PANDEMIC RESPONSE ACCOUNTABILITY COMMITTEE

A Committee of the Council of the Inspectors General on Integrity and Efficiency

PandemicOversight.gov

Statement of Kenneth R. Dieffenbach
Executive Director, Pandemic Response Accountability Committee

before the

U.S. House of Representatives

Committee on Oversight and Government Reform
Subcommittee on Government Operations

concerning

"Shifting Gears: Moving from Recovery to Prevention of Improper Payments and Fraud"

March 11, 2025

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee:

Thank you for inviting me to testify at today's important hearing about the path forward in preventing fraud and other forms of improper payments and how improved data sharing can help in these efforts. Thanks in no small part to the Committee on Oversight and Government Reform, in March 2020, Congress created the Pandemic Response Accountability Committee (PRAC) as part of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act). I have served as the PRAC's Executive Director since July 2024 where I am privileged to work with a team of dedicated and talented federal employees and contractors. Prior to this role, I spent over 28 years fighting fraud as a law enforcement agent at multiple federal agencies, with a specific focus on federal grant fraud.

With your support, the PRAC is promoting transparency, supporting and coordinating independent oversight of pandemic relief spending, and using advanced data analytics to hold wrongdoers accountable. PRAC Chair Michael E. Horowitz testified in September 2024 before this Subcommittee to highlight systemic weaknesses that if addressed can help save taxpayer dollars from fraud losses. We applaud the Subcommittee's bipartisan commitment to these issues and efforts to identify solutions that can reduce improper payments and fraud. I look forward to continuing that conversation in today's hearing and updating the Subcommittee on the PRAC's progress to date in fraud prevention, detection, and mitigation. Since 2020, we and our partner Inspectors General have alerted agency leadership to potential risks and emerging fraud schemes, investigated thousands of pandemic fraud-related cases, and used data to identify potential fraud and other forms of improper payments more quickly.

The PRAC and our data analytics center are scheduled to sunset on September 30, 2025. In early 2021, Congress provided $40 million in funding to the PRAC to create and operate a data analytics center through Fiscal Year 2025. Congress also gave the PRAC direct hiring authority so we could hire the outstanding data analysts, data scientists, and IT professionals needed to develop and lead an analytics effort. This support from Congress was instrumental in the PRAC's development of our data analytics center, which has proven to be extraordinarily successful in identifying fraud in pandemic relief programs. It has also resulted in recoveries for the taxpayers that far exceed the $40 million that Congress appropriated for us to operate it.

Unfortunately, this fraud-fighting tool, which can and should be expanded to help prevent improper payments in high-risk programs across federal agencies, is instead in danger of disappearing entirely when the PRAC reaches its mandated sunset date on September 30, 2025. The U.S. Government Accountability Office (GAO) stated in their most recent open recommendations report, after noting the

PRAC's sunset date in September 2025, "We recommended that Congress establish a permanent analytic center of excellence to aid the oversight community in identifying improper payments and fraud. We estimate that this could result in a **billion or more** annually in financial benefits." (emphasis added).

One of the themes of this hearing is discussing what more agencies can do to improve program integrity and eliminate improper payments at the front end. We believe your efforts to shift the conversation to fraud prevention and raise awareness of these issues go hand in hand with extending the PRAC and encouraging and requiring agencies to work with the PRAC. That way, agencies have the external support and analytical tools needed to identify and prevent fraudulent payments before money goes out the door. I hope my testimony today will demonstrate the need for the PRAC's cross-agency analytics capability focused on prevention, early detection, investigative support, and program integrity improvements, and how it could be used to better protect taxpayer dollars. When considering the broad topic of fraud prevention, the PRAC is focused on four key issues: the fraud landscape, incentives, risk assessments, and the role of enhanced data sharing and data analytics.

1. *Understanding the Fraud Landscape*

First, the fraud risk landscape is always evolving, and agencies and oversight bodies must keep pace. For example, the government has dramatically reduced the barriers to obtaining public benefits. While this can be a positive step for citizens in need of support, this has also opened a virtual door for fraudsters. As we saw with pandemic-era programs, anyone with a computer can apply for federal benefits from literally any or all the 56 states and territories from anywhere in the world. For example, in a February 22, 2021, memo, the Department of Labor Office of Inspector General (OIG) identified that one Social Security Number (SSN) was used in 40 states in an attempt to gain unemployment benefits—a type of scheme that was virtually impossible to commit or detect a decade ago. The federal government must work with the states to improve data sharing to address these new and ever-changing threats to program integrity. We have reported on these threats and challenges in staffing and antiquated IT systems in our oversight work on the unemployment insurance program.

