United States Government Accountability Office

Report to the Chairman,
Special Committee on Aging,
U.S. Senate

November 2026

MEDICARE
HHS and CMS Should Better Manage Fraud Risks

GAO-27-109072

GAO Highlights

MEDICARE

HHS and CMS Should Better Manage Fraud Risks

GAO-27-109072 November 2026

A report to the Chairman of the Special Committee on Aging, U.S. Senate

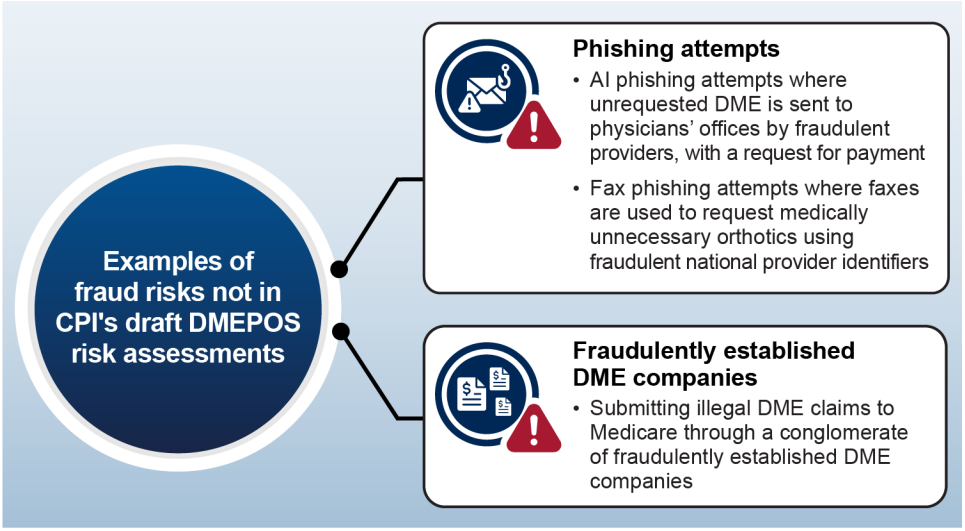
Contact: Seto J. Bagdoyan at BagdoyanS@gao.gov

What GAO Found

The Centers for Medicare & Medicaid Services (CMS)—within the Department of Health and Human Services (HHS)—and its various contractors oversee the traditional Medicare Fee-for-Service program (Medicare). CMS reported spending nearly $481 billion on benefits for about 34 million Medicare beneficiaries in 2025.

CMS uses the Vulnerability Management (VM) Process within the Center for Program Integrity (CPI) to manage fraud risks. However, this process is broader in scope and does not fully reflect the range of fraud risks facing Medicare. Without fully identifying and assessing fraud risks consistent with leading fraud risk management practices, CPI is missing opportunities to fully mitigate fraud risks before they materialize into significant fraud in Medicare. As shown below, based on its review of Inspector General reports, GAO identified fraud risks affecting Medicare that CPI did not identify or assess as part of its VM Process.

Fraud Risks That CPI Did Not Identity or Assess in Its Risk Assessment



CPI - Center for Program Integrity
DME - Durable medical equipment
DMEPOS - Durable medical equipment, prosthetics, orthotics, and supplies

Sources: GAO analysis of interviews and documents from the Department of Health and Human Services' Office of Inspector General and CPI; Icons-Studio/stock.adobe.com (icons). | GAO-27-109072

Further, CPI's VM Process does not align with other leading practices that would help it strategically manage Medicare fraud risks. Specifically, the VM Process does not include an assessment of the likelihood and impact of fraud risks or examine the suitability of existing mitigating fraud controls for Medicare. For example, CPI identified a vulnerability associated with the supplier enrollment screening process, which GAO identified as a significant fraud risk, given its association with cases of alleged Medicare fraud. However, CPI's risk assessment did not assess the likelihood and impact of this vulnerability as a fraud risk. Without including such an assessment, CPI risks overlooking the full scope and impact of fraud risks.

Why GAO Did This Study

Medicare is the largest federal health program. The Medicare program was first included in GAO's High Risk List in 1990 and remains on the list due to its size, complexity, effect on the federal budget and health care sector, and continued susceptibility to fraud, mismanagement, and improper payments. GAO was asked to review HHS's efforts to prevent and minimize fraud in Medicare. This report evaluates, among other things, the extent to which HHS has assessed fraud risks in Medicare.

GAO reviewed documentation related to risk assessments for Medicare and related guidance. GAO also analyzed HHS Inspector General reports, federal court documents, and interviews from various contractors to identify Medicare fraud risks. GAO interviewed and reviewed information reported from HHS's Office of the Assistant Secretary for Financial Resources, CMS, and CPI. GAO compared this information against relevant leading practices from GAO's Fraud Risk Framework and internal control requirements.

What GAO Recommends

GAO is making four recommendations to HHS, including that it update and finalize risk management guidance to include designing and regularly performing comprehensive fraud risk assessments consistent with leading practices and internal control requirements. HHS agreed with three recommendations and did not agree with one recommendation. GAO maintains that all four recommendations remain valid, as discussed in the report.

Contents

Letter 1

Background 4
HHS Has Dedicated Entities to Lead Fraud Risk Management for Medicare, but Their Effectiveness Is Hindered 9
CMS Has Taken Some Steps to Assess Medicare Fraud Risks, but Efforts Are Not Fully Consistent with Leading Practices and Internal Control Requirements 14
Conclusions 27
Recommendations for Executive Action 28
Agency Comments and Our Evaluation 29

Appendix I List of 31 Medicare Risk Assessment Topic Areas Identified by the Center for Program Integrity (CPI) 34

Appendix II Comments from the U.S. Department of Health and Human Services 36

Appendix III GAO Contact and Staff Acknowledgments 43

Table

Table 1: The Center for Program Integrity (CPI) Has Started 10 out of 31 Risk Assessment Topic Areas Since 2022 for Medicare 34

Figures

Figure 1: Department of Health and Human Service's (HHS) Oversight Structure for Medicare Fraud Risk Management 5
Figure 2: Illustrative Example of Medicare Fraud Case 6
Figure 3: The Four Components of the Fraud Risk Framework and Leading Practices 8
Figure 4: Overview of the Center for Program Integrity's (CPI) Vulnerability Management Process 12

Figure 5: Example of Incomplete Current and Planned Mitigation Controls in the Center for Program Integrity (CPI) 2025 Draft Vulnerability Summary 16
Figure 6: The Center for Program Integrity's (CPI) Vulnerability Management Process Excludes a Suitability Examination of Existing Controls 20
Figure 7: Five DMEPOS Cross-Cutting Risk Factors Identified by the Center for Program Integrity (CPI) 23
Figure 8. Examples of DMEPOS Fraud Risks Not in the Center for Program Integrity's (CPI) 2024 DMEPOS Draft Risk Assessment 25
Figure 9: Example of a Fraud Risk Opportunity Where a DMEPOS Owner and Manager Allegedly Circumvented the Center for Program Integrity's (CPI) Supplier Screening Process 26

Abbreviations

ASFR	Office of the Assistant Secretary for Financial Resources
CMS	Centers for Medicare & Medicaid Services
CPI	Center for Program Integrity
DOJ	U.S. Department of Justice
DME	durable medical equipment
DMEPOS	durable medical equipment, prosthetics, orthotics, and supplies
FPS	Fraud Prevention System
FRAP	Fraud Risk Assessment Portal
Fraud Risk Framework	*A Framework for Managing Fraud Risks in Federal Programs*
HHS	U.S. Department of Health and Human Services
OIG	Office of Inspector General
OMB	Office of Management and Budget
UPIC	Unified Program Integrity Contractor
VM	Vulnerability Management

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

November 18, 2026

The Honorable Rick Scott
Chairman
Special Committee on Aging
United States Senate

Medicare is the largest federal health program by expenditure, significantly affecting the entire health care sector. Over the next decade, spending is expected to increase significantly as the U.S. population ages and more individuals receive Medicare benefits. The U.S. Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services' (CMS) Center for Program Integrity (CPI), and its various other components and contractors, are responsible for overseeing the Medicare program.

Medicare generally makes payments directly to health care providers, such as hospitals, physicians, and suppliers for durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS).[1] These Fee-for-Service payments are based on medical claims submitted for services that are rendered to beneficiaries. CMS reported having spent nearly $481 billion in Medicare benefits for about 34 million Medicare beneficiaries in calendar year 2025.[2]

Medicare was first included in GAO's High Risk List in 1990. It remains on the list due to its size, complexity, effect on the federal budget and health care sector, and continued susceptibility to fraud, mismanagement, and improper payments.[3] The sheer amount of payments in the Medicare program creates significant fraud risks. Our extensive reporting since

[1]This report focuses on the traditional Medicare Fee-for-Service program, which covers Parts A and B of the Medicare program. Other Medicare programs were not part of our review, including the Medicare Advantage or Prescription Drug programs. For this report, we refer to traditional Medicare (Parts A and B) as Medicare.

[2]*2026 Annual Report of the Boards of Trustees of the Federal Hospital Insurance and Federal Supplementary Medical Insurance Trust Funds* (Washington, D.C.: 2026).

[3]GAO's High Risk List is a listing of federal programs and operations with serious vulnerabilities to fraud, waste, abuse, mismanagement, or need for transformation. GAO, *Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness,* GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

1990 has reflected the persistent challenges that CMS has faced in managing program integrity risks, including those related to fraud.[4]

Recent Medicare fraud cases reported by the U.S. Department of Justice (DOJ) and HHS's Office of Inspector General (OIG) demonstrate that Medicare continues to face significant threats from fraudsters. For example, in June 2025, DOJ announced charges against dozens of individuals, alleging that they schemed the Medicare program by fraudulently billing over $10 billion for DMEPOS that beneficiaries never requested, received, or needed.[5] In addition, in July 2026, HHS OIG reported that its investigations led to a company's chief executive officer being sentenced to 15 years in prison and ordered to pay $452 million in restitution for fraudulently running a billion-dollar Medicare scheme involving telemedicine and durable medical equipment.[6]

Managers of federal programs, like Medicare, are responsible for managing fraud risks and implementing leading practices for combating those risks. Effectively managing fraud risks helps to ensure that federal programs' services fulfill their intended purpose, that funds are spent effectively and efficiently, and that program assets are safeguarded. In July 2015, we issued A *Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework). The Fraud Risk Framework provides a comprehensive set of leading practices that serve as a guide for agency managers to use when developing efforts to combat fraud in a strategic, risk-based way.[7]

[4]See for example, GAO, *Medicare and Medicaid: Additional Actions Needed to Enhance Program Integrity and Save Billions,* GAO-24-107487 (Washington, D.C.: Apr. 16, 2024); *Medicare: CMS Needs to Address Risks Posed by Provider Enrollment Waivers and Flexibilities,* GAO-23-105494 (Washington, D.C.: Dec. 19, 2022); and *Medicare and Medicaid: CMS Needs to Fully Align Its Antifraud Efforts with the Fraud Risk Framework,* GAO-18-88 (Washington, D.C.: Dec. 5, 2017).

[5]U.S. Department of Justice, Press Release, *National Health Care Fraud Takedown Results in 324 Defendants Charged in Connection with Over $14.6 Billion in Alleged Fraud* (June 30, 2025).

[6]HHS OIG continues to prioritize Medicare for fraud investigations. U.S. Department of Health and Human Services, Office of Inspector General, *Spring 2026 Semiannual Report to Congress* (Washington, D.C.: July 10, 2026).

[7]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015). For this report, we refer to this as the "Fraud Risk Framework."

You asked us to review HHS's efforts to prevent and minimize fraud in Medicare. This report evaluates the extent to which HHS has (1) established an organizational structure with a dedicated antifraud entity to lead, oversee, coordinate, and communicate fraud risk management activities for Medicare; and (2) assessed fraud risks in Medicare.

To address our first objective, we reviewed guidance and information reported from HHS's Office of the Assistant Secretary for Financial Resources (ASFR), CMS, and CPI and interviewed officials from these agencies and reviewed their written responses. We compared this information against selected leading practices under the first overarching concept in the Fraud Risk Framework.[8] Specifically, we selected leading practices that were most relevant to our objectives and that represent key steps in creating a structure with a dedicated entity to lead fraud risk management activities. We also compared the information reviewed with requirements in the Standards for Internal *Control in the Federal Government* for communicating relevant internal control information internally and externally.[9] Additionally, we compared this information with HHS's draft 2021 Fraud Risk Management Implementation Plan.[10]

To address the second objective, we reviewed documentation related to the extent HHS has planned regular fraud risk assessments and identified and assessed fraud risks in Medicare. We also interviewed officials within CMS, CPI, and ASFR. We compared their responses and the information

[8]We selected leading fraud risk management practices under the commit component of the Fraud Risk Framework that were most relevant to this audit objective. The commit component represents key steps in creating a structure with a dedicated entity to lead fraud risk management activities and hold employees and external entities accountable for their duties and activities for managing fraud risks. GAO-15-593SP.

[9]GAO, *Standards for Internal Control in the Federal Government*, GAO-25-107721 (Washington, D.C.: May 15, 2025).

