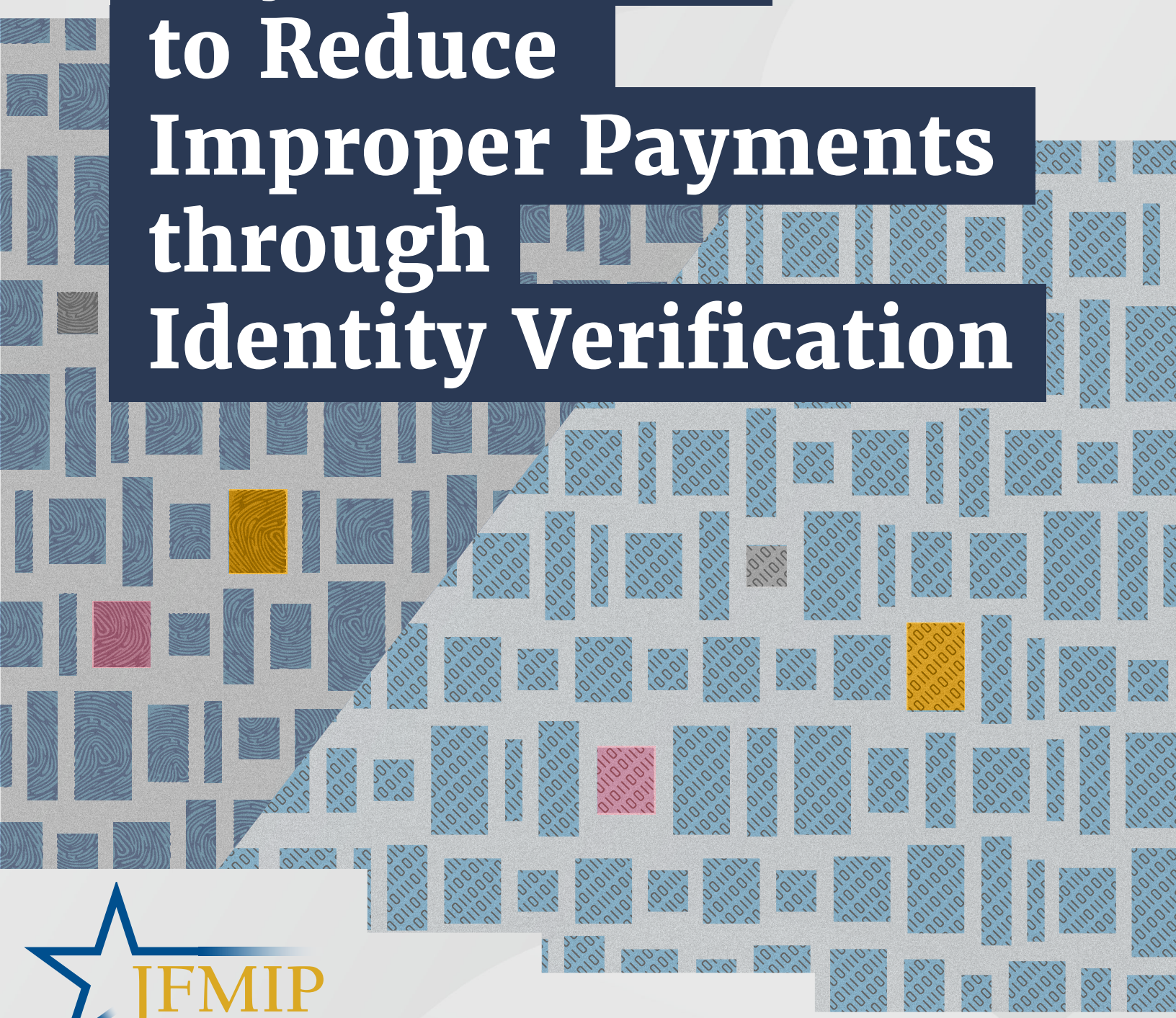
# Key Practices to Reduce Improper Payments through Identity Verification



JFMIP
The Joint Financial Management Improvement Program

July 2022

# Contents

# Executive Summary

## Identifying the Problem and Its Dimensions

The federal government spends trillions of dollars each year addressing public needs. The funds are distributed through payments made directly and through partners at the state and local levels. Improper payments have been a long-standing challenge for the federal government, with annual estimates of improper payments sometimes reaching totals in the hundreds of billions of dollars—$281 billion for fiscal year 2021, about a $75 billion increase from fiscal year 2020.[1] Further, fiscal year 2021 estimates of improper payments generally do not include estimates related to the expenditures to fund urgent response and recovery efforts for the COVID-19 pandemic, so estimates of improper payments may further increase in the future.

There are many complex causes of improper payments. One potentially significant factor is applicant identity—verifying that the person who is attempting to interact with a federal program office is who they claim to be.[2] Verification of individuals' identities is essential to preventing improper payments in several contexts, including those involving fraudulent activity, as failure to do so properly could cause harm to both individuals and organizations.[3] For example:

- Payments to real people who want to hide their identities in order to avoid having their eligibility questioned.
- Payments to those using authentic identity data elements to create synthetic identities.[4]
- Payments to those assuming the identities of other people.

[1] Official Website of the U.S. Government, accessed Jan. 14, 2022, https://www.paymentaccuracy.gov/.

[2] "Applicants" refers to individuals and businesses as program beneficiaries, grantees, or contractors or to those that apply on behalf of program beneficiaries that receive benefits, goods, services, or payments from federal, state, and local governments.

[3] Improper payments, fraud, and fraud risk are related, but distinct, concepts. While unintentional error may cause improper payments, fraud involves obtaining something of value through willful misrepresentation. Whether an act is fraudulent is determined through the judicial or other adjudicative system. Fraud risk exists when individuals have an opportunity to engage in fraudulent activity.

[4] A synthetic identity is a new fabricated identity that usually consists of a real identifier, such as a Social Security number or driver's license number, with other fake information.

- Payments to those who erroneously provide inaccurate information regarding their identities.

The federal government is responsible for ensuring that the right recipient receives the right amount when it makes payments to or on behalf of individuals and businesses. As such, federal agencies and oversight bodies have recently taken steps to determine the significance of misrepresented identity as a cause of improper payments and have begun to focus on identity verification as a means to improve payment integrity.

Identity verification consists of the process, including controls, to confirm the claimed identity of the individual presenting identity evidence. An important first step in identity verification is performing a risk assessment to determine the extent to which misrepresented identities pose a program risk. Program offices can consider performing further research and risk assessments on any abnormal patterns of payment data to identify new and emerging previously unknown identity misrepresentation schemes. Following this, program offices could establish risk tolerances for improper payments caused by misrepresented identity to determine the acceptable level of risk and to determine the appropriate type of internal control system to respond to the risks.

Program offices face challenges to implementing identity-verification processes. This includes ensuring that socioeconomically vulnerable individuals do not face increased burdens when attempting to verify their identities. In addition, government-wide considerations, such as the framework to govern the role of identity credentials, must be addressed to help to facilitate program offices' implementation of identity-verification controls.

In light of wide-spread reports of fraud in programs across the range of federal programs—due in part to identify verification issues—the executive branch has recently taken action to estimate the extent of fraud due to misrepresented identity and to identify actions to address the challenge. This report provides a framework to consider and evaluate additional potential options or practices to address identity misrepresentation. It also recognizes that efforts to address identity verification may potentially occur at the individual program level or through actions taken by a central management entity. As such, the considerations and specific controls relevant to each are separately presented in this report.

## Steps Taken

### Executive Branch Efforts

The Office of Management and Budget's (OMB) Circular A-123 Appendix C, *Requirements for Payment Integrity Improvement* (OMB M-21-19), provides guidance for executive agencies' implementation of the Payment Integrity Information Act of 2019.[5] It includes requirements for identifying and adequately assessing payment integrity risks; developing a sampling and estimation methodology plan to identify the amount of improper payments;[6] properly identifying the true root causes of improper payments and payment integrity risks; developing appropriate, adequate, and effective controls to mitigate payment integrity risk; and identifying and achieving a tolerable level of improper payments and payment integrity risk.[7]

Additionally, in 2020, a cross-agency team working on the President's Management Agenda Cross-Agency Priority Goal of Getting Payments Right concluded that agencies did not consistently track the amount of identity-related improper payments in federal programs. As a result, OMB required agencies to start tracking and reporting this information for the first time in 2021, and agencies attributed approximately $7.7 billion of their improper payment estimates for fiscal year 2021 to identity issues. Despite this, some agencies are still in the beginning phases of determining whether misrepresented identity is a significant cause of improper payments and the total impact of misrepresented identity is still largely unknown.

Recently, the Executive Office of the President has undertaken a number of new initiatives to combat improper payments, as well as fraud, which relate to misrepresented identity with an objective to immediately prevent and deter fraud and improper payments. For example, in May 2021, the President called for the American Rescue Plan Coordinator and OMB, in consultation with the Pandemic Response Accountability Committee, Inspectors General, and the Government Accountability Office to take government-wide steps to prevent individuals from defrauding public benefits programs. The work of this initiative will include making government-wide recommendations as part of the

[5]Pub. L. No. 116-117, 134 Stat. 113 (2020), *codified at* 31 U.S.C. §§ 3351-3358.

[6]As defined by OMB, the Sampling and Estimation Methodology Plan is the statistical sampling and estimation method that a program designs and implements to produce a statistically valid improper payment and unknown payment amount estimate. (See OMB M-21-19.)

[7]OMB M-21-19, issued on Mar. 5, 2021, became effective starting in fiscal year 2021.

President's forthcoming executive order on preventing and detecting identity theft involving public benefits, while protecting privacy and civil liberties and preventing bias that results in disparate outcomes.

## JFMIP Initiative

### Exploring Options for Strengthening Payment Integrity through Identity Verification

In response to the significant improper payment estimates reported and the lack of historical data related to identity-related root causes, the Joint Financial Management Improvement Program (JFMIP) began an initiative in October 2020 to (1) report key considerations in effective identity verification to ensure payment integrity and (2) gather empirical data, through targeted studies, on the significance of misrepresented identity as a root cause of improper payments and analyzing the effects. The initiative is to be completed in two phases, with each objective representing a phase.[8] This initiative aims to augment the actions undertaken by individual agencies, including the Executive Office of the President, by providing a resource for agencies to use over the long-term to address the significant challenge of reducing improper payments.

Throughout the first half of 2021, the JFMIP reviewed relevant studies on identity verification and interviewed experts to discuss processes and control activities that government and private industry use, as well as known implementation challenges and unintended consequences. In June 2021, the JFMIP convened a panel of experts from federal, state, and international governments; financial institutions; nonprofit organizations; and private industry to discuss the following topics related to identity verification:

- key considerations for effective verification,
- determining the most appropriate authoritative sources for data,
- cost of implementing verification controls and processes,
- a potential implementation framework for the U.S. government,
- unintended consequences of implementing verification processes, and
- methods for estimating improper payments that misrepresented identity caused.

[8]The JFMIP is a cooperative venture between the Government Accountability Office, OMB, the Office of Personnel Management, and the Department of the Treasury in support of continuously improving federal financial management.

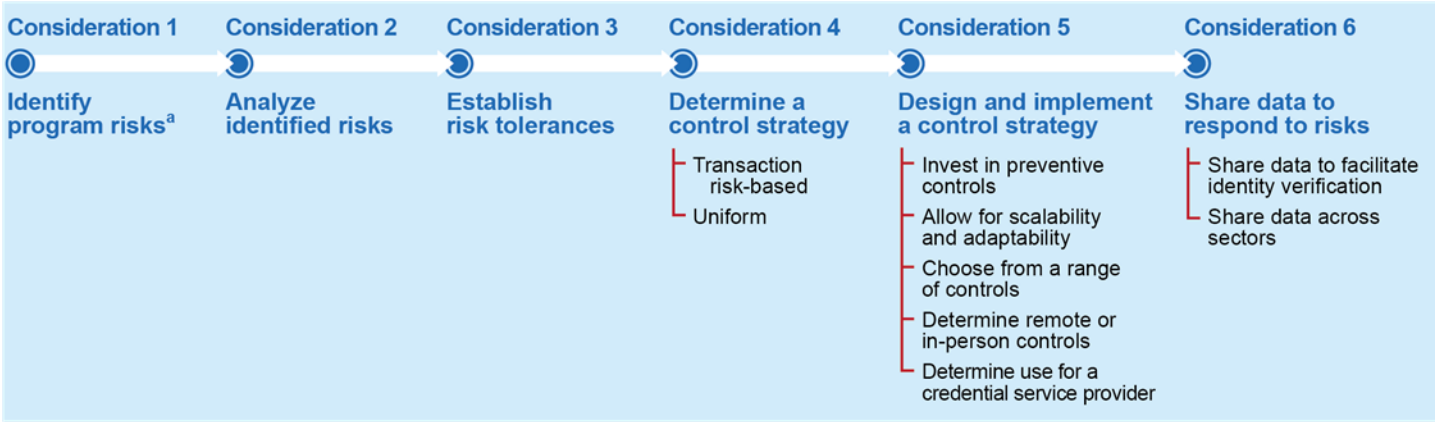
Following the expert panel, the JFMIP analyzed and distilled the discussion in light of its prior review of selected studies and interviews with subject matter experts. This report distills concepts and ideas that an expert panel discussed into a set of key considerations that the JFMIP identified. The key considerations identified above and described in further detail in the executive summary illustrate the range of considerations included in the report.

The JFMIP incorporated the results in this report into an illustrative simulation tool intended to allow users to further explore the benefits and trade-offs of incorporating identity-verification controls and processes.[9] The simulation tool icon in the left margin of the report denotes a concept readers can further explore in the Identity Verification Controls Simulator via clicking the icon or navigating to https://gaoinnovations.gov/id_verification. This tool allows users to modify certain characteristics of a hypothetical program and uses hypothetical data to demonstrate the effects of identity-verification controls on the proportion of improper and proper payments prevented, administrative costs, and the program's reputation.

## Key Program Office Considerations, Successful Control Strategies, and Actions to Address Implementation Challenges and Unintended Consequences

### *Considerations at the Program Level*

The figure below summarizes key considerations for a program office to explore.




Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Program (JFMIP).

[a] Part of identifying program risks includes performing data analytics to identify the impact of improper payments caused by misrepresented identity. See the *Improve Identification of Improper Payments Caused by Misrepresented Identity* report section for more details.

[9]The outcomes of a particular control configuration in this highly stylized simulation are not generalizable to real-world scenarios

Experts discussed a number of key considerations for program offices to consider when verifying identity. They emphasized the importance of identifying and analyzing risks and establishing risk tolerances before designing a system of identity-verification controls to respond to the risks. For example, to identify risks, a program office could consider the types of misrepresented identity that are associated with individuals' applications for benefits or requests for payments.

Following the risk assessment, program offices could consider how to respond to the risks and implement a strategy accordingly. For example, a program office could choose from a range of identity-verification controls and apply them uniformly to all transactions or calibrate its controls based on risks that each transaction presents. Experts noted the importance of allowing for scalability and adaptability when considering the design of a system of controls in order to quickly respond to changing circumstances without sacrificing the program office's ability to verify identities. A program office could also consider whether to self-implement the controls, use a credential service provider, or both. Experts also mentioned that sharing data among federal program offices, and accessing data from the states and private sector, where allowable, could augment the effectiveness of identity verification and reduce the opportunity for improper payments.

To help program offices identify program risks related to misrepresented identity, experts discussed specific strategies to use historical data to determine the extent to which misrepresented identity is a significant cause of improper payments. Specifically, the panel discussed analytical techniques, data repositories, and existing capabilities and resources that program offices could leverage to potentially improve their ability to identify improper payments associated with misrepresented identities. For example, program offices can reexamine historical payment data and look for indications of anomalous payments in order to identify, recover, and design future controls to mitigate improper payments associated with misrepresented identities. In addition, panelists noted that program offices can leverage existing resources, such as the Department of the Treasury's Bureau of the Fiscal Service's payment data, to perform data analytics and identify improper payments that misrepresented identity caused. See the *Improve Identification of Improper Payments Caused by Misrepresented Identity* report section for more details.

*Successful Identification-Verification Controls Identified by Expert Panel*

Panelists discussed a number of effective identity-verification strategies that federal and state program offices, international governments, and private industry have successfully adopted. The table below summarizes the identity-verification controls that program offices can use for identity verification and authentication. Further discussion of these controls can be found in Step 5: Design and Implement a Control Strategy to Respond to Risks in the report.

Table: Summary of Identity-Verification Controls

| Control | High-level summary | Examples |
|---|---|---|
| Digital footprint | Identifies information about an applicant's hardware, software, and behavioral biometrics in order to connect past and future interactions.<br><br>May not be ideal for those who lack access to a personal electronic device. | A program office reviews the internet protocol (IP) address of an application and determines if it originated from an unexpected location, such as out of the country.[a]<br><br>A program office reviews the applicant's computer keystroke, mouse patterns, or both to determine if the behavior suggests the application was completed by a bot. |
| Bank account verification | Compares banking information with information the applicant supplied.<br><br>May not be ideal for individuals who lack a U.S. bank account. | Program office compares known name and bank account information with information on the application.<br><br>Additionally, the program office can initiate micro-deposits and ask the applicant to verify these amounts to establish ownership of the bank account. |

| Control | High-level summary | Examples |
|---|---|---|
| Physical address verification | Verifies an individual's identity by mailing information, such as a personal identification number (PIN), to the individual's physical address.[b]<br><br>Slower than other remote verification options, but may be necessary for those without the means to verify their otherwise.<br><br>Individuals who lack a physical address or reside at an address different from the mailing address may not be able to receive the information. | Program office mails out a PIN to an applicant's home. Applicant is required to provide the PIN before proceeding with the application. |
| Email or phone verification | Verifies an applicant's identity during initial account setup by electronically sending information, such as a PIN, to the applicant's phone number or email address.<br><br>Individuals who lack an email address or phone number may not be able to receive verification using this method. | Program office texts a PIN to a phone number that the applicant provides. Applicant is required to provide the PIN before proceeding with the application. |
| Physical biometrics[c] | Verifies an applicant based on biological characteristics.<br><br>Can be collected in person or remotely. | Applicant provides fingerprint scan, which is compared to the appropriate database.<br><br>Program office verifies a government photo identification to a photo of the individual. |
| Applicant notification | Program office notifies an individual when an application has been submitted using their identity. | Program office notifies an individual of an application through physical mail, email, text message, or phone call. |

Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Programs (JFMIP)

[a]An IP address is a unique identifier tied to every internet-connected device.

[b]Physical address may be the location where an individual sleeps, which is important for those in the homeless population who may be applying for government benefits without permanent residences.

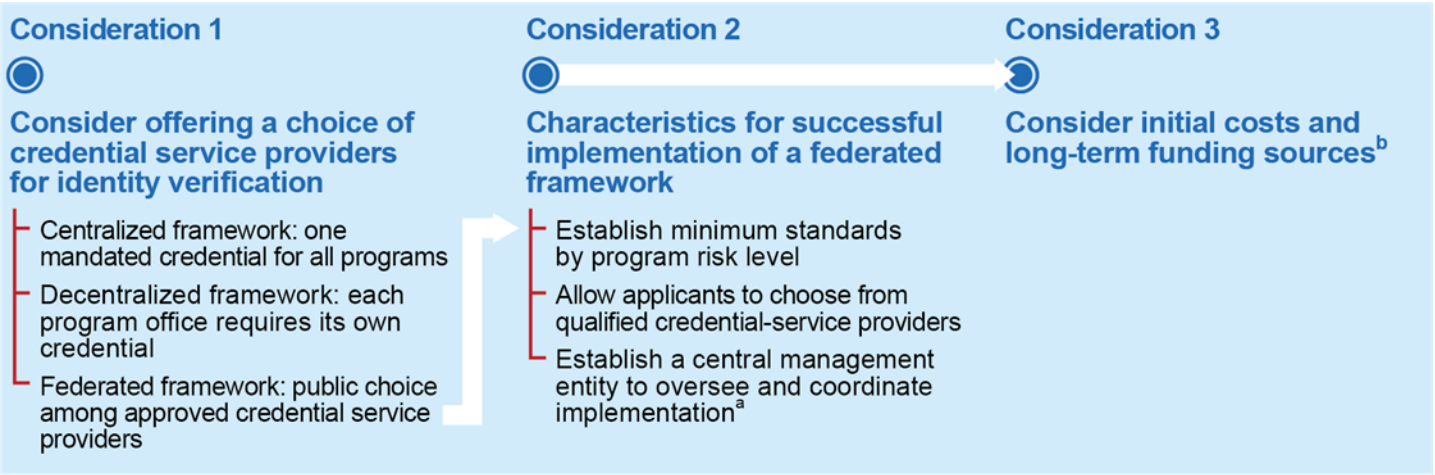
[c]While biometrics can be used for both authentication and verification, the privacy considerations differ for each use. For verification, an applicant may have to provide biometric information to a program agency. On the other hand, authentication options exist that do not require collecting applicant biometric information.