In response to the widespread fraud that occurred in pandemic relief programs, the PRAC moved quickly to establish our data analytics center to help us identify anomalies in millions of applications and transactions. Through our innovative data analytics tools, we have flagged weaknesses in programs that led to payments made to applications associated with foreign IP addresses, deceased individuals, individuals under the age of 10, individuals over the age of 110, and more. We've uncovered schemes used by fraudsters to evade program controls, such as "floating dot" email, the use of commercial mail receiving addresses, and falsified supporting documents. Using a central data analytics platform has allowed us to connect seemingly unconnected bad actors, find "multi-dippers" (those who use the same identifiers across multiple programs), applicants who fabricated the formation date of their businesses, applicants who misrepresented their income to different programs, and lenders who conducted poor due diligence.

As one example, using advanced network analytics and information from some of our more than 60 major data sources, the PRAC proactively identified numerous hidden connections and other anomalies in Small Business Administration (SBA) pandemic loan applications. Working with our partner Inspectors General, we identified a criminal fraud conspiracy that involved multiple members of the same family who submitted over 100 Paycheck Protection Program (PPP) and COVID -19 Economic Injury Disaster Loan (EIDL) applications involving over 50 related businesses. To date, six individuals have been convicted and ordered to pay a total of over $1.6 million in restitution.

2. *Incentivizing Fraud Prevention*

Second, while we all know that "pay and chase" is a losing game, it is important to consider if we have the right incentives in place to encourage federal and state government agencies to prioritize prevention of fraud and other types of improper payments. For example, are program implementors required to follow through on risk mitigation plans, including the use of a data analytics function like the PRAC offers to identify potentially fraudulent applications, and to own and document the risks they have chosen to accept? In our Blueprint for Enhanced Program Integrity (Blueprint), the PRAC extensively documented lessons learned and best practices to help strengthen federal programs and protect them from fraud. One of the many highlights in the Blueprint is that we must "Prepare for the Next Disaster Now."

Additionally, a critically important factor, and perhaps the most difficult to address, is culture and "tone at the top." As the PRAC and member OIGs have repeatedly raised in our work, fraud prevention must be considered part of an agency's core mission. Does the average grant or contract manager believe that finding fraud or preventing fraud in their program is good for their career or organization? Does the agency culture encourage or discourage that behavior? What message are senior leaders sending? Have agency officials struck the right balance between pre-award due diligence and getting funds obligated to meet timeliness metrics?

3. *Requiring Agencies to Conduct Risk Assessments*

Third, every effort related to preventing fraud must begin with a robust risk assessment process. GAO, OIGs, and the PRAC have all reported on the need to assess and accept risk on the front end. This process must include ongoing collaboration with state and regional government stakeholders, who manage over 80% of federal grant dollars and fraud awareness training for front line program staff. Finally, a dialogue at senior levels in forums such as the PRAC-initiated Gold Standard meetings involving the program agency, OIG, and Office of Management and Budget leadership can identify and address program weaknesses, before program implementation.

According to the Federal Program Inventory, in Fiscal Year 2024 there were over 2,600 federal programs with a total of $7 trillion in expenditures. Each of these programs requires a tailored risk assessment and targeted controls to mitigate the most harmful or costly risks of each distinct program. Each program might require access to different data sets and different types of analytic tools. The PRAC's data analytics center can provide analytic tools and solutions custom to the needs of different programs for agencies or OIGs.

4. *Understanding the Fraud-Fighting Benefits of Enhanced Data Sharing and Data Analytics*

Fourth, enhanced data sharing and a centralized data platform allows for greater visibility and improved opportunities to prevent fraud before money is disbursed. Thanks in part to the special authorities granted by Congress, the PRAC has been at the forefront of responsible and effective data sharing and analysis to identify hidden patterns, networks, and other anomalies among program applications and payment transactions.

This type of analysis is most effective with timely access to as much relevant data as possible. To help address fraud risks that could impact more than one state or territory, relevant data must be collected and shared by states and territories about who applied for and received federal funds. This level of visibility across the landscape can detect hidden patterns and serve as an early warning system for emerging schemes and new criminal enterprises.

The PRAC has access to over 60 major data sources and over a billion data points, including 127,000 known fraud cases, over 15 million potentially compromised internet protocol addresses, emails, banking data, street addresses, Social Security Numbers, Employer Identification Numbers, and law enforcement sensitive data related to known or suspected fraud schemes. This data could be used to flag future applications or payments that are associated with any of these same attributes. We have also built crucial relationships and over 120 data sharing arrangements to enhance our capabilities, including with the Social Security Administration (SSA), partner OIGs, and the Department of Justice's National Unemployment Insurance Fraud Task Force and COVID-19 Fraud Enforcement Task Force.