[10]As discussed in more detail below, HHS tasked its ASFR to lead and oversee the implementation of HHS's Fraud Risk Management Implementation Plan and ensure that all divisions, including CMS, which oversees CPI, are also implementing this plan. This plan requires coordination and communication between ASFR and all HHS divisions about their fraud risks and fraud risk management efforts. As of July 2026, the Fraud Risk Management Implementation Plan was being updated in response to a recommendation that we made in January 2025. In October 2026, ASFR told us that its current efforts include maturing department-wide fraud risk management policies, issuing supplemental fraud risk assessment guidance, and expanding the use of HHS's Fraud Risk Assessment Portal (FRAP) to identify trends and control gaps. ASFR expects these efforts and any changes to its Fraud Risk Management Implementation Plan to be part of a larger rollout strategy under ASFR's Anti-Fraud Governance Program, which it does not expect to be fully finalized before fiscal year 2027.

received with selected leading practices under the second component in the Fraud Risk Framework. This second component relates to planning regular fraud risk assessments and identifying and assessing fraud risks to determine a program's fraud risk profile.[11] Further, we compared this information with related requirements in the Standards for Internal *Control in the Federal Government* and in the Office of Management and Budget's (OMB) guidance for Management's Responsibility for Internal Control, as it pertains to performing and documenting fraud risk assessments.[12] In addition, we conducted our own analysis to identify fraud risks in Medicare by reviewing HHS OIG reports, court documents from ongoing and adjudicated federal court cases, and interviews with various contractors.

We conducted this performance audit from March 2026 through November 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

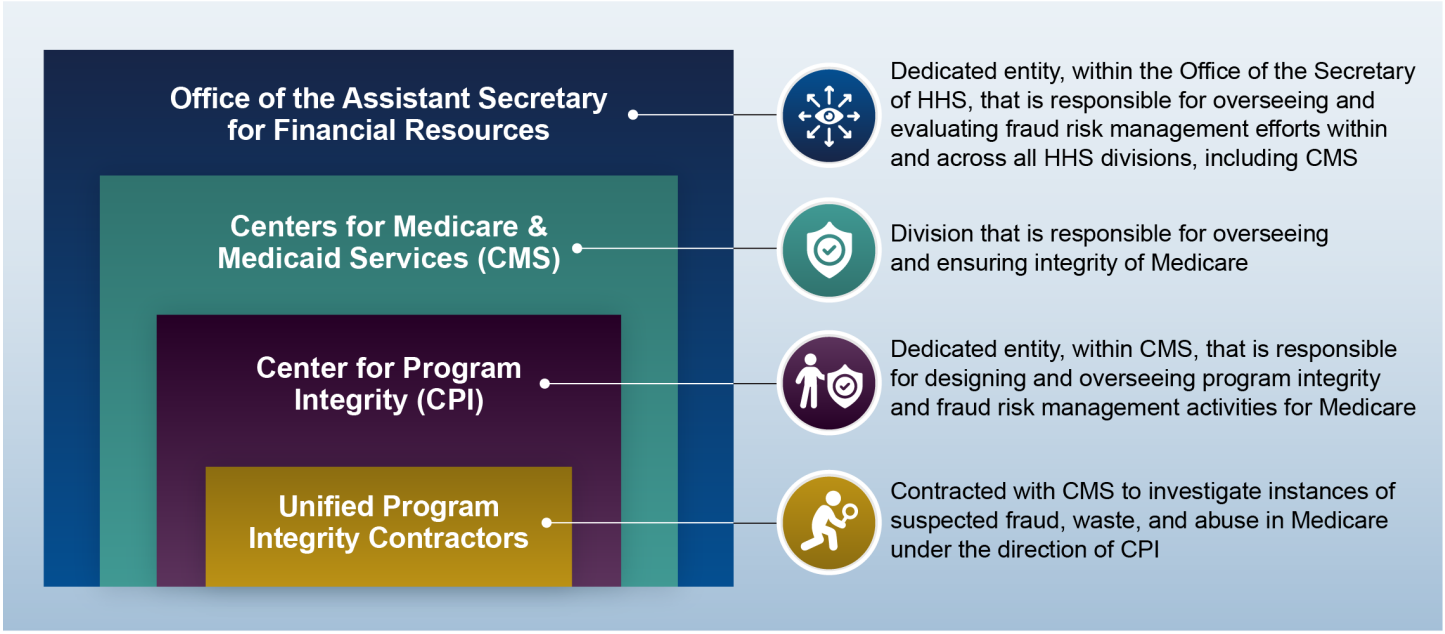
HHS's Fraud Risk Management Structure

Several entities have responsibilities for fraud risk management at HHS. See figure 1 for HHS's fraud risk management structure for Medicare.

[11]We selected leading fraud risk management practices under the assess component of the Fraud Risk Framework that were most relevant to this audit objective. This assess component represents key steps in identifying and assessing fraud risks, which are foundational to effectively and efficiently managing fraud risks. GAO-15-593SP.

[12]GAO-25-107721; and Office of Management and Budget, *Circular No. A-123: Management's Responsibility for Internal Control* (Washington, D.C.: Mar. 10, 2026)

Figure 1: Department of Health and Human Service's (HHS) Oversight Structure for Medicare Fraud Risk Management



Sources: GAO analysis of HHS documentation, HHS Office of Inspector General reports, and GAO reports; Icons-Studio/stock.adobe.com (icons). | GAO-27-109072

HHS's ASFR is the entity dedicated to overseeing the fraud risk management efforts for, and across, all HHS divisions, including CMS. CMS is a component of HHS and is responsible for ensuring the integrity of the Medicare program, including preventing and mitigating fraud. Specifically, within CMS, CPI is the entity dedicated to serving as the focal point for the prevention and detection of all national and state-wide fraud and abuse issues in the Medicare program.[13] As such, CPI is responsible for ensuring that correct payments are made to legitimate providers for covered, appropriate, and reasonable services for eligible beneficiaries in the program. Under the direction of CPI, Unified Program Integrity Contractors (UPIC) perform integrity functions for the Medicare program. This primarily includes investigating instances of suspected fraud, waste, and abuse in Medicare claims. The UPICs develop investigations and take action to ensure that Medicare Trust Fund funds

[13]The President's 2027 budget request for CMS included $127.7 million in discretionary spending for fiscal year 2027 to, among other things, support Medicare's program integrity efforts, including fraud risk assessments to support CMS's vulnerabilities management process for Medicare. See U.S. Department of Health and Human Services, Centers for Medicare & Medicaid Services: *FY 2027 Congressional Justification: Justification of Estimates for Appropriations Committees* (Washington, D.C.: 2026).

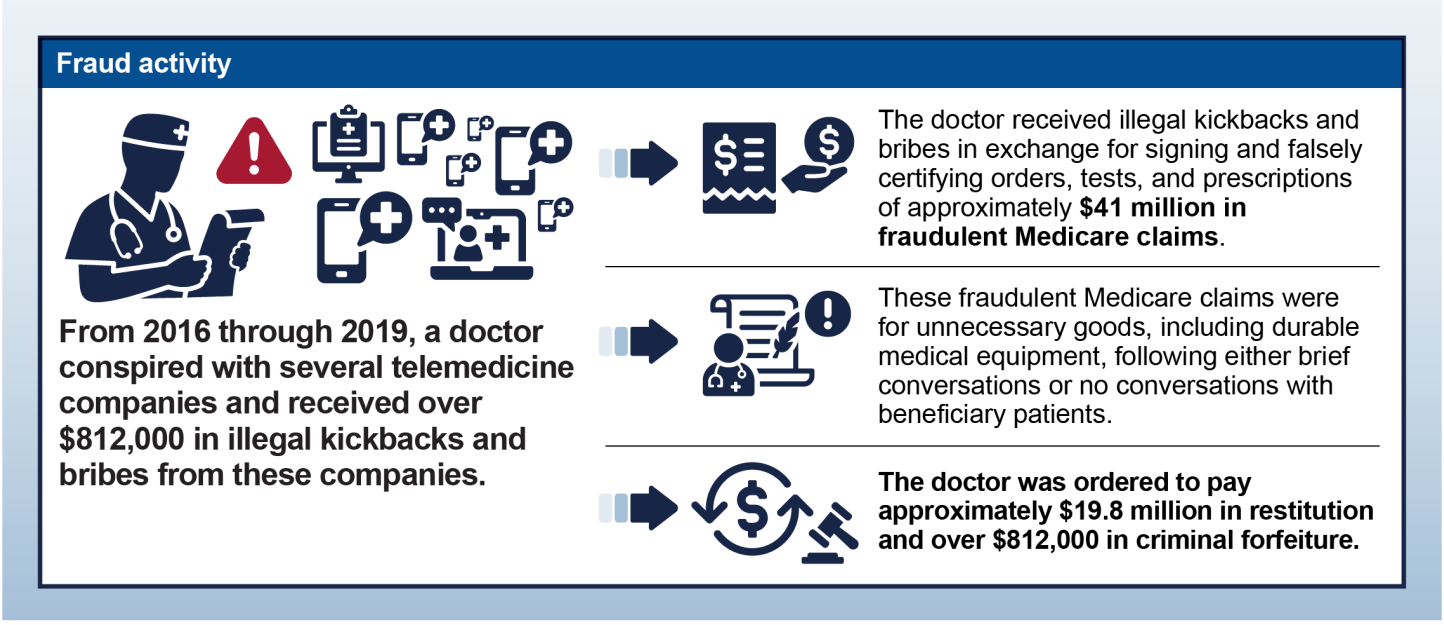
are not inappropriately paid. They also identify any improper payments that are to be recouped by CPI.

Fraud and Improper Payments

Fraud is obtaining something of value through willful misrepresentation. It is characterized by making materially false statements of fact based on actual knowledge, deliberate ignorance, or reckless disregard of falsity. Fraud can involve benefits that do not result in direct financial loss to the government. Whether an act is, in fact, fraud is a determination that is made through the judicial or other adjudicative system.[14]

Medicare fraud may take several forms. This includes fraudulent billing for services or items not provided, providing or supplying services or items that were not medically necessary, and intentionally billing services at a higher payment level than provided or appropriate. In some instances, Medicare fraud can also involve providing compensation—kickbacks—to providers, beneficiaries, or others for participating in the fraud. See figure 2 for an illustrative example of a Medicare fraud case.

Figure 2: Illustrative Example of Medicare Fraud Case



Sources: GAO analysis of Department of Justice press release and court documents; Icons-Studio/stock.adobe.com (icons). | GAO-27-109072

[14]GAO-15-593SP.

Fraud Risk Management

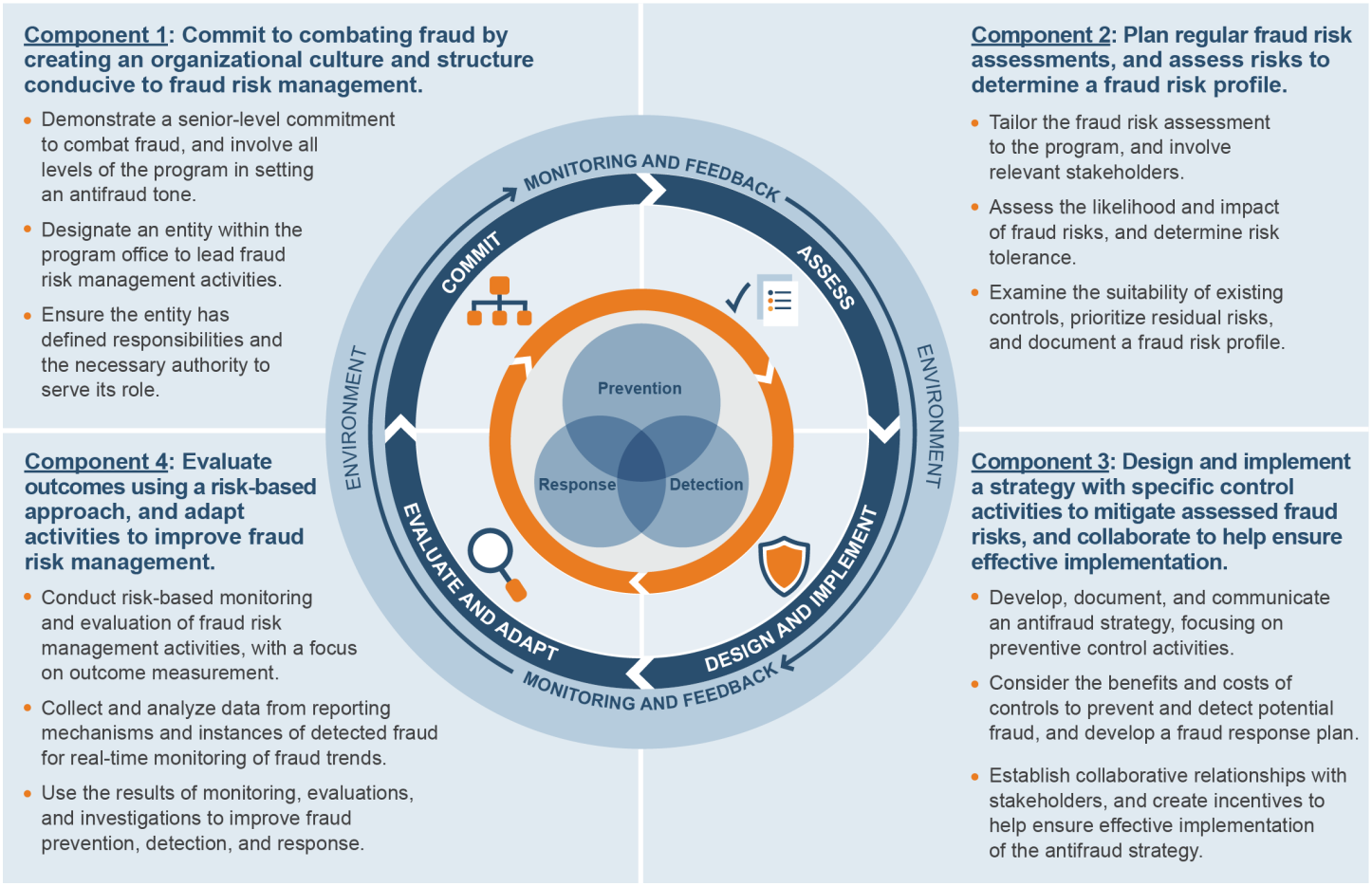
The objective of fraud risk management is to ensure program integrity by continuously and strategically mitigating both the likelihood and the impact of fraud. Effectively managing fraud risks helps to ensure that federal programs' services fulfill their intended purpose, that funds are spent effectively and efficiently, and that assets are safeguarded. Fraud risk (which is a function of likelihood and impact) exists when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or can rationalize committing fraud. A fraud risk can exist even if actual fraud has not yet been identified or occurred. The existence of fraud risks does not necessarily indicate that actual fraud exists or will occur. However, fraud risks are often present when fraud does occur. Although the occurrence of fraud indicates there is a fraud risk, a fraud risk can exist, even if actual fraud has not yet been identified or occurred.

