qualitative Improper Payment Risk Assessment: A technique used to quantify risk associated with IPs and UPs. For example, a qualitative IP risk assessment methodology prioritizes the identified IP and UP related risks using a pre-defined rating scale. Risks will be scored based on their probability or likelihood of occurring and the impact on IPs and UPs in the program should they occur.

Quantitative Improper Payment Risk Assessment: Focuses on the measurable and often pre-defined data such as the IP and UP amount. For example, a quantitative IP risk assessment will provide numerical IP amounts and assess the probability of their occurrence. In cases where a quantitative IP risk assessment is conducted, it could take one of several forms, such as: a statistical assessment similar to what is required for the regular IP estimate or a non-statistical assessment where a subset of the population is sampled non-randomly and then its ratio of IPs and UPs is projected to the annual outlays.

Questioned Cost: A cost that is questioned by the auditor because of an audit finding: (a) Which resulted from a violation or possible violation of a statute, regulation, or the terms and conditions of a Federal award, including for funds used to match Federal funds; (b) Where the costs, at the time of the audit, are not supported by adequate documentation; or (c) Where the costs incurred appear unreasonable and do not reflect the actions a prudent person would take in the circumstances. A 'questioned cost' could be considered an UP if the auditor is unable to discern whether the payment was proper or improper as a result of insufficient or lack of documentation, however, a 'questioned cost' should not be considered an IP until the transaction has been completely reviewed and is confirmed to be improper.

R.

Realistic and Aggressive Reduction Target: (*See* Aggressive and Realistic Reduction Target)

Reconciliation: The process of ensuring that two or more sets of records are in agreement it is used to ensure that the money leaving an account matches the actual money spent and can help identify overpayments.

Recovery: When a monetary loss type IP is returned to the agency. This can occur as a result of recovery audits or recovery activities.

Recovery Activities: Any non-recovery audit mechanism used by an agency to identify and recapture overpayments. Recovery activities include but are not limited to review of Single Audit reports; self-reported overpayments, statistical samples conducted under PIIA, and agency post-payment reviews.

Recovery Audit: A review and analysis of an agency's or program's accounting and financial records, supporting documentation, and other pertinent information supporting its payments, that is specifically designed to identify overpayments. It is not an audit in the traditional sense covered by Generally Accepted Government Audit Standards. Rather, it is a detective and corrective control activity designed to identify and recapture overpayments, and, as such, is a management function and responsibility.

Recovery Audit Contingency Contract: A contract for recovery audit services in which the contractor is paid for its services as a percentage of overpayments actually collected. The contractor must provide clear evidence of overpayments to the appropriate agency official.

Recovery Audit Contract: A contract for Recovery Audit services.

Recovery Audit Contractor: An individual or group of individuals procured through a contract to perform a Recovery Audit.

Recovery Audits and Activities Program: An agency's overall performance of recovery audits and recovery activities. The agency head will determine the manner and/or combination of recovery activities to use that are expected to yield the most cost-effective results.

Recovery Audit Plan: (*See* Recovery Audits and Activities Program)

Recovery Audit Recaptures: Recovered overpayment identified through a Recovery Audit.

Recovery of Overpayments: (*See* Recovery)

Reduce the Improper Payment and Unknown Payment Risk: Action is taken to reduce the likelihood or magnitude of the IP and UP risk.

Reduction Target: (*See* IP and UP Reduction Target)

Reduction Target Plan: (*See* Plan to Meet the IP and UP Reduction Target)

Reduction Target Rate: (*See* IP and UP Reduction Target Rate)

Reliable Improper Payment and Unknown Payment Estimate: IP and UP estimates produced from accurate sampling populations, testing procedures, and estimation calculations.

Review: A formal assessment or examination of something with the possibility or intention of instituting change if necessary. Reviews can be a mechanism for identifying overpayments.

Reported Improper Payment and Unknown Payment Estimate: The annual published percentage of program IPs and UPs.

Reported Improper Payment and Unknown Payment Rate: (*See* Reported IP and UP Estimate)

Right Amount: The correct quantity of a payment.

Right Recipient: The correct person or entity that receives a payment.

Risk Appetite: The broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives. Risk appetite is often captured in published Risk Appetite Statements that provide risk guidance from senior level leaders to portfolio and program level leaders. The Payment Integrity Risk Appetite statement should be used to set risk tolerance and include a materiality threshold for what percentage of payments from a given universe must be tested for the sample population to be considered "complete".

