United States Government Accountability Office

Report to Congressional Requesters

May 2019

2020 CENSUS

Additional Actions Needed to Manage Risk

Accessible Version

GAO Highlights

Highlights of GAO-19-399, a report to congressional requesters

May 2019

2020 CENSUS

Additional Actions Needed to Manage Risk

Why GAO Did This Study

With less than 1 year until Census Day, many risks remain. For example, the Bureau has had challenges developing critical information technology systems, and new innovations—such as the ability to respond via the internet—have raised questions about potential security and fraud risks. Fundamental to risk management is the development of risk mitigation and contingency plans to reduce the likelihood of risks and their impacts, should they occur.

GAO was asked to review the Bureau's management of risks to the 2020 Census. This report examines (1) what risks the Bureau has identified, (2) the risks for which the Bureau has mitigation and contingency plans, (3) the extent to which the plans included information needed to manage risk, and (4) the extent to which the Bureau's fraud risk approach aligns with leading practices in GAO's Fraud Risk Framework. GAO interviewed officials, assessed selected mitigation and contingency plans against key attributes, and assessed the Bureau's approach to managing fraud risk against GAO's Fraud Risk Framework.

What GAO Recommends

GAO is making seven recommendations, including that the Bureau set clear time frames for developing mitigation and contingency plans, require that mitigation and contingency plans include all key attributes, hold risk owners accountable for carrying out their risk management responsibilities, and update its antifraud strategy to include a fraud risk tolerance and OIG referral plan. The Department of Commerce agreed with GAO's recommendations.

View GAO-19-399. For more information, contact Robert Goldenkoff at (202) 512-2757 or goldenkoffr@gao.gov or Rebecca Shea at (202) 512-6722 or shear@gao.gov.

What GAO Found

As of December 2018, the Census Bureau (Bureau) had identified 360 active risks to the 2020 Census. Of these, 242 required a mitigation plan and 232 had one; 146 required a contingency plan and 102 had one (see table). Mitigation plans detail how an agency will reduce the likelihood of a risk event and its impacts, if it occurs. Contingency plans identify how an agency will reduce or recover from the impact of a risk after it has been realized. Bureau guidance states that these plans should be developed as soon as possible after a risk is added to the risk register, but it does not establish clear time frames for doing so. Consequently, some risks may go without required plans for extended periods.

2020 Census Risks with Required Mitigation and Contingency Plans

Plan	Risks requiring plan	Risks with plan
Mitigation	242	232 (96%)
Contingency	146	102 (70%)

Source: GAO analysis of U.S. Census Bureau 2020 Census risk registers as of December 2018. | GAO-19-399

GAO reviewed the mitigation and contingency plans in detail for six risks which the Bureau identified as among the major concerns that could affect the 2020 Census. These included cybersecurity incidents and integration of the 52 systems and 35 operations supporting the census. GAO found that the plans did not consistently include key information needed to manage the risk. For example, three of the mitigation plans and five of the contingency plans did not include all key activities. Among these was the Bureau's cybersecurity mitigation plan. During an August 2018 public meeting, the Bureau's Chief Information Officer discussed key strategies for mitigating cybersecurity risks to the census—such as reliance on other federal agencies to help resolve threats—not all of which were included in the mitigation plan.

GAO found that gaps stemmed from either requirements missing from the Bureau's decennial risk management plan, or that risk owners were not fulfilling all of their risk management responsibilities. Bureau officials said that risk owners are aware of these responsibilities but do not always fulfill them given competing demands. Bureau officials also said that they are managing risks to the census, even if not always reflected in their mitigation and contingency plans. However, if such actions are reflected in disparate documents or are not documented at all, then decision makers are left without an integrated and comprehensive picture of how the Bureau is managing risks to the census.

The Bureau has designed an approach for managing fraud risk to the 2020 Census that generally aligns with leading practices in the commit, assess, and design and implement components of GAO's Fraud Risk Framework. However, the Bureau has not yet determined the program's fraud risk tolerance or outlined plans for referring potential fraud to the Department of Commerce Office of Inspector General (OIG) to investigate. Bureau officials described plans to take these actions later this year, but not for updating the antifraud strategy. Updating this strategy to include the Bureau's fraud risk tolerance and OIG referral plan will help ensure the strategy is current, complete, and conforms to leading practices.

Contents

Tables

Figures

Abbreviations

Bureau	Census Bureau
CIO	Chief Information Officer
Commerce	Department of Commerce
DHS	Department of Homeland Security
ERM	Enterprise Risk Management

IT	Information Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SRQA	Self-Response Quality Assurance
Standards for Internal Control	Standards for Internal Control in the Federal Government

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

May 31, 2019

Congressional Requesters

The federal government is constitutionally mandated to count the U.S. population every 10 years.[1] However, achieving a complete count is complex and costly. For example, the U.S. Census Bureau (Bureau) must meet certain immutable deadlines, including counting the population as of April 1, 2020 (Census Day); delivering state apportionment counts to the President by December 31, 2020; and providing redistricting data to the states by April 1, 2021. To meet these deadlines, the Bureau—an agency within the Department of Commerce—carries out thousands of interrelated activities which, for 2020, the Bureau estimates will cost $15.6 billion after adjusting for inflation to the current 2020 Census time frame (fiscal years 2012 to 2023), which would be the most expensive decennial census to date. In February 2017, we added the 2020 Census to our High-Risk List because operational and other issues were threatening the Bureau's ability to deliver a cost-effective enumeration, and the census remains on our 2019 High-Risk List as these issues have persisted.[2]

With less than 1 year remaining until Census Day, many risks remain. For example, as discussed in our high-risk reports, the Bureau decided to scale back census field testing in 2017 and 2018 citing budget uncertainty, and the Bureau has had challenges developing critical information technology systems. Moreover, new innovations—such as an option for the public to respond to the census using the internet—have raised questions about potential security and fraud risks. Adequately addressing risks is critical not just for individual operations but also for ensuring a cost-effective and high-quality census. In our prior work, we noted that problems with one operation can have a cascading effect and affect subsequent activities and thus the entire enumeration.[3]

[1] U.S. Const., art. I, § 2, cl. 3.

[2] GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

[3] GAO, *2010 Census: The Bureau's Plans for Reducing the Undercount Show Promise, but Key Uncertainties Remain*, GAO-08-1167T (Washington, D.C.: Sept. 23, 2008).

You asked us to review the Bureau's efforts to manage risks to the 2020 Census. This report (1) describes the risks to the 2020 Census that the Bureau has identified, (2) identifies the risks for which the Bureau has mitigation and contingency plans, (3) assesses the extent to which the Bureau's mitigation and contingency plans included information needed to manage risk, and (4) assesses the extent to which the Bureau's approach to managing fraud risks to the 2020 Census aligns with leading practices outlined in our Fraud Risk Framework.[4]

To answer our first three objectives, we reviewed Bureau documentation of its approach to managing risks facing the 2020 Census—including its decennial risk management plan; operational plan; governance management plan; guidance and training documents; and meeting minutes and agendas from the Bureau's 2020 Census Risk Review Board, which is responsible for identifying, assessing, managing, monitoring, and reporting risks to the 2020 Census. In addition, we interviewed Bureau officials responsible for overseeing risk management for the 2020 Census.

To describe what risks to the 2020 Census the Bureau has identified and the risks for which the Bureau has mitigation and contingency plans, we also reviewed the Bureau's portfolio- and program-level decennial risk registers. These registers catalogue information regarding all risks to the 2020 Census that the Bureau has identified, including risk descriptions and mitigation and contingency plans.

To assess the extent to which the Bureau's mitigation and contingency plans included information needed to manage risk, we selected a nongeneralizable sample of six risks from the Bureau's risk registers based on factors such as likelihood of occurrence and potential impact. For each selected risk, we reviewed relevant Bureau documentation—including risk mitigation and contingency plans—and we conducted semistructured interviews with the Bureau officials responsible for managing the risk. In addition, drawing principally from our Enterprise Risk Management (ERM) framework as well as secondary sources, we identified seven key attributes for risk mitigation and contingency plans to

[4] GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 28, 2015).

help ensure they contain the information needed to manage risks.[5] We assessed the risk mitigation and contingency plans entered in the Bureau's risk registers as of December 2018—as well as the separate mitigation and contingency plans for the six selected risks—against the seven key attributes.

To evaluate the extent to which the Bureau's approach to managing fraud risks to the 2020 Census aligns with leading practices outlined in our Fraud Risk Framework, we reviewed Bureau documentation related to the 2020 Census antifraud strategy.[6] This strategy includes a fraud risk assessment that identifies and evaluates scenarios in which fraudulent activity could impact the 2020 Census results. It also includes a risk response plan that uses the fraud risk assessment to develop risk responses and its fraud detection systems. In addition, we interviewed Bureau officials responsible for antifraud efforts for the 2020 Census. We evaluated the information gathered based on selected components of our Fraud Risk Framework.

Our assessment was limited to a review of the presence or absence of leading practices from the framework, not whether they were sufficient. We also did not assess the Bureau's approach against leading practices in the "evaluate and adapt" component of the framework because the Bureau will not be able to implement practices in this component until the 2020 Census begins. Appendix I presents a more detailed description of our scope and methodology.

We conducted this performance audit from May 2018 to May 2019 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.

[5] GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, GAO-17-63 (Washington, D.C.: Dec. 1, 2016). To determine key attributes for mitigation and contingency plans, we also reviewed risk management publications from sources including the Office of Management and Budget, the Project Management Institute, and the Chief Financial Officers Council and Performance Improvement Council.

[6] GAO-15-593SP.

Background

The decennial census produces data vital to the nation. The data are used to apportion the seats of the U.S. House of Representatives; realign the boundaries of the legislative districts of each state; allocate billions of dollars each year in federal financial assistance; and provide a social, demographic, and economic profile of the nation's people to guide policy decisions at each level of government. Furthermore, businesses, nonprofit organizations, universities, and others regularly rely on census data to support their work.

Given the importance of the decennial census to the nation, it is important for the Bureau to manage risks that could jeopardize a complete, accurate, and cost-effective enumeration. To assist federal government leaders in managing such complex and inherently risky missions across their organizations, in prior work we developed an ERM framework that, among other things, identifies essential elements for federal ERM and good practices that illustrate those essential elements.[7] Notably, these elements and practices apply at all levels of an organization and across all functions—such as those related to managing risks to the 2020 Census. Furthermore, Office of Management and Budget (OMB) Circulars No. A-11 and A-123 require federal agencies to implement ERM to ensure their managers are effectively managing risks that could affect the achievement of agency strategic objectives.[8] As discussed in our ERM Framework, ERM is a decision-making tool that allows leadership to view risks as an interrelated portfolio rather than addressing risks only within silos.

Fundamental to ERM is the development of risk mitigation and contingency plans. Mitigation plans detail how an agency will reduce the likelihood of a risk event and its impacts, should it occur. Contingency plans identify how an agency will reduce or recover from the impact of a risk after it has been realized. Among other things, these plans provide the roadmap for implementing the agency's selected risk response and the vehicle for monitoring, communicating, and reporting on the success

[7] See GAO-17-63.

[8] OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (June 2018); and *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123 (July 15, 2016).

of that response. In developing these plans, it is important that agencies keep in mind the interaction of risks and risk responses, as the response to one risk may affect the response to another or create a new risk entirely.

We also developed a Fraud Risk Framework to provide a comprehensive set of leading practices that serves as a guide for agency managers developing and enhancing efforts to combat fraud in a strategic, risk-based manner.[9] The framework is designed to focus on preventive activities, which generally offer the most cost-efficient use of resources since they enable managers to avoid a costly and inefficient pay-and-chase model of recovering funds from fraudulent transactions after payments have been made.

The Bureau Identified 360 Active Risks to the 2020 Census

Consistent with our ERM framework, the Bureau developed a decennial risk management plan which, among other things, requires that it identify risks to the 2020 Census at the portfolio and program levels.[10] Portfolio risks are those that could jeopardize the success of the 2020 Census as a whole, and they typically span several years with many potential risk events over the period. Program risks are narrower—they could jeopardize the success of an individual program, including the 35 operations that support the 2020 Census as well as the 2018 End-to-End Test.[11]

As of December 2018, the Bureau had identified 360 active risks to the 2020 Census—meaning the risk event could still occur and adversely impact the census.[12] Of these, 30 were at the portfolio level and 330 were at the program level. As shown in figure 1, the greatest number of active

[9] GAO-15-593SP.

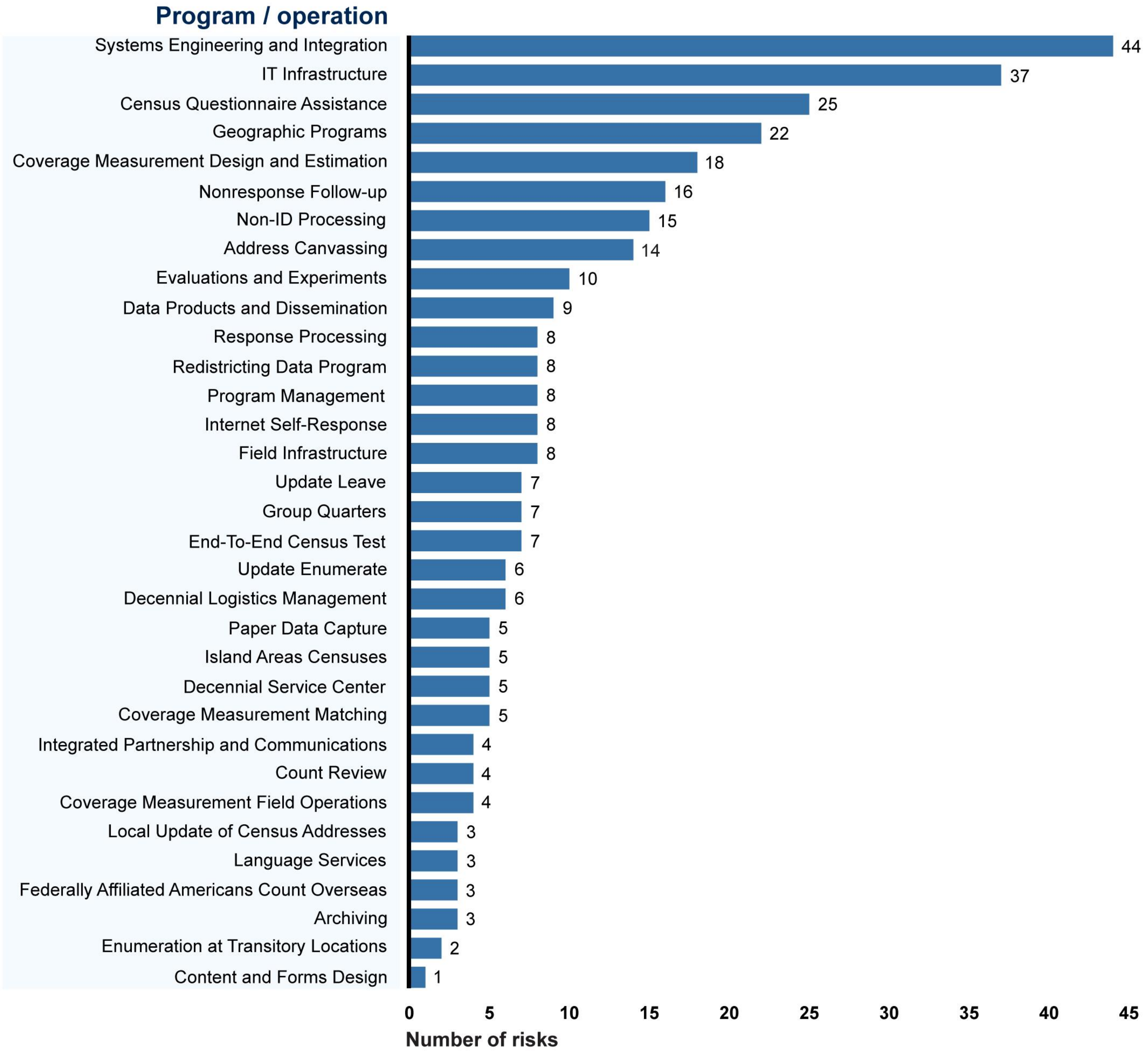
[10] Our ERM framework identifies six essential elements for federal ERM, the second of which is risk identification. See GAO-17-63. In April 2018, the Bureau updated its decennial risk management plan and, in doing so, changed its terminology for the two risk levels from program and project to portfolio and program.

[11] See appendix II for an overview of the 35 operations.

[12] Throughout this report, when referring to risks we are referring to both portfolio and program risks, unless otherwise indicated.

program risks was to the Systems Engineering and Integration operation which manages the Bureau’s delivery of an IT “System of Systems” to meet 2020 Census business and capability requirements. For example, the Bureau’s description of one of the risks to this operation indicated that if certain key system test plans and schedules are not clearly communicated among and collaborated on by relevant Bureau teams, then the 2020 Census systems are at risk of not meeting performance, cost, and schedule goals and objectives.

