A Prepared Federal Government

Preventing Fraud and Improper Payments in Emergency Funding

Steve Goodrich
The Center for Organizational Excellence, Inc.

Bob Westbrooks
Fellow, National Academy of Public Administration

NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

IBM Center for The Business of Government

A Prepared Federal Government:
Preventing Fraud and Improper Payments in Emergency Funding

Steve Goodrich

The Center for Organizational Excellence, Inc.

Bob Westbrooks

Fellow, National Academy of Public Administration

AUGUST 2024

IBM Center for
The Business of Government

Table of Contents

Foreword

On behalf of the National Academy of Public Administration (NAPA) and the IBM Center for The Business of Government, we are pleased to present this new report, *A Prepared Federal Government: Preventing Fraud and Improper Payments in Emergency Funding*, **by Steve Goodrich of the Center for Organizational Excellence, Inc. and Bob Westbrooks of NAPA.**

When the government distributes supplemental funding to address various national emergencies such as the global pandemic, time is of the essence. Putting money quickly in the hands of Americans in need benefits vulnerable segments of the American population and stabilizes the nation in a time of crisis. At the same time, transparency and accountability mechanisms are essential to safeguard these taxpayer dollars and maintain public trust.

Rapid program delivery and program integrity are not mutually exclusive, but it can be difficult to establish the appropriate controls and checks and balances and produce the desired outcome in a fast-moving crisis. With a combination of new programs, additional funding, and broader program eligibility, the risk of waste, fraud, and improper payments increases significantly.

This report began with a roundtable discussion of experts in government fraud and improper payments in December 2023. Leaders and experts from the budget, financial management, data and oversight communities came together with those with experience in implementing efficient, effective, and lawful tracking and safeguarding of taxpayer dollars during emergency situations. These roundtable discussions generated insights on how the government can ensure integrity while meeting policy and programmatic goals in increasingly frequent emergency situations.

This report documents the challenges that governments experience with fraud and improper payments, especially during a national emergency. It also profiles the many collaborative initiatives currently underway to create lasting solutions to reduce fraud and improper payments. In addition to these initiatives, this report recommends others to provide a holistic capacity for the next funding emergency. It includes 27 recommendations that Congress and federal agencies can use to ensure the integrity, efficacy, and protection of funds distributed in increasingly frequent emergency situations.

This report builds on prior reports about government funding released by the IBM Center, including *Risk Management and Reducing Improper Payments: A Case Study of the U.S. Department of Labor* by Dr. Robert Greer and Justin B. Bullock; *The Partnership Fund for Program Integrity Innovation* by Jonathan C. Tucker; and *Managing Recovery: A View from Inside* by G. Edward DeSeve.

We hope that the insights and findings in this report help government leaders and stakeholders as they continue to mature their emergency funding capabilities, while ensuring effective safeguards and oversight methods.

Daniel J. Chenok
Executive Director
IBM Center for
The Business of Government
chenokd@us.ibm.com

Teresa W. Gerton
President and CEO
National Academy of Public
Administration
tgerton@napawash.org
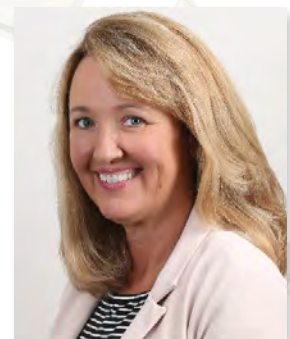
Lauren Craig
Partner, US Federal Civilian
Agencies, IBM
laurenc@us.ibm.com

Introduction

Emergency funding to support a national crisis requires rapid design, policy, and execution, and often involves many federal, state, and local agencies—making it particularly susceptible to human error and downstream management and oversight issues. This is often due to lack of timely guiding protocols, tools, resources, data, and systems. In a national emergency, the government must disburse vast amounts of money, at speed, through new or expanded programs, to unfamiliar parties. Although this may qualify as a policy success for addressing critical needs during a national emergency, it also often results in taxpayers being taken advantage of and public trust challenged. While federal agencies performed an incredible job addressing the pandemic in rapid fashion with valuable programs, they must learn lessons from both the positives and the negatives to be prepared with the appropriate policy and infrastructure before the next emergency requiring massive federal funding hits the United States.

When an emergency has subsided, the federal government typically goes back to business as usual, does little to identify lessons learned, and rarely acts on them to be prepared for the next national crisis. But in the case of the pandemic, agencies are proactively addressing many lessons learned. The federal government, through the combined and collaborative efforts of the Department of the Treasury (Treasury), Office of Management and Budget (OMB), Pandemic Response Accountability Committee (PRAC) of the Council of the Inspector's General on Integrity and Efficiency (CIGIE), General Accountability Office (GAO), Congress, and agency program offices, are actively addressing some shortfalls with solution to fraud and improper payments.

This report is intended to assist in the process of capturing lessons learned and providing a whole-of-government perspective. The effort leading to this report began with a roundtable discussion of experts in government fraud and improper payments in December 2023 (see Acknowledgements for list of attendees). This roundtable brought together leaders and experts from the budget, financial management, data and oversight communities, as well as those with experience in implementing efficient, effective, and lawful tracking and safeguarding of taxpayer dollars during emergency situations. The roundtable discussions generated insights on how the government can ensure integrity while meeting policy and programmatic goals in increasingly frequent emergency situations. This effort was designed to address the following:

1. Identify the specific management and oversight challenges associated with distributing government funds under emergency conditions prior to and after distribution.

2. Make recommendations to ensure effective safeguards and oversight methods (policy, practices, tools, resources, systems, and authorities) to be ready for the next emergency funding need.

Background on Emergency Funding

For each emergency, the federal government legislates programs and releases funding through a defined disaster declaration process. Agencies are typically prepared to manage and fund many of them. Various laws and programs are already in place, such as the Public Health Emergency Fund in the Department of Health and Human Services (HHS). The Federal Emergency Management Agency (FEMA) is poised and ready to support natural disasters, and the Department of Housing and Urban Developments (HUD) has a Public Housing Capital Fund designed to support housing needs during disasters.

> *If you open up a bank window and say, give me your application and just promise me you are who you say you are, you attract a lot of fraudsters, and that is what happened here.*
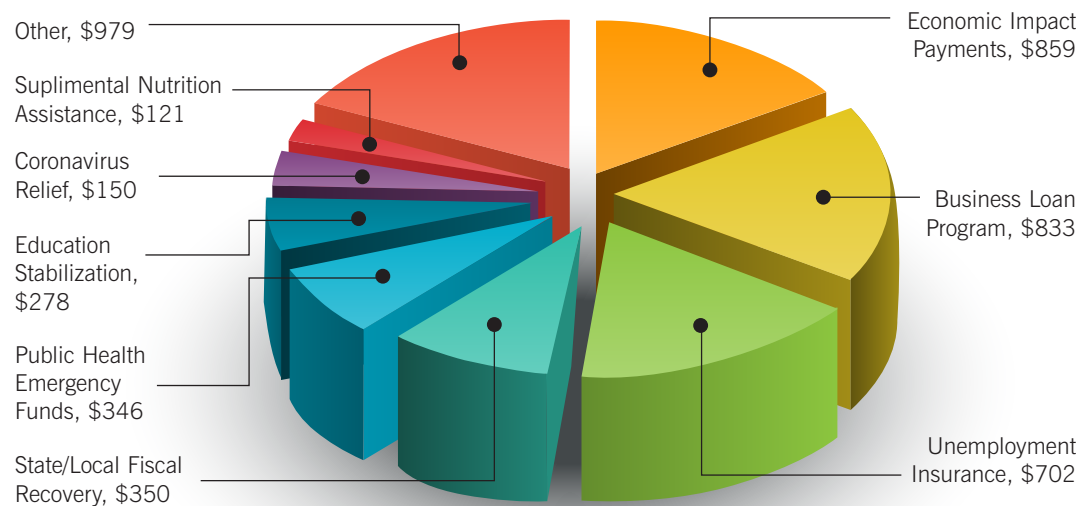>
> Michael Horowitz
> DOJ Inspector General, PRAC Chair

Yet government programs are not always prepared for emergencies of significant magnitude such as hurricanes Katrina or Sandy, or the most recent emergency, the COVID-19 pandemic of 2020–2023, which hobbled the U.S. economy and healthcare system and resulted in over 1.1 million deaths in the U.S. and over three million deaths worldwide. Moreover, the increased flow of funds in response to the COVID-19 pandemic exposed existing vulnerabilities in federal and state government payment systems and processes that resulted in increased improper payments—including fraud—in federal programs.