### *Actions to Address Implementation Challenges and Unintended Consequences*

Implementing identity-verification processes includes challenges at the program office and government-wide level. Program offices may want to familiarize themselves with potential implementation challenges included in this report to improve the identification and prevention of improper payments that result from misrepresented identity. Experts discussed a number of actions to address implementation challenges that program offices may encounter when implementing identity-verification controls. For example, as it relates to the decision to implement in-person or remote identity-verification controls, program offices should consider that certain segments of the population, such as socioeconomically vulnerable individuals, may face an increased burden when verifying their identities. This may occur because these individuals may not have the required data elements or documentation or may not have the means to supply the required information. As a result, experts suggested offering multiple channels for applicants to verify their identities, such as in-person and remote, in order to overcome the variety of obstacles that these individuals may face.

## Government-wide Considerations for a Central Management Entity

The figure below summarizes key considerations for a central management entity when attempting to address identity verification issues.




Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Program (JFMIP).

[a] The government may also consider establishing a central information hub to share insights and analytics related to improper payments caused by misrepresented identity. See the *Establish Information Hubs to Facilitate Data Sharing and Analytics* report section for more details.

[b] Data sharing, where permitted and appropriately authorized, among program offices, with states, and with the private sector may be a way to share the costs involved in identity verification. See the *Share Data to Strengthen Responses to Risks* report section for more details on data sharing.

In addition to providing considerations for program offices, the panel discussed government-wide considerations for facilitating identity verification, including various frameworks to govern the role of identity credentials and shape the environment in which identity-verification controls and processes exist. Panelists discussed the advantages and challenges of a centralized model that uses a single identity credential across multiple programs and a decentralized model in which each program office can require its own identity credential. Several panelists suggested that a federated framework, which falls in between the centralized and decentralized models, has the most potential for success. A federated framework gives the public the option to choose between multiple providers to verify their identities and obtain a portable credential that they can use across program offices.

---

The information in this report, and accompanying simulation tool, aim to further augment the steps taken by federal agencies to reduce improper payments that misrepresented identity caused. This report distills considerations, concepts, ideas put forth by an expert panel hosted by the JFMIP. It also identifies successful verification strategies used by a range of entities. This report does not represent an exhaustive list of strategies that currently exist in the public and private sectors. The ideas, considerations and strategies discussed in this report are for informational and exploratory purposes only. This report is not guidance that agencies are required to follow. Further, the JFMIP did not assess whether agencies could implement the controls identified by experts under their existing legal framework.

## Next Step

In the next phase of this initiative, the JFMIP will conduct targeted studies to demonstrate the effects of selected, enhanced identity-verification controls at executive branch agencies.

# Foreword

Reducing improper payments—such as payments to ineligible recipients or duplicate payments—is critical to safeguarding federal funds. From fiscal years 2003 through 2021, estimated government-wide improper payments have totaled around $2.2 trillion, which equates to $7,000 in improper payments per U.S. citizen over the 19-year span.[10]

In October 2020, the Joint Financial Management Improvement Program (JFMIP), a cooperative venture between the Government Accountability Office, the Office of Management and Budget, the Office of Personnel Management, and the Department of the Treasury, began an initiative to identify key considerations to enhance identity verification and potentially reduce improper payments. The JFMIP is in a unique position to address government-wide financial management issues, such as improper payments, because of its collaborative approach that includes outreach to various organizations and staff throughout the federal government. This initiative complements continuing efforts of individual agencies working on improper payment mitigation strategies and aims to accelerate their efforts.

The two objectives of this initiative are

1. reporting key considerations in effective identity verification for purposes of payment integrity and
2. gathering empirical data, through targeted studies, on the significance of misrepresented identity as a root cause of improper payments, and analyzing the effects.

This report addresses the JFMIP initiative's first objective by providing the considerations discussed by the JFMIP-convened panel of experts and subsequent research. The first two sections of this report discuss considerations of key identity verification practices and actions to address implementation challenges for individual agencies. The third section discusses actions for a central management entity to consider when implementing a potential government-wide framework for identity credentials. The fourth and final section discusses considerations for both individual agencies and a central

[10]These figures do not all represent a loss to the government. For purposes of federal agency estimation and reporting, an "improper payment" is defined as any payment that should not have been made or that was made in an incorrect amount. These reported estimates include both overpayments and underpayments and are not adjusted based on any correction or recovery of funds. Further, if, in developing an estimate, an agency finds that it cannot determine whether a sampled payment is proper, it must treat the payment as improper. 31 U.S.C. §§ 3351(4), 3352(c).

management entity on improving identification of improper payments that relate to misrepresented identity. Further, the JFMIP created a simulation tool hosted on the JFMIP website (https://www.cfo.gov/jfmip/) to illustrate potential benefits and trade-offs for both an agency and the public when implementing various identity-verification controls.

The JFMIP is grateful for the opportunity to collaborate across agency boundaries on this critical topic. We thank the diverse expert panelists who met to share valuable insights, experience, challenges, and considerations related to identity verification and improper payments (see app. III for a list of contributors).

Beryl H. Davis
Managing Director
Financial Management and Assurance
U.S. Government Accountability Office

Deidre Harrison
Deputy Controller
Office of Federal Financial Management
Office of Management and Budget

Taka Ariga
Chief Data Scientist and Director of Innovation Lab
Science, Technology Assessment, and Analytics
U.S. Government Accountability Office

Douglas A. Glenn
Chief Financial Officer
Office of Personnel Management

Linda Claire Chero
Assistant Commissioner, Payment Management and Acting Assistant Commissioner, Debt Management Services
Bureau of the Fiscal Service
Department of the Treasury

# Introduction

Improper payments have been a long-standing challenge for the federal government. For fiscal year 2021, estimates of improper payments totaled $281 billion, about a $75 billion increase from the prior year. Further, fiscal year 2021 estimates of improper payments generally do not include estimates related to the expenditures to fund urgent response and recovery efforts for the COVID-19 pandemic, so estimates of improper payments may further increase in the future.

An *improper payment* is any payment that should not have been made or that was made in an incorrect amount under statutory, contractual, administrative, or other legally applicable requirements.[11] Since fiscal year 2004, federal law has required executive agencies to estimate and report on improper payments in risk-susceptible programs they administer.

The majority of the programs that report significant improper payment estimates involve federal agencies making payments to or on behalf of individuals who must meet specific eligibility criteria.[12] There are many systemic factors that contribute to complex causes of improper payments, including the effectiveness of simultaneous screening for multiple eligibility criteria that an applicant must meet prior to receiving a payment. One potentially significant contributing factor relates to applicant identities—verifying that applicants interacting with a federal program office are who they claim to be.[13] Prior to 2021 reporting, agencies had not been required to isolate and report on the amount of improper payments that may have been the result of the government's inability to identify recipients accurately.

Securing the transactions in which individuals engage when applying for federal benefits and services or requesting payments is a complex endeavor.

---

[11]Improper payments also include any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, and any payment for a good or service not received (except for such payments where authorized by law). 31 U.S.C. § 3351(4)(B). Further, when an agency is producing an improper payment estimate and cannot determine, because of lacking or insufficient documentation, whether a payment is proper or not, the payment shall be treated as an improper payment. 31 U.S.C. § 3352(c)(2)(a). It is important to note that reported improper payment estimates may or may not represent a loss to the government.

[12]An executive agency program is considered susceptible to significant improper payments—and therefore subject to annual estimation and reporting requirements—if the total of the program's previous-year improper payments and payments whose propriety cannot be determined may have exceeded either (1) both 1.5 percent of program outlays and $10,000,000, or (2) $100,000,000 (regardless of the percentage of program outlays). 31 U.S.C. § 3352(a)(3)(A).

[13]In this report, *applicant* refers to individuals or entities that apply to a federal benefits program or that request a payment, such as a tax refund.

Verification of individuals' identities is essential to preventing improper payments in several contexts, including those involving fraudulent activity, as failure to do so properly could cause harm to both individuals and organizations.[14] For example:

- Payments to real people who want to hide their identities in order to avoid having their eligibility questioned.
- Payments to those using authentic identity data elements to create synthetic identities.[15]
- Payments to those assuming the identities of other people.
- Payments to those who erroneously provide inaccurate information regarding their identities.

The federal government is responsible for ensuring that the right recipient receives the right amount when it makes payments to or on behalf of individuals and businesses, such as program beneficiaries, grantees, or contractors. Office of Management and Budget (OMB) guidance requires agencies that report improper payment estimates for programs to also describe the root causes of the improper payments in each program.[16] However, prior to March 2021, agencies were not required to isolate the amount of improper payments that occurred because of an inability or failure to establish that someone is uniquely who they claim to be prior to issuing a payment.[17] As such, 2021 was the first year that agency estimates quantified improper payments related to misrepresented identity.

The Executive Office of the President has recently undertaken a number of new initiatives to combat improper payments, as well as fraud, which relate to misrepresented identity with an objective to immediately prevent and deter

---

[14]Improper payments, fraud, and fraud risk are related, but distinct, concepts. While unintentional error may cause improper payments, fraud involves obtaining something of value through willful misrepresentation. Whether an act is fraudulent is determined through the judicial or other adjudicative system. Fraud risk exists when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or are able to rationalize committing fraud.

[15]A synthetic identity is a new fabricated identity that usually consists of a real identifier, such as a Social Security number or driver's license number, with other fake information.

[16] Per OMB, a root cause is something that would directly lead to an improper payment and if corrected would prevent the improper payment.

[17]In March 2021, OMB released an update to its Circular A-123 Appendix C, which includes identity as a subset of certain information-related cause categories. OMB, *Transmittal of Appendix C to OMB Circular A-123, Requirements for Payment Integrity Information*, Memorandum No. M-21-19 (Mar. 5, 2021).

fraud and improper payments. For example, in May 2021, the President called for the American Rescue Plan Coordinator and OMB, in consultation with the National Security Council, Pandemic Response Accountability Committee, Inspectors General, and the Government Accountability Office to take government-wide steps to prevent individuals from defrauding public benefits programs. This initiative, working together with the cybersecurity team of the National Security Council, will be making government-wide recommendations as part of the President's forthcoming executive order on preventing and detecting identity theft involving public benefits, while protecting privacy and civil liberties and preventing bias that results in disparate outcomes.

The JFMIP initiative aims to augment the actions undertaken by individual agencies, including the Executive Office of the President, by providing a resource for agencies to use over the long-term to combat the significant challenge of reducing improper payments. This report presents considerations and potential actions that emerged from the JFMIP-convened panel discussion that agencies could consider using to enhance identity verification and potentially reduce improper payments. It also includes considerations that the experts discussed for a framework to broaden implementation of identity-verification controls throughout federal government programs. In addition, the report presents a "simulation tool" icon that links to the accompanying simulation tool's website.[18] This icon appears whenever the report discusses a concept that users can further explore in the simulation. The simulation tool is an illustrative model that allows users to understand the potential benefits and trade-offs of implementing various identity-verification tools and processes. The considerations and potential actions do not represent an exhaustive list of ideas that currently exist in the public and private sectors. The ideas included in this report are for informational purposes only, and this report is not guidance that agencies are required to implement.

[18] The outcomes of a particular control configuration in this highly stylized simulation are not generalizable to real-world scenarios.

# Background

## Identity Verification

Identity verification confirms the claimed identity and establishes a link between it and the real-life existence of the individual presenting identity evidence. This verification may occur in person or remotely. With in-person verification, a trained professional verifies an individual's identity by directly comparing the individual's physical features and other evidence (such as a driver's license or passport) with official records.

Remote verification most commonly occurs through interaction with an organization's website or other forms of digital interface. Remote identity proofing involves two major steps: (1) resolution and (2) validation and verification.[19] During resolution, an organization determines which specific identity an applicant is claiming when the applicant first attempts to initiate a transaction, such as enrolling for federal benefits or services, remotely. The organization begins the resolution process by requiring the applicant to provide identifying information, typically through a digital form.

Examples of information an organization may collect for identity resolution include given name(s), family name, mailing address, date of birth, and Social Security number (SSN). The organization then electronically compares the applicant's identifying information with available electronic records it already maintains in its databases or with authoritative sources.[20] The organization may also corroborate identifying information with records another entity, such as a consumer credit reporting agency, maintains to distinguish which identity is being claimed. For example, if an individual bearing a common name such as Jane Doe applied for payment, then the organization would obtain enough identifying information to determine the particular "Jane Doe" from other individuals bearing that name. Similarly, the organization would obtain sufficient information to distinguish the applicant's personally identifiable information (PII) from the PII of other individuals named Jane Doe.

[19] While identity verification is one step within the identity-proofing process, it is also used informally as a term to encompass a range of techniques to collect and resolve data to a particular person and validate that the data provided are legitimate and accurate for that person.

[20] An authoritative data source determines the accuracy, integrity, and provenance of the data; performs due diligence on contributors to the data; and conducts third-party vetting and auditing of the data.

Once the organization completes the resolution process, it begins the processes of validation, to confirm that the claimant is the same person as the owner of the user account, and verification, to establish an authenticated connection between the applicant and the PII or evidence provided. In these processes, organizations take steps to determine whether the applicant is really who the applicant claims to be.

For example, in the case of Jane Doe, it is not enough simply to determine which Jane Doe is being claimed, because the claimant may not really be Jane Doe. Therefore, as part of the validation process, the individual claiming the specific Jane Doe identity must provide electronic evidence to support the claim, such as a picture of a Jane Doe's driver's license. Once the organization confirms the evidence is genuine and authentic, it then begins the verification process, which matches the evidence to the claimant's identifying characteristics, such as comparing the claimant's facial features to the picture on the driver's license that the claimant provided.

Because identity verification involves individuals' information, it can also create privacy risks. According to the National Institute of Standards and Technology (NIST), organizations could potentially mitigate these risks by assessing the risk associated with online transactions and selecting the appropriate assurance level needed for each. This strategy, however, is a delicate balance: A low assurance level reduces the amount of personal information that organizations must collect but increases the risk of improper transactions. On the other hand, a high assurance level may increase the burden on applicants, including those who are not misrepresenting their identities.

Successful authentication—verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources—provides reasonable risk-based assurance that the individual accessing the service today is the same individual who accessed a service previously. Ongoing authentication is central to associating applicants with their online activity; it is not a onetime activity that is only associated with applying for a benefit or requesting a payment. Organizations authenticate applicants by verifying that the claimant controls one or more authenticators associated with a given applicant.[21]

[21]An authenticator is something the claimant possesses and controls, such as a password that is used to authenticate the claimant's identity.

Authentication establishes that the individual attempting to access a digital service is in control of the technologies used to authenticate themselves. Digital authentication is the process of determining the validity of one or more authenticators an applicant uses to claim a digital identity.

Authentication strength is determined by the number of factors used in the authentication process. There are three factors:

1. Something the applicant knows (such as the user ID and password/passphrase).
2. Something the applicant has (such as a chip-based smart card or a digital token).
3. Something the applicant is (such as a fingerprint or facial recognition).

Authenticators may rely on a single factor or aggregate multiple factors. Authentication strength is higher when authenticators use two or more factors together, which is commonly referred to as multifactor authentication.[22] Credential service providers (CSP) maintain a record of all authenticators associated with each identity and information required for regulating authentication attempts.[23]

Eligibility and identity are distinct, but interrelated, elements of the verification process. *Eligibility verification* is the process of validating specific criteria (e.g., statutory requirements, citizenship, income, SSN, etc.) that must be met to receive a payment, service, or benefit. On the other hand, *identity verification* confirms the claimed identity of an individual seeking a payment or benefit without regard to the individual's ability to meet the program's eligibility requirements. While these are two separate processes, they can be interrelated. For example, if a program requires an individual to be a certain age to be eligible for benefits, then a program's eligibility and identity verification processes may both use a document such as a driver's license as evidence.

---

[22] The Office of Management and Budget (OMB) provides specific multifactor authentication requirements for federal agencies, including for public-facing programs. Office of Management and Budget, *Moving the U. S. Government Toward Zero Trust Cybersecurity Principles*, OMB Memorandum M-22-09 (January 2022).

[23] A CSP is a trusted entity that issues or registers applicant authenticators and issues electronic credentials to applicants. A CSP may be an independent third party or issue credentials for its own use. When a CSP is involved in the authentication process, the individual proves control of the credential to the CSP, which in turn asserts the individual's identity to the program office.

## Standards Related to Identity Verification

NIST develops information-security standards and guidelines, including minimum requirements for federal information systems. Its guidance on digital identity states that for non-federated systems, organizations select two components of identity assurance, which NIST refers to as Identity Assurance Level (IAL), and Authenticator Assurance Level (AAL).[24] The IAL refers to the robustness of the identity-verification process to determine the identity of an individual confidently, and organizations select an IAL to mitigate potential identity-verification errors. The AAL establishes a match between an authenticator and a specific individual's identifier, and organizations select an AAL to mitigate potential authentication errors. Depending on the type of interaction between an individual and an organization, the individual would be subject to varying levels of verification.

## Statutory Requirements and OMB Guidance Related to Improper Payments

The Payment Integrity Information Act of 2019 (PIIA) was signed into law in March 2020 and consolidated and revised key provisions from the following statutes into a single subchapter of the U.S. code: the Improper Payments Information Act of 2002, the Improper Payments Elimination and Recovery Act of 2010, the Improper Payments Elimination and Recovery Improvement Act of 2012, and the Fraud Reduction and Data Analytics Act of 2015 (FRDAA).[25] Office of Management and Budget (OMB) Circular A-123, and Appendix C, *Requirements for Payment Integrity Improvement* (OMB M-21-19), provides guidance for executive agencies' implementation of PIIA and provides requirements for identifying and adequately assessing payment integrity risks; developing a sampling and estimation methodology plan to identify the amount of improper payments;[26] properly identifying the true root causes of improper payments and payment integrity risks; developing appropriate, adequate, and effective controls to mitigate payment integrity risk; and identifying and achieving a tolerable level of improper payments and payment integrity risk.[27]

---

[24]National Institute of Standards and Technology, *Digital Identity Guidelines*, Special Publication 800-63-3 (Mar. 2, 2020).

[25]Pub. L. No. 116-117, 134 Stat. 113 (2020), *codified at* 31 U.S.C. §§ 3351-3358.

[26]As defined by OMB, the Sampling and Estimation Methodology Plan is the statistical sampling and estimation method that a program designs and implements to produce a statistically valid improper payment and unknown payment amount estimate. (See OMB M-21-19.)

[27]OMB M-21-19, issued on Mar. 5, 2021, became effective starting in fiscal year 2021.

## Criteria Related to Existing GAO and OMB Guidance

Several considerations that the experts discussed relate to requirements and leading practices in Government Accountability Office (GAO) and OMB guidance.[28] Panelists discussed the need for a risk-based approach to identity verification. Several principles in GAO's *Standards for Internal Control in the Federal Government* involve assessing and responding to risks, including fraud risks.[29] Similarly, GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework) provides comprehensive leading practices to federal program managers for conducting fraud risk assessments, which involves identifying inherent fraud risks affecting the program and using the results as part of a robust antifraud strategy.[30] As mentioned above, OMB M-21-19 provides executive agencies with guidance and requirements for identifying, assessing, and mitigating payment integrity risks. Similarly, OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* provides guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities.[31] Relevant GAO and OMB standards and guidance are cited throughout this report when it supports considerations noted by the panelists.

[28]This report uses the term "guidance" to include directives, guidelines, standards, and leading practices published by a federal entity for use by other federal agencies in the operation of their programs.

[29]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).

[30]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015). The Fraud Risk Framework helps managers meet their responsibilities to assess and manage fraud risks, as required by federal internal control standards (see GAO-14-704G). The leading practices of the Fraud Risk Framework are also required to have been incorporated into OMB guidelines and agency controls under FRDAA and its successor provisions in PIIA. FRDAA, Pub. L. No. 114-186, 130 Stat. 546 (2016), enacted in June 2016, required OMB to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. The act further required OMB to incorporate the leading practices from the Fraud Risk Framework in the guidelines. Although FRDAA was repealed in March 2020, PIIA, Pub. L. No. 116-117, 134 Stat. 113 (2020), requires these guidelines to remain in effect, subject to modification by OMB as necessary and in consultation with GAO. See 31 U.S.C. § 3357. Also see Office of Management and Budget, *OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Memorandum M-16-17 (July 2016).