Figure 1: The Bureau Identified 330 Active Program Risks to the 2020 Census as of December 2018

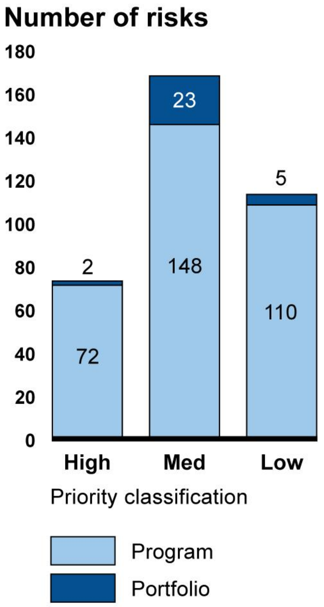


Source: GAO analysis of U.S. Census Bureau 2020 Census risk registers. | GAO-19-399

The Bureau Classified 21 Percent of Active Risks as High Priority

The Bureau's decennial risk management plan requires that it classify risks by priority level. These classifications are intended to highlight the most critical risks and identify where to allocate additional resources. Figure 2 shows how the Bureau had classified the 360 active risks as of December 2018.

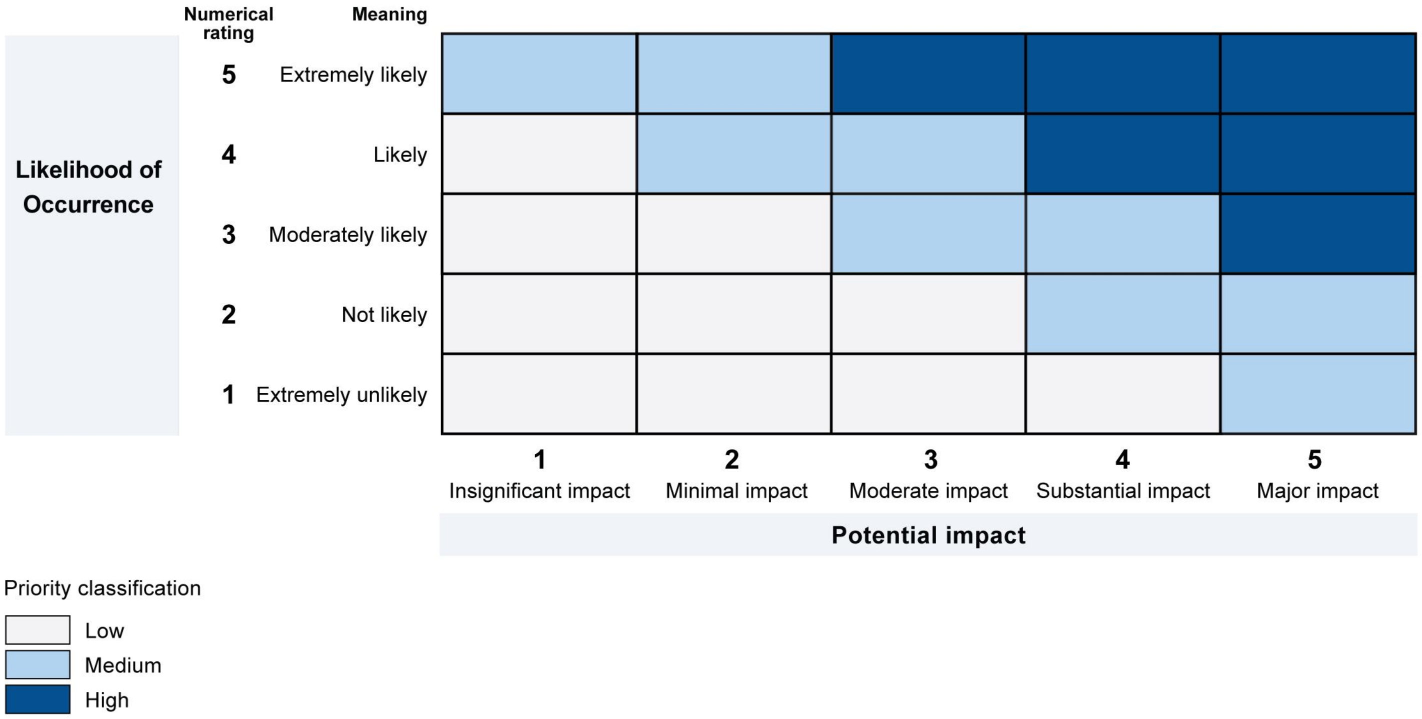
Figure 2: Active Risks to the 2020 Census as of December 2018, by Priority Classification



Source: GAO analysis of U.S. Census Bureau 2020 Census risk registers. | GAO-19-399

To determine risk priority, the Bureau's decennial risk management plan requires that it assign each risk numerical ratings for likelihood of occurrence and potential impact. When multiplied, the result is a numerical priority rating, which the Bureau divides into three classifications for high priority, medium priority, and low priority (see figure 3).

Figure 3: 2020 Census Risk Priority Calculation



Source: GAO analysis of U.S. Census Bureau decennial risk management plan. | GAO-19-399

The Bureau Determined That It Should Mitigate 67 Percent of Active Risks

According to the Bureau's decennial risk management plan, all portfolio-level risks must be mitigated to reduce the likelihood of the risk event and its impacts, should it occur. In contrast, when a program-level risk is identified, risk owners—the individuals assigned to manage each risk—are to select from the following risk responses.

- **Mitigate.** This may be an appropriate response where there are actions or techniques that will reduce the likelihood of the risk event and its impact, should it occur.
- **Watch.** This may be an appropriate response where a trigger event can be identified far enough in advance so that mitigation activities can be delayed until then.

- **Accept.** This may be an appropriate response where the probability and potential impact of the risk is so low that mitigation actions do not appear necessary or the impact can be absorbed if the risk occurs.

As of December 2018, the Bureau planned to mitigate 67 percent of the active risks it had identified (see table 1). Notably, this signifies that the Bureau determined there were actions it could take or techniques it could employ to reduce the likelihood of the majority of risks to the enumeration or their impact, should they occur.[13]

Table 1: Active Risks to the 2020 Census as of December 2018, by Risk Response

Risk level	Risk response Mitigate	Risk response Watch	Risk response Accept	Total
Portfolio	30	0	0	30
Program	212	42	76	330
Total	242	42	76	360

Source: GAO analysis of U.S. Census Bureau 2020 Census risk registers. | GAO-19-399

The Bureau Had Mitigation and Contingency Plans for Most Risks, but Not Clear Time Frames for Plan Development and Approval or a Clear Status for Mitigation Plans

The Bureau Had Mitigation and Contingency Plans for Most Risks That Required Them

The Bureau's decennial risk management plan sets out the following requirements for developing mitigation and contingency plans:

- Mitigation plans are required for all active portfolio risks and for all active program risks with a mitigate risk response.[14]

[13] According to the Bureau's decennial risk management plan, there may be situations where actions or techniques exist to reduce the likelihood of a risk, but the associated cost or resources required are prohibitive and hence mitigation is not selected as the risk response.

[14] As previously discussed, the Bureau's decennial risk management plan requires risk owners to mitigate all portfolio-level risks and to mitigate, watch, or accept program-level risks.

- Contingency plans are required for all active portfolio risks with a high- or medium-priority rating, and a moderate or higher likelihood of occurrence.
- Contingency plans are also required for active program risks with a high- or medium-priority rating, a moderate or higher likelihood of occurrence, and a risk response of mitigate or accept.

Of the 360 active risks to the census as of December 2018, 242 (67 percent) met the Bureau's criteria for requiring a mitigation plan (see table 2). According to the Bureau's risk registers, 232 of these risks (96 percent) had a mitigation plan. In addition, 146 of the active risks (41 percent) met the Bureau's criteria for requiring a contingency plan. According to the Bureau's risk registers, 102 of these risks (70 percent) had a contingency plan.

Table 2: Risks to the 2020 Census with Required Mitigation and Contingency Plans, as of December 2018

	Mitigation plan		Contingency plan	
Risk level	Risks requiring plan	Risks with plan	Risks requiring plan	Risks with plan
Portfolio	30	29 (97%)	12	7 (58%)
Program	212	203 (96%)	134	95 (71%)
Total	**242**	**232 (96%)**	**146**	**102 (70%)**

Source: GAO analysis of U.S. Census Bureau 2020 Census risk registers. | GAO-19-399

Our prior reporting similarly found that earlier in the decennial cycle, the Bureau did not have mitigation and contingency plans for all risks that required them. In November 2012, we found that the Bureau had mitigation and contingency plans for each of the portfolio risks it had identified at the time, but none for the program risks.[15] We reported that such plans were needed to help the Bureau fully manage associated risks, and we recommended that the Bureau develop risk mitigation and contingency plans for all program risks. In April 2014, the Bureau provided us with program-level risk registers that contained both risk mitigation and contingency plans where appropriate, and we closed the recommendation as implemented. However, as of December 2018, the Bureau is missing required mitigation and contingency plan for both portfolio and program risks.

[15] GAO, *2020 Census: Initial Research Milestones Generally Met but Plans Needed to Mitigate Highest Risks*, GAO-13-53 (Washington, D.C.: Nov. 7, 2012).

The Bureau Has Not Set a Clear Time Frame for Developing Mitigation and Contingency Plans

Some of the risks that were missing required plans had been added to the risk registers in recent months, but others had been added more than 3 years earlier. Specifically, the 10 risks without mitigation plans were added from June to December 2018, and the 44 risks without contingency plans were added from June 2015 to December 2018. The one portfolio risk without a required mitigation plan was added in December 2018, and the five portfolio risks without required contingency plans were added in July 2015, July 2016, October 2017, August 2018, and December 2018, respectively. In some instances, a risk may not meet the Bureau's criteria for requiring a mitigation or contingency plan when first added to the risk register. However, we found that all 10 risks without required mitigation plans and 37 of the 44 risks without required contingency plans met the Bureau's criteria for requiring such plans within a month of being added to the register (of the 37 risks without a required contingency plan, five were at the portfolio level and 32 were at the program level).

Example of 2020 Census Risk Without Required Contingency Plan

In July 2016, the Bureau added a risk titled, Major Disasters, to its portfolio risk register. The Bureau's description of the risk stated that if a major disaster—such as an earthquake—occurs during final preparations for or implementation of the 2020 Census, then census operations may not be executed as planned, leading to increased costs, schedule delays, or lower quality data.

Leading up to the 2010 Census, Hurricane Katrina devastated the coastal communities of Louisiana, Mississippi, and Alabama; a few weeks later, Hurricane Rita cut across Texas and Louisiana. Damage was widespread. Among other things, in the aftermath of Katrina, the Red Cross estimated that nearly 525,000 people were displaced and their homes were declared uninhabitable.

If a major disaster, such as a hurricane, occurs leading up to or during the 2020 Census, having a contingency plan would help ensure that housing units and their residents are accurately counted, particularly when hundreds of thousands of people—temporarily or permanently—may migrate to other areas of the country. As of December 2018, however, the Bureau had neither a draft nor approved contingency plan for this risk, although it required one since first added to the risk register nearly 2.5 years earlier.

According to the Bureau, though not documented in a contingency plan, it is taking actions to respond if this risk is realized. However, if such actions are reflected in disparate documents or no documents at all, then decision makers are left without a comprehensive picture of how the Bureau is managing this risk to the 2020 Census.

Source: GAO analysis of U.S. Census Bureau 2020 Census risk registers and prior work. | GAO-19-399

The Bureau's decennial risk management plan states that mitigation and contingency plans should be developed as soon as possible after risks requiring such plans are added to the risk registers, but it does not include a clear time frame for doing so. According to the Bureau's 2020 Census Portfolio Risk and Issue Process Manager—responsible for developing, maintaining, and administering the risk management process for both portfolio and program risks to the 2020 Census—no time frame is included because risk owners are aware of their responsibility and a specific time frame would not speed up the process given competing demands on their time.

However, the official said the Bureau would consider adding a specific time frame when it updates the decennial risk management plan in 2019. *Standards for Internal Control in the Federal Government* (*Standards for Internal Control*) states that management should define objectives in specific terms—including the time frames for achievement—so that they are understood at all levels of the entity.[16] In addition, OMB Circular No. A-123 states that effective risk management is systematic, structured, and timely. Without setting a clear time frame for developing mitigation and contingency plans, some risks may go without them for extended periods, potentially leaving the 2020 Census open to the impact of unmanaged risks.

The Bureau's Risk Registers Clearly Indicated the Status of Contingency but Not Mitigation Plans

The Bureau's decennial risk management plan requires that both portfolio and program risk registers include the word "draft" or "approved"

[16] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

alongside each contingency plan. As of December 2018, this status showed that 41 percent of contingency plans in the Bureau's risk registers were still in draft form and had not been approved by management (29 percent at the portfolio level and 42 percent at the program level). Specifically, management had approved 60 of the 102 contingency plans (five at the portfolio level and 55 at the program level) but not the remaining 42 (two at the portfolio level and 40 at the program level).

On the other hand, the Bureau's decennial risk management plan includes no requirements for indicating the status of either portfolio or program risk mitigation plans in the risk registers. Our review of the risk registers found that some of the portfolio risk mitigation plans included the word "draft" alongside the plan, but none included any indication of whether the plan had been approved by management. In addition, none of the program risk mitigation plans indicated whether the plan was in draft or had been approved by management, but we found that at least some appeared to be in draft. For example, one program risk mitigation plan stated that the Risk Review Board had recommended contacting three individuals for next steps; however, the plan did not appear finalized because it did not discuss any next steps and it is not clear that further action had been taken.

Although the Bureau had mitigation plans in place for 96 percent of risks that required them, without a clear indication of the status of these plans in the risk registers, we were unable to determine how many had been approved by management. According to Bureau officials, the risk registers are Bureau management's primary source of information regarding risks to the census. *Standards for Internal Control* states that management should use quality information from reliable sources and clearly document internal controls to achieve the entity's objectives and respond to risks.[17] Including a clear indication of the status of both mitigation and contingency plans in the risk registers would help to support Bureau officials' management of risks to the census; in addition, it would help to ensure that those plans are finalized and that the census is not left open to unmanaged risks.

[17] GAO-14-704G.

The Bureau Does Not Have a Clear Time Frame for Obtaining Management Approval of Mitigation and Contingency Plans

Of the 42 contingency plans awaiting approval, many had been added to the risk registers in recent months, but others had been added more than 4 years earlier. Specifically, the two portfolio risks were added in September 2014 and August 2017, and the 40 program risks were added from October 2015 to December 2018. Moreover, we found that both of the portfolio risks and 34 of the 40 program risks without finalized contingency plans met the Bureau's criteria for requiring such a plan within a month of being added to the register.

The Bureau's decennial risk management plan requires risk owners to present mitigation and contingency plans to management for approval as soon as possible after risks requiring such plans are added to the risk registers. However, as with development of the mitigation and contingency plans, the Bureau's decennial risk management plan does not include a clear time frame for doing so because, according to the Bureau's 2020 Census Portfolio Risk and Issue Process Manager, a specific time frame would not speed up the process given competing demands on risk owners' time. As previously noted, *Standards for Internal Control* states that management should define objectives in specific terms—including the time frames for achievement—so that they are understood at all levels of the entity.[18] In addition, OMB Circular No. A-123 states that effective risk management is systematic, structured, and timely. Without setting a clear time frame for approving draft mitigation and contingency plans, some risks may not be finalized.

The Bureau Did Not Consistently Include Key Information for Managing Risks in the Mitigation and Contingency Plans We Reviewed

Mitigation and contingency plans assist agencies in managing and communicating to agency stakeholders the status of risks. We reviewed the mitigation and contingency plans for six portfolio-level risks to the 2020 Census which the Bureau identified as among the "major concerns

[18] GAO-14-704G.

that could affect the design or successful implementation of the 2020 Census" (see table 3).[19] We found that the Bureau's mitigation and contingency plans for these risks did not consistently include key information needed to manage them. These six risks, if not properly managed, could adversely affect the cost and quality of the 2020 Census.