To address this pandemic, Congress responded with programs and emergency funding to support businesses, health care, COVID testing, the supply chain, healthcare workers, mental health, unemployment insurance, rental assistance, and more. Never has so much money been injected into the U,S. economy in such a short period of time. Funded programs and their amounts are profiled in below.[1]

Major COVID-19 Spending

- Other, $979
- Suplimental Nutrition Assistance, $121
- Coronavirus Relief, $150
- Education Stabilization, $278
- Public Health Emergency Funds, $346
- State/Local Fiscal Recovery, $350
- Economic Impact Payments, $859
- Business Loan Program, $833
- Unemployment Insurance, $702

---

1. Government Accountability Office, COVID-19 Relief: Funding and Spending, GAO-23-106647.

IBM Center for The Business of Government

It is estimated that with most of the $5 trillion appropriated, **over $600 billion was taken fraudulently and/or subject to improper payments**. Relative to the rapid promulgation of legislation, developing program management rules and capacity, distributing funds, training staff, developing data systems, measuring the impact, and providing for proper oversight, the government was trailing with proper and effective tools and practices to prevent significant fraud or improper payments. This approach reduced the impact that these programs may have and reduced the government's effectiveness as a steward of taxpayer funds.

Unfortunately, U.S. citizens, international entities, corporations, and others have received funds incorrectly due to government inaction or error with little to no certification, or were stealing taxpayer funds. Some used stolen identities, fraudulent bank accounts, falsified work histories, and moved across state lines to commit multiple frauds.[2] Lack of systems, organizational silos, increased sophistication of fraud schemes with the rise of AI, regulations, data, accelerated digital interactions causing challenges with identity verification and account takeover, and federal state collaboration were just some contributing factors making it difficult for the government to manage and oversee the proper administration of and return of taxpayer dollars. As of the writing of this report, about $1.4 billion of the $600 billion stolen has been returned to the federal government, and over 3,500 people have been criminally charged.[3] As SBA IG Mike Ware predicted in a 2021 interview, the amount of fraud from COVID relief programs was "larger than any government program that came before it."[4]

Two key definitions help to frame an understanding of the nature and extent of this challenge.

*   **Improper payments** are payments that should not have been made. This may be due to wrong amounts (either over or under), payments to the wrong person or corporation, or payments that did not follow statutory requirements. They may or may not include some level of fraud.

*   **Fraud** involves paying an entity that is not entitled to the payment based on misrepresentation.

Both require effective prepayment controls and post-payment oversight and corrective action protocols to be put into place when programs are established and executed.

The Government Accountability Office (GAO) identifies **root causes** of improper payments and fraud to include:[5]

Improper Payment Root Causes

*   Failure to access data/information needed

*   Data/information needed does not exist

*   Lack of documentation from recipients to determine eligibility

2. Pandemic Response Accountability Committee, Why Unemployment Insurance Fraud Surged During the Pandemic, pandemicoversight.gov, April 2024.
3. Feds have Seized More Than $1.4 Billion From Fraudulent Covid Relief Recipients, Forbes, James Farrell, April, 9, 2024.
4. Unprecedented Fraud Penetrated Roll Out of COVID-19 Small Business Loans, Watchdog Warns, ABC News, Lucien Bruggeman, August 5, 2021.
5. Government Accountability Office, Improper Payments and Fraud: How They Are Related but Different, Report to Subcommittee on Legislative Branch, Committee on Appropriations, House of Representatives, GAO-24-106608, December 7, 2023.

Fraud Root Causes

- Opportunity, incentive, and rationalization on the part of the perpetrator

- Weak internal controls

- Undetected misrepresentations, falsifications, social engineering, data breaches, cyber-crime, or coercion

- Lack of independent verification of applicant's information

---

Not Enough Capacity or Oversight Results in Unsatisfactory Outcomes: Some Factoids

Examples of fraud include:

- California man fraudulently received $5 million in COVID funds to buy sports cars

- New York woman fraudulently received $9.1 million in PPP loans

- Texas man defrauds government of $17 million for medical supplies and buys a Rolls Royce

Examples of challenging management practices:

- Application and receipt of funds to companies without certification of eligibility

- Fraudsters not checked against government databases to determine eligibility

- SBA barred from reviewing tax returns to determine eligibility

---

Many entities are involved in a rapid response environment; effective management, skills, collaboration, and having the right tools in place are essential before any emergency takes place. Congress and the White House, established and new agency programs, the Treasury Department, Inspectors General (IGs), and newly established entities under emergency legislation such as the PRAC, the PRAC's Pandemic Analytics Center of Excellence (PACE), must all engage with each other and create new management and oversight systems and tools before the next emergency—so they are no longer "behind the curve" to properly respond to the issues of fraud and improper payments, such as those identified in the text box above.

IBM Center for The Business of Government

Historically the government has been ill-prepared to manage funds effectively due to the need to quickly infuse needed funding in an emergency, to bolster the economy and support Americans in need. To address these issues, many government entities and experts have made recommendations about systemic corrective actions needed. While this report identifies some actions already taken, including those under laws listed below, additional practices can help to increase the federal government's preparedness for the next crisis—to ensure that agencies can mobilize efficiently and effectively, while reducing fraud and improper payments.

To support the pandemic, Congress passed multiple laws:

1. The Families First Coronavirus Response Act, 2020

2. The Coronavirus Aid, Relief, and Economic Security Act (Cares Act), 2020

3. Continued Assistance Act, 2020

4. The Paycheck Protection Program and Health care Enhancement Act

5. The Coronavirus Response and Relief Supplemental appropriations Act, 2021 Consolidated Appropriations act, 2021

6. The American Rescue Plan of 2021

7. The Coronavirus Preparedness and Response Supplemental Appropriations Act

Other laws to support proper payments:

1. Payment Integrity Information Act (PIIA)

2. Fraud Risk Reduction and Data Analytics Act (FRRDA) of 2015

3. Federal Funding Accountability and Transparency Act (FFATA)

4. Digital Accountability and Transparency Act (DATA Act)

5. The 2023 House Report 117-389 requires GAO to provide quarterly reports to Congress on improper payments

6. The Computer Matching and Privacy Protection Act

7. The Payment Recovery and Reinvestment Act

This report seeks to help ensure that there is not a zero-sum trade-off between getting money out quickly, serving the nation, protecting program integrity, and minimizing fraud. The government is expected to be an effective custodian of taxpayer funds. Putting the policy, tools, and programmatic infrastructure into place now without overburdening agencies and the budget is essential. Taxpayer funds must be managed effectively, efficiently, and equitably to address an emergency, ensure proper use of public funds, and build the trust of the public.

Why Government Needs to Create Systemic Solutions

The need to create a systemic solution to fraud and improper payments is evident in the examples discussed below. If done right, payment integrity solutions can also improve customer experience and reduce the friction for people seeking benefits. Key challenges and events affecting agencies in this arena follow.

> *I think the bottom line is regardless of what the number is, it emanates overwhelmingly from three programs that were designed and originated in 2020 with too many large holes that opened the door to criminal fraud.*
>
> —Gene Sperling
> White House American Rescue Plan Coordinator

The Scope of Fraud and Improper Payments is Significant

GAO has estimated that the government has cumulatively made $2.7 trillion in improper payments over the past 20 years. According to GAO,[6] the government made $236 billion in improper payments in 2023. More than 80% of these payments were cocnentrated in five programs: Medicare, Medicaid, the Earned Income tax credit, Pandemic Unemployment Assistance, and the Paycheck Protection Program Loan Forgiveness.

In addition, GAO estimates $232–$521 billion is lost to fraud each year, which in budget terms would make it equvalent to the "sixth largest agency in government."[7] This is not a mere accounting issue; this is real money from real taxpayers that could be of great use.

---

6. gao.gov/blog/federal-government-made-236-billion-improper-payments-last-fiscal-year, March 26, 2024.
7. Our First-Of-A-Kind Estimate of Fraud in the Federal Government, General Accountability Office, Watchdog Report, April 16, 2024.

Pandemic Emergency Funding is Highly Susceptible to Fraud and Improper Payments

As previously stated, Congress authorized over $5 trillion in relief and stimulus aid in response to the COVID-19 pandemic. Although this level of spending was justifiable given the unprecedented scale of the public health emergency, three pandemic relief programs were highly susceptible to fraud and improper payments due to the expedited way some aid was distributed, federal agencies' failure to mitigate third-party risk, and poor program integrity controls:

- Unemployment Insurance (UI), a group of programs overseen by the Department of Labor (DOL) and administered through 54 state workforce agencies

- The Paycheck Protection Program (PPP), administered by the U.S. Small Business Administration (SBA) through designated lenders

- The Economic Injury Disaster Loan Program, administered directly by the SBA with a third-party vendor for loan application processing

Almost immediately, law enforcement officials determined that fraudsters (both domestic and international) were targeting these programs. The nation was soon confronting the most expansive public fraud crime wave in U.S. history. During the pandemic, nefarious applicants submitted online applications using inexpensive stolen identity credentials and how-to fraud tutorials available on the dark web. Federal agencies were not ready to respond with appropriate management controls to detect and prevent a significant portion of this fraud.