Federal agency managers are responsible for managing fraud risks and implementing practices for combating those fraud risks. This includes using fraud risk assessments to clearly assess fraud risks identified through data analytics and other sources or internal control mechanisms and establishing collaborative relationships with other relevant agencies to communicate relevant fraud risk management information.

The Fraud Risk Framework provides a comprehensive set of key components, overarching concepts, and leading practices that guide agency managers when developing activities to combat fraud in a strategic, risk-based manner.[15] As depicted in figure 3, the Fraud Risk Framework describes leading practices within four components: (1) commit, (2) assess, (3) design and implement, and (4) evaluate and adapt.

[15]GAO-15-593SP.

Figure 3: The Four Components of the Fraud Risk Framework and Leading Practices



Source: GAO. | GAO-27-109072

The Fraud Risk Framework acknowledges that agencies may incorporate fraud risk management activities into other risk management initiatives to manage fraud risks. That, however, does not eliminate the need for separate and independent fraud risk management efforts, in a complementary manner.[16] Agencies that effectively manage fraud risks demonstrate a senior-level commitment to integrity and combating fraud. Establishing an organizational structure with a designated antifraud entity

[16]GAO-15-593SP; and GAO, *Federal Employees Health Benefits Program: OPM Should Take Timely Action to Mitigate Persistent Fraud Risks*, GAO-25-106885 (Washington, D.C.: July 17, 2025).

to design and oversee the fraud risk assessment process is integral to fraud risk management.

In 2016, Congress enacted the Fraud Reduction and Data Analytics Act of 2015. This act required OMB to establish guidelines for federal agencies to create controls to identify and assess fraud risks and to design and implement antifraud control activities. The act further required OMB to incorporate the leading practices from the Fraud Risk Framework in these guidelines. The act was repealed and replaced in 2020 by the Payment Integrity Information Act of 2019, which required these guidelines to remain in effect.[17]

In its 2026 Circular No. A-123, OMB states that "fraud is a risk that all agencies must consider." The circular further establishes that agencies are to have "internal controls … that support the achievement of mission objectives by mitigating the likelihood and impact to risks, including fraud." According to Circular No. A-123, all levels of an agency are responsible for identifying and evaluating fraud risks and internal controls, and their risk assessments should include the consideration of vulnerabilities to fraud. This includes assessing the likelihood and significance of potential fraud scenarios, including monetary and nonmonetary fraud. The circular further explains that agencies should identify where fraud risk is most likely to occur and ensure that fraud risk is considered when setting risk tolerances and determining appropriate responses to identified risks.

HHS Has Dedicated Entities to Lead Fraud Risk Management for Medicare, but Their Effectiveness Is Hindered

The Fraud Risk Framework calls for dedicated antifraud entities to design and oversee fraud risk management activities. In that role, the entities should serve as the repository of knowledge on fraud risks and antifraud controls. They may also facilitate communicating such information to stakeholders.[18] Further, the Standards for Internal *Control in the Federal Government* require agencies to communicate relevant information internally and externally and to document policies and procedures that explain what implemented actions are expected to help mitigate risks to an agency's objectives to acceptable levels.[19]

[17]Pub. L. No. 116-117, 134 Stat. 113 (codified at 31 U.S.C. §§ 3351-58).

[18]GAO-15-593SP.

[19]GAO-25-107721.

Consistent with leading practices, HHS has multiple entities dedicated to mitigating fraud risks across the department and its various programs, including Medicare. In 2016, HHS designated ASFR as the department-wide entity leading the oversight and evaluation of all programs' fraud risk management work, including Medicare within CMS.

As explained in HHS's draft May 2021 Fraud Risk Management Implementation Plan, ASFR, as the dedicated entity, is responsible for leading HHS's efforts to establish and maintain proper internal control over reporting and ensuring that requirements are met under OMB *Circular No. A–123*. ASFR is also responsible for facilitating integrated and comprehensive fraud risk assessments across HHS. ASFR serves as an oversight entity to ensure that HHS operations and divisions are on track with their fraud risk management activities and to provide technical support, if necessary.

HHS's Fraud Risk Management Implementation Plan lays out coordinated fraud risk management roles and responsibilities for ASFR and HHS divisions, including for CPI within the CMS division. As laid out in the plan, ASFR is expected to serve as a liaison regarding how the HHS divisions, including CMS through its CPI, are implementing the requirements for fraud reduction within the Payment Integrity Information Act of 2019 or the Fraud Risk Framework. Further, ASFR is expected to collaborate on the divisions' methods to address fraud risks and collect data on, and monitor, the divisions' fraud risk management activities across HHS. The purpose of ASFR collecting these data is to determine how divisions are preventing and mitigating fraud and then to evaluate and report on the divisions' progress over time. ASFR's role and responsibility is to bring together fraud risk management data from across HHS to allow for a cross-cutting view of all fraud risks across the department. This allows HHS to identify current practices, tools, templates, and other guidance that can be leveraged for use by its divisions, according to the plan.

The Fraud Risk Management Implementation Plan specifies that divisions, such as CMS through its CPI, are expected to regularly assess and mitigate fraud risks for their programs. The plan also expects divisions to work with ASFR to provide information on their current fraud risk management efforts and assist ASFR in evaluating the impact of any control measures they have in place to prevent fraud or mitigate its impact.

For Medicare, CMS designated CPI's Vulnerability Collaboration Council as the entity dedicated to designing and overseeing fraud risk management activities for the Medicare program, including risk assessments tailored to the program. Despite what is called for in HHS's Fraud Risk Management Implementation Plan, there is limited coordination between ASFR and CMS's CPI, as it pertains to CPI sharing fraud risk management information with ASFR. ASFR officials told us they have not evaluated CPI's risk assessment process to ensure it is consistent with leading practices in the Fraud Risk Framework. Further, ASFR told us that there is no routine mechanism for CPI to communicate its fraud risks or fraud risk management efforts to ASFR as it pertains to Medicare. ASFR also told us that it does not directly coordinate with key CPI stakeholders of CPI's risk assessment process.

To help implement HHS's Fraud Risk Management Implementation Plan, ASFR developed the Fraud Risk Assessment Portal (FRAP) in fiscal year 2023 as a mechanism to centralize fraud risk management information and streamline and standardize fraud risk assessments across all HHS programs.[20] The FRAP's intended use is to generate actionable information for ASFR and division program managers. In written responses, ASFR stated that the FRAP was designed to assist HHS divisions that did not have mature fraud risk management programs or fraud risk assessment approaches. The FRAP is intended to serve as a complementary tool to existing division policies and procedures. It does not replace or rescind other program policies or procedures that exist to promote integrity in HHS business practices and compliance with laws, rules, and regulations. ASFR uses the FRAP as a mechanism to monitor department-wide fraud risk management information across HHS's divisions. Several divisions across HHS have used the FRAP to help prevent, detect, and mitigate fraud.

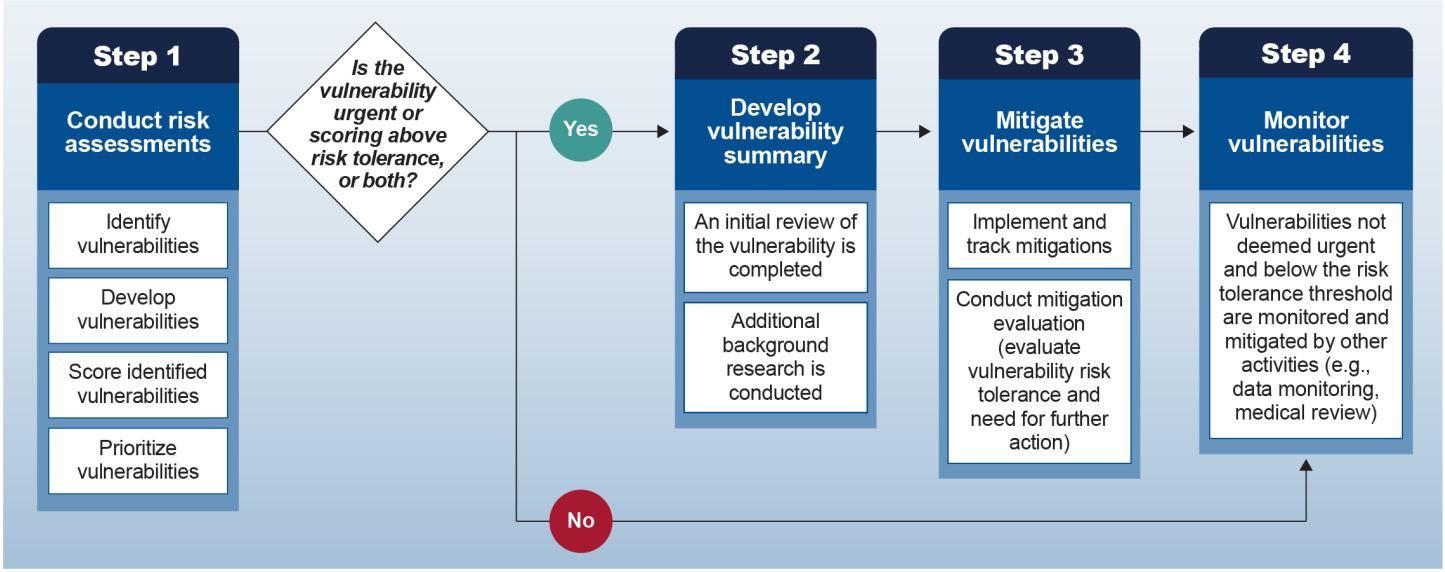
CPI does not use the FRAP. Rather, it uses its Vulnerability Management (VM) Process to broadly assess program vulnerabilities that include broad program integrity risks. According to HHS officials, CPI does not use FRAP because the VM Process predates the FRAP. Further, the FRAP is considered optional for all HHS divisions.[21] CPI's VM Process is not

[20]According to ASFR, the FRAP is a tool that enables all HHS program divisions to identify applicable fraud schemes, assess gaps in internal controls, and document mitigation strategies.

[21]During our review, the FRAP was considered optional for all HHS divisions. According to ASFR, it has plans to develop guidance for completing program-specific fraud risk assessments in the FRAP and to expand its use across HHS.

integrated with FRAP and, thus, CPI does not use ASFR's FRAP to communicate fraud risks and fraud risk management activities for Medicare. Figure 4 outlines CPI's VM Process.

Figure 4: Overview of the Center for Program Integrity's (CPI) Vulnerability Management Process



Source: GAO analysis of CPI documentation. | GAO-27-109072

The first major step in CPI's VM Process is to use risk assessments to identify potential vulnerabilities that could pose a risk to the integrity of various CPI programs, including Medicare. The risk assessment's vulnerabilities are identified from a variety of sources, such as HHS's OIG reports and information from UPICs, and then documented in CPI's risk assessments and vulnerability summaries. Identified vulnerabilities are scored for each criterion of dollars at risk, the likelihood they will occur, and the potential beneficiary harm. If an identified vulnerability in a risk assessment is considered urgent or above CPI's risk tolerance level, or both, CPI will draft a vulnerability summary that includes mitigation plans for addressing the vulnerability.[22] Vulnerabilities not deemed urgent or that are below the risk tolerance threshold, or both, are monitored on a periodic basis for an increase in risk that would warrant further action.