Table 3: Selected Risks to the 2020 Census GAO Reviewed

Risk	Description
Administrative records and third-party data—external factors	The Bureau plans to use administrative records and third-party data for various purposes, such as reducing the need to follow up with nonrespondents through identification of vacant housing units. However, external factors or policies—such as congressional action—could prevent the Bureau from using the records and data as planned, in which case the Bureau may be unable to meet its cost goals for the census, among other impacts.
Cybersecurity incidents	The Bureau plans to put in place information technology (IT) security controls to protect the confidentiality, integrity, and availability of its IT systems and data for the 2020 Census. However, if a cybersecurity incident occurs, additional technological efforts may be required to repair or replace the systems affected to maintain secure services and data.
Insufficient levels of staff with subject-matter skillsets	Due to factors including hiring freezes, budgetary constraints, and staff eligible for retirement before 2020, the Bureau may be unable to hire and retain staff with the appropriate skillsets at sufficient levels. As a result, it may be difficult to achieve the goals and objectives of the 2020 Census.
Late operational design changes	After key planning and development milestones for the 2020 Census are completed, stakeholders may disagree with the planned innovations behind the 2020 Census and decide to modify the design, resulting in late operational design changes. In this event, costly design changes may have to be implemented, increasing the risk for a timely and complete 2020 Census.
Operations and systems integration	The Bureau plans to use 52 different IT systems to carry out 35 operations supporting the 2020 Census. If the various operations and systems are not properly integrated prior to implementation, then the strategic goals and objectives of the 2020 Census may not be met.
Public perception of ability to safeguard response data	If a substantial segment of the public is not convinced that the Bureau can safeguard its data against data breaches and unauthorized use, then response rates may be lower than projected, leading to increased cases for follow-up and greater cost.

Source: GAO analysis of U.S. Census Bureau 2020 Census risk registers. | GAO-19-399

According to the Bureau's decennial risk management plan, for each portfolio-level risk the risk owner must develop mitigation and contingency plans using the Bureau's mitigation and contingency plan templates (see appendixes III and IV for the Bureau's templates). Those templates require, among other things, that the Bureau specify key activities for reducing the likelihood of the risk and its impacts. We found that the

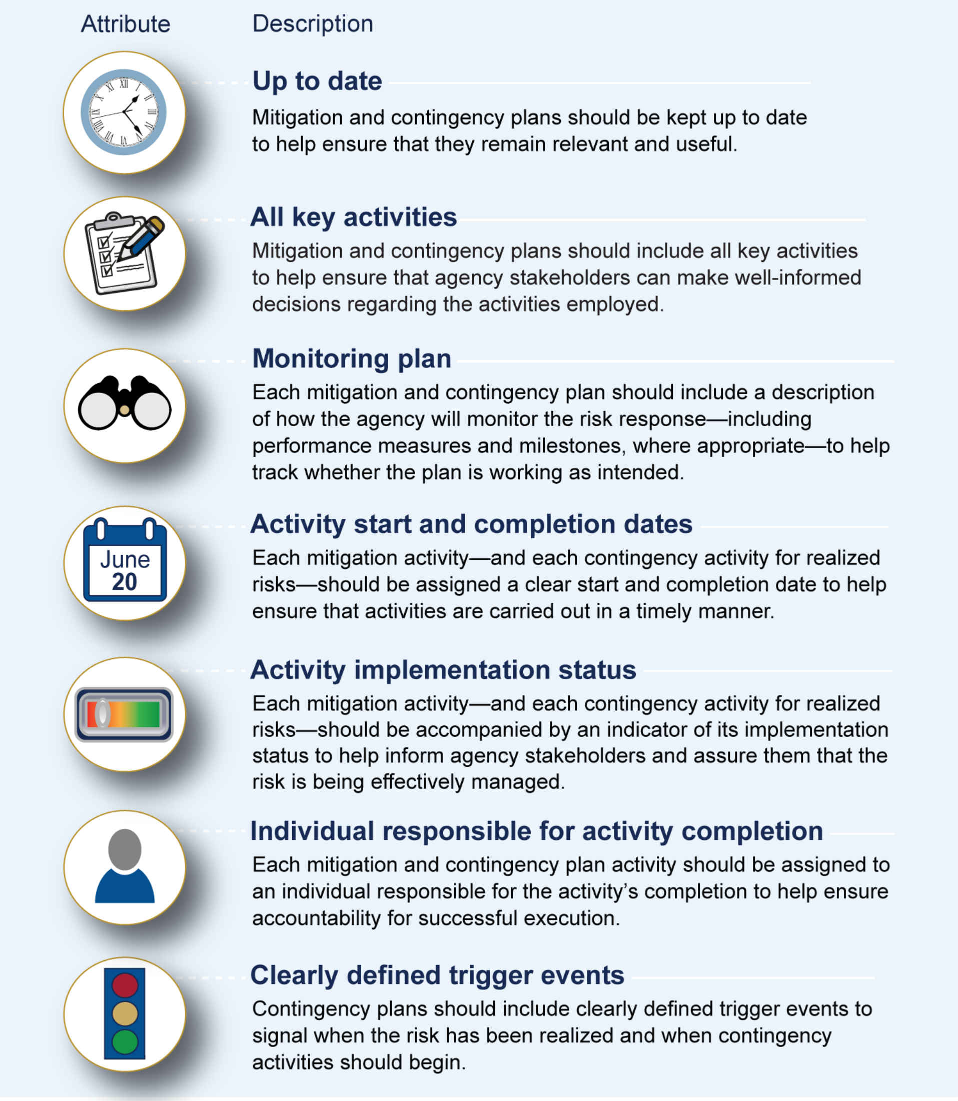
[19] To select these risks, we began with the 12 risks identified by the Bureau in its 2020 Census Operational Plan as the "major concerns that could affect the design or successful implementation of the 2020 Census." Next, we sorted the risks by numerical priority rating as of June 2018, a Bureau-assigned figure calculated by multiplying numerical scores for likelihood of occurrence and potential impact. We then selected the six risks with the highest priority ratings.

Bureau's decennial risk management plan generally aligns with our ERM framework which is designed to help agencies, among other actions, identify, assess, monitor, and communicate risks.[20] However, we also found some instances where the Bureau's risk management plan did not require mitigation and contingency plans to include certain key attributes we identified, which we discuss below.[21] See figure 4 for a list of key attributes that we used when reviewing mitigation and contingency plans. As indicated in the attribute descriptions, six of the seven attributes are applicable to mitigation plans. Clearly defined trigger events do not apply to mitigation plans because they signal when a risk has been realized and contingency activities must begin. Each of the seven attributes are applicable to contingency plans, although two attributes—activity start and completion dates and activity implementation status—are only applicable if the risk has been realized.

[20] GAO-17-63.

[21] As previously discussed, to determine key attributes for mitigation and contingency plans, we drew principally from our ERM framework, as well as risk management publications from sources including OMB, the Project Management Institute, and the Chief Financial Officers Council and Performance Improvement Council.

Figure 4: Key Attributes for Risk Mitigation and Contingency Plans



Attribute Description

Up to date

Mitigation and contingency plans should be kept up to date to help ensure that they remain relevant and useful.

All key activities

Mitigation and contingency plans should include all key activities to help ensure that agency stakeholders can make well-informed decisions regarding the activities employed.

Monitoring plan

Each mitigation and contingency plan should include a description of how the agency will monitor the risk response—including performance measures and milestones, where appropriate—to help track whether the plan is working as intended.

Activity start and completion dates

Each mitigation activity—and each contingency activity for realized risks—should be assigned a clear start and completion date to help ensure that activities are carried out in a timely manner.

Activity implementation status

Each mitigation activity—and each contingency activity for realized risks—should be accompanied by an indicator of its implementation status to help inform agency stakeholders and assure them that the risk is being effectively managed.

Individual responsible for activity completion

Each mitigation and contingency plan activity should be assigned to an individual responsible for the activity's completion to help ensure accountability for successful execution.

Clearly defined trigger events

Contingency plans should include clearly defined trigger events to signal when the risk has been realized and when contingency activities should begin.

Source: GAO analysis of risk management publications from GAO and others. | GAO-19-399

Note: To determine key attributes for mitigation and contingency plans we drew principally from our ERM framework, as well as risk management publications from sources including the Office of Management and Budget, the Project Management Institute, and the Chief Financial Officers Council and Performance Improvement Council.

As of December 2018, the results of our review of the Bureau's mitigation and contingency plans for the six portfolio-level risks we selected were in most cases mixed: some mitigation and contingency plans aligned with a particular key attribute, while others did not (see table 4). For two attributes—activity start and completion dates and activity implementation status—we found the Bureau generally included the relevant information across the six selected mitigation plans, which should help ensure that activities are carried out in a timely manner and that agency officials and stakeholders are informed and assured that the risks are being effectively managed.[22] On the other hand, none of the mitigation or contingency plans included a monitoring plan, which would help the Bureau to track whether plans are working as intended.

Table 4: Alignment of Key Attributes with Mitigation and Contingency Plans for Selected Risks, as of December 2018

		Key attribute						
Risk	**Plan**	**Up to date**	**All key activities**	**Monitoring plan**	**Activity start and completion dates**	**Activity implementation status**	**Individual responsible for activity completion**	**Clearly defined trigger events**
Administrative records and third-party data—external factors	Mitigation	No	Yes	No	Yes	Yes	Yes	N/A
	Contingency	No	No	No	N/A	N/A	No	No
Cybersecurity incidents	Mitigation	No	No	No	Yes	Yes	No	N/A
	Contingency	No	No	No	N/A	N/A	No	No
Insufficient levels of staff with subject-matter skillsets	Mitigation	No	Yes	No	Yes	Yes	No	N/A
	Contingency	Yes	Yes	No	No	No	No	Yes
Late operational design changes	Mitigation	No	Yes	No	Yes	Yes	No	N/A
	Contingency	No	No	No	N/A	N/A	No	No
Operations and systems integration	Mitigation	No	No	No	□ Plan did not include dates	■Plan included incorrect status	Yes	N/A
	Contingency	No	No	No	N/A	N/A	No	Yes
Public perception of ability to safeguard response data	Mitigation	No	No	No	□	Yes	No	N/A
	Contingency	No	No	No	N/A	N/A	No	No

Legend: N/A = Not applicable
□ = Plan did not include start dates, or included incorrect dates, for some activities
■ = Plan included the incorrect implementation status for some activities

Source: GAO analysis of U.S. Census Bureau 2020 Census risk mitigation and contingency plans. | GAO-19-399

[22] In all the selected mitigation plans, each activity was accompanied by an indicator of its implementation status, although one plan included an incorrect implementation status for two activities. In addition, the Bureau included activity start and completion dates in all the selected mitigation plans, with the exception of two plans that each had no start date for two activities. One plan also had incorrect start and completion dates for two activities.

We found that where attributes are required but not consistently implemented, the gap stems from the Bureau not always holding risk owners accountable for fulfilling all of their risk management responsibilities, such as keeping plans up to date. Bureau officials responsible for overseeing risk management for the 2020 Census stated that they encourage risk owners to complete all of their risk management responsibilities; however, risk owners do not always do so because they have competing demands on their time. Therefore, the officials said they are generally satisfied if the risk owners have completed at least some of their risk management responsibilities. However, they also agreed that risk management should be among the Bureau's top priorities and that risk owners should fulfill all of their risk management responsibilities.

Bureau officials also stated that the Bureau is managing risks to the census, even if not always reflected in the mitigation and contingency plans. We acknowledge that the Bureau is taking actions to manage risks to the 2020 Census beyond those reflected in its mitigation and contingency plans. However, if these actions are reflected in disparate documents or are not documented at all, then Bureau officials, program managers, and other decision makers are left without an integrated and comprehensive picture of how the Bureau is managing risks to the 2020 Census. Consequently, the Bureau's risk management efforts are neither clear nor transparent, which may create challenges for decision makers' ability to quickly and accurately identify essential information to set priorities, allocate resources, and restructure their efforts, as needed, to ensure an accurate and cost-effective enumeration. In addition, where mitigation and contingency plans are not clearly documented and only certain individuals know about them, there is potential for the loss of organizational knowledge, particularly as key personnel change roles or leave the agency altogether. Below we provide examples of gaps, by attribute, in the Bureau's mitigation and contingency plans for the six risks we reviewed.

Up to Date

Keeping plans up to date helps to ensure that they remain relevant and useful. The Bureau's decennial risk management plan requires that risk mitigation plans, but not contingency plans, be kept up to date. All six mitigation plans and five of the six contingency plans were not up to date, as shown in the following examples.

Administrative Records and Third-Party Data—External Factors. Administrative records are information already provided to the government as it administers other programs, such as Social Security; third-party data are information provided by commercial entities, such as InfoUSA, which provides data from sources including property taxes, voter registrations, and telephone books. The Bureau plans to use these data for various purposes including updating the address file for the nation's housing units. However, external factors or policies could prevent the Bureau from using the records and data as planned. As of December 2018, we found that neither the mitigation nor contingency plan for this risk was up to date. The mitigation plan included 13 activities, but the status column for nine of the activities had not been updated since December 2015, one since August 2016, and three since March 2017. For example, the three activities last updated in March 2017 pertained to the Bureau's development of a communication plan for outreach to external stakeholders concerning how administrative records would be used for the 2020 Census. According to Bureau officials, they took numerous actions to communicate such use to external stakeholders, including multiple public briefings and updates to their operational plan for the 2020 Census.

However, the mitigation plan indicated that the communication plan had been drafted, but there was no indication when, or if, it had been finalized or implemented. In August 2018, the Bureau provided us a copy of the communication plan, dated April 2017. It was still in draft form. The use of administrative records and third-party data is one of four innovation areas the Bureau is implementing to reduce costs and increase accuracy for the 2020 Census.[23] Thus, it is important that the Bureau keep external stakeholders informed about its use of administrative records and third-party data for the 2020 Census by finalizing and implementing the communication plan.

Regarding the contingency plan, when we spoke to Bureau officials in August 2018 about the risk, there was no contingency plan in place. In December 2018, the Bureau provided us with a draft contingency plan for the risk, which indicated that the Bureau planned to use a rapid response approach. According to the Bureau's decennial risk management plan, this approach does not require the Bureau to specify contingency

[23] The Bureau's three other innovation areas for the 2020 Census are (1) making greater use of local data, imagery, and other office procedures to build its address list; (2) improving self-response by encouraging respondents to use the internet and telephone; and (3) re-engineering field operations using technology to reduce manual effort and improve productivity.

activities in the event the risk is realized. Bureau officials stated that a rapid-response approach is generally appropriate where specific contingency activities cannot be identified ahead of time. However, Bureau officials responsible for managing this risk told us that the Bureau took steps to build into the census design the ability to recover from this risk, if it is realized. Nevertheless, the Bureau has not documented these steps in its contingency plan, despite the fact that it has considered what the steps need to be.

Public Perception of Ability to Safeguard Response Data. According to the Bureau, if a substantial segment of the public is not convinced that the Bureau can safeguard its data against data breaches and unauthorized use, then response rates may be lower than projected, leading to increased cases for follow-up and greater cost. In addition, the Bureau indicates that security breaches or the mishandling of data at other government agencies or in the private sector could impact the public's perception of the Bureau's ability to safeguard its own response data, especially if a data breach at another agency were to occur close to Census Day. Multiple high-profile data breaches have affected federal agencies in recent years. For example, in 2015 the Office of Personnel Management announced that two separate but related intrusions had affected the personnel records of about 4.2 million individuals, and the systems and files related to background investigations for at least 21.5 million.

A 2017 report by the Pew Research Center found that 28 percent of Americans are not confident at all that the federal government can keep their personal information safe and secure from unauthorized users, while 12 percent have a very high level of confidence that the government can keep their personal information safe and secure. More recently, the Bureau found that roughly a quarter of respondents to a 2018 survey were concerned about the confidentiality of answers to the 2020 Census, and that racial and ethnic minorities were significantly more concerned about confidentiality than non-Hispanic whites.[24] Furthermore, Bureau officials told us they anticipate misinformation efforts similar to those used in the 2016 and 2018 national elections may be used to disrupt the 2020 Census, which could further undermine public perception of the Bureau's ability to safeguard its data.

[24] U.S. Census Bureau, *2020 Census Barriers, Attitudes, and Motivators Study Survey Report, A New Design for the 21st Century* (Washington, D.C.: Jan. 24, 2019).

The Bureau's mitigation plan for this risk called for it to use a Gallup poll to monitor the "public's perception, trust, and willingness to respond to the census." However, in August 2018, Bureau officials told us that Gallup was no longer conducting the relevant poll and that, instead, the Bureau planned to use an internally administered survey—referenced above—to gauge public perception. In addition, the contingency plan for this risk included an activity of creating a website of frequently asked questions on public trust, but Bureau officials stated that the activity had been added to the plan early in the process and was no longer relevant.[25] As of December 2018, neither plan was up to date, leaving Bureau management and stakeholders with inaccurate information about how the public's perception of the Bureau's ability to safeguard data is being managed.

The Bureau's decennial risk management plan requires risk owners to update mitigation plans at least monthly. However, according to officials responsible for overseeing risk management for the 2020 Census, most risk owners do not update plans monthly, instead doing so in advance of required semiannual meetings before the Bureau's 2020 Census Risk Review Board. In addition, the Bureau's decennial risk management plan states that risk owners should monitor and report the progress of contingency plans, but the plan does not specifically require contingency plans to be kept up to date. Bureau officials responsible for overseeing risk management for the 2020 Census acknowledged that keeping mitigation and contingency plans up to date is important and an area in which the Bureau could improve. However, Bureau officials told us that risk owners have many competing demands on their time and limited resources available to carry out their work; consequently, risk management responsibilities are not always a top priority. Keeping plans up to date is important as Census Day draws closer. When plans are not up to date, Bureau officials are left with dated information regarding how risks to the census are being managed, which limits their ability to make timely decisions about strategies to help ensure a cost-effective and complete enumeration.