[31]OMB M-16-17.

## Objectives, Scope, and Methodology

The objectives of this report are to provide

1. considerations around identity verification in federal programs,
2. actions that program offices can consider taking to address challenges associated with implementing identity-verification controls,
3. considerations for a potential framework that the federal government can use to govern the role of identity credentials, and
4. considerations that could assist agencies in identifying and preventing improper payments that result from misrepresented identity.

The scope of this work focuses on federal programs and activities for which verifying identity is an essential step in ensuring whether payment is proper.

To address this report's objectives, in June 2021, the Joint Financial Management Improvement Program (JFMIP) convened an expert panel to identify critical components of effective identity-verification control activities. The panel included experts from private industry; federal, state, and international government offices; consulting and accounting firms; credential services providers; and nonprofit organizations.

The JFMIP identified considerations based on information we collected from the expert panel, a review of selected studies, and our interviews with subject-matter experts. This report is a distillation of the expert panel's discussion as well as information obtained from that review and those interviews. This report considers both program-level practices as well as a macro-level, whole-of-government strategy to broaden implementation of effective identity verification controls.

Throughout this report, we will refer to the individuals the JFMIP convened for this discussion as the *expert panel*, including *experts*, *panelists*, and *expert panelists*. To describe statements panelists made, we distinguish between issues from a single panelist, some panelists (two to three), and several panelists (four or more). The JFMIP provided this report to the expert panelists for technical review and incorporated their comments as appropriate.

The JFMIP did not assess whether agencies could implement considerations under their existing legal framework or whether doing so would require changes in the legal framework. In addition, the examples provided in this

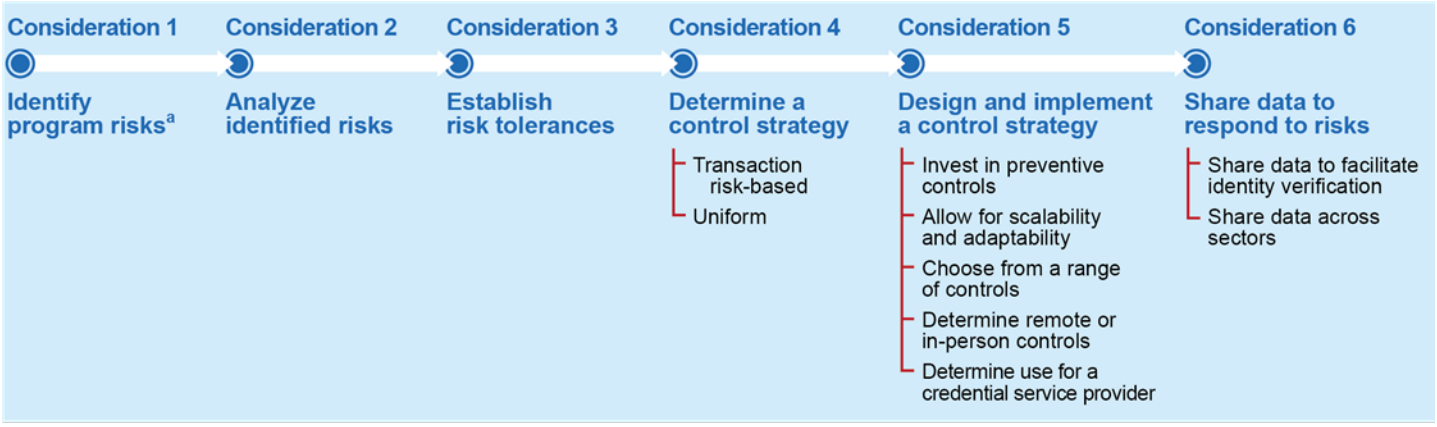
report are for illustrative purposes only and are not exhaustive of all options, or indicative of the best option, available to any particular program office.

## Identity-Verification Capabilities and Controls at the Program Level

The need to guard against applicants misrepresenting their identities to obtain federal benefits or payments requires program offices to consider identity-verification processes and controls. Panelists discussed a number of effective identity-verification strategies that federal and state program offices, international governments, and private industry have successfully adopted. Some controls may also be used for identity verification and authentication. However, before determining which combination of controls best fits a given program, some panelists noted the need to understand the program's risks related to misrepresented identity and determine a strategy to respond to them. Step 1: Identify Program Risks and Step 2: Analyze Identified Risks to Understand Impact below discuss the importance of identifying and analyzing risks to determine the extent to which misrepresented identities pose a program risk.

Figure 1 illustrates a six-step process to facilitate identity-verification capabilities and controls that begins with identifying risks of harm caused by misrepresented identities and resulting in implementation of controls appropriate to the program.

Figure 1: Overview of Practices to Facilitate Identity-Verification Capabilities and Controls




Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Program (JFMIP).

[a] Part of identifying program risks includes performing data analytics to identify the impact of improper payments caused by misrepresented identity. See Improve Identification of Improper Payments Caused by Misrepresented Identity below for more details.

Several panelists highlighted specific controls that program offices could consider implementing commensurate with their particular program risks.[32]

## Step 1: Identify Program Risks

Some experts noted the importance of identifying risks to determine the extent to which misrepresented identities pose a program risk. For example, a program may inadvertently issue an improper payment to an applicant, unknowingly disclose an applicant's personally identifiable information, or be the target of cyberattacks aimed at the program's databases. If identity verification is a potential risk to an agency's objectives, the agency may choose to determine such risks as part of other required internal control assessments or as an independent evaluation.

In order to identify risks related to identity-verification controls, a program office may consider all significant interactions within the program office, with its parent agency, and with external parties. It also may consider changes within the program office's internal and external environment and other internal and external factors. Methods for identifying risk may include qualitative and quantitative ranking of activities that may expose the agency to risk of improper payments because of misrepresented identities as well as related forecasting and considering deficiencies identified through audits and other assessments. Both Government Accountability Office (GAO) and Office of Management and Budget (OMB) guidance separately require an agency to identify and analyze risks.[33] See Improve Identification of Improper Payments Caused by Misrepresented Identity for more details on analytical techniques and program office considerations for identifying, estimating, and reporting improper payments that misrepresented identity caused.

---

[32]OMB's *Requirements for Payment Integrity Improvement* notes that the prevention of improper payments requires a multipronged approach that is continually evolving (OMB M-21-19).

[33]An agency should identify and analyze risks related to achieving its objectives; see GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014). GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015), also known as the Fraud Risk Framework, provides comprehensive guidance to federal program managers for conducting fraud risk assessments, which involves identifying inherent fraud risks affecting the program and using the results as part of a robust antifraud strategy. OMB's *Requirements for Payment Integrity Improvement* requires agencies to determine the risk factors and the associated scoring or risk factor weighting methodology that should be considered for each individual program and risk when conducting an improper payment risk assessment (OMB M-21-19). If identity verification is a significant factor contributing to the agency's susceptibility to improper payments, then the agency should ensure that proper consideration is given to identity when developing their improper payment risk assessment methodology.

## Step 2: Analyze Identified Risks to Understand Impact

Some experts stated that in the absence of reliable data, program offices may consider using "red flag" indicators to determine the likelihood and significance of identity-related improper payment risks. Similarly, GAO and OMB have separately issued guidance noting that after identifying sources of risk, agency managers should analyze the significance of these risks.[34]

Particularly in contexts where data are sparse and the risks associated with misrepresented identity are uncertain, data sharing across entities with additional identity-related data may facilitate risk analysis. Other helpful techniques may include grouping related risks into categories and analyzing them collectively for their likelihood and significance. For example, it may be helpful to consider all forms of document falsification collectively, rather than treating falsified driver's licenses and falsified Social Security numbers (SSN) as separate risks. As part of this analysis, program offices could consider the correlation between different types of identity-verification risks, as this may relate to the significance of these risks.

Another component of risk analysis includes understanding the nature of individuals who are misrepresenting their identities. For example, some misrepresentation may occur because of identity theft.[35] Identity thieves can obtain sensitive personal information through various methods, such as using phishing to trick individuals or employees of an organization into sharing their own or others' sensitive personal information. Identity theft also can occur as a result of the loss or theft of data (a lost or stolen wallet or a thief digging through household trash). Because of the varying nature of how identity theft occurs, identity thieves may have greater or lesser amounts of information available.

For example, GAO previously reported on increased risk of identity theft as a result of data breaches that have exposed sensitive personal information of the

[34]After identifying sources of risk, agency managers should analyze the significance of these risks. In doing so, an agency should consider the magnitude of impact, likelihood of occurrence, and nature of the risk. (GAO-14-704G); The Fraud Risk Framework identifies leading practices associated with assessing the likelihood and impact of inherent fraud risks and notes that in assessing the impact of the fraud risks, it is also important to consider the nonfinancial impacts (GAO-15-593SP); OMB's Requirements for Payment Integrity Improvement notes that 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. Programs should consider the causes of the improper payment and the likelihood of their occurrence in their process of identifying and monitoring payment integrity risks to the program (OMB M-21-19).

[35]Identity theft occurs when individuals' information is used without authorization in an attempt to commit fraud or other crimes.

public, including the 2017 data breach at Equifax, Inc., and the 2020 cybersecurity compromise of SolarWinds Orion.[36] GAO has also found that individuals may reveal sensitive information willingly, such as on social media accounts, which when combined with other information can allow fraudsters to infer identity attributes.[37] Information scraped from public social media accounts may be less sensitive and not, in itself, sufficient to establish a false identity. The information might also be less sufficient to respond to detailed identity-verification questions but might sufficient to answer basic questions successfully.

One program office may find that a recent data breach has increased its risk of receiving applications that use less data in attempts to impersonate individuals, whereas another program office may determine that it is more at risk of receiving applications that use more data to impersonate individuals. Understanding its susceptibility to different types of misrepresentation allows a program office to select the most appropriate verification controls to mitigate those risks.

## Step 3: Establish Risk Tolerances to Determine What Is Not Acceptable

Some panelists noted that program offices could establish risk tolerances for improper payments caused by misrepresented identity and determine the type of internal control system for identity verification.[38] Similarly, GAO and OMB guidance states that agencies should establish risk tolerances.[39] In establishing risk tolerance, management determines the acceptable level of variance in

---

[36]GAO, *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services*, GAO-19-230 (Washington D.C.: Mar. 27, 2019); GAO, *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*, GAO-22-104746 (Washington D.C.: Jan. 13, 2022).

[37]GAO-19-230.

[38]*Standards for Internal Control in the Federal Government* defines risk tolerance as the acceptable level of variation in performance relative to achievement of objectives (GAO-14-704G). *Requirements for Payment Integrity Improvement* defines risk tolerance as 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 (OMB M-21-19).

[39]An agency should design actions to respond to risks so that the risks are within the objectives' defined risk tolerances (GAO-14-704G). An agency should define and document the tolerable level of fraud risk (GAO-15-593SP). OMB's *Requirements for Payment Integrity Improvement* notes that agency senior management must acknowledge that while every action has risk, management's job is to mitigate risk without jeopardizing the mission. With this risk appetite in mind, agency leaders can set risk tolerance bands for improper payments for each program (OMB M-21-19).

performance relative to the achievement of objectives and aligns risk tolerance with risk appetite.[40]

The requirements and expectations may include, for example, making payments quickly or with minimal burden on those seeking payment from the program. The expectation of making payments quickly can contrast with a program office's objective of verifying an applicant's identity. See Establish Business Rules to Account for False Positives and False Negatives below for further discussion on the importance of considering risk thresholds, including the need to consider the burden placed on applicants if a control incorrectly determines that a transaction uses a misrepresented identity.

The risk tolerance may vary across programs. For example, one expert noted that a program office would have a relatively high risk tolerance for misrepresented identity if the program office only accepted payment of taxes rather than both receiving and disbursing funds. Such a program office would not need to design a strict identity-verification control system, as the inherent risk of an individual misrepresenting identity to pay someone else's taxes would be lower than an individual misrepresenting identity in an attempt to receive someone else's funds.

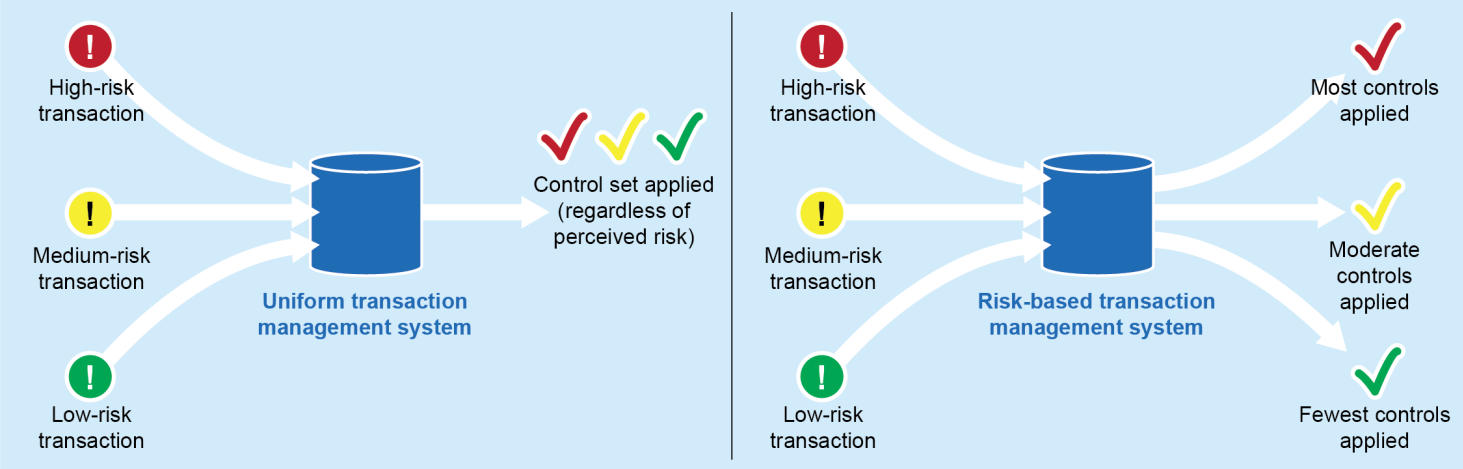
## Step 4: Determine a Control Strategy to Respond to Risks

Program offices can select from two strategies to verify identities—one that applies controls uniformly to all transactions and one that calibrates controls based on a gradation of risks. A program office may find either system ideal depending on its risk assessment. Figure 2 illustrates key differences in both strategies.


Uniform or risk-based system

[40]OMB's *Requirements for Payment Integrity Improvement* defines risk appetite as 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 (OMB M-21-19).

Figure 2: System Configurations




Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Program (JFMIP).

### Uniform System: Identical Controls for Every Transaction

A program office may decide to use a uniform transaction management system if all transactions are similar in risk, if it is not feasible to triage transactions by risk level, or if a program office is legally obligated to treat all transactions identically. A uniform system may be relatively easy to design and may effectively reduce improper payments but, depending on the controls the program office selects, may also cause broad burdens on both administrators and individuals not misrepresenting their identities because the system applies the same set of controls to all transactions regardless of risk. For example, if a program office decides to require all applicants to visit a physical location to verify their identities, the program office may experience a lower rate of improper payments than without this requirement because of the strength of in-person verification. However, requiring all applicants to visit a physical location is burdensome to both applicants, who would need to schedule time to visit the location, and to the program office, which would incur staff and facility costs.

### Risk-Based System: Stricter Controls for Riskier Transactions

A program office may decide to use a risk-based transaction management system if it experiences varying levels of risk in processing transactions or if a program office has sufficient data to accurately assess each transaction's given risk level.[41] This approach uses progressively more-rigorous tiers of controls,

[41]NIST *Digital Identity Guidelines* requires agencies to assess potential risks and identify measures to minimize their impact in order to determine the appropriate level of assurance for a user's asserted identity (NIST SP 800-63-3).

each of which corresponds to a given transaction's risk level. In order to assess a transaction's risk level, several panelists encouraged the use of predictive modeling. OMB guidance notes that when establishing a robust data analytics program, using a predictive approach can move an agency from a "pay-and-chase" approach to one that allows the agency to identify the potential improper payments before they occur.[42]

Consider predictive modeling

Predictive modeling is a class of statistical techniques whereby transactions that have preestablished criteria, patterns, or characteristics are associated with an estimated likelihood of being improper. Program offices can define and apply business rules based on management goals, such as the relative importance of avoiding false positive and false negative classifications. These rules, which can be automated, deem certain transactions higher risk, allowing a program office to control them appropriately during both pre- and postpayment processes.

Relevant identity-related characteristics of a transaction for predicting risk may vary by program. Experts in a prior panel convened by GAO suggested that agencies building a new data analytics program to prevent improper payments take an inventory of current data sources and consider how the data can be used to address improper payment prevention objectives.[43] Examples of identity-related data program offices could potentially include in predictive risk models, but are not limited to: assessed likelihood that submitted documents are inauthentic; match of voiceprint or other biometrics to known fraudsters; or indicators of associated identity theft. A program office could also consider the significance of risk for a transaction, such as the size of the requested payment or the likelihood that the payment would be attempted to be obtained by a misrepresented identity.

If the likelihood and significance of the risk are assessed to be under a set threshold, such as the statutory threshold established in PIIA, the program office may require less-rigorous forms of controls, such as database matching.[44]

---

[42]OMB's *Requirements for Payment Integrity Improvement* defines predictive analytics as a data analytics technique used to prevent improper payments that uses predictive capabilities to identify unobserved attributes that lead to suspicion of improper payments based on known improper payments (OMB M-21-19.).

[43]GAO, Highlights of a Forum: Data Analytics to Address to Address Fraud and Improper Payments, GAO-17-339SP (Washington, D.C.: Mar. 2017).

[44]In a PIIA risk assessment, an executive agency program is considered susceptible to significant improper payments—and therefore subject to annual estimation and reporting requirements—if the total of the program's previous-year improper payments and payments whose propriety cannot be determined may have exceeded either (1) both 1.5 percent of program outlays and $10,000,000, or (2) $100,000,000 (regardless of the percentage of program outlays). 31 U.S.C. § 3352(a)(3)(A). Program offices would consider the risk of improper payments occurring due to misrepresented identity in addition to considerations for any additional improper payment risks when applying the PIIA threshold. (M-21-19).

Over this threshold, the program office may decide to subject transactions to more-rigorous controls, such as in-person verification or fingerprint scanning. As a result of applying more rigorous controls only to transactions the program office assesses to be at an elevated risk, some applicants may receive their benefits in a timelier manner, and administrators may incur lower costs, than in a uniform system.

Control systems that use predictive models are not perfect and depend on the performance of the model used. Poorly performing models may, for example, regularly identify legitimate transactions as improper or fail to identify improper payments. Predictive models are most reliable when historical data is representative of future data.[45] Further, a program office can improve its predictive models if it has access to additional sources of relevant data. However, a program office should consider not using predictive modeling if it possesses limited or unreliable data, or if transactions associated with misrepresented identities are rare. In situations where transactions associated with misrepresented identities are rare, the predictive model's risk determinations would not reliably correlate to the actual risk for each transaction.

One expert noted that database matching could also enhance transaction-level controls. For example, the Department of the Treasury's Bureau of the Fiscal Service's (Fiscal Service) Do Not Pay (DNP) business center collects data elements from a number of sources to assist participating agencies in determining an applicant's payment eligibility. Incorporating these data, which include elements such as SSNs, known aliases, and business names, may help a program office identify anomalies. The program could then use network analysis to further identify potential bad actors. For example, if DNP identifies a physical address as suspicious, a program office could in turn identify the owner and the owner's SSN as additional potential indicators of fraud. The program office would then apply additional controls to any applicant who supplies these data elements on an application.

[45]OMB's *Requirements for Payment Integrity Improvement* notes that predictive analytics is most effective if it is built after a program evolves through more standard capabilities that are also more cost-effective.

## Step 5: Design and Implement a Control Strategy to Respond to Risks

### Invest in Preventive Identity-Verification Controls

Both GAO and OMB have separately issued guidance noting that preventive controls are more effective than a "pay-and-chase" model in which an agency identifies and responds to an improper payment after it has occurred.[46] Several panelists linked this concept to the design of effective identity-verification controls. An expert noted that automated control activities (e.g., automated data-analytic techniques) tend to be more reliable as up-front controls because they are less prone to human error and are usually more efficient. A panelist also noted that if a program office decides not to invest in up-front identity-verification processes, the overall cost to the program in improper payments could be larger.[47] Additionally, the cost to investigate a fraudulent payment—to find the perpetrator and for recovery efforts—can be significant and may end unsuccessfully. In assessing costs and benefits of preventive control investments, some experts also said that program offices could consider nonfinancial benefits, including preventing harm to a program's reputation that improper payments could cause.