[22]A single risk assessment can have multiple vulnerabilities and, thus, multiple vulnerability summaries.

We asked CPI to provide details pertaining to the extent to which its roles and responsibilities for fraud risk management include coordinating on, and communicating specific information on, fraud risks and fraud risk management activities to ASFR. They did not provide examples of routinely sharing information related to fraud risk management activities. Rather, CPI officials said that they have coordinated as needed, such as partnering with ASFR to report improper payments for the Medicare program.

However, reporting improper payments to ASFR is not the same as reporting information on fraud risks and fraud risk management activities pursuant to HHS's Fraud Risk Management Implementation Plan. Further, since CPI does not use the FRAP for Medicare, ASFR told us that there is generally no separate, dedicated channel for CPI to routinely communicate fraud risk management efforts or fraud risks for Medicare to ASFR.

As called for in HHS's Fraud Risk Management Implementation Plan, regularly communicating such information could help inform ASFR's oversight and repository of knowledge about the most significant fraud risks impacting Medicare and how CPI is mitigating those fraud risks. Doing so could also help ASFR ensure that it is regularly carrying out its fraud risk management roles and responsibilities, consistent with HHS's Fraud Risk Management Implementation Plan and federal internal control requirements.

Absent a dedicated channel for CPI to routinely communicate to ASFR the relevant Medicare fraud risks CPI has assessed and fraud risk management activities for mitigating those fraud risks, ASFR is not effectively positioned to oversee and evaluate CPI's VM Process, as called for in HHS's Fraud Risk Management Implantation Plan. This can hinder ASFR's ability to evaluate CPI's antifraud efforts for mitigating fraud risks and cause ASFR and CPI, as dedicated antifraud entities, to miss opportunities to help improve the VM Process so that it is consistent with leading fraud risk management practices and HHS's Fraud Risk Management Implementation Plan. For example, ASFR's evaluation of CPI's VM Process may have helped identify sooner the deficiencies we discuss later in this report related to fraud risk assessments. In this regard, both CPI and ASFR may be hindered in effectively implementing their roles and responsibilities, as called for in HHS's Fraud Risk Management Implementation Plan.

CMS Has Taken Some Steps to Assess Medicare Fraud Risks, but Efforts Are Not Fully Consistent with Leading Practices and Internal Control Requirements

Leading fraud risk management practices call for managers to fully document and complete their assessment of fraud risks. CMS's CPI has taken some steps to assess some fraud risks that are in Medicare, such as developing draft risk assessments. However, CPI's efforts are not fully consistent with leading fraud risk management practices and related internal control requirements. For example, CPI has not finalized key risk assessment documents and guidance used to manage Medicare program integrity risks, including fraud risks. In addition, the VM Process is not designed to assess the likelihood and impact of Medicare fraud risks, to examine the suitability of the effectiveness and efficiency of existing antifraud controls, or to result in the development of a fraud risk profile for the program, consistent with leading fraud risk management practices. Further, CPI has not identified or assessed the full range of fraud risks facing the program.

CPI Has Started, but Not Finalized, Guidance or Risk Assessments for Medicare Consistent with Leading Practices and Internal Control Requirements

As of July 2026, CPI has started, but has not finalized, its draft Medicare Fee-for-Service Risk Assessment Framework guidance. According to Standards for Internal *Control in the Federal Government* and OMB's Circular No. A-123, completed documentation is a necessary part of an effective internal control system.[23] CPI's guidance, in draft form since January 2022, outlines CPI's approach for conducting risk assessments for Medicare, which is an initial step in the VM Process. As discussed in appendix 1, this draft guidance identifies 31 topic areas for risk assessments in Medicare. As we have previously reported, finalizing guidance regarding HHS's fraud risk management efforts can help ensure that ongoing fraud risk management activities are carried out effectively for all HHS programs.[24]

Additionally, it is unclear the extent to which CPI has conducted and documented risk assessments and vulnerability summaries for Medicare that it has started since 2022. According to Standards for Internal *Control in the Federal Government*, federal agencies are required to document the results of risk assessments, including the identification, analysis, and response to risks that are completed, on both a periodic and an ongoing basis. This includes documentation of the consideration of risks related to fraud.[25]

[23]GAO-25-107721; and Office of Management and Budget, *Circular No. A-123.*

[24]GAO-25-107290.

[25]GAO-25-107721.

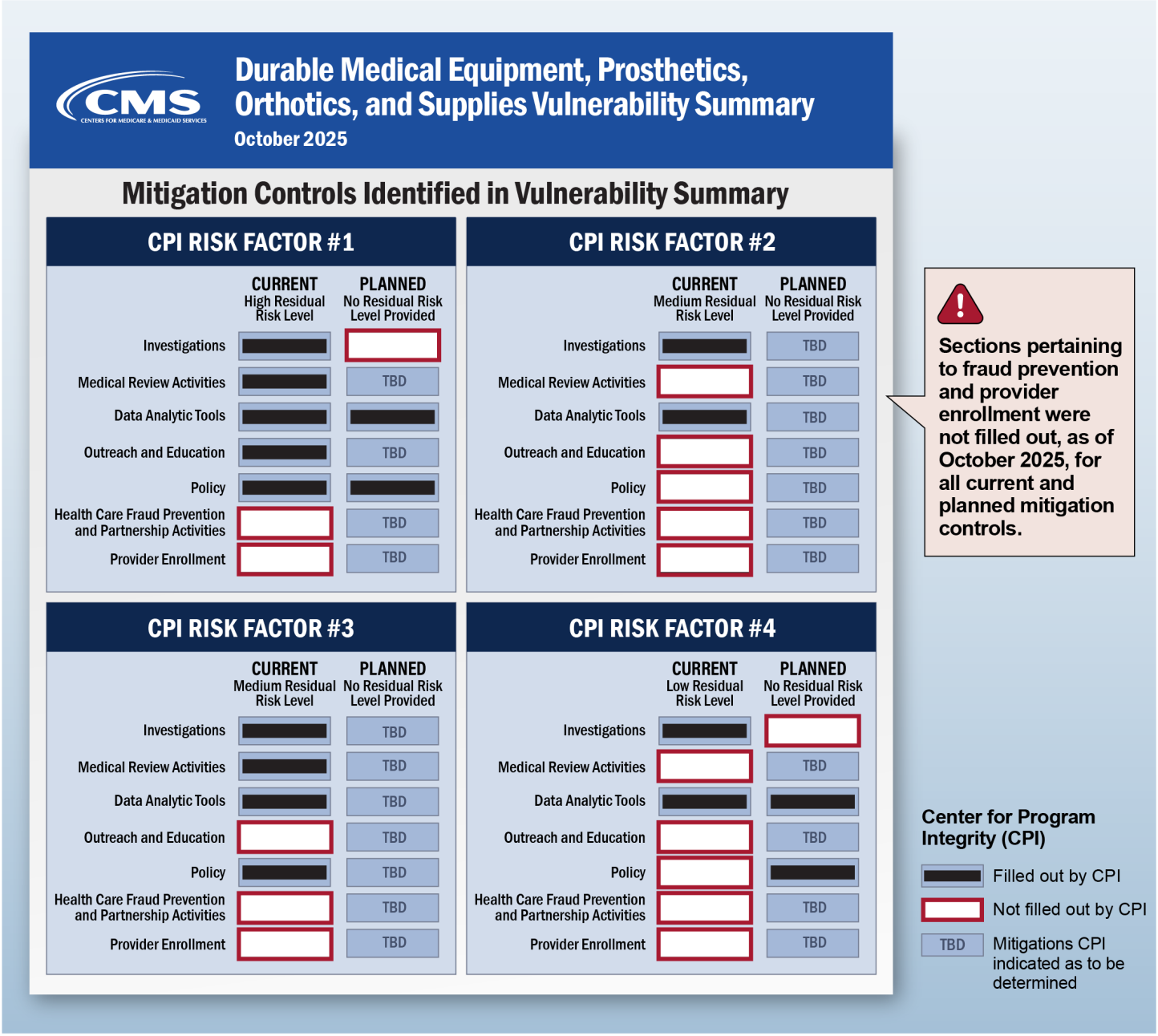
CPI officials informed us that, since 2022, CPI has started risk assessments for 10 out of the 31 Medicare topics and started 28 related vulnerability summaries, as reflected in appendix 1.[26] However, as of July 2026, CPI could not provide us with evidence that it had completed any of these risk assessments or vulnerability summary documents for the Medicare program. CPI officials told us that they have no plans to finalize these documents. Such documents are CPI's key program integrity risk management documents within the VM Process, according to CPI officials.

The effects of CPI not completing and finalizing its guidance and key risk assessment documents are that many of CPI's fraud mitigation efforts could remain incomplete or in the planning stage, as reflected in the draft documents that CPI did provide to us. For example, CPI's 2025 draft Vulnerability Summary for one vulnerability identified in the 2024 DMEPOS draft risk assessment showed that several sections of CPI's current and planned mitigation controls pertaining to fraud prevention partnership activities and provider enrollment are blank, or are in the process of being determined. For example, in the draft Vulnerability Summary, CPI did not fill in information regarding current or future mitigating controls as it relates to provider enrollment or the Health Care Fraud Prevention Partnership.[27] Figure 5 illustrates these and other incomplete current and planned mitigation efforts in the DEMPOS draft Vulnerability Summary. Incomplete and unfinalized documents can hinder or distort accountability efforts and confuse those who rely on, and oversee, such documents for established guidance and actual implemented efforts.

[26]CMS provided us with one draft risk assessment and one draft vulnerability summary, stating that they were sensitive and not for public release.

[27]The Healthcare Fraud Prevention Partnership (the Partnership) is a voluntary public-private partnership that helps detect and prevent health care fraud through data and information sharing. Partners include the federal government, state agencies, law enforcement, private health insurance plans, and health care antifraud associations. The purpose of the partnership is to help the partners improve capabilities to fight fraud, waste, and abuse across the health care sector. See U.S. Department of Health and Human Services, *FY 2024 Agency Financial Report* (Washington, D.C.: Nov. 14, 2024).

Figure 5: Example of Incomplete Current and Planned Mitigation Controls in the Center for Program Integrity (CPI) 2025 Draft Vulnerability Summary



Source: GAO analysis of CPI documentation. | GAO-27-109072

When asked why the risk assessment guidance and documents were still in draft form, CPI officials told us that these documents are continually evolving and subject to changes and revisions. These officials said that, accordingly, there are no plans for CPI to finalize these draft documents.

As we previously reported, without finalized guidance on fraud risk management that includes plans to assess fraud risks regularly and when there are changes to the program or operating environment, HHS programs may be unable to ensure that ongoing fraud risk management activities are carried out effectively and efficiently.[28] In addition, by not completing and finalizing its Medicare risk assessments and vulnerability summaries, CPI will be unable to effectively and fully demonstrate, and be held accountable for, how it is implementing the VM Process and HHS's Fraud Risk Management Implementation Plan that we discussed earlier in this report.

Likelihood and Impact of Inherent Medicare Fraud Risks

Leading fraud risk management practices in the Fraud Risk Framework call for managers to assess the likelihood and impact of fraud risks inherently affecting a program to help determine its fraud risk tolerance for prioritizing fraud risks and mitigation efforts. Such an assessment includes the consideration of fraud risks revealed by various sources, including ongoing and adjudicated fraud cases.[29]

CPI's VM Process is designed to assess the likelihood of improper payments and impact involving beneficiary harm. It is not designed to include an assessment of the likelihood and impact of fraud risks. For example, the design of CPI's likelihood analysis as part of the VM Process focuses on how likely it is for payments associated with a particular vulnerability to be improper, not the likelihood of Medicare fraud. As we have reported previously, not all fraud involves improper payments, and the root cause of fraud can be distinct from the root cause of improper payments.[30] Further, the design of CPI's impact analysis focuses on vulnerabilities associated with financial or physical impacts to beneficiaries but does not include determining the impacts related to

[28]See GAO, *Temporary Assistance for Needy Families: Additional Actions Needed to Strengthen Fraud Risk Management,* GAO-25-107290 (Washington, D.C.: Jan. 28, 2025).

[29]GAO-15-593SP.

[30]See GAO, *Improper Payments and Fraud: How They Are Related but Different*, GAO-24-106608 (Washington, D.C.: Dec. 07, 2024).

Medicare financial or nonfinancial fraud, including fraud stemming from beneficiaries, providers, or suppliers.

Without including such an assessment of fraud risks affecting Medicare, CPI risks overlooking the full scope and impact of Medicare fraud and related fraud risks. It can additionally limit CPI's ability to determine a fraud risk tolerance needed to effectively and efficiently prioritize current or planned mitigation efforts for those fraud risks that are more likely to materialize into actual and substantive fraud and create the largest impacts to the program.

Suitability for Mitigating the Likelihood and Impact of Fraud

Leading fraud risk management practices in the Fraud Risk Framework call for managers to document the examination of the suitability of existing antifraud controls for effectively and efficiently mitigating the likelihood, and impact, of fraud. This step should be performed before prioritizing fraud risks and before documenting a fraud risk profile that informs the antifraud strategy for revising, replacing, or keeping existing antifraud controls.