All Key Activities

Including all key activities in a plan helps to ensure that agency stakeholders can make well-informed decisions regarding the activities

[25] Bureau officials acknowledged this was a mitigation activity, not a contingency activity.

employed. Key activities are those that directly link the agency's selected risk response to the risk itself. The Bureau's decennial risk management plan requires that risk mitigation and contingency plans include all key activities. However, three of the six mitigation plans and five of the six contingency plans did not include all key activities, as shown in the following examples.

Cybersecurity Incidents. The Bureau's information technology (IT) systems supporting the 2020 Census—including the internet self-response instrument, applications on mobile devices used for fieldwork, and data processing and storage systems—could face cybersecurity incidents, such as data breaches and denial of service attacks. According to Bureau risk documents, the Bureau planned to put IT security controls in place to protect the confidentiality, integrity, and availability of the IT systems and data. If a cybersecurity incident occurs, Bureau risk documents indicate that additional technological efforts may be required to repair or replace the systems affected to maintain secure services and data.

We have previously identified significant challenges that the Bureau faces in securing IT systems and data for the 2020 Census including ensuring that individuals gain only limited and appropriate access to census data, and making certain that security assessments are completed in a timely manner and that risks are at an acceptable level.[26] To address these and other challenges, federal law requires, among other things, that the Department of Homeland Security (DHS) provide operational and technical assistance to agencies by conducting system threat and vulnerability assessments. In the last 2 years, DHS provided 17 recommendations for the Bureau to strengthen its cybersecurity efforts. Among other things, the recommendations pertained to strengthening incident management capabilities, penetration testing and web application assessments of select systems, and phishing assessments to gain access to sensitive personally identifiable information. As of February 2019, the Bureau had begun taking action to address the 17 recommendations. We have ongoing work evaluating the Bureau's actions and time frames for fully implementing the recommendations.

[26] GAO, *2020 Census: Continued Management Attention Needed to Address Challenges and Risks with Developing, Testing, and Securing IT Systems*, GAO-18-655 (Washington, D.C.: Aug. 30, 2018).

We found that the Bureau did not include all the key activities in its mitigation plan for this risk. For example, during an August 2018 public meeting, the Bureau's Chief Information Officer (CIO) discussed the Bureau's key strategies for mitigating cybersecurity risks to the 2020 Census. However, not all of the strategies the CIO discussed were included in the Bureau's cybersecurity mitigation plan. For example, the CIO noted the Bureau's reliance on other federal agencies to provide services to resolve threats but none of the mitigation plan activities mentioned such reliance. In August 2018, when we spoke to Bureau officials responsible for managing this risk, they agreed that the mitigation strategies should be included in the mitigation plan.

In September 2018, the Bureau updated the mitigation plan to include a new activity involving, among other things, leveraging cyber threat intelligence from other federal agencies. However, cyber threat intelligence is just one of several services being performed by outside agencies. If the Bureau's plan for mitigating cybersecurity risks to the census omits such key activities, then the Bureau is limited in its ability to track and assess those activities, and to hold individuals accountable for completing activities that could help manage cybersecurity risks.

Late Operational Design Changes. According to the Bureau, after key planning and development milestones for the 2020 Census are completed, stakeholders may disagree with the planned design and decide to modify it, resulting in late operational design changes. Bureau officials responsible for managing this risk stated that the most likely foreseeable late operational design changes were removal of a citizenship question as a result of litigation or congressional action, inability to use administrative records and third-party data as planned, and a change to the planned approach for address canvassing.[27] The mitigation plan for this activity included all key activities. However, the Bureau's contingency plan for this risk included no activities specific to these scenarios that the Bureau could carry out to lessen their adverse impact on the enumeration, should they occur. In early 2019, the U.S. District Courts for the Southern District of New York and the Northern District of California ordered removal of the citizenship question, and the Department of Justice requested that the Supreme Court rule on the

[27] In March 2018, the Department of Commerce announced that the 2020 Census will ask: "Is this person a citizen of the United States?" Multiple lawsuits were filed to block the inclusion of the question.

issue by the end of June 2019.[28] In addition, Members of Congress introduced legislation to prevent the question.[29] Nonetheless, the Bureau's contingency plan for this risk did not have contingency activities in place to guide their actions in the event the question must be removed.

When we spoke with Bureau officials regarding these issues, they stated that the Bureau's contingency plan for this risk is a rapid response approach, which does not require the Bureau to specify contingency activities in the event the risk is realized. As previously discussed, Bureau officials stated that a rapid response approach is generally appropriate where specific contingency activities cannot be identified ahead of time. However, Bureau officials told us they planned various contingency activities they would take if a late design change occurs. For example, they said they would use their change control process to assess impacts and facilitate decision-making.

In addition, they discussed various steps they would take if they must remove the citizenship question, including flexibility to make changes to the automated instruments for internet self-response, census questionnaire assistance, and nonresponse follow-up. Nevertheless the Bureau has not documented these activities in its contingency plan despite the fact that it has considered what the activities need to be. Without including all key activities in the contingency plan for this risk, the Bureau may not be able to respond as quickly to lessen any adverse impacts should a late design change occur.

Operations and Systems Integration. If the Bureau's various operations and IT systems are not properly integrated prior to implementation, then the strategic goals and objectives of the 2020 Census may not be met. In prior reporting, we have identified challenges that raise serious concerns about the Bureau's ability to manage its system development.[30] For example, the Bureau faced significant challenges in managing its schedule for developing and testing systems for operational tests that

[28] *New York v. U.S. Dept. of Commerce*, No. 18-cv-2921, (S.D.N.Y. Jan. 15, 2019); *California v. Ross*, No. 18-cv-01865, (N.D. Cal. Mar. 6, 2019).

[29] 2020 Census Accountability Act, H.R. 5292, 115th Cong. (as introduced March 15, 2018). Ensuring Full Participation in the Census Act of 2019, H.R. 1734, 116th Cong. (as introduced March 13, 2019).

[30] GAO-18-655; GAO, 2*020 Census: Actions Needed to Mitigate Key Risks Jeopardizing a Cost-Effective and Secure Enumeration*, GAO-18-543T (Washington, D.C.: May 8, 2018).

occurred in 2017 and 2018. Regarding the latter, the Bureau experienced delays in its schedule for developing systems to support the 2018 End-to-End Test. These delays compressed the time available for system and integration testing, and several systems experienced problems during the test.

As a result of the lessons learned while completing this test, the Bureau updated its system development and testing schedule for the 2020 Census. However, as of February 2019, the Bureau reported that development work remained for about 39 of the 52 systems that the Bureau plans to use for the 2020 Census, as well as performance and scalability testing for about 43.

To integrate all of the key systems and infrastructure for the 2020 Census, the Bureau is relying heavily on a technical integration contractor. As we reported in August 2018, the contractor's work was initially to include evaluating the systems and infrastructure, acquiring the infrastructure to meet the Bureau's scalability and performance needs, integrating all of the systems, supporting technical testing activities, and developing plans for ensuring the continuity of operations.[31] Since the contract was awarded, the Bureau modified the scope to also include assisting with operational testing activities, conducting performance testing for two internet self-response systems, and providing technical support for the implementation of the paper data capture system.

According to the Bureau, the contractor is also involved in all mitigation steps for this risk that relate to integration planning or system development metrics, and would be involved in all contingency activities should the risk be realized. However, neither the mitigation nor contingency plans discuss, among their activities, the integral role played by the contractor in managing this risk. We have previously reported that the Bureau faced challenges in managing its significant contractor support for the 2020 Census.[32] By largely omitting the role of the technical integration contractor from the mitigation and contingency plans for this risk, Bureau management is hampered in its ability to manage key contractor support and, therefore, to respond to and manage this risk.

[31] GAO-18-655.

[32] GAO-18-655.

The Bureau's decennial risk management plan requires that risk mitigation and contingency plans include all key activities. Plans did not include all key activities because Bureau officials did not hold risk owners accountable for fulfilling all of their risk management responsibilities. When key activities are not included in risk mitigation and contingency plans, Bureau officials are hampered in their ability to make well-informed decisions regarding the activities employed to manage risks to the 2020 Census, including whether those activities are appropriate or should be changed to better ensure a cost-effective and complete enumeration.

Monitoring Plan

Including a description of how the agency will monitor the risk response—with performance measures and milestones, where appropriate—helps track whether the plan is working as intended. According to our ERM framework, monitoring the risk response with performance measures allows the agency to track results and impact on the mission, and whether the risk response is successful or requires additional actions.[33] However, the Bureau's decennial risk management plan does not require that mitigation or contingency plans include a description of how the Bureau will monitor the risk response. Consequently, none of the mitigation or contingency plans included such a description.

Bureau officials told us that they plan to include a new section in the next update to their decennial risk management plan that will cover how mitigation and contingency plans are monitored once they are approved. Including such a section will be a good step toward providing clarity regarding monitoring activities; however, without risk-specific monitoring plans in its mitigation and contingency plans, the Bureau is limited in its ability to track the effectiveness of the activities in those plans, and to determine if additional actions are required to manage the various risks to the 2020 Census.

Activity Start and Completion Dates

Assigning clear start and completion dates helps ensure that activities are carried out in a timely manner. Thus, each mitigation activity, and each contingency activity for realized risks, should include a start and completion date. In accordance with the Bureau's decennial risk

[33] GAO-17-63.

management plan, each of the six mitigation plans generally included this attribute.[34] However, the contingency plan for the one risk that had been realized—Insufficient Levels of Staff with Subject-Matter Skillsets—did not have start or completion dates for any activity.[35] According to the Bureau's mitigation plan for this risk, factors including hiring freezes, budgetary constraints, and retirements could affect the Bureau's ability to hire and retain staff with the appropriate skillsets at sufficient levels.

Bureau officials told us that with a little more than a year until Census Day, they were facing staffing shortages. We previously reported that the Bureau experienced skills gaps in the government program management office overseeing the $886 million IT contract for integrating the IT systems needed to conduct the 2020 Census.[36] As of February 2019, 15 of the 44 positions in this office were vacant, according to Bureau officials. These vacant positions add risk that the office may not be able to provide adequate oversight of contractor cost, schedule, and performance.

The contingency plan for this risk includes seven activities, but it was not clear which ones were underway because the Bureau did not have start and completion dates in the contingency plan. As was the case with other attributes, Bureau officials did not hold risk owners accountable for fulfilling all of their risk management responsibilities. Without clear start and completion dates for contingency activities, the Bureau does not have reasonable assurance that those activities are being carried out in a timely manner.

[34] The Bureau included activity start and completion dates in all the selected mitigation plans. However, the mitigation plan for one risk had "TBD" as the start date for two activities; Bureau officials told us the risk owner had recently changed and that the new owner would be assigning start dates soon. In addition, the mitigation plan for another risk did not have start dates for two activities, but both activities had already been completed. This plan also had incorrect start and completion dates for two activities; specifically, the start dates were in 2018 but the completion dates were in 2017.

[35] We reviewed both the contingency plan for the risk and the separate issue treatment strategy, neither of which included activity start and completion dates.

[36] GAO, *2020 Census: Actions Needed to Mitigate Key Risks Jeopardizing a Cost-Effective Enumeration*, GAO-18-215T (Washington, D.C.: Oct. 31, 2017).

Activity Implementation Status

Accompanying each activity with an indicator of its implementation status helps to inform agency stakeholders and assure them that the risk is being effectively managed. The Bureau's decennial risk management plan requires mitigation plans, but not contingency plans, to include indicators of implementation status for each activity. Each of the six mitigation plans generally included the implementation status for all activities.[37] However, the contingency plan for the one risk that had been realized—Insufficient Levels of Staff with Subject-Matter Skillsets—did not include an implementation status for any of its seven activities.[38] Without such indicators for contingency activities, Bureau officials are left without key information needed to determine the status of activities designed to manage realized risks.

Individual Responsible for Activity Completion

Assigning an individual responsible for completing each activity helps to ensure accountability for successful execution. However, the Bureau's decennial risk management plan contains inconsistent language regarding to whom responsibility for activity completion should be assigned. For example, in one location, the plan states that each mitigation activity should be "assigned to an individual responsible for completing the action." In another location, it states that responsibility can be assigned to an "individual, division, or team." Consequently, we found that four of the six mitigation plans and each of the six contingency plans did not assign individuals responsibility for completing each activity. Bureau officials told us that when they update their decennial risk management plan in late spring 2019, they plan to clarify that responsibility may be assigned to an "individual, division, or team." However, if groups rather than individuals are assigned responsibility for carrying out activities, there is a risk that members of the group will

[37] The Bureau included activity implementation statuses in all the selected mitigation plans. However, the mitigation plan for one risk did so incorrectly in two instances. Specifically, it included one activity with an implementation status indicating it was "on schedule and likely to be completed successfully" but the scheduled completion date had already passed. It included another activity with an implementation status indicating it was "completed and successful" but Bureau officials told us it was due to be completed in fiscal year 2019.

[38] We reviewed both the contingency plan for the risk and the separate issue treatment strategy, neither of which included activity implementation statuses.

assume someone else is taking responsibility and the activity may not be completed.

Clearly Defined Trigger Events

Including clearly defined trigger events in contingency plans helps to signal when the risk has been realized and when contingency activities should begin. The Bureau’s decennial risk management plan includes detailed requirements for contingency triggers. Specifically, it requires risk owners to define the contingency trigger in terms of specific thresholds (such as response rates falling below a minimum expected level), specific events, or specific types of events (such as natural disasters impacting field operations in one or more geographic regions). Furthermore, it notes that each risk may have more than one contingency trigger. For example, it states that a risk related to continued operations of critical infrastructure during disasters may have triggers for delayed access to certain regions or populations, limited access to certain regions or populations, and a displaced population. In addition, it notes that, for the triggers to be useful, they must be defined in such a way that it is possible to monitor the environment for their occurrence. However, we found that four of the six contingency plans did not include clearly defined trigger events, as shown in the following examples.

Public Perception of the Ability to Safeguard Data. In the contingency plan for this risk, the Bureau defines the trigger event as follows: “The public has expressed significant concern and does not trust that the Census Bureau will safeguard their response data.” However, the Bureau did not specify in the plan what constitutes “a significant concern” nor did the Bureau indicate whether high levels of distrust among certain segments of the public—such as certain demographic groups—would trigger the risk. Without such specificity, the Bureau may be unaware when public concern regarding its ability to safeguard data has escalated to levels necessitating contingency activities.

We found that the trigger events for the contingency plans were not clearly defined because, as was the case with other attributes, Bureau officials did not hold risk owners accountable for greater specificity. If contingency triggers are poorly defined, the Bureau may not know when it is time to implement contingency activities to reduce the effect on the census.

After we shared the results of our analysis with the Bureau, Bureau officials updated their mitigation and contingency plans for the six risks we reviewed. In doing so, they addressed some but not all of the issues we raised. For example, in February 2019, the Bureau updated its mitigation plan for Public Perception of Ability to Safeguard Response Data by, among other things, removing the reference to a discontinued Gallup poll that they had intended to use to gauge public perception; they replaced it with a reference to an internally administered survey. Also in February 2019, the Bureau updated its contingency plan for Late Operational Design Changes by removing the term “operational” from the title and adding a reference in the risk description to potential data product design changes; however, the contingency plan did not include activities specific to the three most likely foreseeable late operational design changes.

Furthermore, as of February 2019, the Bureau did not have a finalized contingency plan for Administrative Records and Third-Party Data—External Factors, although the risk required such a plan since it was added to the risk register more than 4 years earlier. The updates to these specific risks are a positive step in the Bureau’s management of those risks. However, ensuring that the mitigation and contingency plans for all risks to the 2020 Census contain the information needed to manage the risks would better position the Bureau to quickly and effectively respond to any of the risks that may occur.

Risk-Register Entries Were Missing Key Information

For each portfolio and program risk mitigation and contingency plan, the Bureau’s decennial risk management plan requires risk owners to enter a description of the plan in the relevant risk register. However, our review of risk register entries for both mitigation and contingency plans across all active risks as of December 2018 found they were missing some key attributes, including monitoring plans, activity start and completion dates for most activities, the implementation status for some activities, individuals responsible for activity completion, and clearly defined trigger events. In some instances, the missing attributes were a result of the Bureau not requiring them in the risk register descriptions.[39]

In other instances, where the Bureau's decennial risk management plan does require the attribute in the risk register descriptions, the gap was due to the Bureau not holding risk owners accountable for them. Some of the attributes missing from the registers were included in the separate mitigation and contingency plans.[40] However, at the program level there are no separate mitigation plans, making the risk registers the only source of information for program-level mitigation activities. According to Bureau officials, after the 2020 Census they plan to require separate mitigation plans for program risks as well. At the same time, Bureau officials noted that they primarily rely on the risk registers to monitor risks to the census and usually do not refer to the separate mitigation and contingency plans.