Further, verifying identity, not just prior to payment but at the very beginning of the application process, prior to eligibility verification, could flag misrepresented identity early in the process. This would make the identity-verification control cost effective because it preempts using additional resources to advance the application.

For example, a panelist noted that a federal benefits program in Australia moved from a process whereby it verified identity at the very end of the claim process to a process in which it verified identity at the beginning to deter improper payments. In addition, individuals provided visas to support their identities, which the program also used to determine that an applicant met residency requirements. This change was beneficial because it helped the program determine certain components of eligibility in addition to making identity determinations.

---

[46]GAO-15-593SP and OMB M-21-19.

[47]According to paymentaccuracy.gov, the federal government collectively recovers less than $0.50 of every $1.00 that is overpaid.

### Allow for Scalability and Adaptability to Changing Circumstances

Some panelists stated that it is important to consider establishing a process and control infrastructure that supports agencies' efforts to increase scalability without sacrificing their ability to verify identities. For example, a program office's system of identity-verification controls may need to adapt to a sudden and significant increase in transactions because of external factors, such as the onset of a recession. Establishing an infrastructure with the ability to select from several available controls could assist program offices in adapting to this change in a timely manner, with the objective of achieving a similar level of assurance that the program office has disbursed the benefit or payment to the correct person.

One expert noted that during the COVID-19 pandemic, state agencies received significantly more unemployment insurance (UI) claims compared with periods prior to the pandemic. For example, according to OMB, in March 2020 initial UI claims rose from 211,000 per week to 6.6 million per week.[48] Additionally, in order to timely process the increased volume of claims, program offices reduced or temporarily suspended internal controls meant to stop fraud and reduce improper payments, including verifying identity. For example, some program offices relied on applicant self-certification of employment, instead of requiring employer certification, which includes an element of identity verification in the process. In this instance, UI program offices may have benefited from a control infrastructure that would have allowed them to continue verifying identities despite the sudden increase in claims.

Explore effect of identity-verification controls

### Choose from a Range of Identity-Verification Controls

Several experts stated that agencies can leverage a growing range of technologies and tools to develop their identity-verification controls. These controls differ in the burden they place on programs, such as administrative costs, and on applicants, such as time and effort to complete and socioeconomic barriers, and in their effectiveness. One panelist also emphasized the importance of establishing metrics to evaluate the effect of controls on applicants and to make adjustments as needed.[49] See Consider

[48]Office of Management and Budget, The White House Briefing Room Blog, *Updated Data on Improper Payments* (Washington, D.C.: Dec. 30, 2021), accessed Jan. 20, 2022, https://www.whitehouse.gov/omb/briefing-room/2021/12/30/updated-data-on-improper-payments/.

[49]GAO guidance includes principles on the monitoring of internal control systems. *Standards for Internal Control in the Federal Government* states that management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. (See GAO-14-704G.)

Unintended Consequences of Disparate Impacts below for further discussion of effects of controls on socioeconomically vulnerable individuals.

- ***Digital footprint*** identifies information about an applicant's hardware and software in order to connect past and future interactions with the same individual. This control may analyze items such as an applicant's internet protocol (IP) address, time zone, language settings, etc. and would alert a program office if any of these features change. For example, if an application's IP address is based out of another country, a program office may assess the transaction at a higher risk and require more stringent controls.[50] Or, a program office reviews the applicant's keystroke and/or mouse patterns to determine if the behavior suggests the application was completed by a bot.[51] A program office may rely on a third-party provider for this control or conduct this control on its own. While the control is not generally rigorous, it may not be ideal for those applicants who lack access to a personal electronic device as these individuals may use public devices with inconsistent settings.
- ***Bank account verification*** compares banking information (e.g., account number, name, address, etc.) with information the applicant supplied. A program office may perform this on its own or rely on a third-party provider. Banking information is an example of something that an applicant has. Reliance on this control depends on establishing access to a third-party data source. Alternatively, or in combination with verification through a data source, the program office can initiate micro-deposits, which are transactions under $1.00, and ask the applicant to verify these amounts to establish ownership of the bank account. Particularly when combined with verification through a data source, micro-deposits can help verify an applicant's identity. Verification through a data source can establish that an applicant owns a particular known bank account, and verified micro-deposits can establish that the applicant controls that bank account. This control may impose a burden on those applicants who do not have bank accounts, and one panelist noted that individuals may be

[50] Individuals may have legitimate reasons for masking their IP addresses. The program office would need to determine if a transaction's unexpected IP address is indicative of a higher risk level.

[51] A program office may need to provide a disclaimer to individuals that their interactions with the application or payment system are being monitored.

reluctant to share their bank account information with the federal government.

- ***Physical address verification*** confirms an individual's identity by mailing information, such as a personal identification number, to the individual's physical address. A program office is likely to perform this control rather than rely on a credential service provider (CSP). Some applicants may find this control to be burdensome because it may take several days for the information to arrive. Those who lack physical addresses or who reside at addresses different from their mailing addresses may not be able to receive the information.
- ***Email or phone verification*** confirms an individual's identity by sending information, such as a personal identification number, to the individual's email address or to their phone via a phone call or text message. A program office or a CSP may perform this control. Those who lack access to a phone or email address may not be able to receive this information.
- ***Physical biometrics*** verify an applicant based on biological characteristics, such as their fingerprint or face.[52] These characteristics can be collected in person or remotely. A program office can either implement this control on its own or rely on a third party for implementation. These controls are an example of something that an applicant is. For example, a program office may remotely compare an individual's photo on a driver's license against an uploaded photo of the individual. Or, a program office may require an applicant to appear in person to submit a fingerprint scan to be compared against a database.
- ***Applicant notification*** refers to a program office notifying an individual when an application has been submitted using their identity. Such a notification may inform an individual that their identity has been used and enable them to determine if the use was legitimate. Notification can occur through one or more of a variety of methods, such as physical mail, email, or text. A program office would likely conduct this control itself.

Once a program office has verified identity, multifactor authentication should be used to authenticate that an individual logging into an account is the same

[52] There are many considerations to take into account when considering the use of biometrics, including but not limited to exchanging biometric data across systems. See *Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information* standard (ANSI/NIST-ITL-1 2011 Update: 2015, NIST SP 500-290e3).

individual who the program office previously verified.[53] Multifactor authentication requires a user to present two or more authentication factors (something an individual knows, has, and is) when logging into account. Examples of these factors include a password or personal identification number, a chip-based smart card, and a fingerprint.[54]

### Determine Whether to Design and Implement Remote or In-Person Controls

Program offices should determine whether the design and implementation of controls should be remote or in-person.

***Remote verification*** allows an agency to verify an individual without physical access to a person or an item.[55] A program office may conduct remote verification directly or rely on a third-party service, such as a CSP. Remote verification of a person (e.g., facial scan, or something a person is) or a document (e.g., driver's license, or something a person has) can occur. Remote verification can occur through various media, such as through the use of digital footprint monitoring, biometrics, bank-account verification, and physical-mail verification.

Remote verification offers applicants and agencies a relatively convenient solution, but the technology to circumvent these controls is constantly adapting. For example, in the event of verification by streaming video, some providers have implemented liveness detection to determine that an applicant is physically present rather than an inanimate artifact or injected data in order to combat attempts at impersonation of a person. A panelist noted that investing in an automated, remote identity-verification infrastructure may reduce costs by requiring less manual effort in the process and increase customer satisfaction, through the convenience of applying from home.

***In-person verification*** requires an applicant to physically visit a location to verify identity. A program office may conduct this service on its own, or it may rely on a third party for this service. Once an applicant arrives at a location, a

---

[53]NIST requires federated identity systems, when a credential service provider provides authentication, to use strong multifactor authentication (NIST SP 800-63-3 and NIST SP-800-63C).

[54]OMB notes that in order to equitably balance security and usability, program offices should provide authentication options to applicants that limit collection of unnecessary information, such as the make or model of user-supplied authenticators (OMB M-22-09).

[55]According to NIST's *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements,* in order to perform remote verification, agencies shall meet identity assurance level 2. NIST further details the verification methods necessary to achieve that assurance level (NIST SP 800-63A).

verifier may analyze the applicant's identity documents, gather the applicant's biometric data, or perform both practices. In-person verification is more costly than remote verification but may be necessary to provide a channel for those who are unable to verify their identities remotely. In addition, this method of identity proofing is generally considered to be a strong approach because it allows for direct physical comparison of an individual's documentation to the individual attempting to enroll.

### Consider Whether to Use a Credential Service Provider

A program office should consider whether operating the system of internal controls in-house or partnering with another entity that specializes in performing identity-verification controls, such as a CSP, will enable it to most efficiently and effectively achieve its objectives. Leveraging a CSP that already has the infrastructure in place to provide control services may be more efficient for a program office than if it were to design and implement these capabilities on its own.

Further, if choosing to use another entity to operate the controls, a program office can either contract with a private entity or use a shared service within the federal government. A number of federal agencies have contracted with entities to offer individuals the ability to use a CSP to manage their identity credentials. For example, the Internal Revenue Service contracts with a private company to manage users' credentials. A shared-services model, in which one entity offers tools to other agencies, may be another efficient way to conduct these control activities. For instance, the Social Security Administration (SSA) provides login.gov, which the General Services Administration operates, as an option for individuals to choose to manage their credentials.

## Share Data to Strengthen Responses to Risks

Share data to facilitate risk analysis and response

Where permitted and appropriately authorized, federal program offices can consider making use of data sharing among their offices, with states, and with the private sector to improve identity verification by providing more complete applicant data. Program offices can use these data to improve existing controls by overcoming potentially incomplete or missing information, as well as to develop new controls that can identify risks that may not have been otherwise evident without the additional shared data. Both GAO and OMB guidance separately discuss data-sharing activities for program offices.[56] Potentially

[56] An agency must communicate externally to gather information necessary to achieve objectives, which may include establishing regular reporting lines for information related to internal control risks (GAO-14-704G). An agency can

valuable information exists across sectors—in the federal government, state governments, and the private sector. Program offices may consider leveraging these sources of information in order to achieve their internal control objectives. A program office may also leverage information hubs to augment data-sharing capabilities.

## Share Data to Facilitate Identity Verification and Improve Controls

Several experts noted that data sharing allows data matching with multiple authoritative data sources.[57] An authoritative source has access to information from an issuing source, so that relying parties such as agencies can validate evidence that an applicant provides. A program office may be more successful in verifying applicant identities if it uses multiple sources because data from the sources are often complementary and provide additional context for verification. Alternatively, if a program office instead relies on a single authoritative source, it may not be able to verify an applicant's identity because the entirety of an applicant's relevant data may not be present in that single source. While using data from multiple sources is important, one panelist emphasized that each specific data element should have only a single authoritative source. For example, if a program office sought to verify an SSN, it would identify SSA as the sole authoritative source for this information despite the availability of other sources that may collect SSNs.

Several panelists noted that data sharing among government agencies and the private sector could increase the effectiveness of identity verification and reduce the likelihood of improper payments. One panelist stated that data sharing can help agencies design and implement controls to respond to identified risks. Both GAO and OMB guidance separately discuss using data matching in control activities.[58] Specifically, an applicant's interactions with

---

pursue access to necessary external data, including pursuing data-sharing agreements (GAO-15-593SP). Further, agencies may enter into data-matching agreements with other agencies to detect and prevent improper payments (OMB M-21-19).

[57] Authoritative sources exist at the federal and state levels as well as in the private sector. Federal data sources hold citizen information for the purpose of either receiving an entitlement or issuing a credential. An example of a federal authoritative source is SSA for verifying SSNs. A state data source also holds citizen information for the purpose of either receiving an entitlement or issuing a credential. For example, each state's Department of Motor Vehicles is an authoritative data source and its data, such as address information, can be used to verify an applicant's identity. A private data source could be the finance industry, which includes banks and credit bureaus. A bank's records could help verify the employment of individuals who are applying for UI benefits.

[58] The Fraud Risk Framework discusses leading practices in designing and implementing control activities, such as conducting data matching to verify key information and conducting data mining to identify suspicious activity or transactions, including anomalies, outliers, and other red flags in the data (GAO-15-593SP). OMB Circular A-123 discusses data matching to detect and prevent improper payments (OMB M-21-19).

trusted partners could be used for knowledge-based verification—asking questions that only the applicant would likely be able to answer. For example, if a program had access to tax records, a program could ask applicants for their adjusted gross income to verify the applicants' identities because only each applicant would likely have access to the requested information. Through data sharing and developing an identity-verification control, a program office could verify the requested information with the partner organization, thus reducing the likelihood of identity misrepresentation.

Some panelists noted that data sharing can facilitate risk modeling, as more data can provide more accurate analytics. Information from telecommunications firms can help verify an applicant's identity, as some actions, such as swapping subscriber identification module cards or porting phone numbers, as one panelist noted, may indicate attempted fraudulent activity.[59] Another expert noted that an agency can review fraud patterns and then consider how to leverage industry's technology for fraud detection to further identify potential cases. Additionally, the agency can analyze information, such as whether the IP address or device ID that the applicant is using are suspicious, to build risk models that identify transactions requiring additional authentication.

For a number of years, GAO and OMB have encouraged federal agencies to share data with each other to identify and prevent fraud as well as other outcomes. For example, GAO reported that enhanced data sharing could improve program integrity and found that an agency could make more accurate and timely decisions for verification purposes if it was able to confirm applicant information with data in an authoritative source.[60] GAO further reported that several officials from benefit programs mentioned access to information in other databases would greatly aid in the administration of their programs.[61] Specifically, access to information in other databases could help improve the payment accuracy if the program office is able to verify identity and prevent improper payments before they occur.

To initially encourage data sharing, OMB required agencies to develop working relationships with other organizations to share information and encouraged

---

[59]Porting phone numbers is the process of keeping an existing phone number when switching service providers. This can be done between wireline, IP, and wireless providers.

[60]GAO, *Benefit and Loan Programs: Improved Data Sharing Could Enhance Program Integrity*, GAO/HEHS-00-119 (Washington, D.C.: Sept. 13, 2000).

[61]GAO, *The Challenge of Data Sharing: Results of a GAO-Sponsored Symposium on Benefit and Loan Programs*, GAO-01-67 (Washington, D.C.: Oct. 20, 2000).

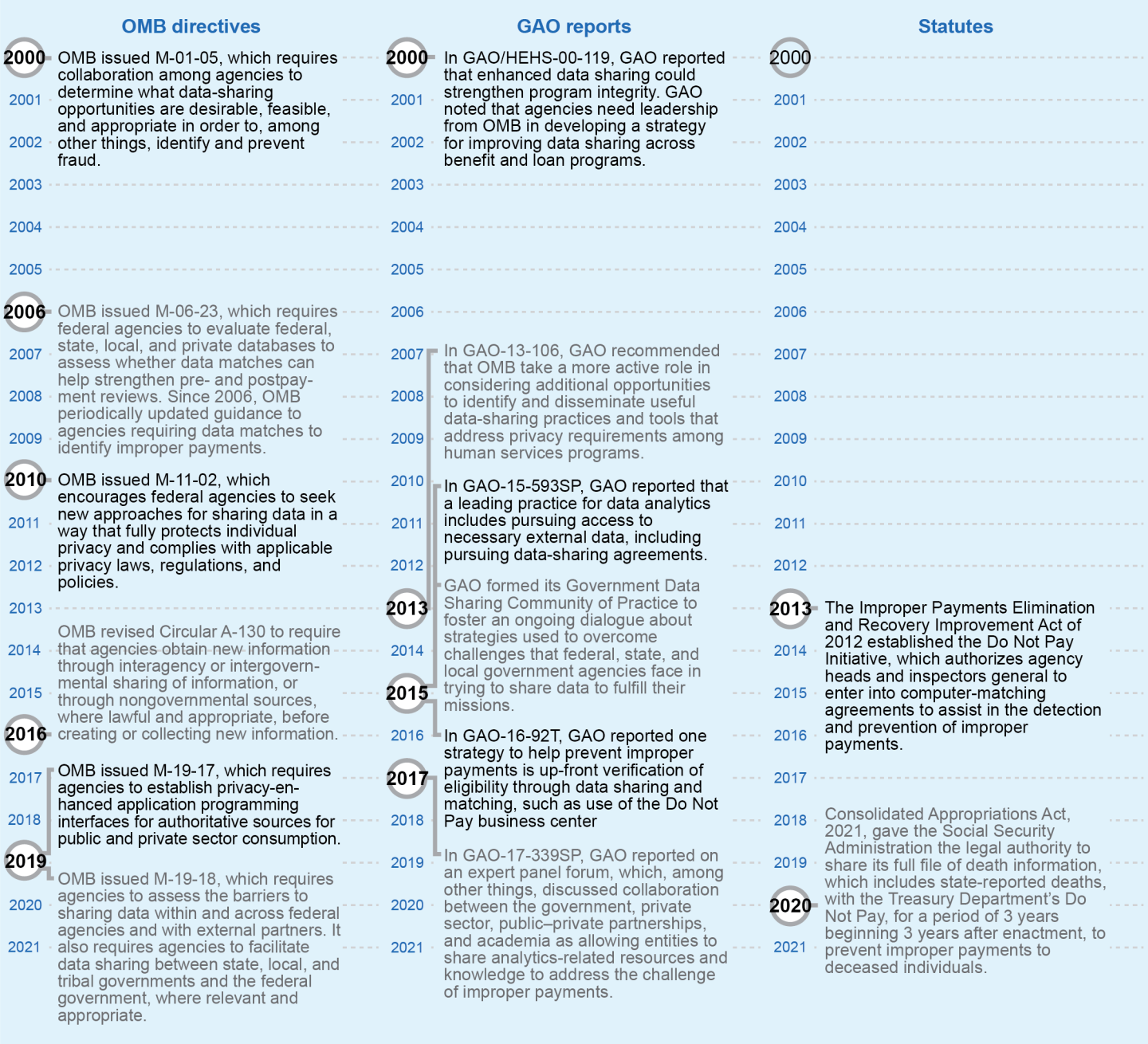
data matching with federal, state, and local databases to identify improper payments.[62] Currently, OMB requires agencies to thoroughly review available databases with relevant information to prevent improper payments and also encourages cross-entity sharing to mitigate improper payments.[63] Further, the Consolidated Appropriations Act, 2021, requires SSA to eventually share, to the extent feasible, its full file of death information with Fiscal Service's DNP to prevent improper payments to deceased individuals.[64] Allowing SSA to share information about deaths can enable programs to verify the applicants' identities and can help ensure that government benefits are not being provided to those using deceased individuals' identities. Figure 3 presents examples of OMB directives, GAO reports, and statutes related to data sharing.

[62]OMB M-06-23, *Issuance of Appendix C to OMB Circular A-123*, required federal agencies to evaluate federal, state, local, and private databases to assess whether data matches can help strengthen pre- and postpayment reviews. Since its issuance, OMB has periodically updated the guidance to include additional requirements related to improper payment prevention and reporting.

[63]OMB M-21-19.

[64]Consolidated Appropriations Act, 2021, Pub. L. No. 116-260. § 801, 134 Stat. 1182, 3201 (Dec. 27, 2020), amending 42 U.S.C. § 405(r). This provision will take effect 3 years after enactment and will be effective for a 3-year period.

Figure 3: OMB Directives, GAO Reports, and Statutes Related to Data Sharing




Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Program (JFMIP).

Efforts to use private sector data could also facilitate federal agencies' ability to verify identities. SSA's Electronic Consent Based Social Security Number Verification (eCBSV) is an example of cooperation between federal and private sector entities. eCBSV allows the private sector to use information held by the federal government. One panelist noted that in accordance with OMB M-19-17, similar data sources—such as the United States Citizenship and

Immigration Services' immigration numbers—could be made widely available to help improve identity verification.[65]

Several experts noted that a similar arrangement in which the federal government is able to use information held by the private sector, such as banking or telecom data, could help federal agencies more effectively and efficiently verify identities. One panelist emphasized that if using data from the private sector, program offices would still need to assess the accuracy of that information. The panelists did not elaborate on specific aspects of the public/private arrangements, such as possible contractual mechanisms or the responsibilities the government should require of a private sector contractor, including liability considerations.