Risk Assessment: Assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses. In the context of payment integrity, the agency has determined the nature and extent of IPs and UPs by establishing well defined goals and objectives for eliminating IPs and UPs and execution of corrective actions, determining where risks exist, what those risks are, and the potential or actual impact of those risks on program goals, objectives, and operations, using risk assessment results to target high-risk areas and focus resources where the greatest exposure exists and return on investment can be maximized, reassessing risks on a periodic basis to evaluate the impact of changing conditions, both external and internal, on program operations, and establishing an inventory of root causes of IPs and UPs and internal control deficiencies to develop corrective action plans for risk-susceptible programs. The inventory should include an explanation of how root causes were identified, prioritized, and analyzed to ensure corrective actions produce the highest return on investment for resolving IP and UP control deficiencies.

Risk Profile: An evaluation of the Agency's risks arising from mission and mission-support operations, with consideration of those risks as part of the annual strategic review process. The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an Agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. The risk profile assists in facilitating a determination around the aggregate level and types of risk that the agency and its management are willing to assume to achieve its strategic objectives. A risk profile is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process.

Risk Tolerance: The acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level, identifies the tolerance band for a specific risk, and is stated in measurable terms. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.

Root Cause: A root cause is something that would directly lead to an IP, and if corrected, would prevent the IP.

Rule-Based Analytics: A data analytics technique used to prevent IPs and UPs. A transaction level technique to prevent common IPs and UPs based on known patterns. This technique results in the identification of departures from expected procedures for additional investigation. Rule based analytics focuses on transactional data which does not adhere to organizationally accepted rules, such as using a purchase card on a Saturday evening or Federal holiday.

S.

Sampling and Estimation Methodology: (*See* Sampling and Estimation Methodology Plan)

Sampling and Estimation Methodology Plan: The statistical sampling and estimation method designed and implemented by the program to produce a statistically valid IP and UP amount estimate. When calculating a program's annual IP and UP amount, agencies should only utilize the known amount paid improperly (i.e. overpayments, underpayments, and technically IPs). UPs identified using the sampling and estimation methodology plan should be reported separately and should not be included in the annual IP and UP amount.

Sampling and Estimation Plan: (*See* Sampling and Estimation Methodology Plan)

Scorecard: (*See* Payment Integrity Scorecard)

Semi-annual or Quarterly Actions: Actions required to be established for a high-priority program that focus on reducing IPs associated with the high-priority program. Reported by programs in Payment Integrity Scorecards.

Senior Agency Official: An agency representative with the authority to make decisions on behalf of the agency.

Service: A system supplying a public need such as transport, communications, or utilities such as electricity and water. A payment for a service not received is an IP, unless the payment was authorized by law.

Share the Improper Payment and Unknown Payment Risk: Action is taken to transfer or share IP and UP risks across the Agency or with external parties.

Significant Improper Payment: Annual IPs and UPs (i.e., the sum of monetary loss IPs, non-monetary loss IPs, and UPs) in the program exceeding (1) both 1.5 percent of program outlays and $10,000,000 of

all program or activity payments made during the FY reported or (2) $100,000,000 (regardless of the IP percentage of total program outlays).

Significant: Exceeding (1) both 1.5 percent of program outlays and $10,000,000 of all program or activity payments made during the FY reported or (2) $100,000,000.

Source Agency: 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.

State: Each State of the United States, the District of Columbia, each territory or possession of the United States, and each Federally recognized Indian tribe.

Statistically Valid: When the results of a statistical study are able to draw conclusions. For purposes of this guidance an IP estimate will be considered statistically valid if there is an associated point estimate and confidence interval.

Statutory Change: Changes to statute that would change conditions giving rise to IPs or UPs.

Statutory Requirements of Program Were Not Met: An exception in that a payment made to an otherwise qualified recipient for the right amount but the payment process failed to meet all regulatory and/or statutory requirements. All Technically IPs will fall into this cause category.

Statutory Threshold: (1) both 1.5 percent of program outlays and $10,000,000 of all program or activity payments made during the FY reported or (2) $100,000,000.

Supporting Documentation: (*See* Documentation)

Susceptible to Significant Improper Payments: Refers to the result of an IP risk assessment that determines the program is likely to have annual IPs exceeding (1) both 1.5 percent of program outlays and $10,000,000 of all program or activity payments made during the FY reported or (2) $100,000,000.

T.

Technically Improper: (*See* Technically Improper Payment)

Technically Improper Payment: A payment made to an otherwise qualified recipient for the right amount but the payment failed to meet all regulatory and/or statutory requirements. A technically IP is a non-monetary loss type IP.