Standards for Internal Control states that management should use quality information from reliable sources that is appropriate, current, complete, accurate, accessible, and provided on a timely basis to achieve the entity's objectives.[41] Similarly, OMB Circular No. A-123 states that effective risk management is based on the best available information. Because the risk registers are Bureau management's primary source of information regarding risks to the census—and currently their only source of information on program-level risk mitigation—including this information in the risk registers would help to support Bureau officials' ability to manage risks to the 2020 Census.

[39] In particular, the Bureau's decennial risk management plan does not require that mitigation and contingency plans entered in the risk registers include monitoring plans, activity start and completion dates, implementation status for contingency activities, individuals responsible for activity completion, or clearly defined trigger events. It does, however, require the risk register entries to include all key activities and the implementation status for mitigation activities. In addition, it requires that mitigation but not contingency plans be kept up to date.

[40] Specifically, the Bureau's decennial risk management plan requires the separate plans, but not the risk register descriptions, to include activity start and completion dates and clearly defined trigger events.

[41] GAO-14-704G.

The Bureau's Approach to Managing Fraud Risk for the 2020 Census Generally Aligns with Selected Components of the Fraud Risk Framework but Does Not Yet Include a Fraud Risk Tolerance or Fraud Referral Plan

The Bureau has designed an approach for managing fraud risk for responses to the 2020 Census.[42] We found that the approach generally aligns with leading practices in the commit, assess, and design and implement components of the Fraud Risk Framework.[43] Specifically, the Bureau demonstrated commitment to combating fraud by creating a dedicated entity to lead antifraud efforts for the 2020 Census, conducted a fraud risk assessment, and developed a risk response plan, among other actions, consistent with leading practices from the selected components.[44] However, the Bureau has not yet determined the program's fraud risk tolerance or outlined plans for referring potential fraud to the Department of Commerce Office of Inspector General (OIG) to investigate. Bureau officials described plans and milestones to address these steps but not for updating the antifraud strategy to include them. *Standards for Internal Control* states that management should clearly document internal controls to achieve the entity's objectives and respond to risks.[45] In addition, management should use quality information that is current and complete. Updating the antifraud strategy to include the Bureau's fraud risk tolerance and plan for OIG referral will help to ensure that the strategy is current, complete, and conforms to leading practices. Appendix IV presents additional details of our review of applicable leading practices.

[42] The Bureau's fraud risk assessment identifies and addresses fraud risks such as those posed by individuals or groups.

[43] We reviewed the Bureau's design for managing fraud risk for the 2020 Census against leading practices in three of four components—commit, assess, and design and implement components. Specifically, we focused on the design for managing fraud risk related to self-responses received via the internet questionnaire, telephone interviews conducted by Census Questionnaire Assistance staff, or paper questionnaires returned to the Census Bureau. Our assessment is limited to a review of the presence or absence of leading practices from our Fraud Risk Framework.

[44] Bureau officials refer to their risk response plan as the Concept of Operations.

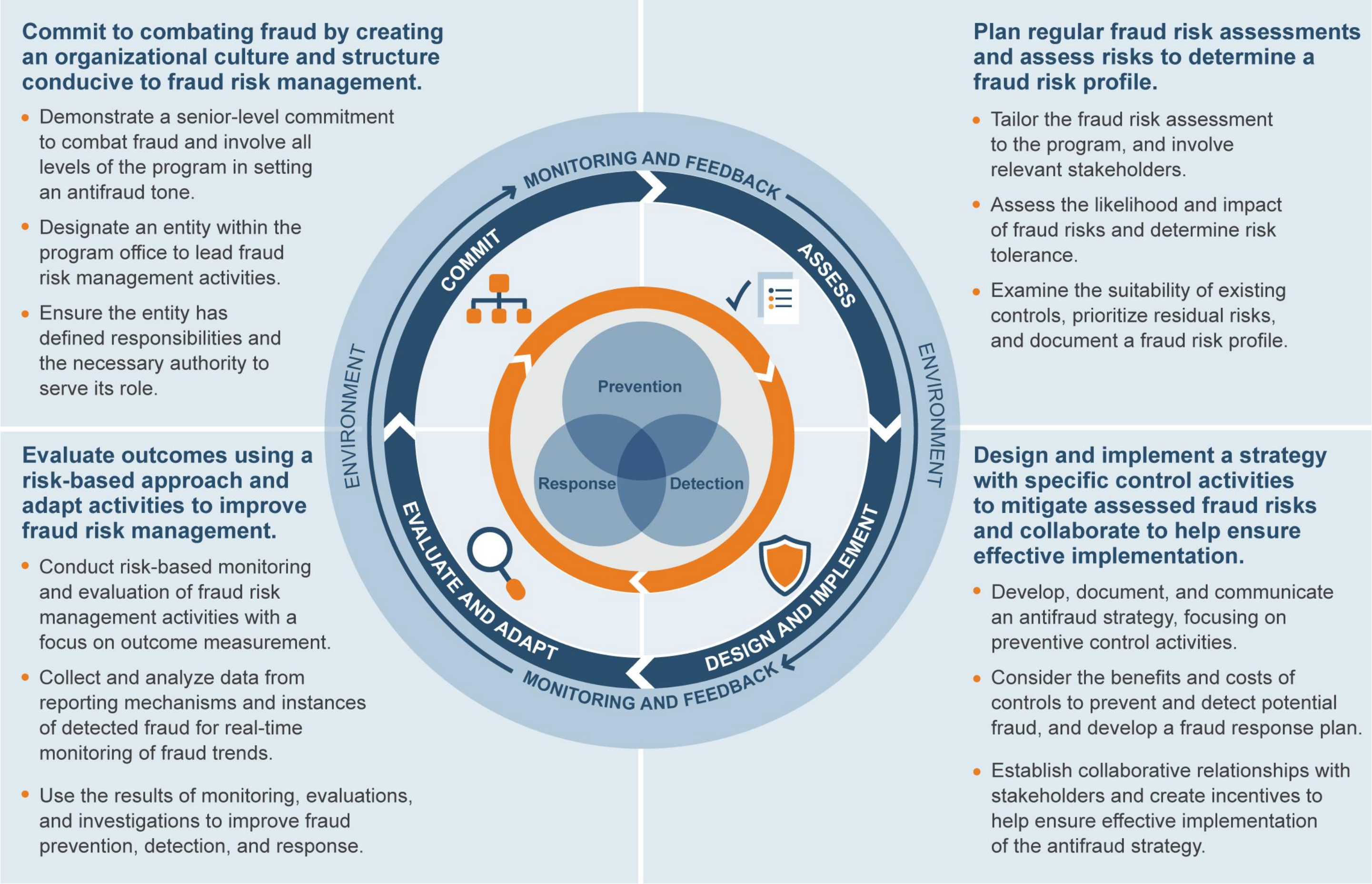
[45] GAO-14-704G.

Managers of federal programs maintain the primary responsibility for enhancing program integrity and managing fraud risks.[46] Those who are effective at managing their fraud risks collect and analyze data, identify fraud trends, and use the information to improve fraud risk management activities. Implementing effective fraud risk management processes is important to help ensure that federal programs fulfill their intended purpose, funds are spent effectively, and assets are safeguarded. The Fraud Risk Framework provides a comprehensive set of leading practices that serve as a guide for agency managers developing and enhancing efforts to combat fraud in a strategic, risk-based manner. The Fraud Risk Framework is also aligned with Principle 8 ("Assess Fraud Risk") of *Standards for Internal Control*.[47] It is designed to focus on preventive activities, which generally offer the most cost-efficient use of resources. The leading practices in the Fraud Risk Framework are organized into four components—commit, assess, design and implement, and evaluate and adapt—as depicted in figure 5.

[46] Fraud and fraud risk are distinct concepts. Fraud—obtaining something of value through willful misrepresentation—is a determination to be made through the judicial or other adjudicative system, and that determination is beyond management's professional responsibility. Fraud risk exists when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or are able to rationalize committing fraud. 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. When fraud risks can be identified and mitigated, agencies may be able to improve fraud prevention, detection, and response.

[47] GAO-14-704G.

Figure 5: The Fraud Risk Management Framework and Selected Leading Practices



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

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

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

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

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

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

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

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

Source: GAO. | GAO-19-399

The Bureau Designated an Entity to Manage Fraud Risk and Took Steps to Develop an Organizational Culture Conducive to Fraud Risk Management

Fraud Risk Framework Component:

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

Source: GAO. I GAO-19-399

The commit component of the Fraud Risk Framework calls for an agency to commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management. This component includes demonstrating a senior-level commitment to integrity and combating fraud, and establishing a dedicated entity to lead fraud risk management activities.

The Bureau has taken steps that align with all applicable leading practices in this component, according to our review. Specifically, senior-level commitment to combating fraud helps create an organizational culture to combat fraud. The Bureau showed this commitment by creating an antifraud group, made up of multiple operational divisions within the Bureau—the Decennial Census Management Division, Decennial Information Technology Division, and Decennial Contracts Execution Office—and staff from the Bureau's technical integration contractor.[48] Staff from these divisions make up the Self-Response Quality Assurance (SRQA) group with the primary purpose of identifying and responding to potentially fraudulent responses received in the 2020 Census.[49] SRQA members were assigned roles and responsibilities to combat fraud in the 2020 Census.

According to the framework, antifraud entities should understand the program and its operations; have defined responsibilities and the necessary authority across the program; and have a direct reporting line to senior-level managers within the agency. We found that SRQA met these leading practices through our interviews with knowledgeable officials who discussed the Bureau's strategy for managing fraud risk for the 2020 Census, and our review of documentation such as the fraud risk

[48] The Bureau tasked the technical integration contractor with providing the Bureau with Fraud Detection capabilities for the 2020 Census. The technical integration contractor developed the initial drafts of the fraud risk assessment to identify and evaluate scenarios in which fraudulent activity could impact the 2020 Census results, and a risk response plan that uses the fraud risk assessment to develop risk responses and its fraud detection systems. SRQA officials provided final versions of the fraud risk assessment and risk response plan in October 2018.

[49] In 2018, the Bureau changed the name of the operation from Fraud Detection to SRQA.

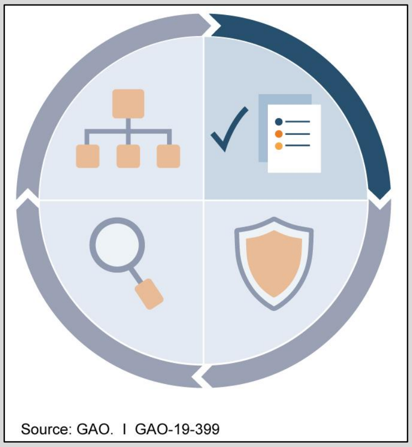
assessment, which listed roles and responsibilities for staff from the divisions in the antifraud group and the technical integration contractor. The group also directly reports to senior-level managers within the agency through weekly status reports that include milestones, activities, and challenges.

According to the Fraud Risk Framework, the antifraud entity, among other things, serves as the repository of knowledge on fraud risks and controls; manages the fraud risk-assessment process; leads or assists with trainings and other fraud-awareness activities; and coordinates antifraud initiatives across the program. The Bureau staffed the antifraud entity with members knowledgeable of the program and tasked them with managing the fraud risk assessment process. Also, the members facilitated communication with management and among stakeholders on fraud-related issues through weekly status reports. According to SRQA officials, issues and concerns are escalated to senior-level managers on an as-needed basis so they can be coordinated across the program.

The Bureau Assessed Fraud Risks and Developed a Risk Profile but Has Not Yet Determined Fraud Risk Tolerances

Fraud Risk Framework Component:

Plan regular fraud risk assessments and assess risks to determine a fraud risk profile



Source: GAO. I GAO-19-399

The assess component of the Fraud Risk Framework calls for federal managers to plan regular fraud risk assessments and to assess risks to determine a fraud risk profile. This includes assessing the likelihood and effect of fraud risks and determining a risk tolerance. Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. In the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks. Risk tolerance can be either qualitative or quantitative, but regardless of the approach, *Standards for Internal Control* states that managers should consider defining risk tolerances that are specific and measurable.[50]

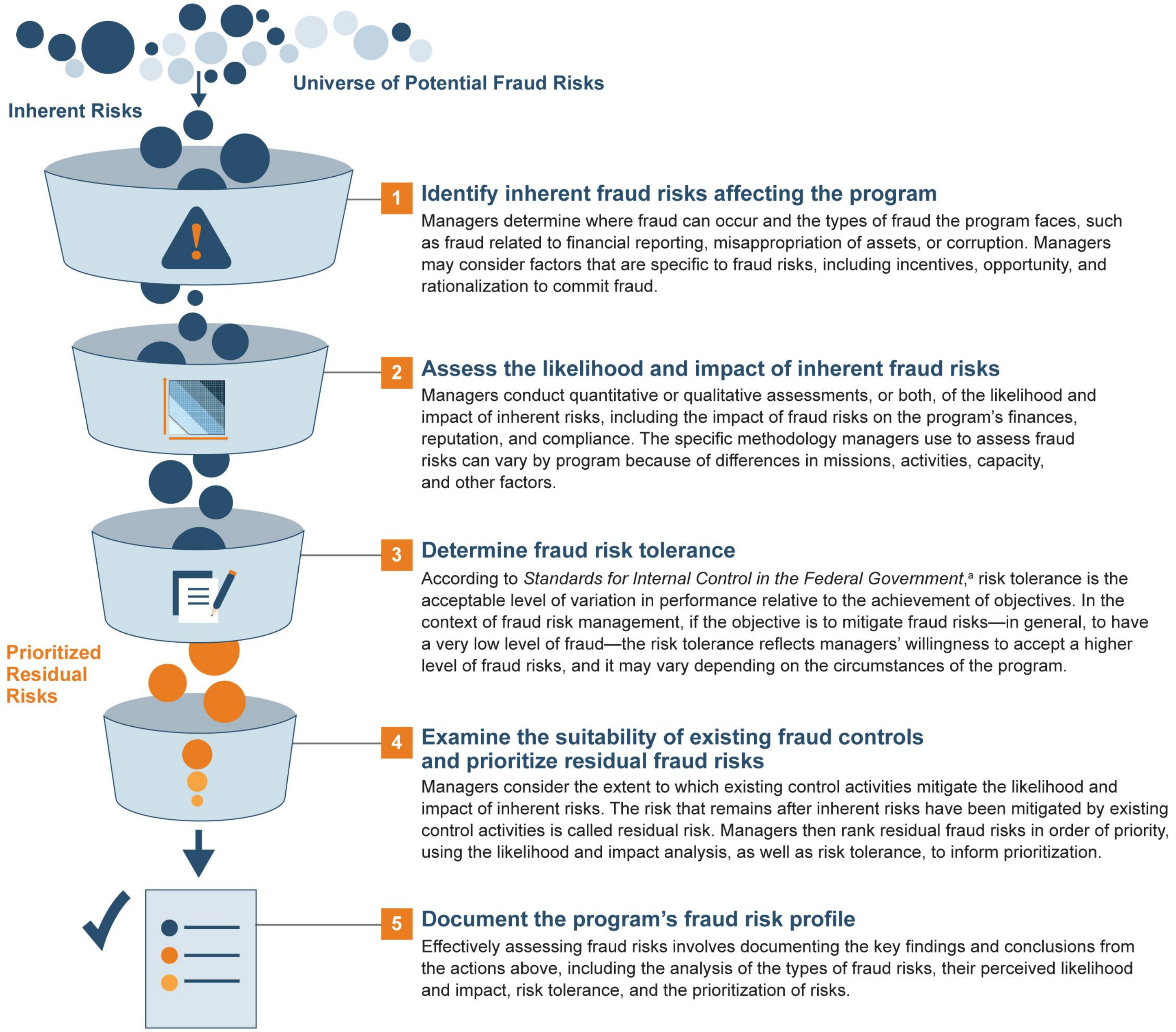
The first part of the fraud risk assessment process includes leading practices on tailoring the assessment to the program; planning to conduct assessments both at regular intervals and when there are changes to the program or operating environment; identifying specific tools, methods, and sources for gathering information about fraud risks; and involving relevant stakeholders in the assessment process. The Bureau has met all the leading practices in the first part of the assess component, according to our review. Specifically, the Bureau tailored the fraud risk assessment to the 2020 Census as this is the first time an internet-response option will be available for a decennial census in the United States. To identify specific tools, methods, and sources for gathering information about fraud risks, the Bureau met with relevant stakeholders, along with subject-matter experts, and conducted focus groups to develop various fraud scenarios that became a key part of the assessment. The Bureau also involved relevant stakeholders in the assessment process by outlining their roles and responsibilities for the 2020 Census. For example, the Decennial Census Management Division serves as the fraud lead and oversees managing risks such as operational implementation, methodology, and workload demands with support from the other operational divisions in the antifraud group.