The exact amount of tax dollars lost to fraud during this public health emergency is unknown, and unknowable with any degree of precision. GAO has estimated that the UI program likely lost between $100 billion and $135 billion during the pandemic. The DOL IG reported that approximately $191 billion of pandemic UI payments could have been improper with "a significant portion attributable to fraud." The SBA IG has estimated that the SBA disbursed over $200 billion in potentially fraudulent pandemic loans.

The federal government and the taxpayer were not the only victims. Legitimate citizens in need were denied UI benefits because a fraudulent claim had already been filed in their name. The initial $400 billion that was authorized for the Paycheck Protection Program (PPP) was depleted in 14 days, and many struggling small businesses were unable to obtain relief.

Leaders Moved with Necessary Speed that Minimized Controls

In times of emergency, Congress and the White House appropriately move quickly to plan and execute programs, funding, and authorities. Basic legal authorizations were put in place in response to the pandemic, and supplemental legislation was passed as needed to fill gaps and unanticipated needs. During the pandemic, Congress had little time to perfect the content and wording of the legislation, often used language from prior emergency legislation without incorporating changes based on previous lessons learned, and coordination with the White House and agencies was limited.

Sufficient Data Sets Were Limited

Law enforcement officials shared fraud threat information early with state and federal officials and financial institutions. Fraud was apparent, but program officials did not always have all the law enforcement and program data and were unable to easily spot links, relationships, or patterns hidden within a dataset or among different datasets. As fraud prosecutions mounted, it was common to see the same individual responsible for scores or even hundreds of UI

claims or small business loan applications, and to see cross-program fraud where the same individual defrauded all three of the vulnerable pandemic programs. The federal government did not have sufficient data sets and tools in place to address the epidemic of fraud.

Federal Counter-Fraud Enforcement Efforts Were Decentralized

Program officials were sometimes slow to tighten fraud prevention controls in response to the information that was shared, and sometimes there were no ways to share data in a coordinated way. For example, the IGs at DOL, SBA, and GAO issued multiple audit reports throughout the pandemic that identified nonexistent or weak fraud controls. Program and law enforcement officials did not always have the data necessary to detect and disrupt fraud. DOL initially indicated it lacked authority to demand unemployment insurance data from the states. The IG's office was forced to issue 54 individual subpoenas to the state workforce agencies for the data. The states' responsiveness to these subpoenas varied, as did data quality. The IG's office expended considerable effort to load and transform this data into a common searchable format. A year and a half into the pandemic, the administration provided partial relief to this data gap in the form of a condition of grants awarded to states under the American Rescue Plan Act. To obtain federal money for their workforce agencies, states were required to provide program data to DOL and its IG.

In some instances, program officials and law enforcement were overwhelmed with data. In the case of the small business pandemic loans, program officials and the IG were awash in data but initially lacked the tools and data analysts to connect the dots at any level of scale. Law enforcement organizations like the U.S. Secret Service (USSS) and other IGs requested and obtained the small business loan datasets to enable their data analysts to search them for hidden links and patterns and other indications of fraud.

The federal government has a decentralized counter-fraud law enforcement model. The Federal Bureau of Investigation (FBI) has authority to investigate all federal crimes not assigned exclusively to another agency. The USSS has authority to investigate financial crime, including identity fraud and crimes affecting federally insured financial institutions. The Secret Service played a major role in identifying and investigating fraud and recovering over a $1 billion in stolen COVID relief funds from banks through forfeiture actions. The Internal Revenue Service Criminal Investigation (IRSCI) unit has authority to investigate tax-related financial fraud, and the U.S. Postal Inspection Service (USPIS) has authority to investigate a broad-range of financial crimes under its mail fraud jurisdiction. Both agencies played a significant role in pandemic fraud enforcement. Federal departments and agencies generally have an office of Inspector General with authority to investigate fraud involving their agency programs, and considerable OIG resources were redirected to focus on pandemic fraud.

There are nearly 75 federal IGs throughout government. Not only can several federal law enforcement organizations investigate the same offense, but it is also common practice in federal law enforcement for agencies to work joint investigations and share resources. Coordinating and deconflicting investigative efforts is a critical function, yet is difficult with added workload in emergency situations.

Some important changes were made during the pandemic emergency. For example, to provide support to the federal law enforcement community as it confronted the COVID-19 fraud crisis, DOJ temporarily extended the mission of its Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center from its role as a platform for interagency information and intelligence aimed at transnational organized crime and drug enforcement. OCDETF analysts reviewed small business loan and unemployment insurance data to uncover fraud and assist law enforcement and prosecutors with case development. The DOJ also created the COVID-19 Fraud Enforcement Task Force, dedicating prosecutors to bring criminal and civil fraud actions.

The Federal Decentralized Counter-Fraud Risk Management Model Led to Uneven Results and a Lack of Clear Direction at Times

Agency management is responsible under federal law to manage its fraud risks, with OMB providing overall guidance. There is little evidence that countering fraud was a high priority in 2020, especially at the beginning of the pandemic. Over time, OMB and agencies have recognized the increased risk. For example, OMB issued guidance in March of 2021 to strengthen program integrity and public trust.[8]

Federal efforts to prevent fraud at the pre-award or prepayment stages were also limited. The Payment Integrity Information Act of 2019 was signed into law on March 2, 2020, approximately two weeks before the pandemic hit the U.S., and less than a month before Congress passed the signature pandemic relief and economic stimulus law (the $2.6 trillion CARES Act). The new payment integrity law expanded the Do Not Pay (DNP) initiative operated by Treasury. This initiative allows, but does not require, federal agencies to check federated databases to determine eligibility. The number of such databases continues to grow, and includes datasets of deceased individuals, incarcerated individuals, individuals and businesses that have been debarred from doing business with the government, and other data. Federal agencies were required "at a minimum" to review their pre-award and prepayment procedures and conduct a thorough review of available databases. The new payment integrity law also permitted states to use the system at no cost.

---

8. OMB Memorandum M-20-21.

Unfortunately, new pandemic relief programs were designed and implemented without regard to the DNP system. Further, due to the requirements of the Computer Matching Act and the Privacy Act, data sharing agreements can take months to establish, and there is no easy way to onboard new programs. However, while the pandemic was ongoing, the SBA OIG was able to engage with DNP officials to detect potential fraud. Alarmed by their significant findings, the IG issued an audit report which ultimately prompted the SBA to begin using the DNP system. This corrective action saved the government an unknown amount of tax dollars from fraud. By this time, though, hundreds of billions in relief aid had already been distributed.

Later in the pandemic, OMB articulated in policy documents and other activities the importance of counter-fraud activities.[9] OMB directed newly implemented federal programs to undergo joint program reviews. These meetings bring together OMB, agency officials, and IG officials to discuss program integrity, accountability, and transparency components of new programs. These reviews began in 2021 with programs implemented under the American Rescue Plan. The administration further institutionalized this practice in a subsequent major spending law, the Infrastructure Investment and Jobs Act. Further, the International Public Sector Fraud Forum, of which the U.S. is a member, advocates for and provides guidance on cross-government collaboration and has published many guidance documents to do so.[10]

Agency IGs Play a Complicated and Limited Role in Fraud Risk Management

IGs are charged with detecting and preventing fraud, waste, and abuse within government programs and operations. Fraud is detected through investigations and data analytics in audits or other reviews. Once an alleged fraud is identified, it is presented to a DOJ prosecutor for consideration of prosecution. Once a case is accepted for prosecution, investigators must follow the guidance of the prosecutor on how much or little information may be shared with management officials during the investigative phase of the prosecution. During the pandemic emergency, the SBA OIG's office was permitted to share some information with SBA program officials so that "holds" could be placed in the SBA's loan application system on subsequent applications from suspected fraudsters who were under investigation. As a result of this collaborative effort, some fraud was prevented.

Agency management is responsible for prevention of fraud, and for the early detection and disruption of fraud activity. Fraud risk information from the IG may be valuable, but management is not obligated to follow IG advice or recommendations. Moreover, such information is typically provided after the fact, and not in real-time when management could take action to mitigate losses. Finally, the IGs must maintain their independence by law and therefore cannot assume any program operating responsibilities, limiting the opportunities for collaboration to prevent fraud. The frequent misalignment between program management and program enforcement responsibilities can result in a less-than-optimal federal counter-fraud approach, although they do share a common framework for detection, evaluation, and investigation.

9. For example, Controller Alert, Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk, CA-23-03, October 2022.
10. https://sfo.govt.nz/counterfraud/cfc/additional-resources/international-resources-2/.