If Congress authorizes an extension, the PRAC can also continue to support law enforcement efforts to investigate fraud as we have done to date related to over 1,000 investigations with 23,000 subjects under investigation with a potential fraud loss of over $2.4 billion.

Enhanced data sharing and analytics makes the investigative process more effective and efficient. For example, if an OIG is investigating a fraud allegation related to research grant dollars, absent a centralized platform, their staff must engage in a manual process to determine what other agencies might have funded that entity or if the funded program overlaps with other federal funding; the OIG must then manually check with as many as a dozen or more other investigative agencies to determine if other complaints or ongoing investigations exist. More problematic is that without a centralized system, hidden connections between different fraud schemes and bad actors might never be detected since things like shared bank accounts, email addresses, phone numbers, and other unique characteristics are virtually impossible to flag manually.

If authorized, PRAC data and methodologies could be used to address a wide range of fraud risks, across a wide swath of federal programs—beyond pandemic funding. For instance, in federal grant programs the PRAC could develop tailored approaches to flag individuals or entities that unqualified for a particular program, applicants using stolen or synthetic identifiers, recipients failing to comply with award terms and conditions, undisclosed organizational and personal conflicts of interest—including undisclosed foreign connections and theft of intellectual property, data, or other assets.

The government can dramatically change the way we address fraud risks by sustaining the approach the PRAC has built, with responsible data sharing, especially across state lines, and subsequent data analysis, built on a solid foundation of data privacy and cybersecurity. Artificial intelligence, machine learning, and other tools allows us to examine, assess, and compare millions of pieces of information virtually in real-time to stay ahead of the evolving risks and gain insights never before possible. This approach helps the government eliminate program integrity blind spots, bolster controls, prevent awards before money is disbursed, and enhance the efficiency and effectiveness of programs and federal oversight.

Enhanced data sharing also allows for the development of risk dashboards which consolidate key data in one place and can automatically analyze high volumes of data for specific red flags, a task that is virtually impossible without these tools. For example, the PRAC built a risk dashboard for the U.S. Department of Treasury OIG which assigned over 80,000 Coronavirus Relief Fund state and local recipients a risk score allowing for more targeted oversight. The OIG used this information to select which entities to desk audit; these audits subsequently identified $2.2 billion in questioned costs. In another instance, the PRAC worked with the Pension Benefit Guaranty Corporation OIG to ingest 10 years of data related to some 2,400 pension plans that had applied for benefits. This risk model flagged numerous applications for follow-up and this effort ultimately led the OIG and the Department of Justice to recover over $165 million in civil settlements. New data is uploaded to these risk models to generate updated risk scores almost instantaneously.

Challenges to consider with enhanced data sharing, especially across state lines, include privacy and cybersecurity. These can be partially addressed with strict adherence to relevant laws and best practices, as well as the use of data minimization principles, such as "Yes/No" validation methods. In this approach, one party shares data with a second party and the second party responds with 'Yes" or "No" to specific questions rather than returning large volumes of sensitive data. The PRAC has successfully used this method in several matches with the SSA, one of which resulted in a Fraud Alert that identified as much as $5.4 billion in potentially fraudulent pandemic loans obtained using over 69,000 questionable Social Security Numbers.

Other federal systems, including Do Not Pay, have not been provided with the investigative authority that the CARES Act provides to the PRAC, and therefore are limited in their ability to hold or use law-enforcement sensitive data that the PRAC is permitted to use for identification of potential improper payments and fraud. Further, the PRAC and OIGs have an exemption to the Computer Matching Act, which Congress provided OIGs in 2016 to enable them to protect taxpayer funds by sharing agency data and then matching that data to identify potential anomalies that may indicate fraud or other types of improper payments.

As we move beyond the pandemic, the focus of the PRAC and its data analytics center should be expanded to prevent and detect fraud and improper payments in all federal government programs, especially those administered by states and territories. We believe the broadened approach should also allow federal agencies, in coordination with their OIG, to utilize the data analytics tools to screen applicants for benefit programs by conducting pre-award and pre-payment checks that will help ensure funding goes to individuals it was intended to help.

Prevention on the front end will reduce the need for resource-intensive investigations and typically ineffective attempts at recovering lost funds. "Pay and chase" does not work. The sustainment and expansion of the PRAC and its capabilities will ultimately ensure that our federal government is better equipped to prevent and mitigate fraud risks in future emergency relief spending as well as regular annual federal government spending.

We look forward to working with the Subcommittee to ensure the oversight community maintains a capability to engage in cutting-edge cross agency analytics to prevent fraud and other types of improper payments, and to improve program integrity.

Thank you again for your continued strong support of the PRAC, the Inspector General community, and independent oversight. That concludes my prepared remarks, and I look forward to your questions.