[50] GAO-14-704G.

According to the Fraud Risk Framework while the timing can vary, effective antifraud entities plan to conduct fraud risk assessments at regular intervals and when there are changes to the program or operating environment, as fraud risk assessments are iterative and not meant to be onetime exercises. The Bureau's assessment takes this into account by acknowledging that risk assessment is an ongoing process. The assessment also states that the SRQA team will continue to evaluate and develop modeling techniques to train against existing fraud scenarios, and SRQA welcomes input from all stakeholders to ensure the Bureau identifies fraud risks, and works to implement controls and mitigation plans throughout the 2020 Census.

The second part of the fraud risk assessment process includes identifying inherent fraud risks affecting the program; assessing the likelihood and effect of inherent fraud risks; determining a fraud risk tolerance; examining the suitability of existing fraud controls and prioritizing residual fraud risks; and documenting the program's fraud risk profile (see figure 6).

Figure 6: Key Elements of the Fraud Risk Assessment Process



1 **Identify inherent fraud risks affecting the program**

Managers determine where fraud can occur and the types of fraud the program faces, such as fraud related to financial reporting, misappropriation of assets, or corruption. Managers may consider factors that are specific to fraud risks, including incentives, opportunity, and rationalization to commit fraud.

2 **Assess the likelihood and impact of inherent fraud risks**

Managers conduct quantitative or qualitative assessments, or both, of the likelihood and impact of inherent risks, including the impact of fraud risks on the program's finances, reputation, and compliance. The specific methodology managers use to assess fraud risks can vary by program because of differences in missions, activities, capacity, and other factors.

3 **Determine fraud risk tolerance**

According to *Standards for Internal Control in the Federal Government*,[a] risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. In the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a very low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks, and it may vary depending on the circumstances of the program.

4 **Examine the suitability of existing fraud controls and prioritize residual fraud risks**

Managers consider the extent to which existing control activities mitigate the likelihood and impact of inherent risks. The risk that remains after inherent risks have been mitigated by existing control activities is called residual risk. Managers then rank residual fraud risks in order of priority, using the likelihood and impact analysis, as well as risk tolerance, to inform prioritization.

5 **Document the program's fraud risk profile**

Effectively assessing fraud risks involves documenting the key findings and conclusions from the actions above, including the analysis of the types of fraud risks, their perceived likelihood and impact, risk tolerance, and the prioritization of risks.

Source: GAO. | GAO-19-399

[a] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014), 6.08.

The Bureau met three out of these five leading practices, including identifying inherent fraud risk; assigning numeric rankings for likelihood and impact of various fraud scenarios; and documenting the 2020 Census fraud risk profile, which outlines the strengths and weaknesses of the program. We concluded that one leading practice, examining the suitability of existing fraud controls and prioritizing residual fraud risks, was not applicable since the fraud detection system is new to the 2020 Census and changes the way the Bureau will detect different fraud scenarios. As a result, all fraud risks for the 2020 Census are residual risks. In reviewing the remaining leading practice in the fraud assessment processes, we found that after identifying inherent fraud risk and assigning numeric rankings for likelihood and impact of various fraud scenarios, the Bureau did not take the next step to determine a fraud risk tolerance.

Some of the steps the Bureau took to develop a risk response plan are similar to steps for developing a fraud risk tolerance. Specifically, the Bureau developed a process that classifies self-responses into risk categories of low, medium, or high. Bureau officials stated that they plan to use the classification to determine appropriate follow-up steps based on risk scores generated by its Fraud Detection Analytics Model that was develop by SRQA for the 2020 Census.[51] However, the Bureau did not define thresholds for the low-, medium-, and high-risk categories. These thresholds, if defined, would meet the intent of a fraud risk tolerance by indicating the acceptable level of variation in self-responses.

SRQA officials stated that they are developing these thresholds, and therefore its fraud risk tolerance, and plan to have them completed in August 2019. This includes reviewing available information collected through the 2018 End-to-End Test, running simulations, defining thresholds, and then evaluating the results to make adjustments. Responses will receive a score, but until the Bureau defines fraud risk tolerance thresholds for the low-, medium-, and high-risk categories, it cannot effectively implement its antifraud strategy to allocate responses for follow-up or inclusion. This may also affect the Bureau's ability to evaluate and adapt its antifraud strategy if initial benchmarks are not in place to use for monitoring, with subsequent adjustments potentially requiring additional time and resources. While officials described steps

[51] The Bureau described its Fraud Detection Analytics Models as a multilayered advanced analytical process that includes both near real-time and batch-job models that detect fraudulent responses.

and time frames to develop a fraud risk tolerance, they did not do so for updating the antifraud strategy to include the tolerance. Updating the antifraud strategy to include the Bureau's fraud risk tolerance will help to ensure that the strategy is current, complete, and conforms to leading practices.

The Bureau Designed a Response Plan and Collaborated Internally to Mitigate Fraud Risks but Did Not Include Plans to Refer Potential Fraud to the Office of Inspector General

Fraud Risk Framework Component:

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

Source: GAO. I GAO-19-399

The design and implement component of the Fraud Risk Framework calls for federal managers to design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation. This includes determining risk responses and documenting an antifraud strategy; designing and implementing specific control activities; developing a plan outlining how the program will respond to identified instances of fraud; and establishing collaborative relationships and creating incentives to help ensure effective implementation of the antifraud strategy.

For determining risk responses and documenting an antifraud strategy, the framework states that managers should (a) use the fraud risk profile to help decide how to allocate resources to respond to residual fraud risks; (b) develop, document, and communicate an antifraud strategy to employees and stakeholders that describes the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation; (c) establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity and external parties responsible for fraud controls, and communicate the role of the Office of Inspector General (OIG) to investigate potential fraud; (d) create timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluations; (e) demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile; and (f) link antifraud efforts to other risk management activities, if any.

The Bureau developed and documented an antifraud strategy (the fraud risk assessment and the risk response plan) and communicated it to applicable employees. Bureau officials provided final versions of the antifraud strategy in October 2018 and stated that all stakeholders were provided with excerpts applicable to their area.[52] The antifraud strategy outlines the beginning and end dates for fraud detection operations, and links to the highest residual fraud risks. The risk response includes links to other risk management activities such as a security layer that is designed, created, and maintained by the technical integration contractor security group in coordination with the Office of Information Security and Decennial Information Technology Division. According to the risk response plan, this group protects the fraud detection system and its associated systems from outside attacks such as hacks and distributed denial of service attacks.

However, we found that the Bureau's approach to managing fraud risk did not fully align with two leading practices in this component. First, until the Bureau defines its fraud risk tolerances, such as defining low-, medium-, or high-risk thresholds, it will not be able to effectively allocate resources to respond to residual fraud risks consistent with the Fraud Risk Framework's leading practices. Second, the Bureau did not initially coordinate with the Department of Commerce (Commerce) OIG about its antifraud strategy, which is not consistent with the leading practices. Such lack of coordination could have precluded the OIG from determining if potentially fraudulent activities should be investigated. After discussing the results of our review with the Bureau, the Bureau contacted and met with the Commerce OIG in February 2019. Based on the Bureau's notes from this meeting, the Bureau is on track to addressing the leading practice regarding coordination.

The framework states that to design and implement specific control activities to prevent and detect fraud, managers should (a) focus on fraud prevention over detection; (b) consider the benefits and costs of control activities to address identified residual risks; and (c) design and implement the control activities such as data-analytics to prevent and detect fraud. The 2020 Census antifraud control activities focus on detecting potentially fraudulent responses. The Bureaus plans to use a combination of data analytics and follow up to review response data before they are added to the Bureau's overall Census counts. The Bureau's efforts for the 2020 Census also focus on minimizing costs.

[52] The antifraud strategy, which includes the fraud risk assessment and risk response plan, are considered administratively restricted and are only distributed to stakeholders with a need to know. According to Bureau officials, this is because the strategy compiles a list of risk vectors that if obtained by the public could be used to avoid detection.

Specifically, if the Bureau's fraud detection can minimize the amount of cases that require manual investigation or work by field operations staff to collect the information again, it can reduce the cost and workload to the Bureau.

The framework states the antifraud strategy should also ensure that responses to identified instances of fraud are prompt and consistent. In addition, effective managers of fraud risks are to refer instances of potential fraud to the OIG or other appropriate parties, such as law-enforcement entities or the Department of Justice, for further investigation. The Bureau's plan describes its process for scoring responses using its Fraud Detection Analytics Model and then sorting responses into a low-, medium-, or high-risk category. The plan also outlines risk responses that depend on the risk category. For example, medium-risk responses are reviewed internally and could be incorporated into the census count or sent for additional follow up.

However, the Bureau's antifraud strategy does not call for instances of potential fraud to be referred to the Commerce OIG. Specifically, the Bureau's fraud risk assessment and risk response plan do not mention the Commerce OIG. Bureau officials stated that the Commerce OIG did not participate in the development of these documents. In February 2019, after we discussed the results of our review with the Bureau, the Bureau met with the Commerce OIG to discuss potential referrals. As a result, the Bureau agreed to develop and share with the Commerce OIG a plan that outlines a potential referral process by summer 2019.

Managers who effectively manage fraud risks collaborate and communicate with stakeholders to share information on fraud schemes and the lessons learned from fraud control activities. The framework describes collaborative relationships as including other offices within the agency; federal, state, and local agencies; private-sector partners; law-enforcement entities; and entities responsible for control activities. In addition, managers should collaborate and communicate with the OIG to improve their understanding of fraud risks and align their efforts to address fraud. The Bureau collaborated internally with groups such as the Security Operations Center that maintain the security layer that protects Bureau systems and the nonresponse follow-up groups that visit households to collect information again. The Bureau also provided contractors with guidance by finalizing the antifraud strategy and incentives by entering into an agreement with the technical integrator contractor, which allows the Bureau to exercise an option to continue the contract for another year.[53] However, the Bureau did not begin to collaborate and communicate with the Commerce OIG to improve its understanding of fraud risks and align efforts to address fraud until after we discussed the results of our review with the Bureau.

Bureau officials viewed the primary purpose of the fraud detection system as a way to improve data reliability, according to interviews. As a result, in 2018, the Bureau changed the name of the operation from Fraud Detection to SRQA. According to Bureau officials, the change better reflects the operation's focus on detecting potential falsification in decennial census response data and referring suspected responses to a field resolution operation to collect the data again. Bureau officials initially stated that SRQA would not conduct investigations that lead to the kind of law enforcement activities traditionally associated with fraud detection. As mentioned above, the Bureau met with the Commerce OIG in February 2019 to discuss the potential for referrals and, according to the Bureau, initiate a process for doing so. However, officials did not discuss steps and a time frame for updating the antifraud strategy to include this process. Doing so will help to ensure that the strategy is current, complete, and conforms to leading practices.

Conclusions

Adequately addressing risks to the census is critical for ensuring a cost-effective and high-quality enumeration. The Bureau has taken important steps to address risks to the 2020 Census, but with less than a year until Census Day, the Bureau has not developed mitigation and contingency plans for all risks that require them. In addition, the Bureau does not have clear time frames for developing and obtaining management approval of mitigation and contingency plans, and some risks have gone without required plans for months and years. Moreover, the status of some plans is unclear and not all plans have received management approval. Some of the plans the Bureau has developed are missing key attributes we identified for helping to ensure the plans contain the information needed

[53] For creating incentives for employees to manage risks, we concluded that this leading practice was not applicable. Specifically, this leading practice may be more relevant at the Bureau level that covers multiple programs than just the 2020 Census that has fraud detection group specifically tasked with reviewing all self-responses submitted for the 2020 Census and identifying potential fraud.

to manage risks. For example, none of the Bureau’s plans described how the Bureau will monitor the risk response, so the Bureau may not be able to track whether the plans are working as intended. These issues have arisen in some instances because the Bureau’s decennial risk management plan does not require mitigation and contingency plans to have each of the seven key attributes we identified; in other instances, the issues have arisen because Bureau officials do not always hold risk owners accountable for fulfilling all their risk management responsibilities. Consistently documenting risk management activities would support management’s ability to more quickly make informed decisions in response to risks confronting the 2020 Census. It would also help protect the Bureau from losing institutional knowledge in the event risk owners change roles or leave the agency.

The Bureau’s fraud risk strategy generally aligned with our Fraud Risk Framework, including developing response plans and collaborating internally to address risks. However, the Bureau has not yet determined the program’s fraud risk tolerance or outlined a plan for referring potential fraud to the Commerce OIG to investigate, but plans to do so later this year. Setting a tolerance would help the Bureau monitor risks, and referring potential fraud to the Commerce OIG would allow it to determine if further investigation is appropriate. In addition to taking these actions, updating the antifraud strategy to include the Bureau’s fraud risk tolerance and plan for OIG referral will help to ensure that the strategy is current, complete, and conforms to leading practices.

Recommendations for Executive Action

We are making the following seven recommendations to the Department of Commerce and the Census Bureau:

The Secretary of Commerce should ensure that the Director of the Census Bureau develops and obtains management approval of mitigation and contingency plans for all risks that require them. (Recommendation 1)

The Secretary of Commerce should ensure that the Director of the Census Bureau updates the Bureau’s decennial risk management plan to include clear time frames for developing and obtaining management approval of mitigation and contingency plans. (Recommendation 2)

The Secretary of Commerce should ensure that the Director of the Census Bureau updates the Bureau’s decennial risk management plan to require that portfolio and program risk registers include a clear indication of the status of mitigation plans. (Recommendation 3)

The Secretary of Commerce should ensure that the Director of the Census Bureau updates the Bureau’s decennial risk management plan to require that risk mitigation and contingency plans, including the risk register descriptions and separate plans, have the seven key attributes for helping to ensure they contain the information needed to manage risk. (Recommendation 4)

The Secretary of Commerce should ensure that the Director of the Census Bureau holds risk owners accountable for carrying out their risk management responsibilities. (Recommendation 5)

The Secretary of Commerce should ensure that the Director of the Census Bureau updates the Bureau’s antifraud strategy to include a fraud risk tolerance prior to beginning the 2020 Census and adjust as needed. (Recommendation 6)

The Secretary of Commerce should ensure that the Director of the Census Bureau updates the Bureau’s antifraud strategy to include the Bureau’s plans for referring instances of potential fraud to the Department of Commerce Office of Inspector General for further investigation. (Recommendation 7)

Agency Comments

We provided a draft of this report to the Secretary of Commerce. In its written comments, reproduced in appendix V, the Department of Commerce agreed with our findings and recommendations and said it would develop an action plan to address them. The Census Bureau also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the Secretary of Commerce, the Director of the U.S. Census Bureau, and the appropriate congressional committees. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report please contact Robert Goldenkoff at (202) 512-2757 or goldenkoffr@gao.gov or Rebecca Shea at (202) 512-6722 or shear@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.

Robert Goldenkoff

Robert Goldenkoff
Director
Strategic Issues

Rebecca Shea

Rebecca Shea
Director
Forensic Audits and Investigative Service

List of Requesters

The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Elijah E. Cummings
Chairman
The Honorable Jim Jordan
Ranking Member
Committee on Oversight and Reform
House of Representatives

The Honorable Gerald E. Connolly
Chairman
The Honorable Mark Meadows
Ranking Member
Subcommittee on Government Operations
Committee on Oversight and Reform
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The objectives of this study were to examine (1) what risks to the 2020 Census the Census Bureau (Bureau) has identified, (2) the risks for which the Bureau has mitigation and contingency plans, (3) the extent to which the Bureau's mitigation and contingency plans included information needed to manage risk, and (4) the extent to which the Bureau's approach to managing fraud risks to the 2020 Census aligns with leading practices outlined in our Fraud Risk Framework.

To answer the first three objectives, we reviewed Bureau documentation regarding its approach to managing risks facing the 2020 Census, including its decennial risk management plan, operational plan, governance management plan, Risk Review Board meeting minutes and agendas, and guidance and training documents. In addition, we interviewed Bureau officials responsible for overseeing risk management for the 2020 Census.

To describe what risks to the 2020 Census the Bureau has identified and the risks for which the Bureau has mitigation and contingency plans, we also reviewed the Bureau's portfolio- and program-level decennial risk registers.

To assess the extent to which the Bureau's mitigation and contingency plans included information needed to manage risk, we selected a nongeneralizable sample of six risks from the Bureau's risk registers based on factors such as likelihood of occurrence and potential impact (see table 3).