As we reported in March 2026, CMS uses its existing preventative antifraud controls, such as its Fraud Prevention System (FPS), to perform data analytics on claims in Medicare to prevent, detect, and respond to potential Medicare fraud.[31] CPI serves as the focal point within CMS for such efforts. For example, FPS's data analytical models are used as antifraud controls to develop leads for investigations and inform administrative actions that can prevent potentially fraudulent Medicare payments. CPI also uses contractors, including its UPICs, that employ their own existing data analytical antifraud controls to identify anomalous billing patterns that may be indicative of potential Medicare fraud.[32]

However, the VM Process does not include an examination of the suitability of these or other antifraud controls for effectively and efficiently mitigating the likelihood, and impact, of Medicare fraud. Specifically, CPI does not systematically examine the suitability of its existing mitigating controls for Medicare before prioritizing its fraud risks and considering whether to maintain or update existing mitigating antifraud controls, or to implement new ones. For example, in our review of CPI's 2024 DMEPOS draft risk assessment and vulnerability summary, we did not identify an

[31]See GAO, *Medicare: CMS's Use of Data Analytics to Identify and Prevent Fraud*, GAO-26-107799 (Washington, D.C.: Mar. 30, 2026).

[32]GAO-26-107799.

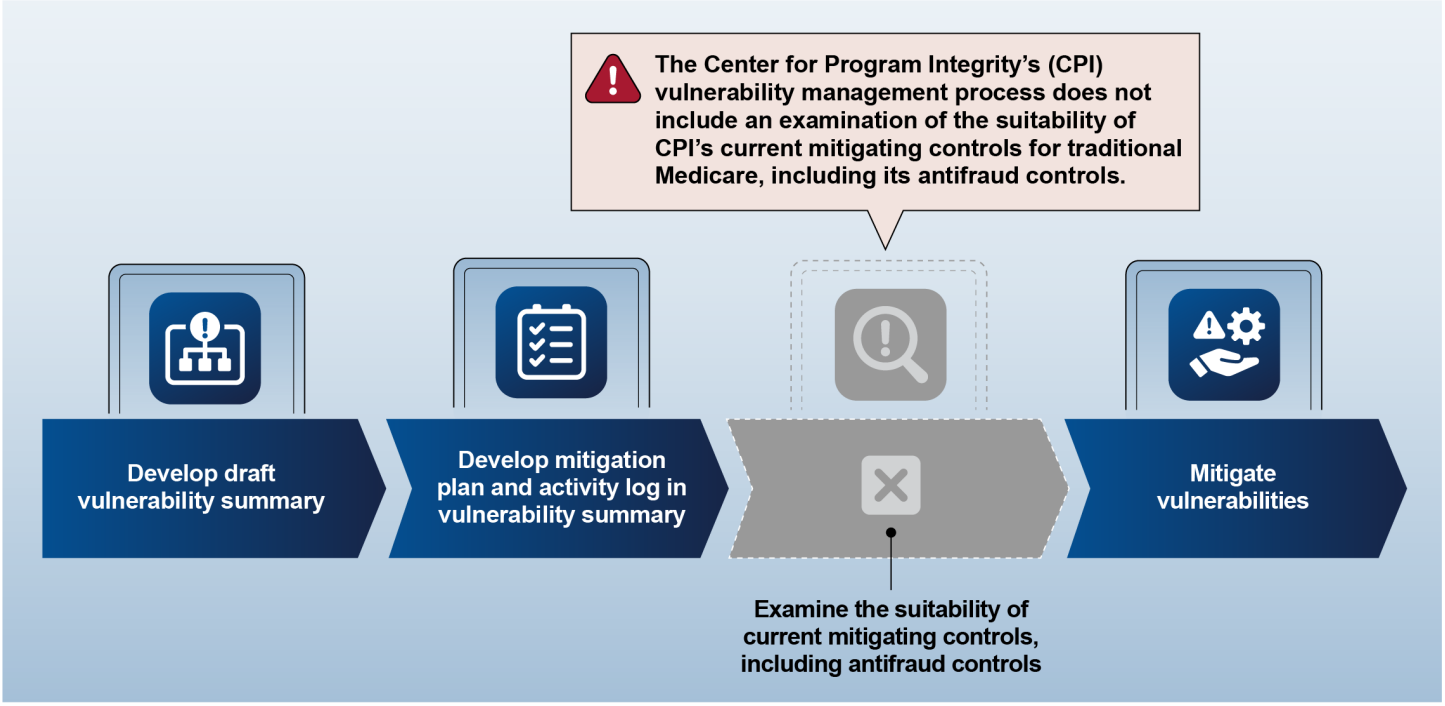
examination of the suitability of the current and existing controls used to mitigate the likelihood, and impact, of fraud-related vulnerabilities, as called for by the Fraud Risk Framework.

One vulnerability that was identified by CPI in the 2024 DMEPOS draft risk assessment—stemming from unnecessary orthotic braces—stated that existing CPI policies and controls may be insufficient to identify and prevent such payments.[33] However, the 2024 DMEPOS draft risk assessment and vulnerability summary did not include a discussion of the suitability of these existing policies and controls to determine the specific gaps causing this vulnerability and whether it pertained to a fraud risk or not.

Figure 6 illustrates that CPI's VM Process proceeds from prioritizing vulnerabilities in the risk assessment process to mitigating them without examining the suitability of current and existing fraud controls in between these steps. Such a practice is inconsistent with leading fraud risk management practices for fraud risk assessments.

[33]This was the single risk assessment that CPI provided us during our audit.

Figure 6: The Center for Program Integrity's (CPI) Vulnerability Management Process Excludes a Suitability Examination of Existing Controls



Sources: GAO analysis of CPI information; Icons-Studio/stock.adobe.com (icons). | GAO-27-109072

Further, although CPI's VM Process Overview Document adopts aspects of the assess component of the Fraud Risk Framework, it specifically does not include those leading practices that pertain to performing and documenting an examination of the suitability of existing antifraud controls for their effectiveness and efficiency in mitigating the likelihood, and impact, of Medicare fraud.

Without examining the suitability of existing antifraud controls before prioritizing fraud risks and documenting a fraud risk profile that informs the antifraud strategy, CPI risks using inefficient or ineffective antifraud controls that are not suitably designed or implemented to reduce Medicare fraud and fraud risks to a tolerable level.

Fraud Risk Profile for Medicare

According to leading fraud risk management practices in the Fraud Risk Framework, agencies should identify and assess risks to determine the program's fraud risk profile. Managers should use a fraud risk profile to document the results of key findings and conclusions from its assessment of fraud risks. This assessment includes the analysis of all the types of

inherent internal and external fraud risks impacting the program; the likelihood, and impact, of fraud risks; the fraud risk tolerance for each fraud risk; an examination of the suitability of existing fraud controls; and the prioritization of residual fraud risks. The fraud risk profile is the basis of informing an agency's development of an effective and efficient antifraud strategy for combating prioritized fraud risks that should be mitigated first.

CPI's VM Process Overview Document indicates that a risk profile is performed for vulnerability risks that CPI identifies and assesses. However, the VM Process Overview Document does not indicate that this risk profile would include a fraud risk profile for any of the risk assessments that it has completed for Medicare. When asked, CPI did not provide a fraud risk profile document for Medicare. Specifically, CPI officials were unsure what we were referring to when we asked them to provide documentary evidence that CPI has performed a fraud risk profile for Medicare.

By developing a fraud risk profile, CPI will be in a better position to demonstrate a comprehensive understanding of fraud risks impacting the Medicare program and to determine which specific control activities to design and implement to combat those fraud risks. However, CPI has not demonstrated that it has developed a fraud risk profile consistent with leading fraud risk management practices because, as we stated earlier, CPI's VM Process is not specifically designed to assess the likelihood, and impact, of Medicare fraud risks, or examine the suitability of existing antifraud controls, all of which should inform and occur before developing a fraud risk profile.

CPI Has Identified and Assessed Some Fraud Risks but Not the Full Range of Fraud Risks Impacting Medicare

According to the Fraud Risk Framework, managers who efficiently and effectively manage fraud risks attempt to fully consider, identify, and assess the full range of fraud risks that a program faces. Further, OMB's 2026 Circular A-123 states that agencies should assess fraud risks in conjunction with other risks that may impact the program's ability to achieve its objectives but should also annotate which of those risks pertain to fraud risks, specifically.[34] CPI's VM Process focuses on all program integrity risks and is a process that is broader in scope and not focused on fraud risks. For example, according to CPI's VM Process Overview Document, a vulnerability is generally defined as a perceived flaw, weakness, or gap in a CPI policy, process, or program activity that

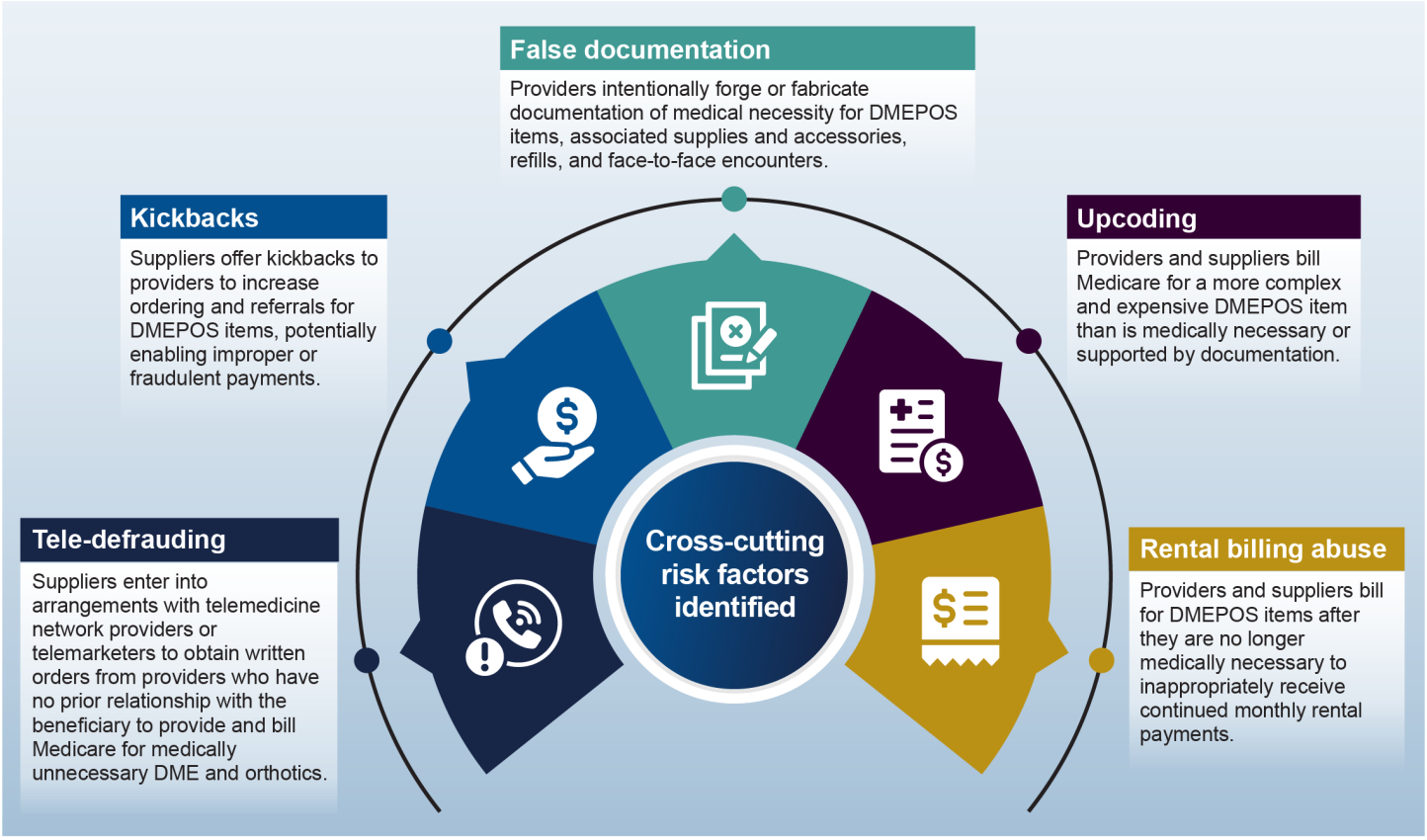
[34]Office of Management and Budget, *Circular No. A-123*.

could result in a risk. According to CPI officials, vulnerability risks could include fraud risks or other risks that may not pertain to fraud, including a risk related to nonfraudulent improper payments.

However, CPI's VM documents and process do not involve annotating which program integrity vulnerabilities pertain to fraud risks. For example, CPI's 2024 DMEPOS draft risk assessment identified five cross-cutting risk factors that appear to pertain to fraud risks. CPI said that these five risk factors were associated with program vulnerabilities, but it was unclear which vulnerabilities pertained to these five risk factors or to specific fraud risks.[35] See figure 7 for an illustration of the five cross-cutting risk factors that CPI identified in its 2024 DMEPOS draft risk assessment.

[35]Some of these cross-cutting risk factors were identified by CPI through public sources, such as DOJ press releases and improper payment data.