## Consider Sharing Data across Sectors

Information that could facilitate identity verification controls exists across sectors. Several of the experts provided examples of data sources that could be shared among federal, state, and local government agencies, and with the private sector. These sources include, but are not limited to, databases in Fiscal Service's DNP business center, the finance and telecommunications industries, payroll processors, and other commercial data sources.

One expert mentioned that federal and state partnerships enable a government agency to verify vital records data from state and jurisdictional levels. For example, Fiscal Service has conducted a pilot with the National Association for Public Health Statistics and Information System's Electronic Verification of Vital Events Fact of Death, which gives it access to state and jurisdiction vital records data from a hub and at scale. One expert noted that an organization's use of an information hub could increase the efficiency of identity verification, as the information hub could provide data-matching and predictive-modeling services.[66] Similar to how airlines use hubs to efficiently route passengers to various destinations, using an information hub for data-matching and predictive-modeling services could allow a program office to obtain verified information while maintaining its focus on conducting its primary mission. See Establish Information Hubs to Facilitate Data Sharing and Analytics below for further discussion on how information hubs can be used.

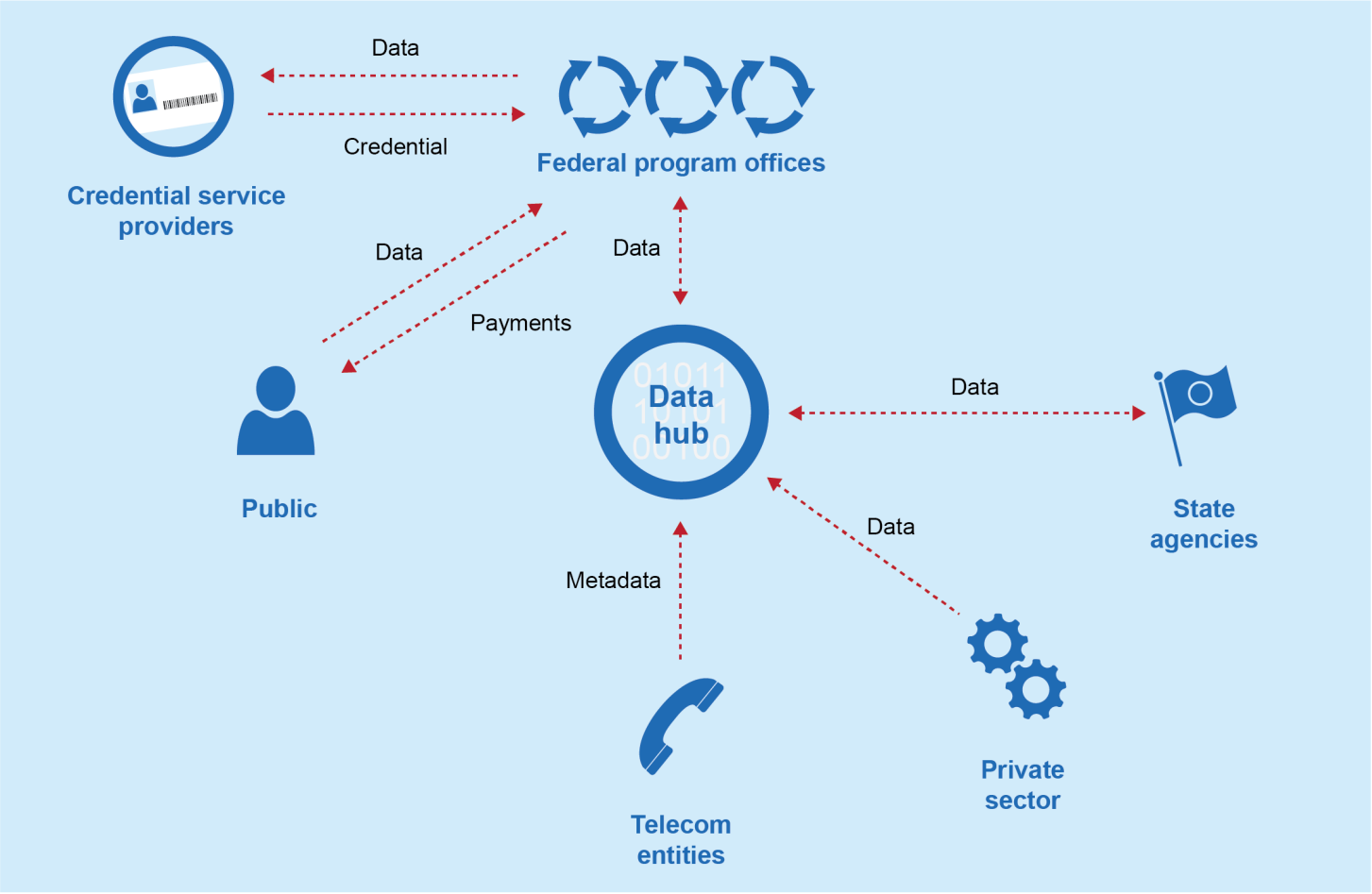
---

[65]OMB, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, Memorandum No. M-19-17 (May 21, 2019).

[66]Data matching is a process in which information is compared between sources to identify inconsistencies.

Similarly, the government could consider leveraging the financial industry's established processes and the compiled data that it uses to verify identities. One panelist noted that the industry spends $9 billion each year on identity verification. Another expert further noted that such a reliance would need to address shared liability concerns over the use of private sector data. Figure 4 below illustrates how federal program offices could use an information hub to aggregate and share data from multiple sources and sectors.

Figure 4: Potential Model for Data Sharing among Federal, State, and Private Entities




Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Program (JFMIP).

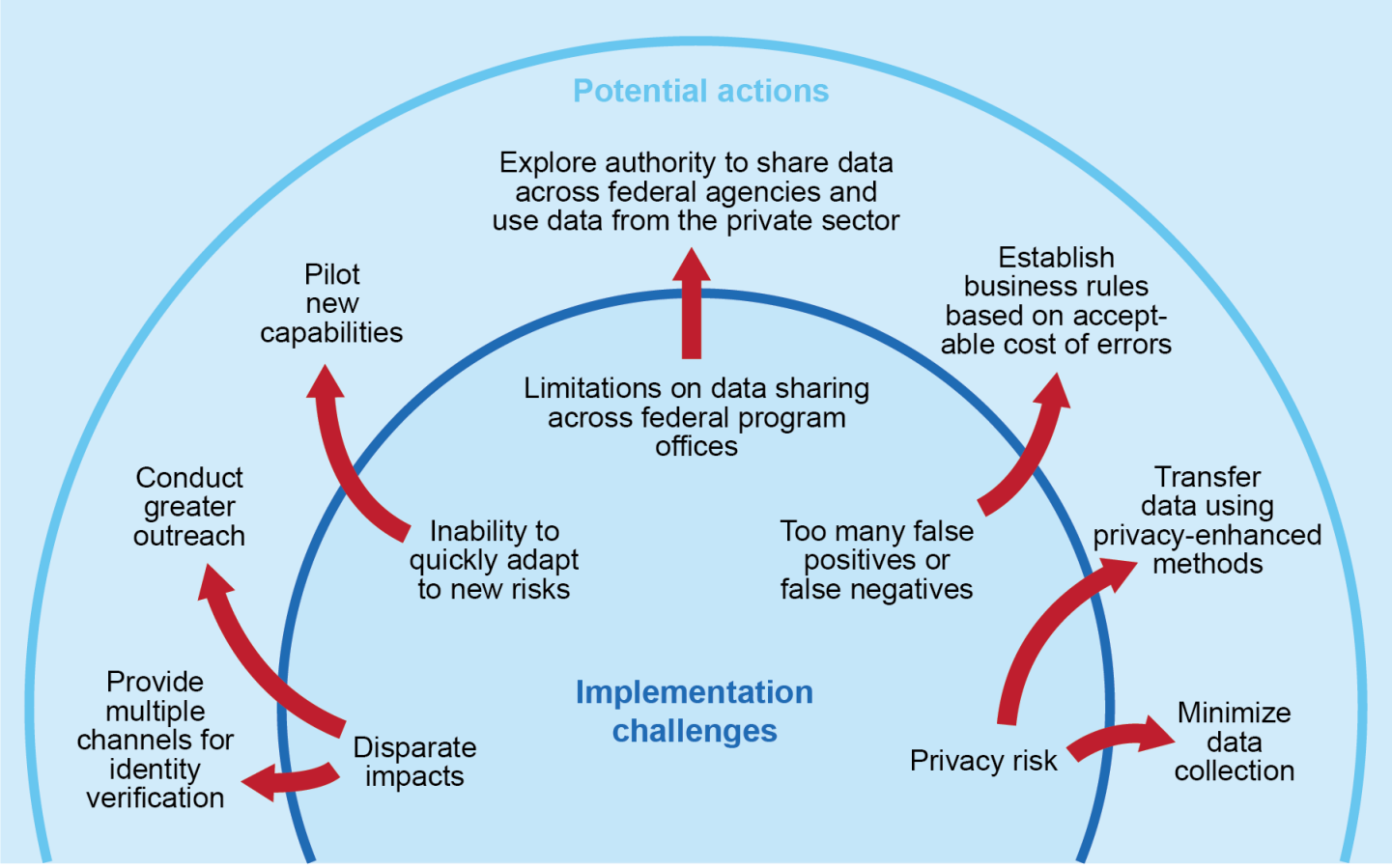
## Actions to Address Implementation Challenges and Unintended Consequences

Implementing identity-verification processes includes challenges at the program office and government-wide level. The panelists identified the following as challenges to implementing identity-verification controls: (1) data-sharing authority, (2) privacy preservation, (3) disparate impacts, (4) management of error in identity-verification controls, and (5) quickly responding to new risks. The panelists discussed the following solutions to these implementation challenges.

- To address data-sharing authority, program offices could explore options generally available to federal agencies as well as those uniquely available to their programs, including using data from the private sector.
- To improve privacy preservation, program offices could minimize data collection, storing only essential information, and store and transfer data using privacy-enhanced methods.
- To address potential unintended consequences of disparate impacts, program offices could conduct greater outreach to socioeconomically vulnerable individuals and offer them multiple avenues to verify their identities in order to overcome technological and other barriers they face when attempting to verify identity.
- To manage the risk of errors in identity verification controls, program offices could explicitly determine the cost of false positives and false negatives and establish business rules for making payments or conducting further manual review based on these costs.
- To address implementation delays and more quickly adapt to new risk, program offices could consider piloting capabilities before expanding them to the entire program.

Figure 5 summarizes these implementation challenges and corresponding potential actions.

Figure 5: Summary of Implementation Challenges and Potential Actions




Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Program (JFMIP).

## Explore Authority within the Executive Branch to Share Data

The obligation to control and protect an agency's data can limit the ability and willingness to share information across the federal government, and several panelists indicated that legal requirements may limit or explicitly prohibit government agencies from sharing data with each other. However, program offices may be able to identify authorities under which data sharing is permissible for the purpose of enhancing identity-verification controls. Two examples of potentially relevant authorities that generally apply to federal agencies follow:

- Data sharing between federal agencies may be allowed if it is for a purpose that is compatible with the purpose for which the data were collected, referred to as routine use.[67]
- Subject to legal requirements,[68] agencies sometimes use computer matching to help ensure that federal benefits are distributed appropriately.[69]

In addition to laws that govern all federal agencies, several panelists stated that some agencies may be governed by laws that are specific to that agency or the kind of data the agency handles. Program offices can explore whether applicable authorities exist for their agency. For example, some experts noted that section 6103 of the Internal Revenue Code prevents the Internal Revenue Service from sharing tax return information.[70] While section 6103 prohibits federal or state officers and employees, among others, from disclosing any tax return or return information, it does include specific exceptions to that prohibition. For example, Internal Revenue Code section 6103(l)(7)(D)(ix) allows the Social Security Administration (SSA) to disclose to the Department of Housing and Urban Development (HUD) certain personal information to verify applicants' information. However, only HUD officers or employees may use the information; HUD cannot further disclose the data to, for example, local housing-authority administrators who need to verify an applicant's information, such as identity.

---

[67]The Privacy Act of 1974 (Privacy Act) governs federal agency collection or use of personal information and limits agencies' collection, disclosure, and use of personal information maintained in systems of records. The Privacy Act generally prevents agencies from sharing personal information in systems of records except pursuant to a written request by, or with prior written consent of, the affected individual. However, the Privacy Act defines a number of specific conditions under which federal agencies may share information from systems of records with other government agencies without the affected individual's consent, including routine use as described above. 5 U.S.C. § 552a.

[68]The Computer Matching and Privacy Protection Act amendments of 1988 and 1990 (CMPPA) amended the Privacy Act and permits federal agencies to conduct matches with one another to establish or verify personal information. However, CMPPA requires the agencies to enter into a matching agreement, and the initial matching agreement is limited to 18 months, which may be followed by a 12-month renewal period. CMPPA requires agencies to meet requirements to ensure procedural uniformity. The matching agreement must include the purpose and legal authority for a match, anticipated results, a cost-benefit analysis, procedures to notify applicants and recipients who are identified in a match, and procedures for verifying the information to be produced. 5 U.S.C. § 552a(o).

[69]Computer matching is a term commonly used to refer to the computerized comparison of information, generally including personally identifiable information, in two or more information systems.

[70]26 U.S.C. § 6103.

See Share Data to Facilitate Identity Verification and Improve Controls for a summary of Office of Management and Budget (OMB) directives, Government Accountability Office (GAO) reports, and statutes relevant to data sharing.

## Manage Data Collection and Storage Policies to Reduce Privacy Risk


Explore effect of data security on database intrusions

Data sharing can help to strengthen identity-verification controls. However, when agencies store and share data, the public deserves confidence that the government safeguards their sensitive information as necessary using applicable privacy and security requirements. Storing and transferring data pose inherent privacy risks to the information owner, including those from unauthorized database intrusions or improper use by agency officials.

Several panelists stated that one risk individuals face is that of their sensitive information being wrongfully disclosed or misused. As the number of agencies and individuals that have access to sensitive information increases, so do the chances of wrongful disclosure and misuse of that information. GAO reported that the federal government and private sector have struggled to protect privacy and sensitive data.[71] Advances in technology have made it easy to correlate information about individuals, and internet connectivity has facilitated sophisticated tracking of individuals and their activities.

The vast number of individuals affected by various data breaches has underscored concerns that sensitive information is not adequately being protected. This sensitive information can include Social Security numbers (SSN), or financial information, such as bank account numbers. For example, SSA has reported that fraudsters have used beneficiaries' sensitive information to illegally redirect direct-deposit benefits.

The experts discussed considerations to reduce privacy risks, such as minimizing data collection, storing only essential information, and sharing data using privacy-enhanced methods.

### Minimize Data Collection for Identity-Verification Controls

Some panelists noted that program offices may consider steps to eliminate unnecessary collection of identifying attributes. Program offices can accomplish this by minimizing collected data and ensuring secure storage. OMB Circular A-130 states that agencies should only create, collect, use, process, store,

[71]GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

maintain, disseminate, or disclose personally identifiable information (PII) that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.[72]

Several panelists suggested that program offices consider creating identity-verification controls that collect the minimum amount of data necessary for controls because aggregating large amounts of data may attract malicious actors. One expert noted that rather than requesting the data specifically, program offices could use a binary, or yes/no, response. For example, if an agency requests verification of an applicant's age, the second agency can respond with "yes/no" rather than providing the full birthday. Providing binary responses limits the sharing of the data, thereby lowering the risk of wrongful disclosure or misuse.[73]

One expert stated that SSA's Electronic Consent Based Social Security Number Verification (eCBSV) is another example of successful privacy-preserving data sharing between the federal government and the private sector. eCBSV allows permitted entities to verify if an individual's SSN, name, and date of birth combination matches Social Security records.[74] SSA returns a binary response—"yes" or "no"—rather than sharing the data specifically.

## Safeguard Sensitive Information for Identity-Verification Controls

One panelist highlighted the importance of establishing and consistently implementing data-protection standards to safeguard and maintain sensitive information. The E-Government Act of 2002 requires federal agencies to conduct privacy impact assessments of privacy risks associated with information technology used to process personal information. Similarly, OMB

[72]OMB Circular No A-130, *Managing Information as a Strategic Resource*, (Washington, D.C.: July 28, 2016).

[73]One panelist also discussed the importance of allowing for close, or "fuzzy," matches when providing binary responses to avoid unnecessary rejections. According to National Institute of Standards and Technology's (NIST) *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*, agencies may employ appropriate matching algorithms to account for differences in personal information because exact matches of information can be difficult to achieve (NIST SP 800-63A).

[74]Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act, directed SSA to modify or develop a database for accepting and comparing permitted entities' electronically provided fraud protection data. SSA created eCBSV, a fee-based SSN verification service, in response to this statutory directive. Enrolled permitted entities include financial institutions and service providers, subsidiaries, affiliates, agents, subcontractors, and assignees of financial institutions.

specified actions that agencies should take to prevent data breaches, such as using encryption to protect PII.[75]

For program offices to achieve a certain level of identity assurance, the public has to provide some identity attributes as part of the verification process. An important consideration regarding sharing personal information among government programs is whether it can be done without sacrificing an individual's right to privacy.

NIST SP 800-53 provides guidelines for selecting and specifying security controls for information systems.[76] The General Services Administration built a number of Application Programming Interfaces (API), covering a range of important data and functionalities, to facilitate data sharing between authoritative federal sources while minimizing privacy risk. An API sets up machine-to-machine communication, which can allow users to obtain real-time data updates. APIs also make consumer-permission data sharing easier, more accurate, and more secure, as they provide the rules for how to request data and exactly what data will be returned. With the use of an API, an organization can allow a customer to better define and manage the data that the customer wants to share with a data aggregator and limit access to unnecessary sensitive customer data. However, APIs only minimize risk during the data-sharing process and do not reduce privacy risks that data pose before or after they are shared between sources.

According to the Department of Health and Human Services, when implementing an API, the following are key areas for program offices to consider:[77]

- Ensure that any electronic access request interface provides individuals with an opportunity to approve the electronic transmission of personal information.

---

[75]Office of Management and Budget, *Safeguarding Personally Identifiable Information*, OMB Memorandum M-06-15 (Washington, D.C.: May 22, 2006), and *Protection of Sensitive Agency Information*, OMB Memorandum M-06-16 (Washington, D.C.: June 23, 2006).

[76]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 (Sept. 23, 2020).

[77]Department of Health and Human Services, *Key Privacy and Security Considerations for Healthcare Application Programming Interfaces* (Dec. 2017), accessed Jan. 20, 2022, www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents//privacy-security-api.pdf.

- Enable technology to provide for and respect individuals' choices and preferences about the specific types of information shared with the third party.
- Provide methods for individuals to revoke permissions for sharing information in a clear and accessible manner.

## Consider Unintended Consequences of Disparate Impacts


Explore effect of controls on socioeconomically vulnerable individuals

Identity-verification controls require certain data elements or documentation in order to verify an individual's identity. As it relates to the decision to implement in-person or remote identity-verification controls, program offices should consider certain segments of the population. For example, certain segments of the population may face an increased burden when verifying their identities because either these individuals may not have the required data elements or documentation or they may not have the means to supply the required information.

Elements of identity include something an individual has, something an individual knows, and something an individual is. Individuals who are more socioeconomically vulnerable, such as individuals with lower incomes or who are homeless, may face difficulties in providing evidence for some or all of the elements of identity. For example, as it relates to something an individual has, some panelists noted that those who are homeless may lack driver's licenses or physical identification because their states' motor vehicle agencies require a physical address in order to issue a driver's license. In this case, a verification process that relies solely on individuals' ability to provide evidence of something they have could be problematic.

As it relates to something an individual is, some identity-verification methods capture biometric data, such as a fingerprint, to authenticate identity. Socioeconomically vulnerable individuals may lack transportation, or the ability to take time off from their jobs, to complete steps necessary for in-person verification. Additionally, they may lack the technology, such as a smartphone or access to the internet, to complete remote verification. In this case, a verification process that relies only on individuals' ability to provide evidence of something they are could be problematic.

These individuals may not be served by the programs because they are unable to supply the required information to verify their identities. In turn, the programs may be unable to fully achieve their goals of providing payments, services, or benefits to the intended populations. Thus, some panelists noted

the importance of offering applicants multiple channels for verifying their identities, such as in person and remote, in order to overcome the variety of obstacles these individuals may face. They further suggested that partnering with agencies that may have a larger physical footprint, such as the United States Postal Service, could magnify a program office's outreach. One expert noted that programs could also consider a trusted referee process, which allows others to act on behalf of or vouch for applicants during the verification process.[78] By providing multiple channels for verifying identity, program offices can attempt to meet the needs of the public, as applicants can select the least burdensome options for their unique circumstances.