A New Independent Pandemic Oversight Organization Enabled Greater Collaboration Among the IGs and Their Law Enforcement Partners

With the passage of the CARES Act in March 2020, Congress created a new independent oversight office, the PRAC. The PRAC was formed as a committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The PRAC was funded with an initial $80 million appropriation, and is scheduled to sunset in 2025.[11] The PRAC members include some IGs designated in the CARES Act and some IGs selected by the PRAC chair.

The PRAC was modeled after the Recovery Accountability and Transparency Board, which was created in 2009 to independently oversee the roughly $800 billion in economic stimulus provided in the American Recovery and Reinvestment Act to address the Great Recession. That Board sunset in 2015. Perhaps the Board's most notable accomplishment was the creation of a cloud-based, whole-of-government data analytics function called the Recovery Operations Center (ROC). ROC data analysts identified potential fraud in the data and sent fraud referrals to IGs. Despite its potential and actual capabilities and notwithstanding its modest operating costs, Congress allowed the ROC to sunset in 2015 along with its parent Recovery Accountability and Transparency Board.

The CARES Act did not specify that the PRAC develop or maintain a centralized data analytics function to support law enforcement akin to the ROC. Most of the PRAC's responsibilities outlined in the CARES Act pertain to public reporting of federal pandemic spending data. Tracking and reporting general government spending is a function of the USASpending.gov system operated by Treasury.

When the pandemic fraud crime wave hit in early 2020, the oversight community lacked a central data analytics function to identify hidden relationships and other indications of fraud within a program or across programs. The PRAC's early emphasis was on creating the *public* spending website that it was legislatively mandated to create and maintain. At the same time, the OIGs at the SBA and DOL were inundated with fraud complaints from a variety of sources, including financial institutions.

Fraud complaints typically only contain, at best, partial information about possible fraud activity. An informant may, for example, have personal knowledge of one fraudulent small business loan application but not be aware of several other applications submitted by the same individual. Data analytics is needed to identify hidden relationships and other indications of fraud. The PRAC recognized the need for an IG community shared data analytics function. For this purpose, the PRAC created the PACE in early 2021. The PACE was loosely modeled after the ROC.

---

11. An additional $40 million was appropriate in March 2021 through the American Rescue Plan Act.

During the Recovery Act era, the ROC correctly suspected that there was contract and grant fraud hidden in the data. ROC analysts interrogated the data and sent fraud referrals to IGs. As a result, IGs were inundated with fraud complaints.

Consequently, the analytical assistance that some IGs required was not only potential case *identification* but support on case *development* as well. As a result, the PACE hired investigative analysts who used data to build leads and identify potential evidence from the data on identified subjects. The PACE was created using a center of excellence model, which recognized that some IG offices had mature data analytics capabilities. For these offices the PACE acted as a data broker, using its legal authorities to acquire federal data and share it with IGs and other law enforcement partners. Some offices required the PACE to perform analysis to identify previously unknown subjects. Others required more data analytics resources for their offices so the PACE created the Data Science Fellows program, using its flexible hiring authorities to augment OIG staffing with experienced analysts. Other OIGs required additional tools for their offices so the PACE created a blanket purchase agreement, which offices could use to rapidly procure software tools or contract analyst support.

PACE data scientists supported OIGs on other activities as well to promote independent oversight. The Treasury OIG, for example, was responsible for overseeing and auditing the $150 billion Coronavirus Relief Fund. Given the large number of prime and subrecipients—about 79,000 in total—advanced data analytics were needed to prioritize audit activities. PACE data scientists developed a risk scoring model for Treasury OIG using 27 risk indicators. Treasury OIG auditors used this model to conduct data-driven, risk-based desk reviews.

It took months to build the PACE. The PRAC had to issue a system of records notice to be legally permitted to gather, maintain, and share data. The PRAC needed to define contract requirements and follow the procurement process. The PRAC also needed to identify and onboard qualified staff to lead and operate the PACE. And the PRAC needed to design the appropriate data system architecture, and to build the system to those specifications to ensure the availability, integrity, and security of the data that it obtained. While this "building" activity was going on, criminals were stealing taxpayer funds.

Based upon the early successes of the PACE, Congress authorized an additional $40 million for data analytics activities. But Congress did not extend the five-year life of the PRAC and therefore the PACE will sunset along with the PRAC in September 2025, unless legislation is passed to extend its life and continue its funding. Congress and the administration allowed the ROC to sunset in 2015. A functioning (and mature) analytic capability would have undoubtedly enabled the early identification of pandemic fraud activity.

Generally, Government Agency Program Officials are not Well-Prepared to Oversee an Emergency Program

As demonstrated on the previous pages, a number of tools now support the identification, management, and oversight of fraud and improper payments. Many were developed during the pandemic, while others still need development, refinement, and leadership support to create an integrated infrastructure for when the next emergency strikes. Likewise, staff in many agencies, including Treasury, IGs, OMB, and GAO, continue to work on these issues. However, when an emergency hits, staff stop their regular duties to address it or are detailed to other support functions. It takes time to build collaborative rapport, establish governance, understand the policies and authorities under which they can function, develop skills and hire talent, compete contracts, learn the tools they have at their disposal and those that need development, and identify barriers that need to be overcome. Assembling teams and tools takes time. In an emergency, such time can be the enemy.

Actions Are Being Taken to Improve the Management and Oversight of Government Program Funding

As referenced in the Introduction, several federal government entities are actively addressing fraud and improper payments through a variety of means.

Legislative Action

President Biden signed into law an extension of the statute of limitations to 10 years for pandemic loan fraud, to ensure criminals do not "run out the clock." To illustrate the magnitude, the SBA IG told Congress that based upon data analytics on actionable leads, his office has "more than 100 years of investigative work."

Legislation cosponsored by Senators Gary Peters, Richard Durban, and Ron Wyden would help address fraud and recover funds. The Fraud Prevention and Recovery Act (S.4089) would provide resources to IGs to investigate pandemic fraud, enhance DNP, provide resources for Treasury to combat and prosecute fraud targeting fraud rings, and provide early warning methods for detecting fraud and supporting taxpayers.

Representatives Abigail Spanberger and Blake More recently introduced the Enhanced Improper Payments Accountability Act (HR 877) requiring more stringent reporting of improper payments to Congress, including identifying the impacted programs, the extent of improper payments, why they occurred, and the steps that agencies are taking to reduce improper payments (similarly the HUD Accountability Act of 2024, HR 6864, would do the same).

Senators John Kennedy and Tom Carper introduced the Ending Improper Payments to Deceased People Act, which amends the Social Security Act to allow the Social Security Administration (SSA) to share the Death Master File with Treasury's DNP system.
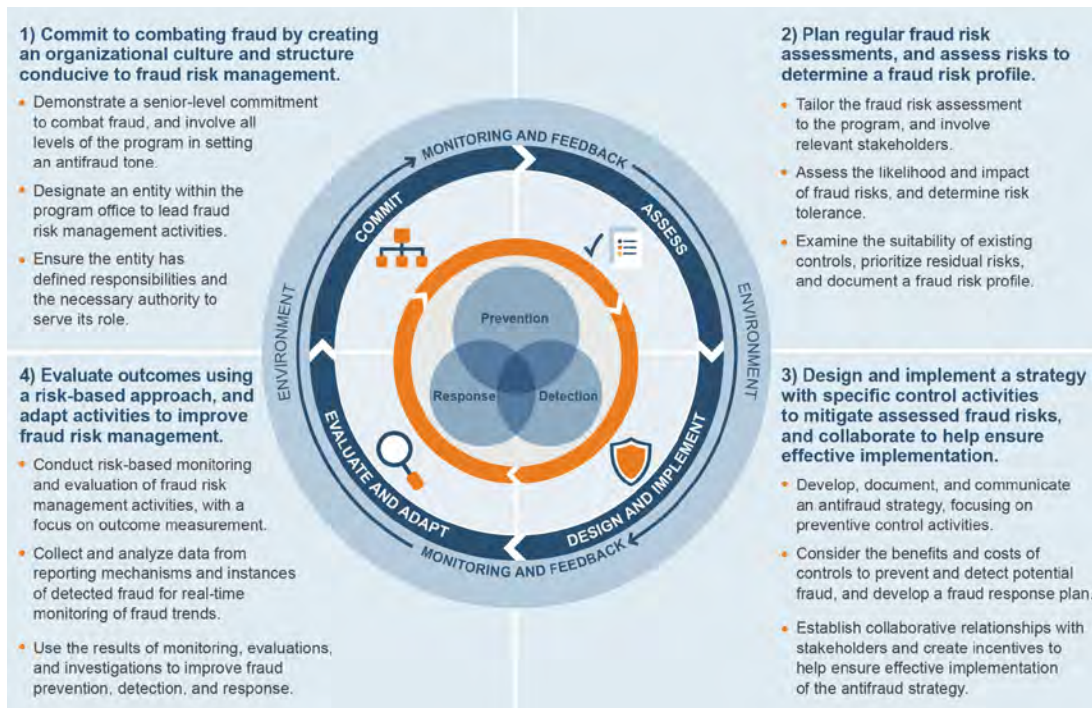
A recent Congressional Research Service Report[12] profiled some requirements that agencies must meet to prevent and detect improper payments or fraud:

---

12. Congressional Research Service, Improper Payments in Pandemic Assistance Programs, R47902, January 19, 2024.

Improper Payments[13]	Fraud[14]
• Establish pre- and post-payment review procedures • Recover overpayments • Assess the risk of improper payments • Report estimates of improper payments for at risk programs • Publish and implement corrective actions to address weaknesses in payment integrity • Report improper payment estimates of less than 10% for each program	• Create a functional entity and culture to manage fraud risk • Conduct regular fraud risk assessments • Design and implement strategies and control activities to mitigate the risk of fraud • Evaluate outcomes to improve fraud risk management

Government Accountability Office Action

The GAO continues to assess fraud and improper payments following its issuance of the Fraud Risk Framework in 2015, shown in the figure below,[15] the purpose of which is to help government managers combat fraud and preserve the integrity of government agencies and programs. The framework addresses guidance at the leadership level as well as in program planning, design, and evaluation.

1) Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.

- Demonstrate a senior-level commitment to combat fraud, and involve all levels of the program in setting an antifraud tone.
- Designate an entity within the program office to lead fraud risk management activities.
- Ensure the entity has defined responsibilities and the necessary authority to serve its role.

2) Plan regular fraud risk assessments, and assess risks to determine a fraud risk profile.

- Tailor the fraud risk assessment to the program, and involve relevant stakeholders.
- Assess the likelihood and impact of fraud risks, and determine risk tolerance.
- Examine the suitability of existing controls, prioritize residual risks, and document a fraud risk profile.

4) Evaluate outcomes using a risk-based approach, and adapt activities to improve fraud risk management.

- Conduct risk-based monitoring and evaluation of fraud risk management activities, with a focus on outcome measurement.
- Collect and analyze data from reporting mechanisms and instances of detected fraud for real-time monitoring of fraud trends.
- Use the results of monitoring, evaluations, and investigations to improve fraud prevention, detection, and response.

3) Design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate to help ensure effective implementation.

- Develop, document, and communicate an antifraud strategy, focusing on preventive control activities.
- Consider the benefits and costs of controls to prevent and detect potential fraud, and develop a fraud response plan.
- Establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy.

Source: GAO (information and icons). I GAO-23-106567

---

13. As required by the Payment Integrity Information Act.
14. As required by the GAO Framework for Managing Fraud Risk in Federal Programs.
15. GAO, A Framework for Managing Fraud Risk in Federal Programs, GAO-15-593SP, July 2015.

GAO repeatedly warned the administration and Congress about increased fraud risk throughout the pandemic emergency. In 2020, it warned about the lack of internal controls over Small Business Administration COVID-19 loans that made them susceptible to fraud. It also warned about substantial fraud in the pandemic unemployment insurance program. Since then, GAO has issued several reports on improper payments, including its February 2023 report identifying the significant improvements needed to address fraud and improper payments in emergency relief spending, its May 2023 report identifying fraud schemes and indicators in SBA's pandemic programs, and its October 2023 report on key elements of COVID-19 fraud schemes and actions to better prevent fraud. In April 2024, GAO issued the first of its kind governmentwide estimate of federal dollars lost to fraud.

Executive Actions

OMB, Treasury, GAO, and the Office of Personnel Management (OPM) recently released the Joint Financial Management Improvement Program (JFMIP),[16] a three-year plan to improve payment integrity. The plan is to take a whole-of-government approach by promoting fraud prevention and payment integrity in federal programs through education, better use of data, guidance updates (e.g., A-123, Appendix C), and collaboration. In addition, OMB is continuing fraud symposiums and lunch and learns, hosting joint review meetings, working to make the PACE permanent, and hosting meetings with other countries to exchange and learn. They also recently updated the Uniform Grants Guidance to safeguard taxpayer resources. The FY 2025 budget requests funding to:

- Enlarge the Department of Justice (DOJ) Fraud Strike Force.

- Provide more resources for the IGs at SBA and DOL.

- Expand DOLs access to UI datasets.

- Expand Treasury's DNP system and authority to access data.

- Allow agencies to validate key information through SSA.

- Upgrade and modernize fraud prevention and identify validation systems.

- Pilot an identity theft early warning system.

- Enhance identifytheft.gov.

- Support victims of identity theft.

The PRAC recently issued a Blueprint for Enhancing Program Integrity[17] which outlines best practices to strengthen federal programs. It addresses culture, adopting fraud risk-management programs, maintaining a crisis ready staff, using technology and data, stronger grant and contract award terms, validating eligibility criteria, and enhanced monitoring and evaluation.

The Department of the Treasury is pursuing a number of legislative proposals[18] for FY25, including the ability to certify bank accounts, bank account comparisons, DNP access to state death data and new hire data, and partnering with credit reporting agencies to validate payee attributes.

---

16. Joint Financial Management Improvement Program, JFMIP-24-02, February 2024.
17. Blueprint for Enhancing Program Integrity, Pandemic Response accountability Committee, Council of the Inspectors general on Integrity and Efficiency, May 2024.
18. Department of the Treasury, Bureau of the Fiscal Service, Congressional Budget Justification and Annual Performance Plan and Report, FY 2025.

A summary of current agency activities to address fraud and improper payments follows.

Tools Currently Available to Combat Fraud and Improper Payments

- Pandemic Response Accountability Committee (PRAC)
- Pandemic Analysis Center of Excellence (PACE)
- Treasury, Governmentwide Spending Data Model (GSDM)
- Electronic Consent Based Verification Service (eCBVS)
- Joint Financial Management Improvement Program (JFMIP)
- OMB M-22-04. Promoting Accountability through Cooperation Among Agencies and Inspectors General
- OMB Controller Alert CA-23-03, Establishing Financial and Administrative Controls to Identify and assess Fraud Risk
- USDA, Food and Nutrition Service National Accuracy Clearinghouse (NAC)
- Automated Standard Application for Payment (ASAP)
- Invoice Processing Platform (IPP)
- GAO, Standards for Internal Controls in the Federal Government
- GAO, Interactive Treasury Playbook
- GAO, A Framework for Managing Improper Payments in Emergency Assistance Programs
- Treasury's Office of Payment Integrity, including the Do Not Pay (DNP) initiative
- GAO, Fraud Risk Management, Key Areas for Federal Agency and Congressional Action, April 2023
- GAO, A Framework for Managing Fraud Risk in Federal Programs
- A-123, Standards for Internal Controls in the Federal Government
- Agency Fraud Risk Management Boards
- Organized Crime Drug Enforcement Task Force (OCDETF)
- Infrastructure Investment and Jobs Act
- Program integrity and fraud symposiums
- DOL Benefits Accuracy Measurement Program
- DOJs Fraud Strike Force
- Identifytheft.gov
- PRAC Blueprint for Enhancing Program Integrity
- USASpending.gov
- DOJs Organized Crime Drug Enforcement Task Force
- HUD Accountability Act of 2024, HR 6864

Recommendations

This report has documented the problems associated with a lack of strong government control and response to fraud and improper payments, especially during a national emergency. It also profiled the many collaborative initiatives currently being taken to create lasting solutions to reduce the incidents of fraud and improper payments. In addition to these initiatives, this report recommends others to provide a holistic capacity for the next funding emergency.

As noted, part of the difficulty in managing emergency funds is not just the many moving parts, but the speed at which the government must act to get needed aid distributed to serve its intended purpose. While some waste or inefficiency is expected, agencies and the states are not always afforded the time during a crisis required for establishing a program, developing policy and regulations, digitizing, putting the infrastructure in place, building data sets and repositories, establishing internal controls, and ensuring safeguards are in place to ensure the funds are used as intended.

The goal of these recommendations is for the government to be ready and more effective when the next emergency strikes, while attempting to not add significant expenditure of funds during nonemergency times.

There is an entire ecosystem of accountable and independent entities that must take integrated action to better manage and reduce the number of incidents of fraud and improper payments and be prepared for the next emergency. Individual and cross-government actions are needed that include Congress, OMB, Agencies, states, IGs, Treasury, and others. While the recommendations provided below focus on emergency funding initiatives, many can also be applied to existing agency funding programs. The recommendations are, in part, supported by the The Public Sector Fraud Model shown below as published in the Public Sector Counter Fraud Journal.[19] This model demonstrates the wider counter fraud environment and the layers associated with its defense.