Figure 7: Five DMEPOS Cross-Cutting Risk Factors Identified by the Center for Program Integrity (CPI)



DME - Durable medical equipment
DMEPOS - Durable medical equipment, prosthetics, orthotics, and supplies

Sources: GAO analysis of CPI documentation; Icons-Studio/stock.adobe.com (icons). | GAO-27-109072

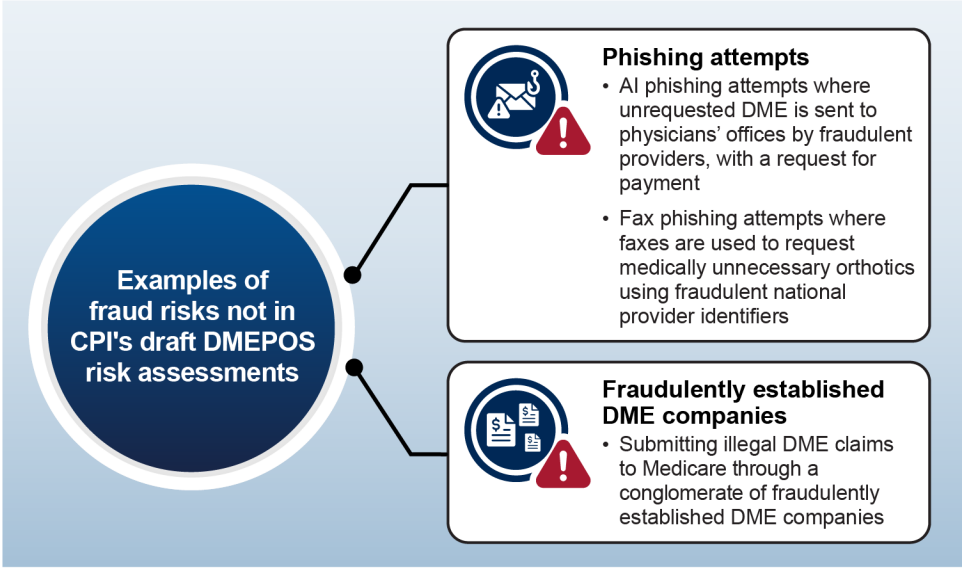
According to CPI, cross-cutting risk factors are typically systemic issues that are distinctive to a risk assessment topic, related to a topic's unique policy landscape, or that appear to be contributing to many vulnerabilities within the risk assessment topic. These five cross-cutting risk factors contributed to 41 vulnerabilities identified in the 2024 DMEPOS draft risk assessment that we received. Although some of the five cross-cutting risk factors appear to be associated with fraud risks, CPI did not indicate which of the 41 vulnerabilities identified were associated with each of these cross-cutting risk factors. In addition, the majority of the 41 vulnerabilities identified in the 2024 DMEPOS draft risk assessment were flagged by CPI as vulnerabilities because of insufficient or fraudulent documentation, but no details were provided beyond that. The assessment did not specify which vulnerabilities were associated with the

five risk factors or specific fraud risks, which is inconsistent with OMB's Circular No. A-123 requirement for annotating which risks are considered fraud risks.

As we mentioned earlier, a fraud risk (which is a function of likelihood and impact) exists when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or can rationalize committing fraud. Neither CPI's VM Process Overview Document nor the draft Medicare Fee-for-Service Risk Assessment Framework for Medicare requires that its risk assessment or vulnerability summary identify and specifically annotate which vulnerabilities pertain to fraud risks impacting the Medicare program. When asked to provide the number of vulnerabilities identified that were related to fraud risks in Medicare, CPI stated that it was unable to review each risk assessment due to the limited resources available to review each risk assessment and provide such information to us. Had identifying and assessing fraud risks been a part of CPI's VM Process and guidance, CPI could have been able to readily provide such information and be positioned to use that information to manage its fraud risks.

We also identified DMEPOS fraud risks from our independent review of HHS's OIG reports and agency interview responses that were not identified in CPI's 2024 DMEPOS draft risk assessment, as illustrated in the two examples in figure 8.

Figure 8. Examples of DMEPOS Fraud Risks Not in the Center for Program Integrity's (CPI) 2024 DMEPOS Draft Risk Assessment



CPI - Center for Program Integrity
DME - Durable medical equipment
DMEPOS - Durable medical equipment, prosthetics, orthotics, and supplies

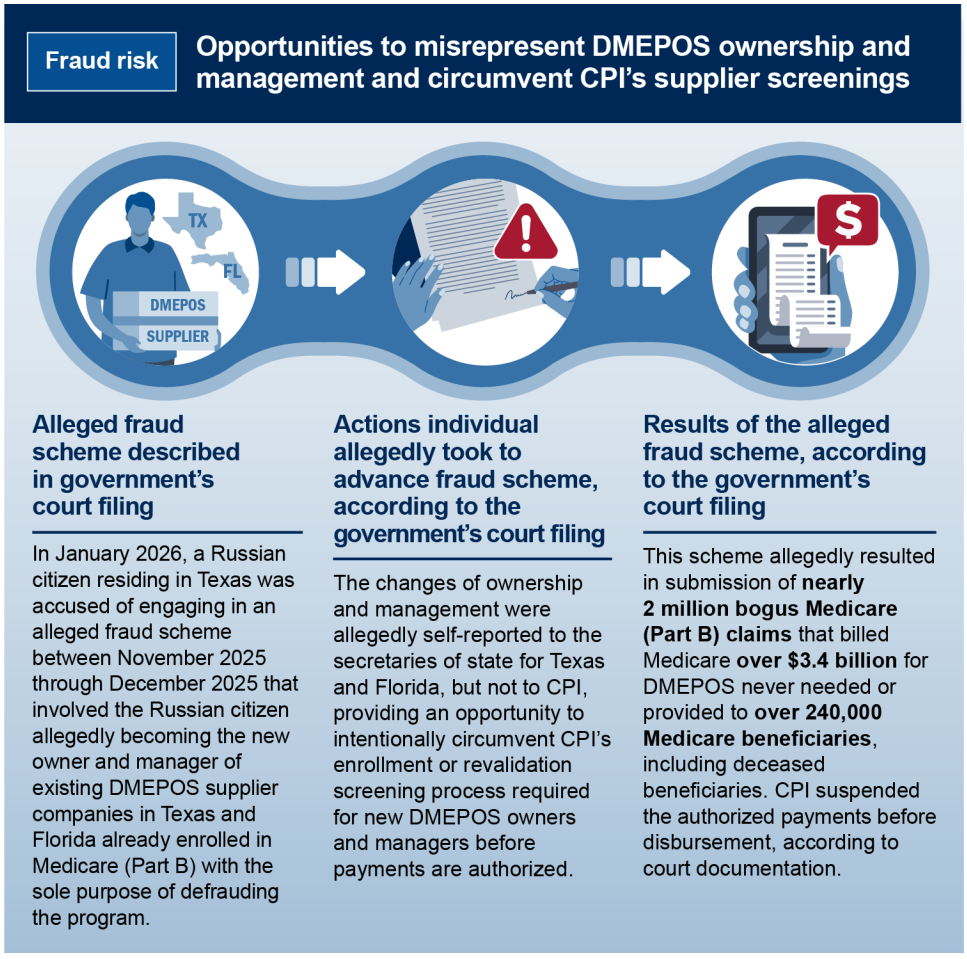
Sources: GAO analysis of interviews and documents from the Department of Health and Human Services' Office of Inspector General and CPI; Icons-Studio/stock.adobe.com (icons). | GAO-27-109072

Further, we identified a significant fraud risk that CPI's 2024 DMEPOS draft risk assessment flagged as a vulnerability but did not fully assess as a fraud risk consistent with leading fraud risk management practices. CPI's 2024 DMEPOS draft risk assessment acknowledged that its supplier screening process was a vulnerability because it may not have adequate controls in place to effectively screen DMEPOS suppliers during the enrollment or revalidation process. CPI determined that this vulnerability's risk level fell below, instead of above, its established threshold for when it determines there is a prioritized need for implementing mitigating controls. However, through our review of ongoing federal court cases, we determined that there is a significant fraud risk associated with Medicare's supplier screening process.

Specifically, we identified unadjudicated case examples of numerous Medicare participants and DMEPOS companies being accused of intentionally misrepresenting or hiding the true owners and managers of their DMEPOS supplier companies from CMS and the Medicare program, thus providing opportunities to intentionally circumvent Medicare's enrollment or revalidation screening process. The Medicare program's

enrollment and revalidation screening process requires the self-reporting and self-certification of changes in ownership and management of existing DMEPOS suppliers already enrolled in the program, before authorized payments are made. See figure 9 for one example of potential fraud and a related fraud risk that we identified and involved opportunities for a DMEPOS company owner and manager to circumvent CPI's supplier screening process.

Figure 9: Example of a Fraud Risk Opportunity Where a DMEPOS Owner and Manager Allegedly Circumvented the Center for Program Integrity's (CPI) Supplier Screening Process



CPI - Center for Program Integrity
DMEPOS - Durable medical equipment, prosthetics, orthotics, and supplies

Sources: GAO analysis of federal court documentation from *United States v. Machutadze*, 9:26-mj-8086 (S.D.F.L. 2026); GAO and Tartila/stock.adobe.com (illustrations). | GAO-27-109072

Note: As of November 3, 2026, this case is in the prearraignment stage, which is an early step in the legal process. All defendants are legally presumed innocent until proven guilty in a court of law.

CPI officials told us that they prefer not to review unadjudicated allegations of fraud. However, according to the Fraud Risk Framework, fraud risks can stem from alleged fraud that has not been fully investigated or adjudicated, and agencies could benefit from fully identifying and assessing such fraud risks before they materialize into actual fraud.[36]

Had CPI fully identified and assessed the supplier screening vulnerability as a specific fraud risk in its draft 2024 DMEPOS risk assessment consistent with leading fraud risk management practices that include assessing the likelihood and impact of fraud risks, it might have rated this vulnerability at a higher risk that exceeded its established threshold for further prioritization and additional fraud risk mitigation. Further, CPI could have also been able to determine what specific antifraud control weaknesses exist that warrant prioritized attention to its enrollment or revalidation screening process, or other mitigation strategies, especially given the likelihood and impact of the potential fraud involved. Therefore, CPI did not fully assess the supplier screening vulnerability as an identified fraud risk that is consistent with leading practices in the Fraud Risk Framework.

CPI officials explained to us that the VM Process is not intended to determine whether a vulnerability will lead solely to fraud. Instead, according to CPI officials, the VM Process focuses on identification of a range of general program integrity risks and vulnerabilities. However, without fully identifying and assessing fraud risks contributing to each vulnerability identified in such a way that is consistent with leading fraud risk management practices, CPI is not demonstrating a full understanding of the fraud risks the program faces. This can create missed opportunities for CPI to fully identify, assess, and mitigate specific Medicare fraud risks efficiently and effectively, before they materialize into actual and significant fraud.

Conclusions

Given the size of the Medicare program, not only in terms of expenditures, but also the number of Americans who depend on the program, it is critical that HHS and CMS strategically manage the fraud risks facing the program. Developing or using an existing mechanism for

[36]GAO-15-593SP.

CPI to communicate to ASFR the relevant Medicare fraud risks CPI has assessed, including fraud risk management activities for mitigating those fraud risks, will position ASFR to effectively oversee and evaluate CPI's VM Process to ensure it is consistent with leading fraud risk management practices and HHS's Fraud Risk Management Implementation Plan.

In addition, fully identifying and assessing Medicare fraud risks consistent with leading fraud risk management practices and internal control requirements would help CPI more effectively and efficiently safeguard the Medicare program and participants from fraudulent payments, bogus providers and beneficiaries, and unnecessary Medicare services and goods. CPI does take some steps to detect, prevent, and respond to potential fraud in the Medicare program. However, further strengthening and improving its fraud risk management processes, assessments, summaries, guidance, and communication efforts so that they are consistent with leading fraud risk management practices, internal control requirements, and HHS guidance would enhance CPI's efforts. For example, focusing on an overall process centered on general improper payment vulnerabilities may obscure or cause CPI to miss fully identifying and assessing actual and significant fraud risks impacting the Medicare program. This can reduce the relevance and materiality of specific fraud risks and undermine CPI's ability to manage them effectively and efficiently, consistent with leading fraud risk management practices. Taking action can provide CPI with more efficient and effective ways to mitigate individuals and companies from defrauding the program—depleting funds and services meant for legitimate providers and beneficiaries—and could strengthen the integrity of the Medicare program.