To select these risks, we began with the 12 risks identified by the Bureau in its 2020 Census Operational Plan as the "major concerns that could affect the design or successful implementation of the 2020 Census."[1] Next, we sorted the risks by numerical priority rating as of June 2018, a Bureau-assigned figure calculated by multiplying numerical scores for

[1] U.S. Census Bureau, *2020 Census Operational Plan: A New Design for the 21st Century*, Version 3.0 (Washington, D.C.: Sept. 30, 2017).

likelihood of occurrence and potential impact (see figure 3). We then selected the six risks with the highest priority ratings. For each selected risk, we reviewed relevant Bureau documentation—including risk mitigation and contingency plans—and we conducted semistructured interviews with the Bureau officials responsible for managing the risk.

In addition, drawing principally from our Enterprise Risk Management (ERM) framework as well as secondary sources, we identified seven key attributes for risk mitigation and contingency plans to help ensure they contain the information needed to manage risks (see figure 4). Specifically, we reviewed our ERM framework and other relevant prior work on risk management, as well as commonly used risk management publications from sources including the Office of Management and Budget, the Project Management Institute, and the Chief Financial Officers Council and Performance Improvement Council. We analyzed these publications to identify portions relevant to risk mitigation and contingency planning. Next, we synthesized the information and derived attributes that appeared most important for effective risk mitigation and contingency plans. We assessed the attributes against the essential elements laid out in our ERM framework and found that each attribute aligned with one or more of the elements. Six of the seven attributes—all but clearly defined trigger events—are applicable to mitigation plans. Each of the seven attributes are applicable to contingency plans, although two attributes—activity start and completion dates and activity implementation status—are only applicable if the risk has been realized. We assessed the risk mitigation and contingency plans entered in the Bureau’s risk registers as of December 2018, as well as the separate mitigation and contingency plans for the six selected risks, against the seven key attributes.

To evaluate the extent to which the Bureau’s approach to managing fraud risks to the 2020 Census aligns with leading practices outlined in our Fraud Risk Framework, we reviewed Bureau documentation related to the 2020 Census antifraud strategy. This strategy includes a fraud risk assessment that identifies and evaluates scenarios in which fraudulent activity could impact the 2020 Census results. It also includes a concept of operations that uses the fraud risk assessment to develop risk responses and its fraud detection systems. In addition, we interviewed Bureau officials responsible for antifraud efforts for the 2020 Census. We evaluated the information gathered based on the commit, assess, and design and implement components of our Fraud Risk Framework.

Our assessment was limited to a review of the presence or absence of leading practices from the framework, not whether they were sufficient. We also did not review the leading practices for the "evaluate and adapt" component of the framework. This component focuses on evaluating outcomes using a risk-based approach and then adapting activities established in the other components to improve fraud risk management. Because the census is not scheduled to start until 2020, the Bureau will not be able to implement leading practices such as:

- monitoring and evaluating the effectiveness of preventive activities;
- measuring outcomes, in addition to outputs, of fraud risk management activities;
- or using the results of monitoring and evaluations to improve the design and implementation of fraud risk management activities.

We conducted this performance audit from May 2018 to May 2019 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.

Appendix II: U.S. Census Bureau Operations Supporting the 2020 Census

Table 5: 2020 Census Operations

Area	Operation	Purpose
Program Management	Program Management	Define and implement program management policies, processes, and the control functions for planning and implementing the 2020 Census to ensure an efficient and well-managed program.
Census / Survey Engineering	Systems Engineering and Integration	Manage the delivery of an Information Technology (IT) “System of Systems” to meet 2020 Census business and capability requirements.
	Security, Privacy, and Confidentiality	Ensure all 2020 Census operations and systems adhere to laws, policies, and regulations that ensure appropriate systems and data security, and protect respondent and employee privacy and confidentiality.
	Content and Forms Design	Identify and finalize content and design of questionnaires and other associated nonquestionnaire materials. Ensure consistency across data collection modes and operations. Provide optimal design and content of the questionnaires to encourage high response rates.
	Language Services	Assess and support language needs of non-English speaking populations. Determine the number of non-English languages and level of support for the 2020 Census. Optimize the non-English content of questionnaires and associated nonquestionnaire materials across data collection modes and operations. Ensure cultural relevancy and meaningful translation of 2020 Census questionnaires and associated nonquestionnaire materials.
Frame	Geographic Programs	Provide the geographic foundation to support 2020 Census data collection and tabulation activities within the Master Address File/Topologically Integrated Geographic Encoding and Referencing System. This system serves as the national repository for all spatial, geographic, and residential address data needed for census and survey data collection, data tabulation, data dissemination, geocoding services, and map production.
	Local Update of Census Addresses	Provide an opportunity for tribal, federal, state, and local governments to review and improve the address lists and maps used to conduct the 2020 Census as required by Public Law 103-430.
	Address Canvassing	Deliver a complete and accurate address list and spatial database for enumeration and determining the type and address characteristics for each living quarter.
Response Data	Forms Printing and Distribution	Print and distribute internet invitation letters, reminder cards or letters or both, questionnaire mailing packages, and materials for other special operations, as required. Other materials required to support field operations are handled in the Decennial Logistics Management operation.
	Paper Data Capture	Capture and convert data from the 2020 Census paper questionnaires, including mail receipt, document preparation, scanning, optical character and mark recognition, data delivery, checkout, and form destruction.

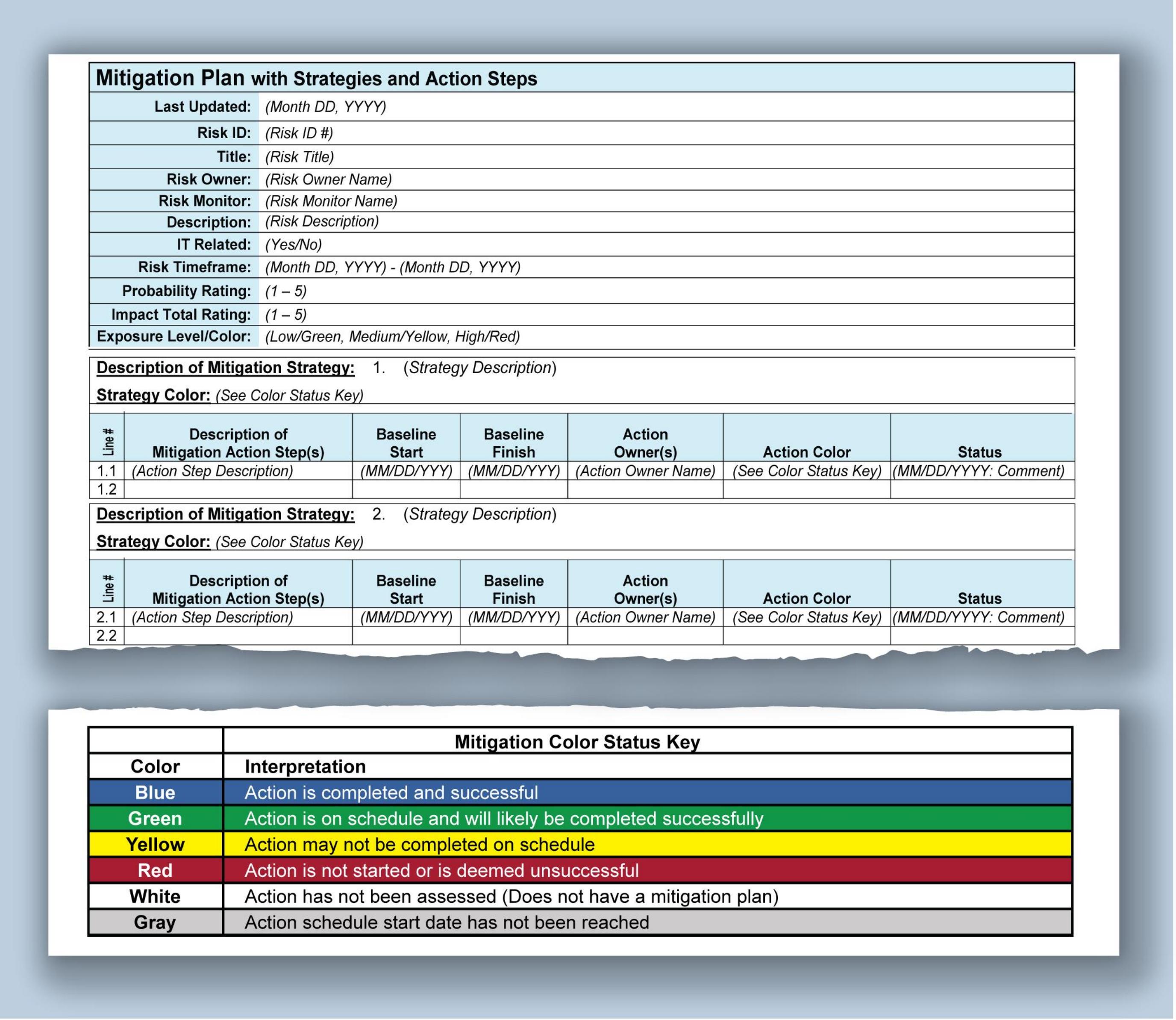
Area	Operation	Purpose
	Integrated Partnership and Communications	Communicate the importance of participating in the 2020 Census to the entire population of the 50 states, the District of Columbia, and Puerto Rico to support field recruitment efforts, engage and motivate people to self-respond (preferably via the internet), raise and keep awareness high throughout the entire 2020 Census to encourage response, and effectively support dissemination of Census data to stakeholders and the public.
	Internet Self-Response	Maximize online response to the 2020 Census via contact strategies and improved access for respondents. Collect response data via the internet to reduce paper and nonresponse follow-up.
Response Data	Non-ID Processing	Make it easy for people to respond anytime and anywhere to increase self-response rates by providing response options that do not require a unique Census ID. Maximize real-time matching of non-ID respondent addresses to the census living quarters address inventory, assigning nonmatching addresses to census blocks.
	Update Enumerate	Update the address and feature data and enumerate respondents in person. Designated to occur in areas where the initial visit requires enumerating while updating the address frame, particularly in remote geographic areas that have unique challenges associated with accessibility.
	Update Leave	Update the address and feature data and leave a choice questionnaire package at every housing unit identified to allow the household to self-respond. Designed to occur in areas where the majority of housing units do not have a city-style address to receive mail.
	Group Quarters	Enumerate people living or staying in group quarters and provide an opportunity for people experiencing homelessness and receiving service at service-based locations, such as soup kitchens, to be counted in the census.
	Enumeration at Transitory Locations	Enumerate individuals in occupied units at transitory locations who do not have a usual home elsewhere, such as recreational vehicle parks, campgrounds, racetracks, circuses, carnivals, marinas, hotels, and motels.
	Census Questionnaire Assistance	Provide questionnaire assistance for respondents by answering questions about specific items on the census form or other frequently asked questions about the 2020 Census, and provide an option for respondents to complete a census interview over the telephone. Also provide outbound calling support of nonresponse follow-up reinterview and coverage improvement.
	Nonresponse Follow-up	Determine housing unit status for nonresponding addresses that do not self-respond to the 2020 Census and enumerate households that are determined to have a housing unit status of occupied.
	Response Processing	Create and distribute the initial 2020 Census enumeration universe, assign the specific enumeration strategy for each living quarter based on case status and associated paradata, create and distribute workload files required for enumeration operations, track case enumeration status, run postdata collection processing actions in preparation for producing the final 2020 Census results, and check for fraudulent returns.
	Federally Affiliated Count Overseas	Obtain counts by home state of U.S. military and federal civilian employees stationed or deployed overseas and their dependents living with them.
Publish Data	Data Products and Dissemination	Prepare and deliver the 2020 Census population counts to the President of the United States for congressional apportionment, tabulate and disseminate 2020 Census data products for use by the states for redistricting, and tabulate and disseminate 2020 Census data for use by the public.
	Redistricting Data	Provide to each state the legally required Public Law 94-171 redistricting data tabulations by the mandated deadline of 1 year from Census Day (April 1, 2021).

Area	Operation	Purpose
	Count Review	Enhance the accuracy of the 2020 Census through remediating potential gaps in coverage by implementing an efficient and equitable process to identify and correct missing or geographically misallocated large group quarters and their population, and positioning remaining count issues for a smooth transition to the Count Question Resolution Operation.
	Count Question Resolution	Provide a mechanism for governmental units to challenge their official 2020 Census results.
	Archiving	Coordinate storage of the materials and data and provide 2020 Census records deemed permanent, including files containing individual responses, to the National Archives and Records Administration and to the National Processing Center to use as source materials to conduct the Age Search Service. Also store data to cover in-house needs.
	Island Areas Censuses	Enumerate all residents of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the U.S. Virgin Islands; process and tabulate the collected data; and disseminate data products to the public.
Test and Evaluation	Coverage Measurement Design and Estimation	Develop the survey design and sample for the Post-Enumeration Survey of the 2020 Census and produce estimates of census coverage based on the Post-Enumeration Survey.
	Coverage Measurement Matching	Identify matches, nonmatches, and discrepancies between the 2020 Census and the Post-Enumeration Survey for both housing units and people in the same areas. Both computer and clerical components of matching are conducted.
	Coverage Measurement Field Operations	Collect person and housing unit information (independent from the 2020 Census operations) for the sample of housing units in the Post-Enumeration Survey to help understand census coverage and to detect erroneous enumerations.
	Evaluations and Experiments	Document how well the 2020 Census was conducted, and analyze, interpret, and synthesize the effectiveness of census components and their impact on data quality or coverage or both. Measure the success of critical 2020 Census operations. Formulate and execute an experimentation program to support early planning and inform the transition and design of the 2030 Census and produce an independent assessment of population and housing unit coverage.
Infrastructure	Decennial Service Center	Support 2020 Census field operations for decennial staff (i.e., headquarters, PDC, Regional Census Center, Area Census Office, Island Areas Censuses, remote workers, and listers/enumerators.)
	Field Infrastructure	Provide the administrative infrastructure for data collection operations covering the 50 states, the District of Columbia, and Puerto Rico.
	Decennial Logistics Management	Coordinate space acquisition and lease management for the regional census centers, area census offices, and the Puerto Rico area office; and provide logistics management support services (e.g., kit assembly, supplies to field staff).
	IT Infrastructure	Provide the IT-related Infrastructure support to the 2020 Census, including enterprise systems and applications, 2020 Census-specific applications, Field IT infrastructure, mobile computing, and cloud computing.

Source: GAO analysis of U.S. Census Bureau 2020 Census Operational Plan. | GAO-19-399

Appendix III: 2020 Census Portfolio Risk Mitigation and Contingency Plan Templates

Figure 7: 2020 Census Portfolio Risk Mitigation Plan Template



Mitigation Plan with Strategies and Action Steps

Last Updated:	*(Month DD, YYYY)*
Risk ID:	*(Risk ID #)*
Title:	*(Risk Title)*
Risk Owner:	*(Risk Owner Name)*
Risk Monitor:	*(Risk Monitor Name)*
Description:	*(Risk Description)*
IT Related:	*(Yes/No)*
Risk Timeframe:	*(Month DD, YYYY) - (Month DD, YYYY)*
Probability Rating:	*(1 – 5)*
Impact Total Rating:	*(1 – 5)*
Exposure Level/Color:	*(Low/Green, Medium/Yellow, High/Red)*

Description of Mitigation Strategy: 1. (*Strategy Description*)

Strategy Color: *(See Color Status Key)*

Line #	Description of Mitigation Action Step(s)	Baseline Start	Baseline Finish	Action Owner(s)	Action Color	Status
1.1	*(Action Step Description)*	*(MM/DD/YYY)*	*(MM/DD/YYY)*	*(Action Owner Name)*	*(See Color Status Key)*	*(MM/DD/YYYY: Comment)*
1.2						

Description of Mitigation Strategy: 2. (*Strategy Description*)