Additionally, GAO has reported that programs can conduct greater outreach to socioeconomically vulnerable communities as a solution to accessing government services.[79] Regarding identity verification, if a program office determines that a certain channel for verifying identity is underutilized, it may consider reaching out to the segment of the population that may benefit most from the given channel. For instance, a program office could communicate the locations that provide in-person verification that better fits the needs of the socioeconomically vulnerable communities.

Some panelists emphasized the importance of establishing metrics to evaluate the effect of these efforts on various populations, including socioeconomically vulnerable individuals, and adjusting controls if they do not perform equitably across the various populations. GAO guidance similarly includes principles regarding the evaluation of internal control systems.[80] For example, an expert noted that some program offices previously chose not to implement a control that matched an applicant's facial features against government-issued documents because of equity concerns.

## Establish Business Rules to Account for False Positives and False Negatives

Several panelists noted that implementing identity-verification controls can result in false positives and false negatives, which could create a burden on

[78]In certain circumstances NIST's *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements* allows CSPs to use trusted referees, such as notaries, legal guardians, medical professionals, or persons with power of attorney, that can vouch for or act on behalf of the applicant in accordance with applicable laws, regulations, or agency policy, when applicants cannot use normal verification processes (NIST SP 800-63A).

[79]GAO, *Homelessness: Barriers to Using Mainstream Programs*, GAO/RCED-00-184 (Washington, D.C.: July 6, 2000).

[80]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014), states that management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

both the program office and the applicants. In the context of detecting misrepresented identities, a "false positive" is incorrectly determining that a transaction is associated with a misrepresented identity, when in reality, an applicant has not misrepresented identity. For example, a control might fail to recognize a match between an applicant's current appearance and an older driver's license photo on file and incorrectly determine that the applicant is not who the applicant claims to be. A "false negative" is incorrectly determining that a transaction is not associated with a misrepresented identity, when in reality, the applicant has misrepresented identity. For example, identity thieves might alter their appearances digitally with a video filter so that they resemble their victims; controls might fail to detect such alteration.

According to NIST, organizations that implement identity proofing generally seek to balance cost, convenience, and security for both the provider and the individual, which may include assessing the trade-off between false positives and false negatives. NIST also explains that, taking steps to reduce false negatives in identity verification can result in increased risk of false positives and user abandonment.[81] For example, an applicant may become discouraged if a program office incorrectly flags the transaction as high risk and imposes additional controls, such as requesting that the applicant visit an office for in-person verification. On the other hand, according to NIST, reducing the burden of identity verification to improve the applicant's experience can result in an increased risk of false negatives.[82] A false negative may result in an improper payment.

The costs of false negatives and false positives will vary by program and context. If possible, program offices can explicitly determine the cost of false positives and false negatives and make this trade-off for their programs. Program offices can decide on a threshold based on their tolerance for false negatives and their willingness to commit resources, such as the staffing resources needed to sift through a large amount of false positive results to prevent an improper payment.

For example, in a low-risk scenario, such as automatic identification of an individual's image taken for admission to the commissary, a mismatch may only result in an unauthorized person shopping in the store. Therefore, the commissary may not want to commit resources, such as staff time, to scrutinize

[81]National Institute of Standards and Technology, *Measuring Strength of Identity Proofing* (Dec. 16, 2015), accessed Jan. 24, 2022, https://www.nist.gov/document/nstic-strength-identity-proofing-discussion-draftpdf.

[82]National Institute of Standards and Technology, *Measuring Strength of Identity Proofing*.

every shopper rigorously. On the other hand, in a high-risk scenario, such as identification of individuals applying for large federal grants for energy research, a program office may likely determine that preventing improper grant payments is much more important than the cost to some legitimate applicants of additional up-front scrutiny.

One panelist suggested that program offices establish business rules to manage positive and negative models and control results to mitigate the risk of false positives and false negatives. Another panelist further noted that more complex algorithms may better account for potentially conflicting signals presented by various controls. For example, additional controls or manual inspections of positive results may reduce the impact of false positives on program outcomes. More rigorous but reliable controls may be appropriate for managing initial positive results. For example, for all instances of misrepresented identity, an agency could offer in-person verification to applicants with suspected misrepresented identities—at the cost of travel time for the applicants and administrative time for the agency. Alternatively, program offices could require in-person verification for only a subset of transactions with misrepresented identity, based on each transaction's risk level, in order to reduce this burden while still trying to achieve greater program integrity.

## Pilot Capabilities to More Quickly Adapt to New Risks

Innovative control systems can be challenging to implement. Specifically, a panelist noted that the federal government sometimes tests capabilities to a level that hinders innovation, such as when a program office does not implement a new process until it is deemed "perfect."

To combat this problem, some experts suggested that program offices could consider pilot testing to launch new capabilities more quickly to address timeliness challenges in implementing new and innovative control systems. A pilot project is an initial small-scale implementation that is used to prove the viability of a project idea. Reviewing the results of pilot testing a program could uncover potential unintended consequences of the new capabilities.

For example, an agency considering a partnership with the United States Postal Service to verify applicants' mailing addresses may wish to first test this capability in selected communities to determine its success before deploying it nationwide. Following the pilot, the agency may realize that the partnership was not useful in helping individuals who are homeless apply for benefits. In this example, piloting this capability on a selected basis allows the agency to refine

the process based on its analysis before fully deploying the capability to the entire program.

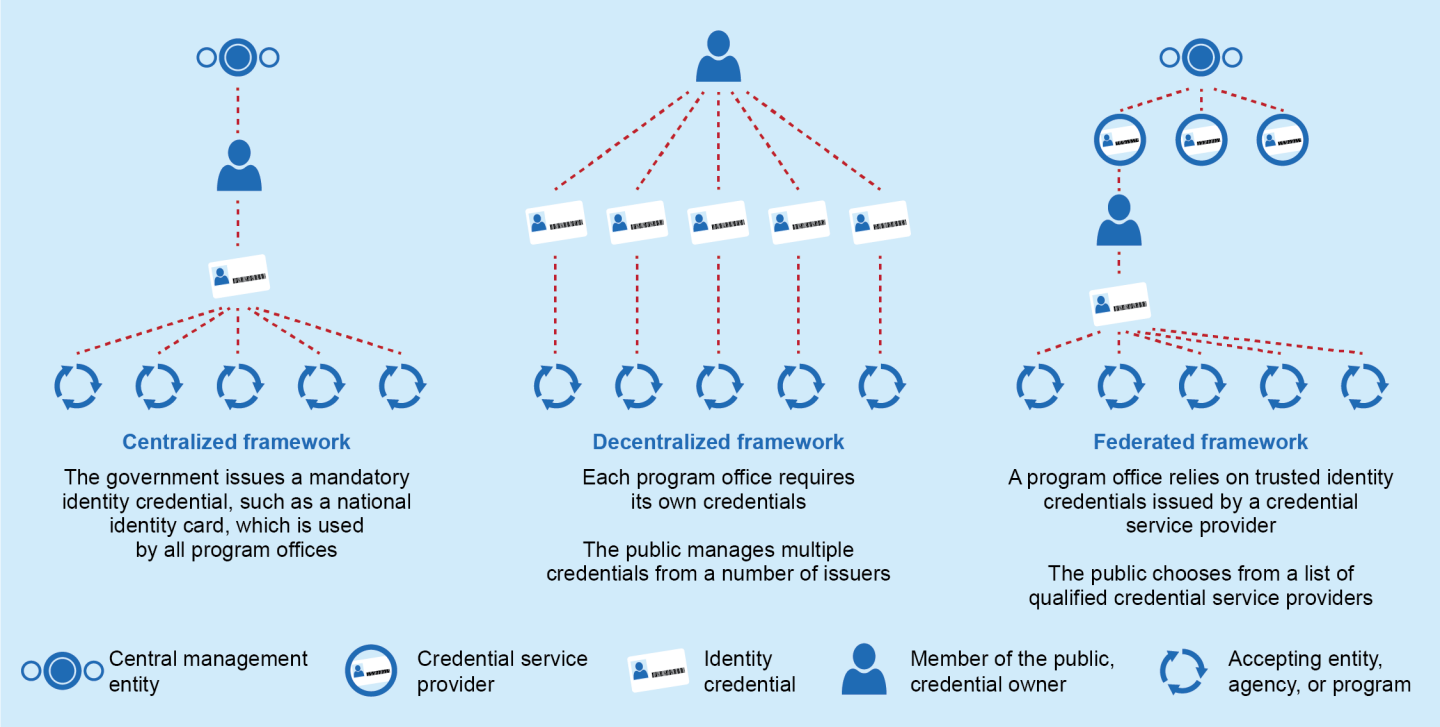
## Consider Offering a Choice of Credential Service Providers for Identity Verification

Identity verification is complicated given the diversity of technologies and processes involved for individuals to verify their identities. The Identity, Credential, and Access Management (ICAM) is a framework of tools, policies, and systems to provide an overarching structure to the verification process and that an entity can use to enable the right individual to access the right authentication resources, at the right time, for the right reasons, in support of specific programmatic objectives. In the federal government, ICAM would govern the role of identity credentials and shapes the environment in which identity-verification controls and processes exist. For instance, the type of framework the government adopts may determine whether program offices may delegate identity-verification services to credential service providers (CSP), if the public may use a single credential to interact with multiple program offices, and whether a central management entity has a role in coordinating and overseeing the implementation of the framework.[83]

The panel discussed three models for an implementation of ICAM: centralized, decentralized, and federated. Figure 6 illustrates the three conceptual identity-verification frameworks. In a *centralized framework*, the central management entity issues a mandatory identity credential that all program offices must accept. At the other end of the spectrum, in a *decentralized framework*, each program office may require its own identity credentials. In the middle of the spectrum is a *federated framework*, in which a program office relies on identity credentials issued by a CSP.

[83]A CSP is a trusted entity that issues security tokens or electronic credentials to subscribers.

Figure 6: Conceptual Identity-Verification Frameworks




Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Program (JFMIP).

Several panelists agreed that the *federated framework*, which falls in between a centralized and decentralized model, has the best potential to be successful in the U.S. government. Under a federated framework, a program office can gain reasonable assurance that identity credentials issued by a third-party accurately determine an applicant's identity, potentially without the program office needing to save information containing identity-authentication attributes.[84] A framework could also use attributes from more than one model, as appropriate.

Program offices within the federal government that interact with the public currently use both federated and decentralized approaches to managing identity credentials. Some program offices operate in a federated ICAM by using CSPs, such as login.gov, which allows the public to reuse an established credential among participating program offices. Other program offices, reflecting a decentralized approach, require their own credentials that are not portable.

A successful identity-verification framework cost effectively improves identity determinations while avoiding undue burden on affected individuals and helps to prevent and reduce improper payments. Panelists noted that successful

[84]Reasonable assurance refers to the ability of the identity credential to help achieve the control objective of accurately verifying a person's identity.

implementation of a federated ICAM must consider the need for standardization, applicant choice, and coordination throughout the federal government. Experts further noted the need to consider initial costs and long-term funding mechanisms.

The expert panel discussed the appropriateness of the three conceptual frameworks for implementing identity-verification controls for the federal government. The panel discussed the strengths and challenges of each approach in regard to consistency, administrative burden, and data security, as well as initial considerations for developing the infrastructure and lessons learned from other countries' implementation of them. Table 1 highlights some of the advantages and challenges that the panelists discussed for each framework.

Table 1: Some Advantages and Challenges of Centralized, Decentralized, and Federated Frameworks

| Advantages/challenges | Consistency | Administrative burden | Data security |
|---|---|---|---|
| **Centralized framework**<br>The central management entity issues a mandatory identity credential, which all program offices accept. | This is the simplest framework to achieve consistency and confidence in an applicant's identity.<br>Individual agencies would all have to commit to a consistent implementation, relinquishing independent control. If implemented nationwide, states would be relinquishing control to the federal government. | The identity-verification process is minimally burdensome to the applicant because it is only performed once. All program offices accept the identity credential.<br>If the framework is implemented nationwide, the American public may not be receptive to the notion of a single identity credential when such a document has the potential to be used for objectives other than verifying identity. | The framework achieves simplicity for program offices in managing access to information needed to verify identity.<br>It may create information-security and privacy risks by centralizing large amounts of people's sensitive information. |

| Advantages/challenges | Consistency | Administrative burden | Data security |
|---|---|---|---|
| **Decentralized framework**<br>Each program office requires its own credentials. The public manages multiple credentials from a number of issuers. | This framework makes it difficult to establish standardization and consistency because each program office would require its own credentials. | Each program office is responsible for the identity-verification process and managing the associated identity credentials.<br>Applicants would face an increased burden to repeatedly verify identity and maintain multiple identity credentials. | The framework reduces aggregation of data, providing better safeguards of sensitive information used to verify identity.<br>The framework would increase exposure of identity attribute data. It would require the public to repeatedly provide identity-attribute information to obtain program office credentials.<br>The framework would increase the risk of fraud, compared with centralized or federated frameworks, by requiring a citizen to engage with many different parts of government, which could make it possible for multiple identifiers to exist for one individual. |
| **Federated framework**<br>A program office relies on trusted identity credentials that a credential service provider (CSP) issues. The public chooses from a list of qualified CSPs. | Reliance on CSPs could offer program offices increased identity-credential assurance. It would also offer the public choice: an option of CSPs.<br>The framework would require risk-based standards that support identity-verification standardization and consistency, which may be difficult given the number of program offices and varying risk levels related to misrepresented identity. | The framework provides the public with portable ID credentials to use with multiple program offices, which would mean less engagement with the government, reducing applicant burden of reapplying with every program office.<br>It reduces up-front costs because it requires the least amount of change to the current infrastructure.<br>Effective implementation requires adoption by program offices and the public. | This framework only collects the minimal viable amount of identity evidence. It may require varying levels of data collected in order to establish appropriate verified credentials to reach needed assurance before payment issuance. |

Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Programs (JFMIP)

## Centralized Framework: One Mandated Credential for All Program Offices

In a *centralized identity-verification framework*, the central management entity issues a mandatory identity credential that all program offices must accept. One strength of a centralized ICAM would be that it is the simplest for achieving confidence in an applicant's identity because of the consistency of identity-

verification processes and centralizing access to information needed to verify identity.

Estonia is an example of a country that implemented a centralized ICAM nationwide. As described by an official in Estonia's Office of Information Systems Authority, the Estonian government requires that identification cards contain an electronic chip, which holds all the citizen's information. The identity card, which the police department issues, is mandatory for all its citizens ages 15 and above, and is the country's primary identity document. One must possess an identity card, which is free to Estonian citizens, in order to obtain any other type of identity document, such as a license or passport; to apply for admission to schools; and to interact with government programs.

Some panelists identified security and privacy risks as a challenge of a centralized framework because of the need to centralize large amounts of personally identifiable information (PII). Specifically, a centralized database could be at risk for cybercriminal attacks and, if breached and copied, could be sold to malicious actors. Currently, the United States does not have a minimum federal standard for identification issuance. For example, each state may set different requirements for driver's licenses. As a result, a national identification system using driver's licenses may be less feasible.[85] Finally, if this framework is implemented nationwide, some panelists stated that the American public may not be receptive to the notion of a single identity credential, with one expert specifically noting the potential for it to be used for objectives other than verifying identity.

## Decentralized Framework: Each Program Office Requires Its Own Credentials

In a *decentralized identity-verification framework*, each program office may require its own identity credentials. The public would then need to manage multiple credentials from a number of issuers. A decentralized framework would not require any central management entity or CSP. A strength of a decentralized ICAM is it enables the public and program offices to generate and assert their own identifiers. In theory, this would enable individuals to control who has access to their identity attributes and may reduce privacy risks. In addition, this

[85]Title II of the REAL ID Act of 2005, among other things, established minimum security standards for the issuance of licenses and identification cards that are used for official purposes, as described in the act. Official purposes include boarding federally regulated commercial aircrafts. Pub. L. No. 109-13, div. B, tit. II, 119 Stat. 302, 311-16, *codified at* 49 U.S.C. § 30301 note. Section 205(b) of the act allows the Secretary of Homeland Security to extend the deadlines for states' compliance; the current deadline for REAL ID compliance is May 3, 2023. 6 C.F.R. § 37.5(b).

would avoid the large aggregation of identity data because a decentralized ICAM does not require a central identity-verification system.

South Korea is an example of a country that has launched several decentralized identity initiatives. With developing technology, decentralized identities could allow the public to create, own, and control their identity credentials independently of any program office, operating within the confines of the permissions the public grants for use of their identities. For example, a recent graduate from college may request that the university issue a digital diploma copy. The graduate may choose to present the diploma to anyone—such as a potential employer—who can independently verify its issuer, time of issuance, and status.

Some panelists identified increased administrative burden for both the public and program office as a challenge of a decentralized ICAM. It may increase applicant burden for the public to repeatedly apply to verify their identities and maintain multiple credentials. A decentralized ICAM could make it more burdensome for a program office to assure that an identity is legitimate. This is because the office must independently verify identity attributes rather than rely on identity shared services.[86] In addition, one expert noted several regulatory and legislative barriers associated with a decentralized framework.

Another challenge identified by some panelists is managing risk-based standards that support standardization and consistency. A decentralized framework results in each program office requiring its own identity-verification process, which increases the risk of fraud compared with centralized or federated ICAM frameworks. That is because a decentralized ICAM allows the public to engage in various ways with different program offices, making it possible for multiple identifiers to exist for one individual. For example, this could allow the same individual to apply to the same program within different jurisdictions and receive benefits or payments from each jurisdiction. Since a decentralized framework lacks a central management entity, agencies would have difficulty detecting this activity, increasing the risk of improper payments.

[86]Decentralized identities would require endorsements from existing trust providers and processes, like business, educational institutions, and governments, in order to independently verify who issued an endorsement and when. By accumulating attestations from multiple endorsements, an identity can become more trusted and match increased levels of risk.

## Federated Framework: Public Choice among Approved Credential Service Providers

Using a *federated identity-verification framework,* a program office can gain reasonable assurance that identity credentials a CSP issues accurately determine an applicant's identity, potentially without the program office needing to save information containing identity-authentication attributes. This framework would require a central management entity to qualify CSPs that the public could choose from, in order to prevent the public from using CSPs with ineffectively designed or implemented controls. Some panelists agreed that the American public tends to be more receptive to services that offer choice, with an option to choose the service provider that verifies identity credentials. According to the National Institute of Standards and Technology (NIST), the federated identity providers (e.g., government agencies that maintain certain identifiers in their identity-verification systems) communicate authentication and attribute information to relying parties that use those services (i.e., other government agencies that verify identity).

One expert noted that a federated ICAM is most aligned with how the United States government is constructed today, considering the policy and legislative landscape. Implementing a federated identity-verification framework could reduce up-front costs because it would require the least amount of change to the current infrastructure. Some panelists noted that a federated framework would provide the public with portable identity credentials to be used across various program offices. Portable identity credentials could offer benefits to both the public and program offices: for the former, portable credentials streamline interaction with multiple program offices; for the latter, portable credentials reduce investment costs and may improve accuracy.

For example, Australia implemented the Trusted Digital Identity Framework (TDIF), which is a federated ICAM accreditation framework for digital identity services. The TDIF, operating as the central management entity, sets requirements for providers to achieve accreditation and also includes guidance and templates. To become an accredited provider, TDIF requires applicants to demonstrate how their digital identity service meets requirements for accessibility and usability, privacy protection, security and fraud control, risk management, technical integrity, and more. Once accredited, program offices can confidently rely on the identity credentials that these accredited providers issue. TDIF-accredited providers must continually demonstrate that they meet their TDIF obligations by undergoing annual assessments.

The TDIF in practice operates with the use of a CSP, which offers identity-based services such as creating, maintaining, and managing information about a person's identity. Program offices that rely on such services must be confident that the people to whom they provide a service are who they say they are; identity providers can provide that confidence. They provide identity-credential assurance to relying parties by collecting, verifying, and validating attributes that confirm a person's identity to an appropriate level as the relying party's risk assessment determines. This gives the public the choice to establish a credential with an accredited identity provider, which makes it quicker and easier to access services in future interactions with multiple program offices.

Some panelists identified that a potential challenge of a federated ICAM could be the required participation rate among program offices and the public. A federated framework would require risk-based standards that support identity-verification standardization and consistency, which may be difficult given the number of program offices and varying risk levels related to misrepresented identity. See Establish a Central Management Entity to Oversee and Coordinate Implementation for further discussion on offering the right incentives and establishing widespread adoption.