19.   The Public Sector Counter Fraud Journal, UK Government Counter Fraud Profession, Issue 12, February 2024, p 24.
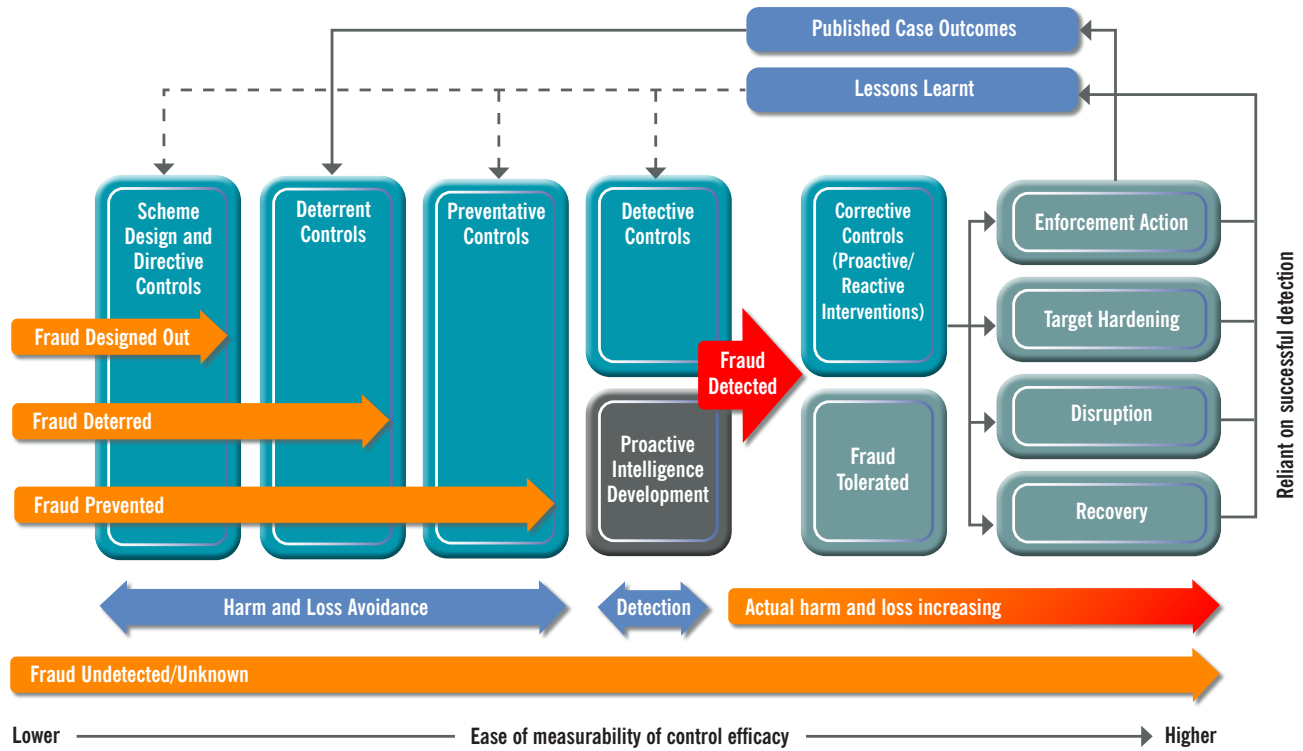
Therefore, the appropriate solutions must be holistic in nature to ensure a system solution and include preparedness, prevention, detection, investigative, and recovery. The table below summarizes the recommendations.

	Preparedness	Prevention	Detection	Investigative	Recovery
Congress	Establish proforma emergency funding legislation. Provide fraud and improper payment requirements in reauthorizations. Immediately direct agencies and the PRAC to enhance existing capacity. Make the PRAC and PACE permanent. Provide stricter sentencing for convicted fraudsters.	Require states to develop fraud control plans. Require agencies and states to use Treasury's DNP. Suspend procurement and hiring rules in emergency funding legislation. Require electronic payments with emergency funding. Expand fraud prevention and detection tools and expanded Treasury authority. Establish a payment integrity fund.	Require states to provide data and reporting.		Provide Treasury the ability to "claw back" electronic funds.

	Preparedness	Prevention	Detection	Investigative	Recovery
OMB	Lead a whole-of-government counter fraud function. Prepare briefing books for administration transition. Formalize a counter fraud workforce.	Participate in the International Public sector Fraud Forum. Pressure test agency programs. Prepare an emergency funding execution playbook.	Adopt GAO guidance under gao-24-105833		Provide Treasury the ability to "claw back" electronic funds.
Treasury	Train government staff in fraud and improper payment and emergency funding preparedness. Serve as the central POC for sharing tools and techniques. Share information on fraud trends and best practices.	Strengthen payment integrity tools (e.g., DNP) based on lessons learned. Continue to add data sets. Participate in the International Public Sector Fraud Forum. Work with states to develop data sets and support fraud and improper payments. Use open and proprietary data.	Develop a risk monitoring and flagging system. Develop a governmentwide monitoring system.		Develop capacity to "claw back" electronic funds.
Inspectors General	Continue to enhance the capacity of the PRAC and PACE.	Continue the Blueprint development and Joint Program Review Meetings. Support training of agency staff. Support agency assessment of program readiness.	Collaborate with Treasury, Justice, OMB and others in taking a whole-of-government approach.		
Agency Programs	Assess agency programs for susceptibility to fraud and improper payments. Work to "harden systems." Assess grants and contracts for appropriate practices. Maintain a fraud risk catalog.	Develop standard risk profiles and continual update. Develop a counter fraud and improper payment plans. Continual test risk mitigation strategies and adapt. Share best practices with others. Collaborate in whole-of-government approach.	Automate internal controls where possible using advanced technologies.	Support Treasury, IG, OMB programs and investigations. Share data—program, validation, source data, etc., including judicial agencies.	
States	Develop fraud and improper payment management and reporting capacity.				

Recommendations for Congressional Action

Create Ready to Go Legislation. Congress, in collaboration with OMB, Treasury, SBA, HHS, HUD, DOL, and perhaps states, could establish proforma legislative language that is ready for adaptation and adoption when a time-sensitive emergency funding need arises. While the language would need to be adapted for a given situation, it would take into consideration all lessons learned from prior emergency funding applications, and provide the level of detail required (e.g., internal controls, validations, certification requirements, support for IGs, use of data systems, suspension of certain rules, reporting).

A select or joint and bicameral committee that crosses multiple Congressional committees should be involved. Both the budget and management side of OMB should be included. The process should take 6-8 months and result in language ready for alignment with the particular issue and quick execution. Once complete, Congress could designate a specific committee to be responsible for its preparation and execution when needed. At the time of execution this legislation should take advantage of other existing legislation and Executive Branch systems, policies, tools, and resources, and also consider more mature programs such as those executed by the Federal Emergency Management Agency (FEMA).

Prepare Now For the Crisis. As new programs or reauthorizations arise, including agency direct-benefit and grants programs, Congress could consider the inclusion of requirements for the use of fraud or improper payment guidelines, systems, data requirements, and so forth by:

- Requiring federal agencies to submit "lessons learned" reports on pandemic program integrity

- Requiring states to establish data systems and report back to the federal programs

- Including these requirements as systemic parts of existing (nonemergency) grants so that data sets are expanding and ready for later analysis

- Requiring federal agencies to prepare "fraud control plans" for emergency spending addressing directive, deterrent, preventative, and detective controls and corrective controls (enforcement, target hardening, disruptive, and recovery) and who is responsible for these components

Provide Direction and Support to Agencies. To ensure readiness, Congress could pursue legislation directing Treasury, agencies, and the PRAC to develop and/or enhance existing guidance, policy, technology platforms, methods, and data systems to address domestic and international fraud and improper payments. Such legislation could make the DNP system mandatory for all related emergency funding programs. Congress could also authorize Treasury to develop and implement a whole-of-government counter-fraud function leading, supporting, and coordinating agency fraud and improper payment functions.

During Emergency Funding Suspend Certain Rules. For example, Congress could suspend procurement rules, require electronic payment (checks are 16X more likely to encounter fraud/anomalies and check fraud has increased 385 percent since the pandemic), and provide for hiring flexibility. This will allow for rapid response to staffing, platform, data, and other needs.

Make Permanent the PRAC and PACE. Legislation could make permanent these resources that are so critical to providing current and emergency funding support. This would allow for additional resources during times of emergencies, and ensure that technology, investigative capacity, and data systems are ready and enabled. Congress could consider the use of advanced technologies for automated internal controls, pre/post award validation, or payee certification.