Text Analytics: A data analytics technique used to identify and prevent IPs and UPs. A technique that involves scraping the internet of things information into a structured form and parsing strings of text to scan for red flags of fraud. The parsing occurs by using natural language processing tools that divide the body of text into segments which are analyzed for text patterns and then described in terms of their syntactic roles, resulting in a sentiment or polarity analysis.

Tolerable Improper Payment and Unknown Payment Rate: The IP and UP estimate achieved with a balance of payment integrity risk and controls. The tolerable IP and UP rate for a program is determined by agency senior management and often includes IPs which are unavoidable and beyond the agency's ability to reduce as well as IPs and UPs which are cost prohibitive or sometimes mission prohibitive for the agency to prevent.

Tolerable Rate: (*See* Tolerable Improper Payment and Unknown Payment Rate)

Treasury Appropriation Fund Symbols: Treasury Appropriation Fund Symbol (TAFS) refers to the separate Treasury accounts for each appropriation title based on the availability of the resources in the account. The TAFS is a combination of Federal agency; allocation agency, when applicable; account

symbol; and availability code (e.g., annual, multi-year, or no-year). *See OMB Circular No. A-11 for additional information.*

Treasury Working System: Centralized data and analytic services performed at Treasury as part of the DNP Initiative functions for all Federal payments. The Treasury Working System includes databases defined by Congress as well as those designated by OMB or a designee and allows agencies to perform pre-payment reviews as well as other activities such as investigation activities for fraud and systemic IPs detection through analytic technologies and other techniques.

Training: Teaching a particular skill or type of behavior; refreshing on the proper processing methods.

U.

Unable to Determine whether Proper or Improper: A payment that could be either proper or improper but the agency is unable to determine whether the payment was proper or improper as a result of insufficient or lack of documentation. All UPs will fall into this cause category.

Underpayment: A payment that is less than what is due. When an underpayment occurs, the improper amount is the difference between the amount due and the amount which was actually paid. An underpayment is a non-monetary loss type IP.

Unknown Payment: A payment that could be either proper or improper, but the agency is unable to discern whether the payment was proper or improper as a result of insufficient or lack of documentation. UPs are not IPs however, UPs are included in the IP risk assessment in Phase 1. UPs are reported in Phase 2 but are reported separately from the IP estimate.

Unknown Payment Estimate: A statistically valid estimate of the total UPs made annually in a program. The amount in UPs divided by the amount in program outlays for a given program in a given FY. It is based on dollars rather than number of occurrences. The UP estimate will be reported as both a percentage and a dollar amount.

V.

W.

Waiver (for reporting, review, etc.): A relinquishment of a requirement.

Waste: The act of using or expending resources carelessly, extravagantly, or to no purpose.

Working System: A system for prepayment and pre-award review of databases that substantially assist in preventing IPs, located within an appropriate agency. A working system shall include not less than three agencies as users of the system and shall include investigative activities for fraud and systemic IP detection through analytic technologies and other techniques, which may include commercial database use or access.

X.

Y.

IX. Appendix 1B: Abbreviations

AFR	Agency Financial Report
CAP	Corrective Action Plan
CY	Current Year
DIB	Data Integrity Board
DNP	Do Not Pay
FRDAA	Fraud Reduction and Data Analytics Act of 2015
FY	Fiscal Year
HP	High-Priority
IG	Inspector General
IP	Improper Payment
IPERA	Improper Payments Elimination and Recovery Act of 2010
IPERIA	Improper Payments Elimination and Recovery Improvement Act of 2012
IPIA	Improper Payments Information Act of 2002
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAR	Performance and Accountability Report
PI	Payment Integrity
PIIA	Payment Integrity Information Act of 2019
PMA	President’s Management Agenda
S&EMP	Sampling and Estimation Methodology Plan
UP	Unknown Payment

X. Appendix 1C: Important Links

Do Not Pay Working System Website: https://fiscal.treasury.gov/DNP/

Improper Payments Community site for Executive Branch: https://community.max.gov/x/tgN6Dw

Paymentaccuracy.gov: https://www.paymentaccuracy.gov/

Payment Integrity Information Act of 2019: https://www.congress.gov/116/bills/s375/BILLS-116s375enr.pdf

Payment Integrity Information Act Required Submissions to OMB site for Executive Branch: https://community.max.gov/x/HsVHg

Payment Integrity Question and Answer site for Executive Branch: https://community.max.gov/x/QJhofg

XI. Appendix 1D: List of Figures and Tables by Guidance Section