## Successful Implementation of a Federated Framework Considers Standardization, Applicant Choice, and a Central Management Entity

The experts discussed characteristics of a successful federated identity-verification framework. Several experts highlighted the importance of establishing minimum standards by program risk level; one expert identified the strength of allowing applicants to choose from qualified CSPs; and another expert cited the need to establish a central management entity to oversee and coordinate implementation.

### Establish Minimum Standards by Program Risk Level

Several panelists suggested establishing risk-based federal standards that support identity-verification standardization and consistency.[87] Given that each program has unique objectives and associated risks, the experts suggested that the government approach this in a risk-based way rather than requiring a

[87]NIST's *Digital Identity Guidelines* requires agencies to implement baseline requirements for digital identity services based on assurance level. Risk assessments determine the extent to which risk must be mitigated by identity verification and are the primary factor in selecting an assurance level (NIST SP 800-63-3). At this time, NIST only has a single level of identity assurance for remote verification and two for in-person verification (NIST SP 800-63A). Several panelists noted that as part of a future revision to identity-verification standards, NIST may consider augmenting these levels with a risk-based approach that would better allow program offices to adapt to their specific assessed levels of risk.

blanket standard for all programs. A risk-based approach would provide a minimum standard that all programs would need to meet, determining appropriate additional requirements based on the risk for a given program. This would allow a program office to collect the minimal viable amount of identity evidence needed to address its assessed level of risk.

The standard could apply to clusters of similar programs for which it makes sense to have a common standard. GAO has previously reported that these kinds of shared standards can help programs with similar goals, that conduct similar activities, or that serve similar populations to improve the effectiveness and efficiency of their efforts.[88] For example, one standard within the set of risk-based standards could apply to multiple programs that share similar risk profiles. Another standard could apply to a program with a different risk profile. This set of risk-based standards would implement a level of consistency across federal program offices and reduce administrative burden on both the program offices and the public.

Establishing such a standard would make a federated framework's implementation easier, facilitate partnerships among program offices, and effectively authenticate identity credentials. Some experts noted the need for program offices to balance the efficiency needed for the public to apply for and access benefits without sacrificing identity-verification controls, which could help mitigate the risk of improper payments.

A panelist shared the example of Unemployment Insurance (UI), which both federal and state payroll taxes fund, but which states operate, under state law. According to the panelist, fraudulent claims overwhelmed the UI program during the COVID-19 pandemic, and bad actors intentionally targeted states with the weakest controls in place. A minimum standard of identity-verification controls in place across program offices could mitigate this type of targeted identity fraud and reduce improper payments. However, the panelist recognized that this may be difficult given the number of program offices across the federal government, with varying risk tolerances for allowable improper payments.

[88]GAO, *2021 Annual Report: New Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Billions in Financial Benefits*, GAO-21-455SP (Washington, D.C.: May 12, 2021).

## Allow Applicants to Choose from Qualified Credential Service Providers

Several experts agreed that the public may be more receptive to the notion of choice, allowing them to select an option from qualified CSPs. A process to approve CSPs would prevent the public from using CSPs with ineffectively designed or implemented controls. As discussed above in Federated Framework: Public Choice among Approved Credential Service Providers, Australia approves CSPs through a qualification process in which the CSP may be required to demonstrate how their identity verification service meets requirements for accessibility and usability, privacy protection, security and fraud control, risk management, technical integrity and more. Agencies may source these service providers federally, for example, login.gov, or commercially. This federated model would offer a marketplace of identity-verification solutions. For example, CSPs would supply a level of confidence in an applicant's identity by collecting, verifying, and validating attributes that confirm an identity to an appropriate authentication level, as the risk-based standard discussed above determines.

Relying on CSPs to perform identity verification, rather than program offices, could make the verification process more standardized and efficient throughout the federal government. CSPs could generate, bind, and manage identity credentials to individuals and provide program offices with risk-based assurances that an individual accessing the service today is the same individual who previously accessed the service.[89] Standardization would allow applicants to choose the provider they trust while still ensuring that the verification meets a program office's needs, thereby reducing the administrative burden for both.

A panelist noted that the federal government could offer a marketplace to allow the public to choose from qualified CSPs through a mechanism similar to quality service management offices, whose mission is to deliver expertise and standard capabilities for federal agencies and other mission-support services.

## Establish a Central Management Entity to Oversee and Coordinate Implementation

The third consideration for successful implementation of a federated ICAM in the United States is a central management entity that could offer the right

[89]Binding is the process of establishing an association between a subscriber identity and an authenticator or given subscriber session.

incentives to both program offices and the public to encourage widespread adoption of the framework.

Successful implementation would depend on program offices' participation, defined as accepting identity credentials that CSPs issued and forgoing independent identity verification. Buy-in from senior leadership across the U.S. government could contribute to widespread adoption of a federated ICAM. Several experts noted the importance of the right incentives for both program offices to adopt this framework and the public to register with CSPs for new identity credentials. These could include cost savings, efficiency, and improved identity determinations.

For example, when the United Kingdom attempted to implement an identity-verification framework, it failed to obtain buy-in from several key UK program offices before moving forward with the project. As a result, some departments chose not to opt into the framework because it did not efficiently address the varying risk related to misrepresented identity that each program office faced. Many of these departments went on to develop their own identity-verification systems. A panelist shared that UK identity-verification experience was unsuccessful at obtaining widespread adoption because UK program offices and the public did not fully adopt the framework.

## Consider Initial Costs and Long-Term Funding Sources

Costs to create and maintain identity-verification processes within a federated ICAM may be substantial, considering direct procurement and deployment, administrative, and hard-to-measure costs, such as time, program reputation, and financial impact of fraudulent activity. Many program offices face a direct trade-off between controlling risks related to a lack of identity verification and effectively achieving goals, such as timely issuing benefits to the correct individuals. The panel discussed funding options, including centralizing funds, leveraging existing investments, and sharing costs among users.

Establishing identity-verification processes is critical to reducing improper payments caused by misrepresented identity. Sufficiently implementing an identity-verification infrastructure within a framework requires adequate funding. The panelists discussed several funding options, specifically focusing on how on funding an identity-verification infrastructure may occur centrally—for example, through the federal government sharing costs among data users and leveraging economies of scale for discounted pricing.

Centralizing the funding for implementing a federated identity framework may ensure long-term stability. Some experts favored centrally funding through the federal government because they view it as the federal government's responsibility to effectively deliver benefits to the public, and noted that the way to do that is via effective identity solutions. One example of this type of fund is the Technology Modernization Fund, which certain agencies may use to improve, retire, or replace existing federal information technology systems.[90] An expert noted that establishing a similar type of fund to allow program offices to invest in identity-verification processes would make more sense than relying on each agency's own appropriated funding. A dedicated source of capital that provides program offices flexibility to invest in new identity-verification projects could generate cost savings and may reduce improper payments.

A panelist pointed out that if identity-verification processes are centrally funded, it removes the cost question from program offices' cost-benefit analysis and allows them to pursue modernizing their abilities as needed. For example, the Australian Commonwealth Government is creating a digital identity system, with an investment of over $600 million by the end of fiscal year 2025.[91] Benefits of the system potentially include reduced processing costs, applicant burden, and improper payments. A panelist noted that to help ensure appropriate and efficient use, this fund would have to be approached strategically. For instance, a program office could submit a project plan to access these funds and require approval from a central management entity.

A centrally funded capital investment may be sufficient for the initial investment of creating an identity-verification infrastructure; however, in the long term, funding would need to be strategically managed. One panelist noted that a challenge of centralizing funding could be that the entity administering the funds may not be able to identify the unique risks and needs of each program office. The panelist further suggested that each program office could receive funding as a percentage of payments or benefits provided to the public,

---

[90]The Modernizing Government Technology Act of 2017 authorized the Technology Modernization Fund for technology-related activities, to improve information technology, and to enhance cybersecurity across the federal government. Pub. L. No. 115-91, div. A, tit. X, subt. G, 131 Stat. 1586, *codified at* 40 U.S.C. § 11301 note. Agencies submit proposals, including those for improving, retiring, or replacing existing federal information technology systems, to the Technology Modernization Board through a two-phase selection process, and if approved, the agencies receive incremental funding tied to project milestones and objectives.

[91]The system is being used across federal and state governments, and once fully developed is intended to be offered to the private sector. The investment covers a range of functions of the system including the development of a government digital identity, an identity exchange to assist in protecting the privacy of PII being shared and an independent governance body to ensure the integrity of the system.

with a dedicated use for identity-verification solutions. This type of funding would allow the individual program offices to have broad discretion over the funding allocation and empower those closest to the problem.

The federal government may be able to reduce up-front costs by leveraging private industry partners who have already established identity-verification tools and technology. Several panelists mentioned that data sharing between government agencies and the private sector may be a way to balance costs. Data sharing provides distinct results, such as identifying the use of deceased individuals' information in opening new financial accounts. Implementing this type of data sharing could result in implementation costs also being shared. For instance, those that want to use the data can either contribute to the data or pay a nominal fee to use it if they contribute no information. See Share Data to Strengthen Responses to Risks for more on data sharing.

One expert acknowledged that volume discounts could contribute to lowered costs, as in most transaction-based agreements. If a program office has a minimal number of interactions with a private sector entity engaged to support identity verification, the cost would likely be higher than approaching such a relationship from a government-wide, multiagency perspective.

## Improve Identification of Improper Payments Caused by Misrepresented Identity

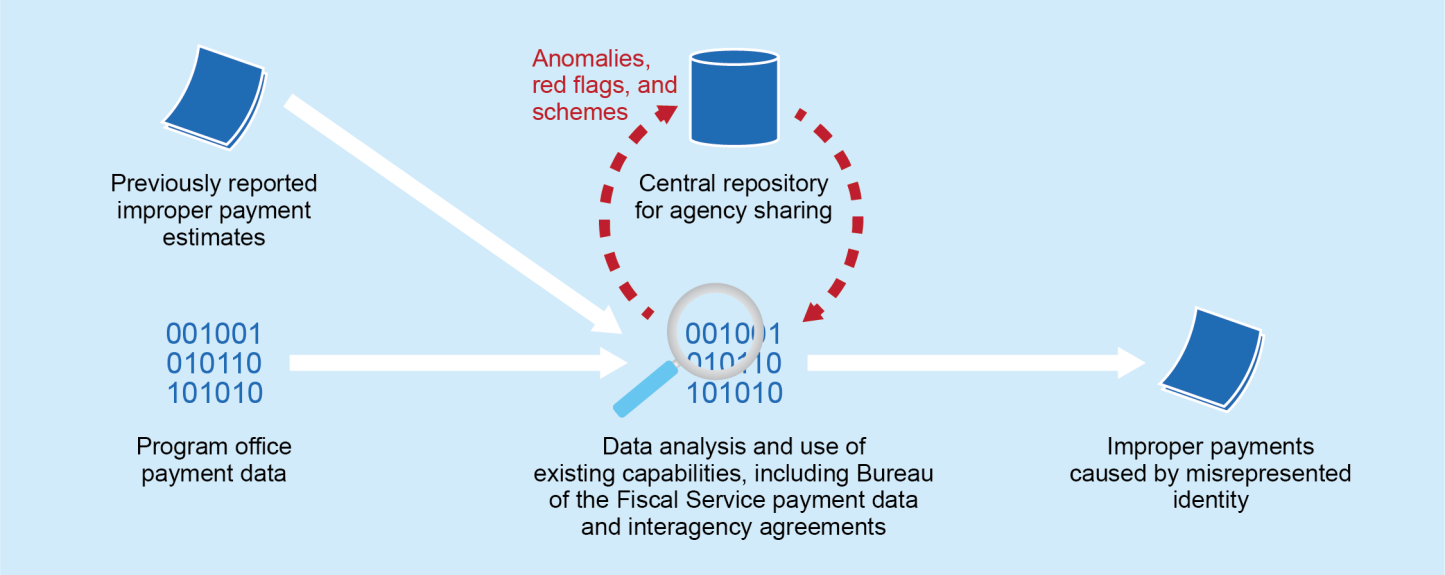
As a result of the discoveries in the Getting Payments Right Cross-Agency Priority Goal, Office of Management and Budget (OMB) guidance began requiring agencies to identify the amount of improper payments caused by misrepresented identity and report this information on paymentaccuracy.gov in 2021. In accordance with PIIA, OMB guidance also began requiring executive agency Offices of Inspector General (OIG) to evaluate whether their agencies followed applicable requirements related to formulating and including the payment integrity information that each agency reported on paymentaccuracy.gov.[92]

By using analytical techniques and data repositories, agencies and their OIGs could potentially improve their identifying, estimating, and reporting of improper payments that misrepresented identity caused. These techniques and data repositories could also help OIGs provide concrete and actionable recommendations that the program offices must take to improve the accuracy of reporting the impact that misrepresented identity has on improper payments.[93] Examples of potentially relevant analytical techniques may include anomaly detection and retrospective analysis. The federal government could consider establishing a central repository to house the anomalies, schemes, and nefarious actors identified through data analysis and share it with program offices. Program offices could also consider leveraging existing capabilities, such as the Bureau of the Fiscal Service's (Fiscal Service) payment data and interagency agreements, to perform analysis. Figure 7 presents a summary of the practices that the experts suggested to help identify the impact of misrepresented identity.

[92] 31 U.S.C. § 3353(a)(3); OMB's *Requirements for Payment Integrity Improvement*, OMB Memorandum M-21-19 (Washington, D.C.: Mar. 5, 2021). PIIA also required further guidance for OIGs to be issued by the Council of the Inspectors General on Integrity and Efficiency. 31 U.S.C. § 3353(a)(4).

[93] OMB's *Requirements for Payment Integrity Improvement*, requires an OIG to annually review the accuracy of the improper payment estimate and the agency's identification of the causes of the improper payments, including identity misrepresentation. If the OIG determines that the agency did not comply with OMB's guidance for identifying improper payments, their root causes, or both, then the OIG is required to provide recommendations to the agency regarding what it must do to improve. (OMB M-21-19.)

Figure 7: Summary of Potential Practices to Help Identify the Impact of Misrepresented Identity




Report number JFMIP-22-01 | Source: Joint Financial Management Improvement Program (JFMIP).

## Historical Data on Identity-Related Improper Payments Are Limited, but Improvements Are Under Way

Until recently, improper payments related to misrepresented identity were not a common data point for program offices to measure. Beginning in 2021, OMB guidance requires programs to report the proportion of their improper payments that were attributed to identity issues. As such, some agencies are still in the beginning phases of determining whether misrepresented identity is a significant cause of improper payments. With limited historical data on identity-related improper payments, evaluating the accuracy of the identifying, estimating, and reporting of improper payments that misrepresented identity caused may improve the likelihood that programs may implement the most appropriate mitigation strategies sooner rather than later.

This section explores methods program offices can consider using to identify improper payments misrepresented identity caused.

## Analyze Anomalies to Identify Potential Improper Payments

Some panelists agreed that using data analytics would be helpful in identifying improper payments related to misrepresented identity. Program offices can consider using analytical methods to detect abnormal patterns that may indicate identity-related schemes to defraud the government even in the absence of specific cases of proven misrepresented identity. For example, anomaly

detection techniques allow program offices to identify aggregate abnormal patterns across data that do not conform to established normal behaviors.[94] Program offices can consider performing further research and conducting risk assessments on these outlying characteristics or anomalies to identify new and emerging previously unknown identity misrepresentation schemes. Program offices can further consider analyzing detected identity-related anomalies to determine the root causes and sharing this information with other program offices to help them detect similar activities.

Program offices can consider looking for anomalies in identity data elements such as physical addresses, email addresses, phone numbers, and internet protocol (IP) addresses. According to a recent Government Accountability Office (GAO) report, Department of Labor officials indicated that the most common fraud schemes include the use of stolen personally identifiable information (PII) to file a claim or multiple claims, the use of synthetic identities (i.e., real identities mixed with fictitious information), and phishing schemes to obtain individual PII to perpetrate future fraud.[95]

Additionally, program offices can consider applying retrospective analysis on proxy data, financial data, and previously reported improper payment estimates to identify indicators of improper payments related to misrepresented identity.[96] This type of data analytics technique allows program offices to reexamine historical payments data and look for indications of recently identified schemes or anomalies to identify improper payments and their causes more accurately.

One expert discussed Fiscal Service's post payment process, which includes performing retrospective analysis and reexamining data sets as time moves on to extract transaction-level data for improving the accuracy of improper payment reporting. Program offices can consider analyzing the post payment data against what they determined to be red flags for improper payments

---

[94]Per OMB M-21-19, anomaly detection uses unsupervised algorithms to identify deviations compared to peer groups based on unknown patterns among common and individual fraudsters. Per GAO, *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care*, GAO-21-7SP (Washington, D.C.: Nov. 2020), an unsupervised algorithm is a machine-learning technique that identifies structure within unlabeled data inputs, by clustering similar data, without any preconceived idea of what to expect. For example, an unsupervised algorithm could cluster images into groups based on similar features, such as a group of cat images or dog images, without being told that the images are those of cats or dogs.

[95]GAO, *COVID-19: Additional Actions Needed to Improve Accountability and Program Effectiveness of Federal Response*, GAO-22-105051 (Washington, D.C.: Oct. 27, 2021).

[96]Proxy data are data that may be used instead of the data of interest when those data cannot be measured directly. For example, multiple payments going to the same physical address may be an indicator of improper payments.

misrepresented identity caused and computing a baseline metric (e.g., a percentage of payments made to unique individuals with the same bank-account information). Program offices could track that metric, along with others, over time to determine the prevalence of the red flags and, in turn, whether that indicates changes are needed to prevent potential improper payments. In addition, program offices could apply these data analytics techniques to existing improper payment sampling and estimation methodology plans in order to isolate subsets of the improper payment estimates that misrepresented identity caused.

## Establish Information Hubs to Facilitate Data Sharing and Analytics

A panelist mentioned that following efforts to use data analytics to identify anomalies, schemes, or suspicious actors, the government can consider establishing a central information hub to share these insights across the government. Doing so could help detect, prevent, and report improper payments related to identity verification across the government.

Information hubs exist in the public sector (e.g., the Do Not Pay (DNP) Business Center, the National Association of State Workforce Agencies' integrity data hub, and the Financial Crimes Enforcement Network's (FinCEN) suspicious activity repository) and private sector (e.g., MITRE's aviation program), and can integrate either data or metadata from other sources.[97] Information hubs rely on well-established, secure data pipelines to improve the efficiency of data sharing. They allow for established mechanisms to request and transfer data between agencies, which reduces the administrative burden for agencies, compared with initiating ad hoc data-sharing requests without a hub.

For example, each executive agency is required to review all payments and awards for all programs using Fiscal Services' DNP Business Center, a public sector information hub database, including, among others, commercial and government death data and delinquent or defaulted federal debt information, to verify eligibility of the payments and awards.[98] In May 2021, OMB designated 12 new databases as part of DNP, including the Bureau of Prisons incarceration data. Program offices can use DNP to determine whether a program applicant provided inaccurate or potentially false information, for

[97] Metadata are information that describes the characteristics of data.

[98] 31 U.S.C. § 3354.

example, by matching an applicant's Social Security number (SSN) with the deceased data; a match would possibly indicate suspicious activity.

One expert also mentioned the National Association of State Workforce Agencies' integrity data hub, which provides a centralized platform for state workforce agencies to compare and analyze Unemployment Insurance data to prevent fraud and improper payments.[99] This integrity data hub offers states access to a suspicious-actor repository; multistate claims data cross matching; bank account verification services; identity-verification scoring; and data analysis tools, such as cross matching similar emails.

Further, some experts suggested that program offices could align their existing records with trusted information hubs, either within or external to the federal government, to bolster their own data analytics efforts. For example, the Federal Aviation Administration enlisted MITRE to oversee the Aviation Safety Information Analysis and Sharing initiative. This program allows U.S. airlines, aircraft manufacturers, and government entities to share and analyze their safety data in efforts to proactively identify and address safety issues. MITRE serves as the information hub to facilitate information sharing and analysis. A similar approach can be considered using government payment data.