Lengthen Statute of Limitations and Impose Stricter Sentences for Emergency Funding Fraud. While a 10-year statute of limitations was enacted, sentencing guidelines should be reviewed and possibly strengthened to address crimes related to stealing from American taxpayers.

Provide for Additional Tools. Congress could provide Treasury with the ability to "claw back" funds from both paper and electronic fund payments. This could involve establishing a voluntary self-disclosure program providing the ability for citizens and others to pay back funds taken or improper payments made.

Expand Fraud Prevention and Detection Tools, Data, and Analytics. Safeguarding taxpayer dollars from increasingly sophisticated fraud schemes and improper payments requires advanced analytics and fraud detection processes. The Treasury, as the central disbursing agency, can support federal programs in detecting new and emerging fraud schemes. This may require expanding Treasury's statutory authority to access data necessary for the purposes of detecting and preventing fraud and improper payments, which is critical to enable timely detection and prevention. This approach emphasizes solutions that support the entire federal enterprise and create economies of scale by creating access to data, analytics capabilities, and expertise.

Establish a Payment Integrity Fund. Congress could establish a payment integrity fund and/or allow federal programs to recoup a percentage of the dollars recovered from fraud prevention. Agencies need funding to build capacity to use data, analytics, and new tools, as well as to adjudicate flagged risk.

Recommendations for Office of Management and Budget Action

Continue the Coordinating and Oversight Role. OMB is taking a comprehensive multipronged approach to addressing the management and oversight of this critical issue. OMB could continue this whole-of-government approach, prepare briefing books on this topic for new officials in the upcoming administration (whether reelected or newly elected), and engage in bipartisan collaboration with Congress. OMB could also play a stronger participating role in the International Public Sector Fraud Forum, and work with Treasury and agencies to improve fraud and improper payment estimates. This cannot be more critical and is probably understated given the significance of the problem.

Assess Agency Program Preparedness and Measure Outcomes. OMB, in working with IGs and Treasury, could "pressure test" the capacity of agency programs, Treasury systems, and supporting data systems to operate in a crisis with little to no increase in fraud and improper payments. This could be accomplished by conducting program reviews, "war-gaming" and scenario planning, and/or by using artificial intelligence to test various scenarios and interoperable systems, including state data systems.

The GAO recommendations related to assessing fraud should be implemented:[20]
- The Director of the Office of Management and Budget, in collaboration with the Council of the Inspectors General on Integrity and Efficiency, should develop guidance on the collection of Office of Inspector General (OIG) data to support fraud estimation. The guidance should (1) identify and establish consistent data elements and terminology for use across OIGs; (2) include a timeline for implementation and key milestones; and (3) leverage existing data systems and processes, as appropriate.

- The Director of the Office of Management and Budget, with input from executive branch agencies, should develop guidance on the collection of executive agency data to support fraud estimation. The guidance should (1) identify and establish consistent data elements and terminology for use across agencies; (2) include a timeline for implementation and key milestones; and (3) leverage existing data systems and processes, as appropriate.

In implementing these recommendations:
- Focus on the most vulnerable programs such as UI, Payroll Protection, and Medicare.

- Use a scenario-based approach for execution. Test internal controls, staff capacity, capacity of data systems, speed, accuracy, determine source of errors, and so forth.

Prepare an Emergency Funding Execution Playbook. This can ensure readiness for the next crisis, so that Standard Operating Procedures (SOPs), authorities, fraud risk inventory, and protocols are in place and ready for execution.

Formalize the Government Counter-Fraud Profession. Similar to the UK, OMB could formalize the counter-fraud workforce to build capacity within federal agencies to detect, prevent, and investigate fraud.

---

20. https://www.gao.gov/products/gao-24-105833.

Recommendations for Treasury Action

Lead an Effort to Prepare People Across Agencies for the Next Emergency. Treasury could develop core competencies and design and implement a training and certification program for Executive Branch employees, IG offices, PRAC, and perhaps state program employees. Also, the agency could develop and maintain standard operating procedures, a knowledge management system, communication tools, and a profile of high risk indicators.

This program would prepare responsible staff in such areas as methods, available tools and programs for managing distribution, reducing fraud and improper payments, authorities, available data systems and analytic tools, related and supporting legislation. This program would ensure a ready cadre of trained and prepared staff who can quickly respond or be detailed to support emergency programs and oversight activity.

Strengthen Treasury's Payment Integrity Tools (e.g., DNP) and make their use mandatory for federal agencies. There is a need for Treasury to continue to evolve the DNP and its data sets and strengthen its capacity to verify payment eligibility. To implement this recommendation, Treasury could:

- Request and obtain statutory authority to make it mandatory for designated programs and allow state use.

- Help states develop their capacity over time to prepare for, develop, and use tools for identifying fraud or potential fraud.

- Continue to add data sets such as death records, new-hire, tax data, criminal data, and so forth.

- Protect the privacy and other rights of American citizens.

- Classify the data at a national security level.

- Require screening prior to certification.

- Develop a risk monitoring and flagging system that would automatically notify stakeholders (such as federal agencies, law enforcement, and IG's).

Assess, Profile, and Create a Centralized Data and Reporting System. Treasury could adapt and/or create a centralized data system that provides critical data requirements and feed from all agencies, so that Treasury can monitor and assess government programs across the government to determine trends, anomalies, and identify opportunities for cross-government improvements.

Strengthen Monitoring of Federal Programs - Serve as the Central Managing Agency for Technology Platforms. Using the Quality Service Management Office (QSMO) model, Treasury could conduct market research and identify effective commercial technology—such as artificial intelligence and machine learning, global positioning, and other technologies—that could serve to support fraud and improper payment detection, management, and response.

Create Capacity for International Fraud Management and Oversight. Treasury could assume a prominent role in the International Public Sector Fraud Forum. This could involve sharing information on fraud trends and best practices with international partners to better enable the U.S. government to identify and stop bad actors. Such a program would foster and better understand relationships between bad actors and entities by using open and proprietary data sources, such as Open corporates, Sayari, or OFAC sanctions.

Improve Collaboration with States and Identify Conditions for State Benefit Acceptance. Continue Treasury's bold vision to empower federally funded and state-administered programs to provide actionable solutions to transform the identification, prevention, and recovery of improper payments and to mitigate the effects of fraud.[21] This could involve working with agencies to identify critical data sets and reporting, and incorporating these data elements into DNP and for use in Treasury and Justice programs.

Recommendations for Inspectors General Actions

Lead Collaborative Activity with Agencies. IGs could continue the blueprint development, lead symposium and Joint Program Review meetings, engage supporting agencies in reviewing revised fraud, develop improper payment program designs, and conduct internal control audits specific to readiness for emergency funding. This could including training Executive Branch staff, and collaborating with Treasury and law enforcement on strengthening programs.

Work With Congress to Make the PRAC Permanent. The IGs could support making the PRAC and PACE permanent programs, and require strengthening of data sets, interoperable systems, and greater collaboration with agencies and states. This could drive opportunities to ensure that the most effective operating and functional design is in place.

Recommendations for Agency Program Actions

Assess Agency Programs for Emergency Capacity. Agencies could collaborate to assess programs for susceptibility to fraud and improper payments. This could be strengthened by developing a standard profile of risk factors, and by identifying program anti-fraud/improper payment strength. Agencies could design, implement, and test risk mitigation strategies including those related to people, platforms, data, internal controls (automated where possible), or legislative limitations. Agencies could participate in OMB or IG led assessments.

Develop a Counter Fraud Plan. Agencies could design, develop, train, and implement a plan for detecting and addressing programs and recipients at high risk for fraud and improper payments. This could involve identifying government resources and having a plan for collaboration. Agencies could seek incentives and develop tools, data sets, and validation methods for reducing incidents of fraud and improper payments.

---

21. Miskell, Renata, Future of Payment Integrity within the U.S. Federal Government, Chapter 12, Transforming the Business of Government, January 30, 2024.

Assess Grants and Contracts for Awardee Alignment with Fraud and Improper Payment Practices. Agencies could review existing agreements to determine if they support or impair proper management, and oversight practices. Data and reporting requirements could be required from awardees that meet established standards, verified through site visits. Through experience, agencies could then make appropriate language changes for the next cycles, and could justify and request OMB or statutory authorities if needed.

Collaborate with Others. Agencies could engage with oversight bodies and others in the design and development of effective practices, data systems, and training of staff on emergency funding preparation. This could drive having data sharing agreements in place and being prepared for case deconfliction, as well as capturing and building new data sources/ tools and supporting Treasury, IGs, Congress, and others. Justice and law enforcement agencies could identify ways to have cleansed and secure data to share with agencies involved in managing, detecting, investigating, and recovering fraudulent payments and improper payments related to fraud. Agencies could establish a structure to identify hidden fraud patterns both domestically and internationally.