Recommendations for Executive Action

We are making the following four recommendations to HHS:

The Secretary of Health and Human Services should direct the Assistant Secretary of Financial Resources and the Administrator of CMS to establish a mechanism for CPI to effectively and regularly report identified Medicare fraud risks and corresponding antifraud efforts to ASFR. (Recommendation 1)

The Secretary of Health and Human Services should direct the Administrator of CMS to ensure that CPI finalizes its Medicare Fee-for-Service Risk Management Framework guidance that is currently in draft, consistent with leading fraud risk management practices and internal control requirements discussed in this report. (Recommendation 2)

The Secretary of Health and Human Services should direct the Administrator of CMS to ensure that CPI updates, completes, and finalizes its risk assessments and vulnerability summaries that are currently in draft, consistent with the leading fraud risk management practices and internal control requirements discussed in this report. (Recommendation 3)

The Secretary of Health and Human Services should direct the Administrator of CMS to ensure that CPI updates its VM Process Overview Document to include designing and regularly performing comprehensive assessments of fraud risks facing the Medicare program that are consistent with leading fraud risk management practices and internal control requirements discussed in this report. (Recommendation 4)

Agency Comments and Our Evaluation

We provided a draft of this report to HHS for its review and comment. HHS's response is reproduced in appendix II and presents its position on each of our four recommendations as well as general comments about recent actions it has taken to better protect federal health care programs, including Medicare, from fraud, waste and abuse. HHS also provided technical comments, which we incorporated, as appropriate.

Regarding our recommendations, HHS concurred with our first three recommendations but did not concur with our fourth, as discussed below. In concurring with our first recommendation, HHS described planned actions to address it. In concurring with our second and third recommendations, HHS stated that instead of finalizing the draft Medicare Fee-for-Service Risk Assessment Framework, risk assessments, and vulnerability summaries, CMS will apply "as-of" dates to clarify the status of these documents. HHS reiterated that these documents are iterative and continually updated and, therefore, should not be considered complete or finalized. While an "as-of" date is informative, adding it to the documents will not fully address our recommendations. As we recommended, updating and finalizing these documents to be consistent with leading fraud risk management practices and federal internal control requirements would establish an authoritative basis for CMS's fraud risk management activities, while still allowing CMS to update the documents as fraud risks and program conditions change. For example, CMS has continued to update its finalized VM Process Overview Document. As discussed in this report, not completing and finalizing these documents risks leaving fraud risk mitigation efforts incomplete, or in the planning stage.

In not concurring with our fourth recommendation, HHS stated that the recommendation is based on our misunderstanding of CMS's VM Process. Specifically, HHS stated that CMS already designs, and regularly performs, comprehensive assessments of Medicare fraud risks through its VM Process, which it considers consistent with the Fraud Risk Framework. We disagree. We recognize that CMS has taken some important actions to prevent, detect, and respond to potential Medicare fraud. However, CMS's VM Process addresses a broader range of program integrity risks and does not specifically require CMS to identify, assess, and document the full range of fraud risks facing Medicare consistent with leading fraud risk management practices and federal internal control requirements.

Further, as HHS acknowledged in its comments, the VM Process is agnostic as to whether identified vulnerabilities involve fraud. Consequently, the process does not ensure that CMS clearly distinguishes fraud risks from other program integrity risks when documenting its risk assessments and vulnerability summaries. This distinction is important, because assessing general program integrity vulnerabilities is not equivalent to systemically assessing the fraud risks associated with those vulnerabilities. This is, in part, because fraud risks may be pervasive and may not be adequately addressed through a general risk assessment process. Additionally, because of its very nature—willful misrepresentation to circumvent controls—the activities needed to prevent, detect, and respond to fraud go beyond those needed to address other program integrity risks and vulnerabilities, such as error, waste, or abuse.

Additionally, as discussed in this report, CMS's VM Process is not designed to systematically assess the likelihood and impact of fraud risks, examine the suitability of existing antifraud controls for mitigating those fraud risks, or develop a fraud risk profile that documents the results of these assessments. Without these elements, CMS may not identify and implement appropriate fraud mitigation measures or adjust existing measures based on the likelihood and impact of specific fraud risks facing Medicare. For these reasons, we reiterate that updating the VM Process Overview Document to explicitly incorporate a process for identifying, assessing, and documenting fraud risks, consistent with our recommendation, would help ensure that CMS's risk management activities address fraud risks in a manner consistent with leading fraud risk management practices and federal internal control requirements.

Regarding its general comments, HHS highlighted recent actions it has taken to better protect federal health care programs, including Medicare, from fraud, waste and abuse. For example, HHS cited a moratorium on

the enrollment of DMEPOS providers to help stem potentially fraudulent activity. We acknowledge these actions, and our report does not suggest that HHS and CMS have not taken any action to address Medicare fraud. However, as we explain in this report, CMS has not updated and finalized its draft guidance, risk assessments, and vulnerability summaries consistent with leading fraud risk management practices and federal internal control requirements. These gaps, including maintaining key documents in draft form, leave critical elements of Medicare's efforts to strategically manage fraud risks incomplete, which limits CMS's ability to identify, assess, and mitigate fraud risks effectively.

Additionally, HHS asserted that its approach to managing fraud risks is consistent with the leading practices in the Fraud Risk Framework and that our draft report contained misconceptions about this approach. In support of this position, HHS cited actions CMS has taken in response to our 2017 report.[37] HHS also emphasized the flexibility the Fraud Risk Framework provides, such as the responsibility of managers to tailor the leading practices to align with program operations. We disagree with HHS's assertions as discussed in the three main points below.

First, we previously determined that, in implementing our 2017 recommendation, CMS's approach to fraud risks assessments was consistent with leading practices in the Fraud Risk Framework. However, that determination does not affect the findings of this review. Specifically, our decision to close a prior recommendation does not prevent us from examining the process CMS subsequently developed or making additional recommendations based on new findings or applicable federal internal control requirements. In this regard, CMS's draft Medicare Fee-for-Service Risk Assessment Framework does not require CMS to identify and specifically annotate which vulnerabilities pertain to Medicare fraud risks, as required by federal internal control requirements. These requirements were not applicable during our prior review and, therefore, were not part of our assessment of CMS's efforts to address the prior recommendation. Accordingly, the closure of the 2017 recommendation does not suggest or validate that CMS's current framework meets leading fraud risk management practices or applicable federal internal control requirements.

Second, the Fraud Risk Framework provides flexibility, and we recognize that agencies should tailor fraud risk management efforts to their program operations. However, as discussed in this report, CMS's tailored

[37]GAO-18-88.

approach has left it with gaps in strategically managing Medicare's fraud risks. For example, our review of HHS's OIG reports and agency interview responses independently identified DMEPOS fraud risks that were not identified in CPI's 2024 DMEPOS draft risk assessment. Additionally, CMS could not provide us with evidence that it had completed any risk assessment or vulnerability summary documents for the Medicare program. In the draft vulnerability summary we reviewed, several sections addressing mitigation controls were blank or indicated "to be determined." These findings illustrate the limitations of CMS's current approach and underscore the need for a more systematic process for identifying, assessing, and mitigating Medicare fraud risks.

Third, HHS asserted that CMS walked GAO through its VM Process, explaining where every element of a fraud risk profile is reflected in its risk assessments and vulnerability summaries. HHS further stated that GAO could not identify which elements from the leading practices were missing. We disagree with this characterization of our findings. Our review identified specific gaps between CMS's process and the leading fraud risk management practices. For example, CMS could not provide evidence that it had completed important foundational elements of fraud risk management needed to develop a fraud risk profile, such as documenting identified fraud risks, their significance, and the measures in place to mitigate them. CMS's explanation of its existing process does not resolve the gaps we identified or demonstrate that CMS's process and documentation meet the leading fraud risk management practices and federal internal control requirements.

We are sending copies of this report to the appropriate congressional committees, the Secretary of HHS, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-6722 or BagdoyanS@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

//SIGNED//

Seto J. Bagdoyan
Director, Forensic Audits and Investigative Service

Appendix I: List of 31 Medicare Risk Assessment Topic Areas Identified by the Center for Program Integrity (CPI)

Table 1: The Center for Program Integrity (CPI) Has Started 10 out of 31 Risk Assessment Topic Areas Since 2022 for Medicare

Number of topics	Topics areas	As of June 2026, risk assessments CPI has started since 2022
1	Acute inpatient hospital and long-term care hospital (e.g., accommodations, supplies, appliances and equipment, nursing and other services)	○
2	Ambulance services	●
3	Ambulatory surgical center services	○
4	Beneficiary eligibility and enrollment	○
5	Chiropractic services	●
6	Coverage of extended care/skilled nursing facility services	●
7	Coverage of hospice services	●
8	Critical access hospitals	●
9	Data and information security (e.g., fraudulent actors obtaining beneficiary information via data breaches)	○
10	Dental services	○
11	Diagnostic laboratory services (e.g., diagnostic x-rays; imaging texts, audiology tests, bone mass measurements)	●
12	Drugs and biologicals services	●
13	Durable medical equipment, prosthetics, orthotics, and supplies services (e.g., prosthetics devices; leg, arm, back, neck braces; trusses; artificial legs, arms, and eyes; therapeutic shoes for individuals with diabetes; surgical dressings; splints; casts; and other devices.)	●
14	End-stage renal disease services (e.g., renal dialysis items and services, transplant services)	○
15	Foot care services	○
16	Home health services	●
17	Home infusion therapy	○
18	Hospital outpatient prospective payment system services	○
19	Hospital psychiatric services (e.g., inpatient psychiatric facility services, partial hospitalization program, community mental health center)	○
20	Inpatient hospital rehabilitation services (e.g., inpatient rehabilitation facility)	○
21	Inpatient hospital services – less routine or limited benefits (e.g., inpatient services in connection with dental services, pregnancy and infertility, cosmetic surgery, noncovered organ transplants)	○
22	Medical devices	○
23	Opioid treatment programs	○
24	Outpatient rehabilitation services (e.g., comprehensive outpatient rehabilitation facility, physical therapy, occupational therapy, speech-language pathology)	○

Appendix I: List of 31 Medicare Risk Assessment Topic Areas Identified by the Center for Program Integrity (CPI)

Number of topics	Topics areas	As of June 2026, risk assessments CPI has started since 2022
25	Physicians or nonphysician practitioner professional services (e.g., evaluation and management, anesthesia, surgery, radiology, clinical psychologist, clinical social worker, nurse practitioner)	●
26	Preventive and screening services (e.g., diabetes self-management and therapeutic services; kidney disease patient education services)	○
27	Provider enrollment	○
28	Rural health clinic and federally qualified health center services	○
29	Services of interns or residents-in-training (e.g., graduate medical education)	○
30	Telehealth services	○
31	Value-based care (e.g., alternative payment models)	○

● CPI has started risk assessment
○ CPI has not started risk assessment

Source: GAO analysis of CPI documentation. | GAO-27-109072

Appendix II: Comments from the U.S. Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

October 6, 2026

Seto J. Bagdoyan
Director, Audit Services
Forensic Audits & Investigative Service
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Bagdoyan:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"MEDICARE: HHS And CMS Should Better Manage Fraud Risks"** (GAO-26-109072).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Gary Andres
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: MEDICARE: HHS AND CMS SHOULD BETTER MANAGE FRAUD RISKS (GAO-25-109072)

The Department of Health and Human Services (HHS) appreciates the opportunity to review and comment on this draft report. HHS is committed to crushing fraud, waste and abuse across all federal healthcare programs. Due to the bold actions this administration has taken to crush fraud, HHS delivered unprecedented results in Fiscal Year (FY) 2025, protecting taxpayer dollars and holding bad actors accountable like never before. Total Medicare program integrity savings surged 59%, from $26.3 billion in FY 2024 to a record-shattering $41.9 billion in FY 2025. The FY 2025 Medicare Return on Investment (ROI) reached $22.3 to 1, up from $14.6 to 1, the highest ROI ever reported. Notably, cost avoidance activities, such as revocations or automated claim denials, accounted for 68% of all FY 2025 savings. HHS is laser-focused on rooting out fraud in Medicare, and we are succeeding.

HHS is also addressing risks in new, decisive ways. In March 2025, the Centers for Medicare & Medicaid Services (CMS) launched the Fraud Defense Operations Center (FDOC), better known as the Medicare Fraud War Room. In its first year, this War Room has become one of the most powerful weapons in the fight against fraud, waste, and abuse in Medicare history, stopping billions of dollars from reaching bad actors. This War Room is a cross-functional strike force uniting elite data analysts, investigators, health policy experts, legal advisors, and law enforcement under one roof with a single mission: stop fraud before taxpayers lose a single dollar. By harnessing rigorous, data-driven intelligence, this War Room detects threats in real time, coordinates rapid intervention, and shuts down inappropriate billing before it ever hits Medicare's books.

One example of these quick actions is the Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) enrollment moratorium to help stem potentially fraudulent activity. On February 26, 2026, CMS announced the imposition of a 6-month nationwide moratorium on the Medicare enrollment of DMEPOS supplier medical supply companies.[1] In determining whether to establish an enrollment moratorium, CMS considers whether a high risk of fraud, waste, or abuse exists. CMS relies on its and law enforcement's longstanding experience with ongoing and emerging fraud trends and activities to make this decision. The moratorium expired in August 2026, and CMS will require probationary prior authorization for certain DMEPOS items billed by newly enrolled suppliers and suppliers undergoing certain changes of ownership, starting October 15, 2026. Prior authorization allows suppliers to ensure that a DMEPOS item meets applicable Medicare coverage, payment, and coding rules before items are delivered. This advance review helps to protect the Medicare Trust Funds from improper payments while ensuring that beneficiaries can receive the DMEPOS items they need in a timely manner.