Some experts agreed that program offices that have had success in identifying improper payments misrepresented identity caused can consider sharing lessons learned through the information hub as well. Information hubs can promote iterative, collaborative development, in which agencies can leverage and build upon the expertise of other agencies. Agencies can share data engineering and analyses with the information hub, which can distribute relevant data, insights, and lessons learned to appropriate parties. For example, the Departments of Labor and the Treasury reported an estimated $7 billion and $682 million in fiscal year 2021, respectively, in improper payments related to identity.[100] The methods these agencies used to identify improper payments misrepresented identities caused can be shared with other agencies through the information hub. By using and reusing data and solutions centralized in the information hub, agencies could potentially reduce costs on initial analytics and identity-

[99]The National Association of State Workforce Agencies represents all 50 state workforce agencies, the District of Columbia, and U.S. territories. The Integrity Data Hub operates in partnership with the Department of Labor, which funds it. MITRE is a private not-for-profit company providing engineering and technical guidance for the federal government by operating federally funded research and development centers. MITRE also operates the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center where data between the Internal Revenue Service, industry, and states are shared and analyzed to detect, prevent, and deter activities related to stolen identity refund fraud.

[100]Official Website of the U.S. Government, accessed Jan. 14, 2022, https://www.paymentaccuracy.gov/.

verification controls and could direct funding toward more advanced analytics and controls.

FinCEN's repository for suspicious activity reported by financial institutions can be considered an information hub. Financial institutions must report known or suspected violations of law or suspicious activity to FinCEN via a Suspicious Activity Report. That information helps FinCEN to identify emerging trends and patterns associated with financial crimes and provide feedback to financial institutions in the form of advisories, bulletins, and other publications.

For example, FinCEN's advisory to financial institutions reported that some red flags of potential suspicious activities may include the following:

- the spelling of names in the account information differs from those on government-issued identification;
- customer log-ins occur from a single device or IP address across multiple seemingly unrelated accounts; and
- the IP address associated with log-ins does not match the stated address on the identity documentation.[101]

Implementing a similar approach in which government agencies could report suspected improper payments misrepresented identity caused could help recognize government-wide patterns in identity misrepresentation attempts.

## Leverage Existing Capabilities and Resources

Program offices can leverage existing capabilities and resources, such as Fiscal Service's payment data and interagency agreements, to perform data analytics and identify improper payments that misrepresented identity caused.

### Fiscal Service Payment Data Could Facilitate Bank Account Ownership Verification

A panelist noted that when payees claim that they did not receive a payment, a program office can consider using Fiscal Service's payment data in conjunction with its own data sets to perform root-cause analysis and determine whether this could indicate an improper payment. The Payment Integrity Center of

[101] Financial Crimes Enforcement Network, *Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the COVID-19 Pandemic,* FIN-2020-A005 (July 30, 2020)

Excellence (PICOE) is an entity within Fiscal Service that manages a centralized repository of government-wide federal payments.[102] The payment data include information such as payee bank account numbers, address information, routing transit numbers, and reason codes for returned bank payments. Indications of suspicious activity may include multiple payments going to the same bank account or the payee name not matching the name on the bank account.

One panelist further suggested leveraging PICOE's Account Verification Service (AVS) to verify the status of an individual's bank account and to help authenticate account ownership. Fiscal Service is currently piloting AVS to evaluate prepayment information about account status (e.g., open, closed, or frozen) and authenticate account ownership throughout the payment life cycle.

For example, an agency can consider sending payee information, such as SSN, payee name, routing transit number, and bank account, to PICOE for prepayment verification of first-time payments and bank-account changes. With access to databases across the federal government, PICOE can verify whether the government paid the payee previously through the same bank account, whether the payee account has been compromised, and whether the bank account was previously closed. The payee's bank account and account ownership is then verified using AVS. PICOE consolidates the results and sends them back to the requesting agency for evaluation. Program offices can then use this information to determine whether to make a payment to a payee or perform further investigations.[103]

## Interagency Agreements May Facilitate Federal Agencies' Identification of Improper Payments

An expert suggested that program offices can consider working with other entities, such as Fiscal Service and OIGs, to further refine improper payment data analysis and identification processes. For example, Fiscal Service can provide program offices with access to resources such as payment data and DNP, which has a variety of data-matching and analytics services to prevent and detect improper payments. OIGs have existing authority exempting them from certain requirements regarding matching programs and data collection by

[102]PICOE is a community of experts within Fiscal Service that assists agencies in reducing improper payments and is dedicated to solving government-wide payment integrity challenges.

[103]Agencies currently partnering with PICOE to leverage AVS include the Social Security Administration, the Internal Revenue Service, and the Federal Emergency Management Agency.

survey.[104] While also considering relevant independence constraints, the OIGs' authority to access data can be used to perform data matching across agencies to help program offices better understand how misrepresented identity has affected improper payments. In addition, GAO has previously reported that information sharing between agencies can improve the effectiveness and efficiency of their efforts.[105] See Share Data to Facilitate Identity Verification and Improve Controls above for further discussion on the merits of data sharing, including relevant GAO reports and OMB guidance.

[104]Inspector General Empowerment Act of 2016, Pub. L. No. 114-317, § 2, 130 Stat. 1595, *amending* Inspector General Act of 1978, Pub. L. No. 95-452, § 6(j)-(k), 92 Stat. 1101, *codified as amended at* 5 U.S.C. app.

[105]GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012).

# Appendix I: Objectives, Scope, and Methodology

This report addresses the first goal of the Joint Financial Management Improvement Program (JFMIP) initiative. It presents key considerations and potential actions to address implementation challenges that program offices can use to enhance identity-verification processes and potentially reduce improper payments. It also includes considerations for a potential overarching framework within which identity-verification controls could operate.

To address the objectives of this report, we identified program office and framework considerations based on information we collected through an identity-verification expert panel we convened, review of selected studies, and interviews with subject-matter experts. We did not assess whether program offices could implement the considerations under the existing legal framework or if this would require changes in the legal framework.

**Information Collection**

***Review of selected studies.*** We conducted a review of selected studies related to accountability, governance, equity, and identity-verification processes. We reviewed various sources, including (1) publications identified during a formal literature search that a Government Accountability Office (GAO) research librarian aided and (2) literature recommendations from external experts, experts we interviewed, and discussions with GAO experts. Our review of selected studies included a search for peer-reviewed materials, government reports, conference papers, association publications, and trade articles, among other sources, in databases such as Scopus, EBSCO, Hein Online, and ProQuest. We conducted the search on December 14, 2020, and limited our results to publications dated from January 1, 2018, to 2021, because this area is rapidly evolving and concepts that existed more than 3 years ago may not be as relevant.

As a result of this search, we identified 17 publications with relevant information on identity-verification processes. We also reviewed relevant guidance such as National Institute of Standards and Technology publications and Office of Management and Budget memorandums. As part of our research, we considered existing Identity, Credential, and Access Management (ICAM) frameworks and guides related to identity verification, including foreign-government publications and legislation.

***Interviews.*** We conducted numerous interviews for the purpose of identifying subject-matter experts for inclusion in the expert panel or further developing our understanding of the subject matter. We identified experts to interview according to criteria including initial outreach to individuals immersed in their communities or sectors asking them for individuals that they believed we should interview, organizations identified during review of our selected study, and interviewee referrals that we received during our engagement (snowballing method). We conducted 15 interviews with officials from federal agencies, departments, and inspector general offices, as well as five interviews with state officials and four international governmental entities. In addition, we interviewed experts from three credential service providers, three consulting and accounting firms, and four financial institutions. We conducted the remaining interviews, with two experts from academia, six from nonprofit organizations, and one from another sector.

***Identity-verification expert panel.*** In June 2021, we convened an expert panel to discuss factors affecting identity verification and identity management in federal government programs. The panel comprised experts from multiple areas, including industry, federal and state government, OIGs, international entities, consulting and accounting firms, credential service providers, and nonprofit organizations.

The panel addressed the following objectives:

| | |
|---|---|
| | • What practices have successfully been used when implementing identity-verification and identity-management capabilities?<br>• What are the most appropriate authoritative sources of data for identity verification and identity management?<br>• What are the costs—both measurable and hard to measure—of implementing identity verification and identity management, and who should be responsible for them?<br>• What should be the implementation framework for identity verification and identity management that the U.S. government could potentially use to reduce improper payments?<br>• What are the unintended consequences of identity verification and identity management, including social inequities and suboptimal use of data?<br>• How can improper payments related to identity verification and identity management be estimated or measured?<br><br>We summarized the views of panelists who participated in the JFMIP Initiative on Payment Integrity Expert Panel throughout the report. Their views informed the considerations in the report. To describe statements panelists made, we distinguish between issues that a single panelist (one), some panelists (two or three), and several panelists (four or more) identified. Panel sessions had four to seven primary discussants. We structured the panel agenda in sessions to address specific topics; see appendix II for the detailed agenda. We had seven moderated panel sessions, with moderation divided among three trained GAO facilitators.<br><br>We selected 27 experts to participate in the expert panel. Twenty-two experts accepted our invitation and participated in our panel discussions. These individuals presented a variety of perspectives, including those of digital commerce, fraud prevention, oversight efforts to address improper payments, computer science, data analytics, management of digital identities and credentials, electronic data interchange, disparate impact issues, information technology and cybersecurity issues, international ICAM framework experience, and privacy and security issues. We assessed each expert to identify potential circumstances that could be viewed as conflicts of interest. Based on our research of publicly available information and initial discussions, we determined that the experts were suitable for the panel. For a list of expert panelists, see appendix III.<br><br>In advance of the expert panel, we prepared and distributed to participants a background reading package, based on publicly available reports and studies in identity verification. The reading package featured a brief overview of the issues to consider in each of the seven sessions. |
| Validation of Considerations and Technical Comments | To validate the considerations presented in this report, we provided a draft of this report to all of the expert panelists (see app. III) for a technical review. Panel participants provided technical comments and edits, which we incorporated as appropriate. |

## Appendix II: Expert Panel Agenda – The JFMIP Initiative on Payment Integrity

| **Tuesday, June 22, 2021 (All times Eastern)** | |
|---|---|
| **10:00 – 10:40 AM**<br>**(2:00 – 2:40 UTC)** | Session 1: Opening Remarks<br>Keynote Speakers:<br>*Gene L. Dodaro, Comptroller General, Government Accountability Office*<br>*Gene Sperling, White House American Rescue Plan Coordinator and Senior Advisor to the President of the United States*<br>*Marshall Henry, Director, Do Not Pay Business Center, Department of the Treasury*<br>Engagement Overview, Goals, Definitions, and Housekeeping Rules |
| **10:40 AM – 12:10 PM**<br>**(2:40 – 4:10 PM UTC)** | Session 2: What practices have successfully been used when implementing identity-verification and identity-management capabilities?<br>Effective identity verification, which is a process that uses evidence to confirm and establish a linkage between a claimed identity and a real-life person or entity, is a potential avenue for reducing improper payments in the federal government. This session explores key practices for identity verification and identity management that the federal government could implement broadly in an effort to increase payment integrity.<br>Primary Discussants: *Lou Anne Alexander, Jordan Burris, Devin Fensterheim, Blake Hall, Carole House, Philip Lam, and Stetson Marshall.* |
| **12:10 –1:10 PM**<br>**(4:10 – 5:10 PM UTC)** | Lunch Break |
| **1:10 – 2:40 PM**<br>**(5:10 – 6:40 PM UTC)** | Session 3: What are the most appropriate authoritative sources of data for identity verification and identity management?<br>National Institute of Standards and Technology Special Publication 800-63-3 defines an authoritative source as an entity that has access to, or verified copies of, accurate information from an issuing source, such that a credential service provider (CSP) can confirm the validity of the identity evidence an applicant supplied during identity proofing. An issuing source may also be an authoritative source. Often, a policy decision of the agency or CSP determines authoritative sources before they can be used in the identity-proofing validation phase. A first step to |

| | |
|---|---|
| | having the accurate verification of an individual is having a reliable source of data.<br><br>Primary Discussants: *Cherian Abraham, Lou Anne Alexander, Bill Danielsen, Randy Gillespie, Jim Harper, Kevin McDaniels* |
| **2:40 – 3:10 PM**<br>**(6:40 – 7:10 PM UTC)** | Break |
| **3:10 – 4:40 PM**<br>**(7:10 – 8:40 PM UTC)** | Session 4: What are the costs—both measurable and hard-to-measure—of implementing identity verification and identity management, and who should be responsible for them?<br><br>Implementing identity-verification and identity-management tools and processes can be costly. However, as we become a more technologically advanced society and information becomes digitized and easily accessible across various platforms, it can be critical to the goal of reducing improper payments a misrepresented identity caused. Further, costs may be offset or reduced through prevention of improper payments and reduced processing times.<br><br>Primary Discussants: *Steven Bernstein, Jon Coss, Denise Davis, Sue Egan, Philip Lam, David Mader* |
| **4:40 – 4:45 PM**<br>**(8:40 – 8:45 PM UTC)** | Day 1 Closing Remarks |

| Wednesday, June 23, 2021 (All times Eastern) | |
|---|---|
| **10:30 – 10:35 AM**<br>**(2:30 – 2:35 PM UTC)** | Day 2 Opening Remarks |
| **10:35 AM – 12:05 PM**<br>**(2:35 – 4:05 PM UTC)** | Session 5: What should be the implementation framework for identity verification and identity management that the United States government could potentially use to reduce improper payments?<br><br>This session will explore ways the federal government could feasibly implement a digital identity framework, including whether it's best to use a centralized, federated, or decentralized framework. This session will also explore the advantages and challenges of each approach, initial considerations for developing this infrastructure, and lessons learned from others' implementation of each approach. For the purposes of this session, a "successful identity verification and identity management process" is one that cost-effectively improves identity determinations while avoiding undue burden on impacted populations and helping to identify and reduce improper payments.<br><br>Primary Discussants: *Jordan Burris, Mark Cheeseman, Randy Gillespie, Darlene Gore, Blake Hall* |
| **12:05 –1:00 PM**<br>**(4:05 – 5:00 PM UTC)** | Lunch Break |
| **1:00 – 2:30 PM**<br>**(5:00 – 6:30 PM UTC)** | Session 6: What are the unintended consequences of identity verification and identity management including social inequities and suboptimal use of data?<br><br>Increasingly, financial transactions and related processes are becoming electronic and more companies are moving towards digital interaction with customers. This session explores the issues and challenges of using identity verification and identity management and whether disparate impacts (for example, age, or the lack of internet, cell phone, or computer) might prevent users from accessing services. This discussion will also discuss false positives and false negatives for identity-verification controls as well as inherent difficulties of implementing identity verification and identity management systems in the federal government.<br><br>Primary Discussants: *Deann Baiza, Devin Fensterheim, Jim Harper, Aaron Klein, Keith Miller* |
| **2:30 – 3:00 PM** | Break |

| | |
|---|---|
| **(6:30 – 7:00 PM UTC)** | |
| **3:00 – 4:30 PM**<br>**(7:00 – 8:30 PM UTC)** | Session 7: How can improper payments related to identity verification and identity management be estimated or measured?<br><br>The federal agencies are required to report information related to improper payments under the Payment Integrity Information Act of 2019 (PIIA) (P.P. 116-117) and Appendix C to Office of Management and Budget Circular A-123. This information is the source for PaymentAccuracy.gov, which tracks the amount of improper payments at federal programs and the root causes. It appears that the most common causes of improper payments are related to eligibility or processing errors. However, this could be because many agencies are not considering or quantifying the number of instances when identity management is the cause for improper payments.<br><br>Primary Discussants: *John Coss, Carole House, Stetson Marshall, Kevin McDaniels* |
| **4:30 – 4:40 PM EDT**<br>**(8:30 – 8:40 PM UTC)** | Day 2 Closing Remarks |

## Appendix III: Expert Panel Participants for the JFMIP Initiative on Payment Integrity

| | |
|---|---|
| **Keynote Speakers:** | Gene L. Dodaro, Comptroller General, Government Accountability Office |
| | Marshall Henry, Director, Do Not Pay Business Center, Department of the Treasury |
| | Gene Sperling, White House American Rescue Plan Coordinator and Senior Advisor to the President of the United States |
| **Expert Panelists:** | Cherian Abraham, Vice President of Digital Identity Platforms, Experian |
| | Lou Anne Alexander, Chief Product Officer, Early Warning Services |
| | Deann Baiza, Director, Submission Processing, U.S. Treasury Inspector General for Tax Administration |
| | Steven Bernstein, Executive Director, Commercial Banking, JP Morgan Chase |
| | Jordan Burris, Former Chief of Staff, OFCIO, Office of Management and Budget |
| | Mark Cheeseman, Director, Government Fraud Function, Cabinet Office, United Kingdom government |
| | Jon Coss, Vice President of Risk, Fraud and Compliance, Thomson Reuters Government |
| | Bill Danielsen, Executive Director, Enterprise Identity Services, Integrity Services Branch, Employment and Social Development Canada |
| | Denise Davis, Director of Return Integrity Verification Program Management, Internal Revenue Service |
| | Sue Egan, Former Director of Identity Program, Business Integrity Division, Services Australia |
| | Devin Fensterheim, Digital Identity Product Line Manager, Social Security Administration |
| | Randy Gillespie, Vice President, National Association of State Workforce Agencies |
| | Darlene Gore, Director, Identity, Credential, and Access Management Division, General Services Administration |
| | Blake Hall, Founder and CEO, ID.me |

| | |
|---|---|
| | Jim Harper, Scholar with Focus on Digital Financial Instruments and Privacy, American Enterprise Institute |
| | Carole House, Director for Cybersecurity and Secure Digital Innovation, National Security Council, The White House |
| | Aaron Klein, Senior Fellow of Economic Studies, Brookings Institution |
| | Philip Lam, Executive Director of Identity, General Services Administration |
| | David Mader, Chief Strategy Officer, Civilian Sector, Deloitte |
| | Stetson Marshall, President/CEO, Comprehensive Consulting Group |
| | Kevin McDaniels, Senior Advisor, Payment Integrity Center of Excellence, Bureau of the Fiscal Service |
| | Keith Miller, Chief Scientist for Identity Intelligence, MITRE |

# Appendix IV: Abbreviations

| | |
|---|---|
| AAL | Authenticator Assurance Level |
| API | Application Programming Interface |
| AVS | Account Verification Service |
| CMPPA | Computer Matching and Privacy Protection Act amendments of 1988 and 1990 |
| COVID-19 | Coronavirus Disease 2019 |
| CSP | credential service provider |
| DNP | Do Not Pay |
| eCBSV | Electronic Consent Based Social Security Number Verification |
| FinCEN | Financial Crimes Enforcement Network |
| Fiscal Service | Bureau of the Fiscal Service |
| FRDAA | Fraud Reduction and Data Analytics Act of 2015 |
| GAO | Government Accountability Office |
| HUD | Department of Housing and Urban Development |
| IAL | Identity Assurance Level |
| ICAM | Identity, Credential, and Access Management |
| IP | internet protocol |
| JFMIP | Joint Financial Management Improvement Program |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PICOE | Payment Integrity Center of Excellence |
| PII | personally identifiable information |
| PIIA | Payment Integrity Information Act of 2019 |
| PIN | personal identification number |
| Privacy Act | The Privacy Act of 1974 |
| SSA | Social Security Administration |
| SSN | Social Security number |
| TDIF | Trusted Digital Identity Framework |
| UI | Unemployment Insurance |

# Appendix V: Contacts and Acknowledgments


| | |
|---|---|
| **Contacts** | Beryl Davis, (202) 512-2623 or DavisBH@gao.gov<br><br>Taka Ariga, (202) 512-6888 or ArigaT@gao.gov |



**Acknowledgments**

In addition to the contacts named above, the following individuals made key contributions to this publication.

**Government Accountability Office:**

Michael Chacon, Melanie Darnell, Heather Dunahoo, Teressa Gardner, Alex Gromadzki, Ryan Guthrie, Andrew Kurtzman, Jenny Li, Joshua Marcus, Steven Putansu, Stephanie Tanaka, Walter Vance, Nicholas Weeks, and Stanley Yau

**Office of Management and Budget:**

Nickole Arbuckle, Jordan Burris, Steven McAndrews, Eric Mill, and Heather Pajak

**Office of Personnel Management:**

Grace Hsu

**Department of the Treasury:**

Linda Chero, Wayne Everett Jr., Marshall Henry, Brian Hewitt, Dominque McCreary, and Kevin McDaniels

---

Also contributing to this publication from the Government Accountability Office were Christina Bixby, Mark Canter, Anthony Clark, Robert Dacey, Michele Grgich, Farahnaaz Khakoo-Mausel, Jason Kirwan, Michael LaForge, J. Lawrence Malenich, Lisa Motley, Amy Pereira, Timothy Persons, Neil Pinney, and Carolyn Yocom.