Share Best Practices. Through OMB symposium or other means, agencies could share agency best practices with others that are proven to be effective—agencies could document, train, and provide profiles ready for adoption by others, and assist other agencies in their adoption and testing. Agencies could maintain a fraud risk catalog to facilitate fraud risk assessment.

Recommendations for State Program Actions

Develop Strong Fraud and Improper Payment Management Capacity. With federal funding and working with federal agencies, states could develop internal capacity to prevent detect, investigate, and recover fraudulently obtained funds or improper payments, and could develop fraud control plans. States could invest in data systems, staff development, and protocol development, utilizing DNP and other federal support. This could help states provide requested data to the federal government.

Acknowledgements

The individuals listed below generously offered their input and expertise. We greatly appreciate their contributions during the roundtable that informed this report. The contents of this paper do not necessarily reflect the views of any individual participants. Additionally, the views expressed by the participants and presented in this paper do not necessarily reflect positions of policies of government or other organizations.

ROUNDTABLE PARTICIPANTS

Alicia Cackley
U.S. GAO

Gary Cantrell
Deloitte

Lena Chang
Senate Homeland Security & Governmental
Affairs Committee

Dan Chenok
IBM Center for The Business of Government

Sheila Conley
U.S. Department of Health and Human Services

Isaiah Crisp
The Center for Organizational Excellence

Kaitlin Devine
HHS OIG

Maggie Frankel
U.S. Senate Subcommittee on Emerging Threats
& Spending Oversight Minority Staff

Terry Gerton
NAPA

Steve Goodrich
The Center for Organizational Excellence

Wilmer Graham
U.S. Department of Housing and Urban
Development

Deidre Harrison
Office of Federal Financial Management, OMB

Liz Hempowicz
Project On Government Oversight

Carter Hirschhorn
Senate Homeland Security & Governmental
Affairs Committee

Elizabeth Hocker
The Center for Organizational Excellence

Christian Hoehner
U.S. House, Committee on Oversight and
Accountability

Bill Hughes
CohnReznick

Ryan Kobb
IBM

Dave Lebryk
U.S. Department of Treasury, Departmental

Karen Lee
MITRE

Lauren Lombardo
House Committee on Oversight and Accountability

Dave Mader
Deloitte Consulting

Emily Manna
HSGAC Majority

Sean McPhilomy
The Center for Organizational Excellence

ROUNDTABLE PARTICIPANTS

Shelley Metzenbaum
The BETTER Project

Linda Miller
Audient Group, LLC

Renata Miskell
U.S. Treasury Department

Joe Mitchell
NAPA

Dawn Oliver
OMB

Jonathan Pasquale
IBM

Rebecca Shea
GAO

Sheldon Shoemaker
SBA OIG

Emily Vose
IBM

Bob Westbrooks
Gracie House LLC

Stephanie Winker
OMB

John Yee
U.S. GAO

About the Authors

Steve Goodrich
President and CEO
The Center for Organizational Excellence, Inc.

E: sgoodrich@center4oe.com
W: www.center4oe.com

Steve Goodrich has more than 40 years of leading organizations and advising top government and private sector leaders in organizational effectiveness strategies to improve performance and effectiveness. Steve's passion for excellence is the foundation for creating and guiding COE to serve the American people and care about our clients and staff.

Steve is routinely engaged in helping government leaders solve organizational effectiveness problems and developing supporting legislation and policy. He currently serves as Chairman of the Board of the federal Shared Services Coalition and was the co-founder and vice chair of the Government Transformation Initiative (GTI). He regularly appears at conferences, and in the media.

Steve began his career in education and then transitioned into consulting in the power generation industry. As a division director in a large technology solutions firm, he guided the integration of technology into the workplace. He has held senior leadership positions in small and large firms. He served on many government committees, roundtables, and engages in pro-bono support to our government. He was also the Chairman of the Board for the Association of Management Consulting Firms, and Renovating America. Steve has taught at the university level and serves on a number of corporate boards.

Steve holds a master's degree in industrial management from the University of Maryland and a bachelor's degree in education from Fitchburg State University.

Steve is also the author of countless articles, thought pieces, and three books all available on Amazon— *Transforming Government from Congress to the Cubicle*, *A Little Instruction Book for Congress*, and *A Little Instruction Book for Overcoming Racism and Prejudice*.

IBM Center for The Business of Government

Bob Westbrooks
Fellow, National Academy of
Public Administration

E: rawestbrooks@outlook.com
W: https://bobwestbrooks.com/

Bob Westbrooks is an attorney, certified public accountant, certified internal auditor, former federal investigator, and fraud and corruption risk expert. His work focuses on strengthening the capacity of U.S. and foreign public sector oversight organizations to provide independent, risk-based, data-driven insights for policymakers and the public.

Prior to leaving federal service in 2022, Bob spent 28 years in the oversight community, and served as an Inspector General prior to being designated as Executive Director of the Pandemic Response Accountability Committee at the beginning of the national pandemic emergency.

Bob previously served for five years as Inspector General of the Pension Benefit Guaranty Corporation where he helped protect the pensions of over 35 million American workers, and before that served as Deputy Inspector General at the U.S. Small Business Administration. Bob was elected chair of the Professional Development Committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and to the CIGIE Executive Council. As chair, Bob promoted leadership at all levels and led CIGIE-wide inclusion initiatives.

Bob is the author of *Left Holding the Bag: A Watchdog's Account of How Washington Fumbled its COVID Test*, about government accountability and transparency during the pandemic crisis, and is the author of a chapter on risk management ('Creating a Win-Win Relationship') for the 2019 book, *Public Sector Enterprise Risk Management*.

Recent Reports from the IBM Center for The Business of Government
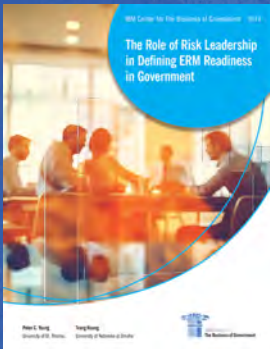
The Role of Risk Leadership in Defining ERM Readiness in Government

by Peter C and YoungTrang Hoang
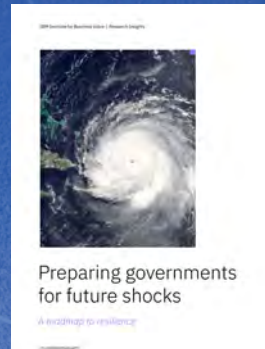
Managing the New Era of Deterrence and Warfare: Visualizing the Information Domain

by Chris Mihm

Opportunities for Management when Budgeting

by Steve Redburn

Building On Regulatory Foundations and Bridging to the Future
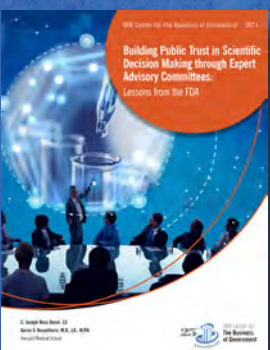
by Dan Chenok and Susan Dudley

AI and the Modern Tax Agency

by Caroline Bruckner and Collin Coil

Quantum Computing for Public Value: Insights from Australia

by Kevin C. Desouza and Dr. Samar Fatima

Building Public Trust in Scientific Decision Making through Expert Advisory Committees

by C. Joseph Ross Daval and Aaron S. Kesselheim

Improving Performance with Intergovernmental Grants - Lessons from the Continuum of Care Homeless Assistance Program

by J. Woody Stanley, Jordy Coutin, and Juliet Musso

For a full listing of our reports, visit www.businessofgovernment.org/reports

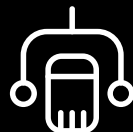# 25 YEARS CONNECTING RESEARCH TO PRACTICE

Five Easy Ways to Connect
businessofgovernment.org

Blog **Reports** **Interviews** **Magazine** **Books**

IBM Center Research Announcement

The IBM Center for The Business of Government connects research to practice, supporting work by scholars that benefits government through real-world experience and analysis. Our Center's reports are intended to spark the imagination—crafting new ways to think about government. We identify trends, new ideas, and best practices in public management and innovation.

We encourage applicants to review our research areas closely in selecting a topic, or a cross-cutting set of topics. We are looking for very practical findings and actionable recommendations—not just theory or concepts—in order to assist executives and managers to more effectively respond to mission and management challenges.

For more details on our latest proposal deadlines and application form, please visit: **https://www.businessofgovernment.org/content/research-stipends**.

We look forward to hearing from you!

**IBM Center for
The Business of Government**

Insights | Conversations | Information | Action

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, D.C. 20005
(202) 551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the
IBM Center on:.

IBM Center for
**The Business
of Government**