These successes require continuous evaluation of known and emerging program integrity risks, a precise and methodical risk identification and assessment process, and organized teams to quickly remove bad actors. CMS developed the Original Medicare Risk Assessment Framework to guide this work in Original Medicare. The Risk Assessment Framework is based on GAO's Fraud Risk Framework and was created as a result of a prior GAO recommendation that CMS implement an antifraud strategy.[2] We are pleased to note that GAO has closed that

[1] https://www.govinfo.gov/content/pkg/FR-2026-02-27/pdf/2026-03971.pdf
[2] https://www.gao.gov/products/gao-18-88

recommendation, stating that CMS' development of an organized approach for conducting fraud risk assessments and development of an antifraud strategy "are consistent with leading practices identified in GAO's Fraud Risk Framework."

CMS appreciates the GAO's recognition that "[m]anagers are responsible for determining the extent to which the leading practices presented in the Framework are relevant to their program and for tailoring the practices, as appropriate, to align with the program's operations. In doing so, managers consider applicable laws and regulations, the specific risks the program faces, and the associated benefits and costs of implementing each practice."[3] In fact, GAO has stated that "[t]here is no universally accepted approach for conducting fraud risk assessments, since circumstances between programs vary…"[4]

CMS has applied this flexibility in two key methods. First, CMS adapts the risk assessments to target a wider range of program integrity risks to include all fraud, waste, and abuse, which are of critical concern within all CMS programs. This process is designed to be flexible as programs and risks change. Because CMS' Risk Assessment Framework focuses on fraud, waste, and abuse, it can address a broader range of risks, intervene comprehensively at the beginning of policy and regulatory development, and protect resources more effectively than would be possible if assessing fraud alone. CMS further evaluates each identified risk (including all identified fraud risks) through a Risk Assessment. Findings from these Risk Assessments guide policy priorities and program integrity interventions going forward.

Second, CMS reorders and adjusts the Key Elements of a Fraud Risk Process (Fraud Risk Framework, Figure 4)[5] to better tailor the practices to CMS's programs. The Fraud Risk Framework lists the following Key Elements:

1. Identify inherent fraud risks affecting the program
2. Assess the likelihood and impact of inherent fraud risks
3. Determine fraud risk tolerance
4. Examine the suitability of existing fraud controls and prioritize residual fraud risks
5. Document the program's fraud risk profile

Because Medicare has operated for more than 50 years with robust, longstanding program integrity controls, assessing risks without considering those controls does not provide meaningful or actionable information. Inherent risks are theoretical, difficult to quantify, and often already mitigated through existing safeguards. GAO's Framework permits agencies to tailor practices to their specific operational realities, and CMS has determined that focusing on residual risks – those that persist despite current controls – allows CMS to direct enforcement, policy development, corrective actions, and rapid interventions (such as the DMEPOS moratoriums) to the areas where they matter most and best supports leadership prioritization. The result is the following:

1. Identify residual program integrity risks affecting the program
2. Assess the likelihood and impact of residual program integrity risks
3. Determine program integrity risk tolerance
4. Examine the suitability of existing program integrity controls and prioritize residual program integrity risks

[3] https://www.gao.gov/assets/gao-15-593sp.pdf

[4] https://www.gao.gov/assets/gao-15-593sp.pdf
[5] https://www.gao.gov/assets/gao-15-593sp.pdf

5. Document the program integrity risk profile

As GAO confirmed by closing the prior recommendation, these modifications align with GAO's Fraud Risk Framework.

While CMS values GAO's review and feedback, CMS would like to clarify three main misconceptions within GAO's report. First, GAO claims that CMS' Vulnerability Management process does not assess likelihood and impact of fraud risks and instead "is designed to assess the likelihood of improper payments and impact involving beneficiary harm." This is a misunderstanding of CMS's process. As stated in the Vulnerability Management Process Overview, provided to GAO, CMS assesses risk through three separate metrics: likelihood of occurrence, dollars at risk, and beneficiary harm. Likelihood is a measurement of how often the risk occurs; dollars at risk is a measurement of the financial harm (impact) to the program if the risk occurs; beneficiary harm is a measurement of financial and non-financial harm to the beneficiary if the risk occurs. The measurements are agnostic as to whether the risk is a result of fraud or some other program integrity vulnerability.

This measurement methodology is consistent with the GAO Fraud Risk Framework, which provides an example of how an agency might measure the likelihood and impact of fraud risks, but also explicitly states that "[t]he specific methodology managers use to assess fraud risks can vary by program because of differences in missions, activities, capacity, and other factors."[6]

Second, GAO claims that CMS does not assess suitability of anti-fraud controls for mitigating fraud risk. This is inaccurate. CMS' Vulnerability Management Process sets a risk tolerance threshold for every risk that is assessed. When a vulnerability exceeds that risk tolerance threshold, as measured by the likelihood, dollars at risk, and beneficiary harm, CMS then performs a vulnerability summary. A vulnerability is only escalated for further action *because* existing mitigating controls have already been assessed and found insufficient to bring the risk to a tolerable level. At that point, CMS evaluates whether to maintain, update, or implement new anti-fraud controls. The suitability assessment is inherent to the process — it is the reason a vulnerability is elevated to this stage in the first place.

Third, GAO states CMS has not finalized a fraud risk profile for Medicare, nor identified or assessed the full range of fraud risks facing the program. This is also inaccurate. CMS' Vulnerability Management Process includes the elements of a fraud risk profile that CMS has deemed relevant to our programs (i.e., for reasons elaborated above, CMS does not document "Inherent risk likelihood and impact" or "inherent risk significance"). During this audit, CMS walked GAO through every element of a fraud risk profile in Appendix V of the Fraud Risk Framework,[7] and explained where these elements are reflected in CMS's Risk Assessments and Vulnerability Summaries. CMS asked for further clarification about which element(s) GAO did not believe were present, and GAO could not provide an answer. The draft report also does not answer this question. As stated above, GAO's Fraud Risk Framework states that "[m]anagers are responsible for determining the extent to which the leading practices presented in the Framework are relevant to their program and for tailoring the practices, as appropriate, to align with the program's operations."

[6] https://www.gao.gov/assets/gao-15-593sp.pdf

[7] https://www.gao.gov/assets/gao-15-593sp.pdf

As evidence that these three claims demonstrate that CMS' Vulnerability Management Process is insufficient, GAO cites CMS' 2024 DMEPOS risk assessment. The DMEPOS risk assessment found provider screening and enrollment to be a vulnerability, but it determined that this vulnerability's risk level did not exceed the risk tolerance threshold, and CMS therefore did not prioritize strengthening controls. GAO cites an unidentified number of unadjudicated cases related to DMEPOS provider enrollment it found in the federal court system as evidence that CMS' assessment of the risk level was incorrect. However, as stated above, CMS' calculation of a vulnerability risk level involves a complex calculation that map likelihood of occurrence, dollars at risk, and beneficiary harm. A mere survey of unadjudicated federal court cases is insufficient to calculate a risk score or to target prioritization of that vulnerability over other vulnerabilities. Most notably, however, GAO's focus on process and documents ignores other tools that CMS uses to take quick action in the face of emerging program integrity risks, including the recent 6-month nationwide moratorium on the Medicare enrollment of DMEPOS supplier medical supply companies further described above. CMS' recent actions show that we are not constrained by a risk level calculation. We continually assess all risks and act swiftly when appropriate.

GAO's recommendations and HHS' responses are below.

GAO Recommendation 1
The Secretary of Health and Human Services should direct the Assistant Secretary of Financial Resources and the Administrator of CMS to establish a mechanism for CPI to effectively and regularly report identified Medicare fraud risks and corresponding antifraud efforts to ASFR.

HHS Response
HHS concurs with this recommendation. The Department continues to engage stakeholders and refine its broader fraud risk governance framework through development of the enhanced multi-year Anti-Fraud Governance Program. This program – now HHS's primary vehicle for modernizing fraud risk oversight – will define roles, responsibilities, and authorities across the Department and is expected to be fully finalized no earlier than FY 2027.

To strengthen fraud risk management in the interim, HHS will issue supplemental fraud risk assessment guidance by the end of FY 2026. This guidance will serve as the authoritative source for assessment scope, frequency, methodology, documentation, review, and approval requirements. It also outlines the mechanism that programs will use to report identified fraud risks and corresponding antifraud activities to ASFR.

Divisions will submit or update fraud risk information on a regular basis or triggered by relevant risk indicators. These include but are not limited to: major changes in program outlays; significant process or procedural changes; emergency funding; suspected or confirmed fraud; audit or review findings; improper payment findings; emerging fraud schemes; and the time elapsed since the last comprehensive fraud risk assessment. This approach ensures ASFR receives timely, substantive, and actionable fraud risk information.

GAO Recommendation 2
The Secretary of Health and Human Services should direct the Administrator of CMS to ensure that CPI finalizes its Medicare Fee-for-Service Risk Management Framework guidance that is currently in draft, consistent with leading fraud risk management practices and internal control requirements discussed in this report.

HHS Response
HHS concurs with this recommendation. The Medicare Fee-for-Service Risk Assessment Framework is reevaluated as the scope of Medicare coverage evolves, due to legislative and regulatory changes, among other reasons. As we have previously stated, our risk assessment processes are iterative and undergo continuous re-evaluation as our programs change. Because the term "draft" in this context appears to cause concern, CMS will apply "as-of" dates to provide clarification and underscore the evolving nature of these documents.

GAO Recommendation 3
The Secretary of Health and Human Services should direct the Administrator of CMS to ensure that CPI updates, completes, and finalizes its risk assessments and vulnerability summaries that are currently in draft, consistent with the leading fraud risk management practices and internal control requirements discussed in this report.

HHS Response
HHS concurs with this recommendation. As discussed during this audit, consistent with the GAO's Fraud Risk Framework, the CMS Vulnerability Management Process continually accounts for internal and external factors that may affect CMS programs, such as new initiatives, evolving technologies, new legislative requirements, and emerging fraud schemes. Risk assessments and vulnerability summaries are therefore not "completed" or "finalized" because they are continually updated and revised, and some of the topics listed have been refreshed or iterated multiple times since their initial creation in 2022. As the term "draft" in this context appears to cause concern, CMS will apply "as-of" dates to provide clarification and underscore the evolving nature of these documents.

GAO Recommendation 4
The Secretary of Health and Human Services should direct the Administrator of CMS to ensure that CPI updates its VM Process Overview Document to include designing and regularly performing comprehensive assessments of fraud risks facing the Medicare program that are consistent with the leading fraud risk management practices and internal control requirements discussed in this report.

HHS Response
HHS does not concur with this recommendation because it is based on a fundamental misunderstanding of CMS' Risk Assessment process and how these assessments are used to achieve meaningful results in a dynamic and fast-shifting environment. As stated above, CMS' Risk Assessment Framework is based on GAO's Fraud Risk Framework and was created as a result of a prior GAO recommendation that CMS implement an antifraud strategy. CMS is pleased to note that GAO has closed that recommendation and called CMS' process "consistent with leading practices identified in GAO's Fraud Risk Framework."As further detailed above, through the Vulnerability Management process, CMS has already designed and regularly performs comprehensive assessments of fraud risks facing the Medicare program that are consistent with the leading fraud risk management practices and internal control requirements discussed in this report.

The three key leading fraud risk management practices and internal control requirements discussed in this report are: Assessing the likelihood and impact of fraud risks, assessing the suitability of anti-fraud controls, and identifying and assessing the full range of fraud risks facing the program. First, CMS's process does assess likelihood and impact of risks with three metrics: likelihood of occurrence, dollars at risk, and beneficiary harm. These measures capture how

often a risk occurs and its potential financial and beneficiary impact, regardless of whether the underlying risk results from fraud or another program integrity vulnerability. This approach is consistent with GAO's Fraud Risk Framework, which recognizes that specific risk assessment methodologies may vary based on a program's mission, activities, capacity, and other factors.

Second, CMS's Vulnerability Management process incorporates assessments of suitability of current controls directly and sets a risk tolerance threshold for every risk that is assessed. When a risk exceeds CMS's risk tolerance threshold, CMS evaluates the vulnerability because existing controls have not reduced the risk to a tolerable level. CMS then determines whether existing controls should be maintained or updated, or whether new controls are needed. Thus, assessing the suitability of existing controls is inherent in CMS's process.

Finally, CMS' Risk Assessment Framework identifies and asesses the full range of fraud risks facing the program by addressing fraud, waste, and abuse comprehensively, rather than assessing fraud alone. In this manner, it is able to address a broader range of risks, intervene at the beginning of policy and regulatory development, and protect resources more effectively than would be possible if assessing fraud alone.

HHS thanks GAO for their efforts on this issue and looks forward to working with GAO on this and other issues in the future.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Seto J. Bagdoyan (202) 512-6722, BagdoyanS@gao.gov

Staff Acknowledgments

In addition to the contact named above, Erica Varner (Assistant Director), Flavio Martinez (Analyst in Charge), Bobby Younce II, Ava Kargosha, and Claire Rueth made significant contributions to this report. Also contributing to this report were Maria McMullen, James Murphy, and Jeff A. Larson.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on X, LinkedIn, Instagram, and YouTube.
Subscribe to our Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us



Please Print on Recycled Paper.