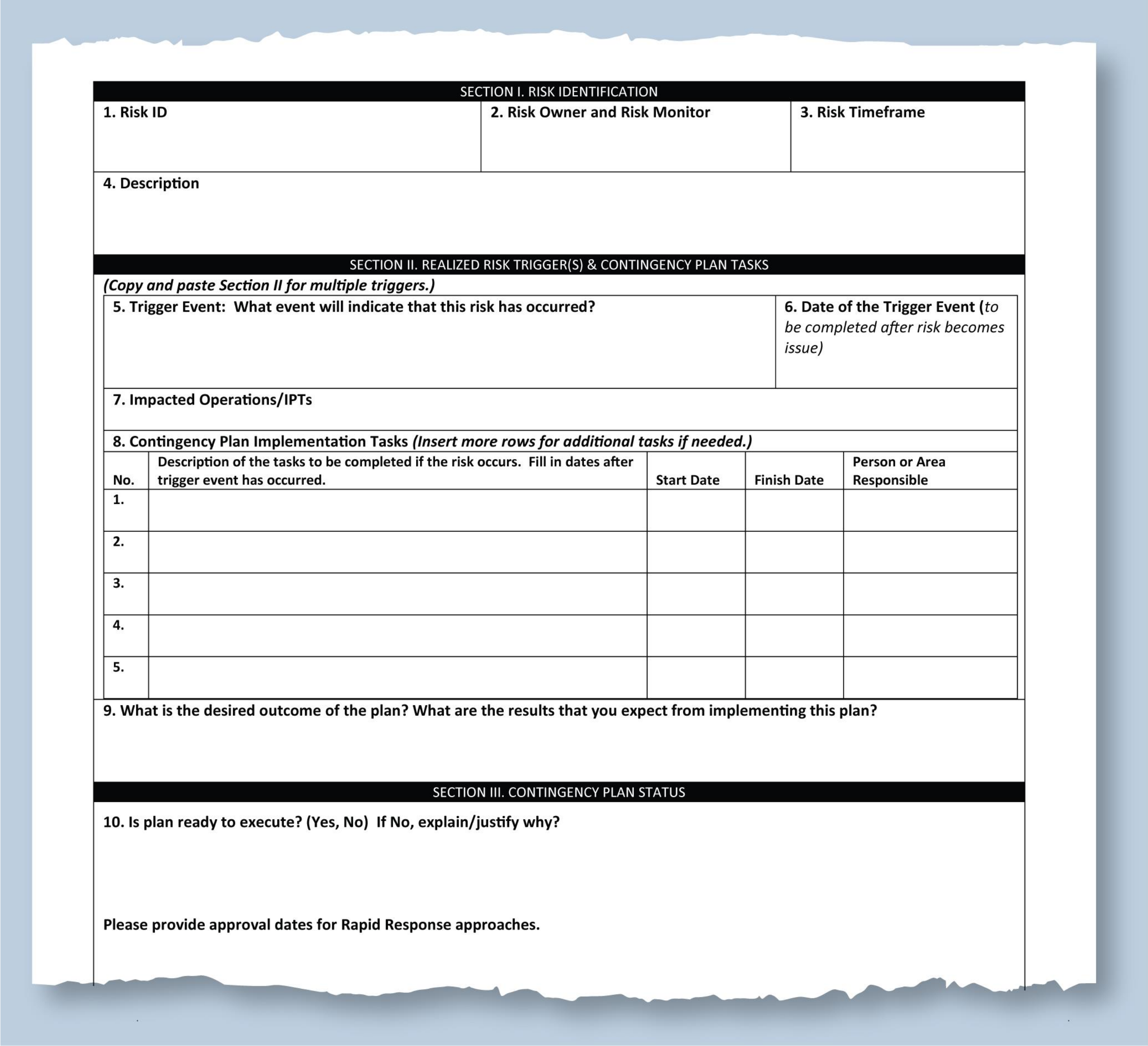
Strategy Color: *(See Color Status Key)*

Line #	Description of Mitigation Action Step(s)	Baseline Start	Baseline Finish	Action Owner(s)	Action Color	Status
2.1	*(Action Step Description)*	*(MM/DD/YYY)*	*(MM/DD/YYY)*	*(Action Owner Name)*	*(See Color Status Key)*	*(MM/DD/YYYY: Comment)*
2.2						

	Mitigation Color Status Key
Color	Interpretation
Blue	Action is completed and successful
Green	Action is on schedule and will likely be completed successfully
Yellow	Action may not be completed on schedule
Red	Action is not started or is deemed unsuccessful
White	Action has not been assessed (Does not have a mitigation plan)
Gray	Action schedule start date has not been reached

Source: U.S. Census Bureau. I GAO-19-399

Figure 8: 2020 Census Portfolio Risk Contingency Plan Template



SECTION I. RISK IDENTIFICATION

1. Risk ID	**2. Risk Owner and Risk Monitor**	**3. Risk Timeframe**

4. Description

SECTION II. REALIZED RISK TRIGGER(S) & CONTINGENCY PLAN TASKS

(Copy and paste Section II for multiple triggers.)

5. Trigger Event: What event will indicate that this risk has occurred?	**6. Date of the Trigger Event (***to be completed after risk becomes issue)*

7. Impacted Operations/IPTs

8. Contingency Plan Implementation Tasks *(Insert more rows for additional tasks if needed.)*

No.	Description of the tasks to be completed if the risk occurs. Fill in dates after trigger event has occurred.	Start Date	Finish Date	Person or Area Responsible
1.				
2.				
3.				
4.				
5.				

9. What is the desired outcome of the plan? What are the results that you expect from implementing this plan?

SECTION III. CONTINGENCY PLAN STATUS

10. Is plan ready to execute? (Yes, No) If No, explain/justify why?

Please provide approval dates for Rapid Response approaches.

Source: U.S. Census Bureau. I GAO-19-399

Appendix IV: Leading Practices from GAO's Fraud Risk Framework

For the 2020 Census, the Census Bureau (Bureau) is trying to increase participation and reduce costs by offering more self-response options to households. This includes self-responses received via internet, phone, or mail. In 2018, the Self-Response Quality Assurance group finalized its antifraud strategy that includes a fraud risk assessment and risk response plan that focuses specifically on these responses. We developed a data collection instrument to structure our review of the antifraud strategy as it related to the commit, assess, and design and implement components of our Fraud Risk Framework.

Our assessment was limited to a review of the presence or absence of leading practices from the framework, not whether they were sufficient. We also did not assess the Bureau's approach against leading practices in the "evaluate and adapt" component of the framework because the Bureau will not be able to implement practices in this component until the 2020 Census begins. The following table summarizes our comparison of the Bureau's antifraud strategy to leading practices in the fraud risk framework.

Table 6: Leading Practices from GAO's Fraud Risk Framework Reflected in the Bureau's Antifraud Strategy for Self-Response Program as of February 2019

Component	Overarching concept	Leading practice	Element present
Commit	1.1 Create an Organizational Culture to Combat Fraud at All Levels of the Agency	Demonstrate a senior-level commitment to integrity and combating fraud.	Yes
		Involve all levels of the agency in setting an antifraud tone that permeates the organizational culture.	Not applicable[a]
	1.2 Create a Structure with a Dedicated Entity to Lead Fraud Risk Management Activities	Designate an entity to design and oversee fraud risk management activities that • understands the program and its operations, as well as the fraud risks and controls throughout the program; • has defined responsibilities and the necessary authority across the program; • has a direct reporting line to senior-level managers within the agency; and • is located within the agency and not the Office of Inspector General (OIG), so the latter can retain its independence to serve its oversight role.	Yes
		In carrying out its role, the antifraud entity, among other things • serves as the repository of knowledge on fraud risks and controls; • manages the fraud risk-assessment process; • leads or assists with trainings and other fraud-awareness activities; and • coordinates antifraud initiatives across the program.	Yes
Assess	2.1 Plan Regular Fraud Risk Assessments That Are Tailored to the Program	Tailor the fraud risk assessment to the program.	Yes
		Plan to conduct fraud risk assessments at regular intervals and when there are changes to the program or operating environment, as assessing fraud risks is an iterative process.	Yes
		Identify specific tools, methods, and sources for gathering information about fraud risks, including data on fraud schemes and trends from monitoring and detection activities.	Yes
		Involve relevant stakeholders in the assessment process, including individuals responsible for the design and implementation of fraud controls.	Yes
	2.2 Identify and Assess Risks to Determine the Program's Fraud Risk Profile	Identify inherent fraud risks affecting the program.	Yes
		Assess the likelihood and impact of inherent fraud risks. • Involve qualified specialists, such as statisticians and subject-matter experts, to contribute expertise and guidance when employing techniques like analyzing statistically valid samples to estimate fraud losses and frequency. • Consider the nonfinancial impact of fraud risks, including impact on reputation and compliance with laws, regulations, and standards.	Yes
Assess		Determine fraud risk tolerance.	No
		Examine the suitability of existing fraud controls and prioritize residual fraud risks.	Not applicable[b]

Component	Overarching concept	Leading practice	Element present
		Document the program's fraud risk profile.	Yes
Design and Implement	3.1 Determine Risk Responses and Document an Antifraud Strategy Based on the Fraud Risk Profile	Use the fraud risk profile to help decide how to allocate resources to respond to residual fraud risks.	Partially[c]
		Develop, document, and communicate an antifraud strategy to employees and stakeholders that describes the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation.	Yes
		Establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity and external parties responsible for fraud controls, and communicate the role of OIG to investigate potential fraud.	Partially[d]
		Create timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluations.	Yes
		Demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile.	Yes
		Link antifraud efforts to other risk management activities, if any.	Yes
	3.2 Design and Implement Specific Control Activities to Prevent and Detect Fraud	Focus on fraud prevention over detection and response.	Yes
		Consider the benefits and costs of control activities to address identified residual risks.	Yes
		Design and implement the following control activities to prevent and detect fraud: • data-analytics activities, • fraud-awareness initiatives, • reporting mechanisms, and • employee-integrity activities.	Yes
	3.3 Develop a Plan Outlining How the Program Will Respond to Identified Instances of Fraud	Develop a plan outlining how the program will respond to identified instances of fraud and ensure the response is prompt and consistently applied.	Yes
		Refer instances of potential fraud to the OIG or other appropriate parties, such as law-enforcement entities or the Department of Justice, for further investigation.	No
	3.4 Establish Collaborative Relationships with Stakeholders and Create Incentives to Help Ensure Effective Implementation of the Antifraud Strategy	Establish collaborative relationships with internal and external stakeholders, including other offices within the agency; federal, state, and local agencies; private-sector partners; law-enforcement entities; and entities responsible for control activities to, among other things, • share information on fraud risks and emerging fraud schemes, and • share lessons learned related to fraud control activities.	Partially[e]
		Collaborate and communicate with the OIG to improve understanding of fraud risks and align efforts to address fraud.	No
Design and Implement		Create incentives for employees to manage risks and report fraud, including • creating performance metrics that assess fraud risk management efforts and employee integrity, particularly for managers; and • balancing fraud-specific performance metrics with other metrics related to employees' duties.	Not applicable[f]

Component	Overarching concept	Leading practice	Element present
		Provide guidance and other support and create incentives to help external parties, including contractors, effectively carry out fraud risk management activities.	Yes

Source: GAO.analysis of U.S. Census Bureau information.| GAO-19-399

[a] The Decennial Census is only one of the Bureau's programs. In this context setting an antifraud tone that permeates the organization culture would be more appropriate at the agency level and not specific to the 2020 Census.

[b] The fraud detection system is new to the 2020 Census and changes the way the Bureau will detect different fraud scenarios. As a result, all fraud risks for the 2020 Census are residual risks.

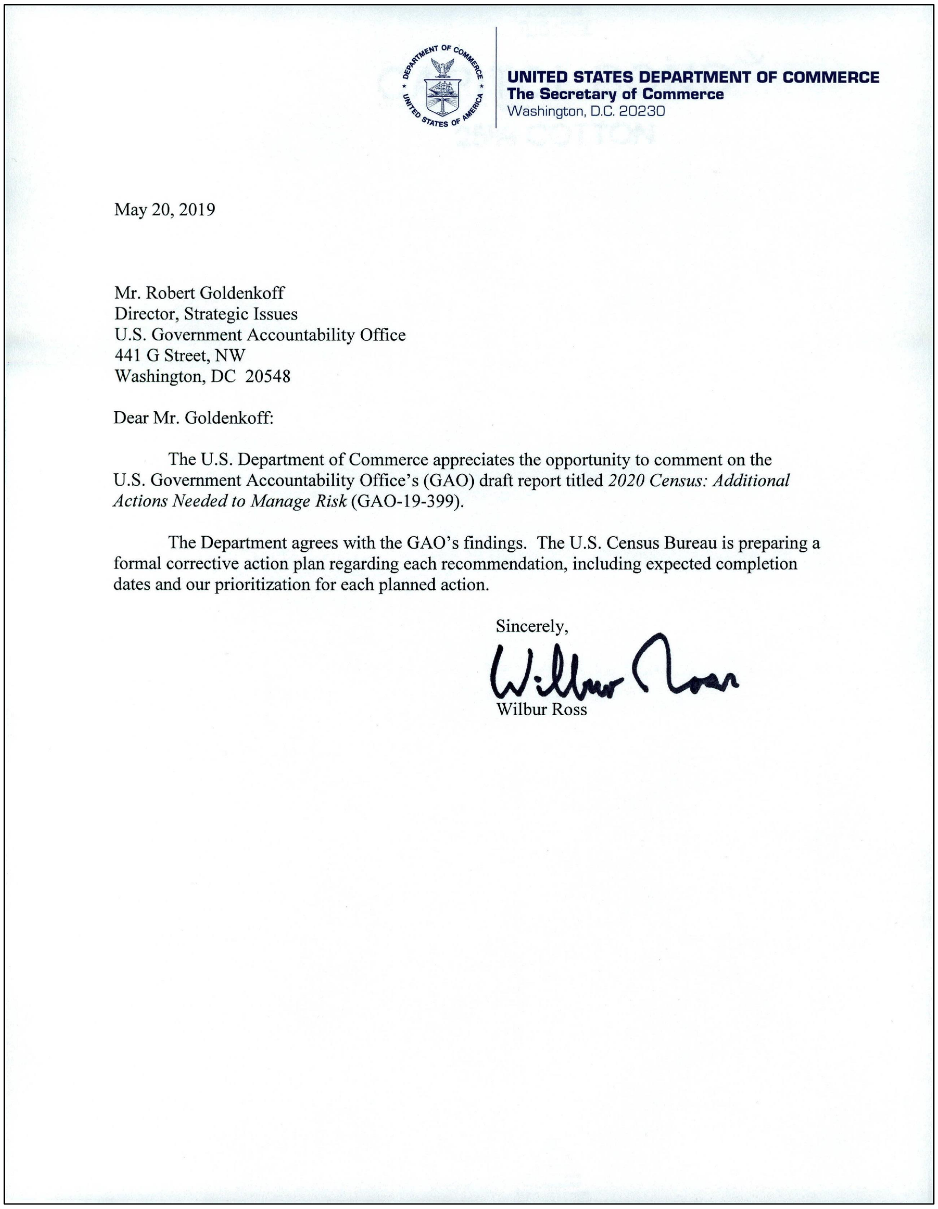
[c] Part of the fraud risk profile includes establishing a fraud risk tolerance. However, the Bureau did not define this tolerance, which affects its ability to allocate resources to respond to residual fraud risks.

[d] The Bureau did not involve the Department of Commerce (Commerce) OIG when developing their antifraud strategy.

[e] The Bureau collaborated internally with groups such as the Security Operations Center that maintain the security layer that protects Bureau systems and the nonresponse follow-up groups that visit households to collect information again. However, they did not coordinate externally with the Commerce OIG.

[f] Because the Bureau covers multiple programs, this leading practice may be more relevant across the Bureau than just the 2020 Census.

Appendix V: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

May 20, 2019

Mr. Robert Goldenkoff
Director, Strategic Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Goldenkoff:

The U.S. Department of Commerce appreciates the opportunity to comment on the U.S. Government Accountability Office's (GAO) draft report titled *2020 Census: Additional Actions Needed to Manage Risk* (GAO-19-399).

The Department agrees with the GAO's findings. The U.S. Census Bureau is preparing a formal corrective action plan regarding each recommendation, including expected completion dates and our prioritization for each planned action.

Sincerely,

Wilbur Ross

Wilbur Ross

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

Robert Goldenkoff, (202) 512-2757 or goldenkoffr@gao.gov

Rebecca Shea, (202) 512-6722 or shear@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Lisa Pearson and Philip Reiff (Assistant Directors), Emmy Rhine Paule and Ariel Vega (Analysts-in-Charge), Carole Cimitile, Ann Czapiewski, Robert Gebhart, Maria McMullen, Ty Mitchell, James Murphy, Carl Ramirez, Kayla Robinson, Kate Sharkey, Andrea Starosciak, Michael Steinberg, Umesh Thakkar, and Jon Ticehurst made significant contributions to this report.

Appendix VII: Accessible Data

Data Tables

Data Table for Figure 1: The Bureau Identified 330 Active Program Risks to the 2020 Census as of December 2018

Program / operation	Number of risks
Content and Forms Design	1
Enumeration at Transitory Locations	2
Archiving	3
Federally Affiliated Count Overseas	3
Language Services	3
Local Update of Census Addresses	3
Coverage Measurement Field Operations	4
Count Review	4
Integrated Partnership and Communications	4
Coverage Measurement Matching	5
Decennial Service Center	5
Island Areas Censuses	5
Paper Data Capture	5
Decennial Logistics Management	6
Update Enumerate	6
End-To-End Census Test	7
Group Quarters	7
Update Leave	7
Field Infrastructure	8
Internet Self-Response	8
Program Management	8
Redistricting Data	8
Response Processing	8
Data Products and Dissemination	9
Evaluations and Experiments	10
Address Canvassing	14
Non-ID Processing	15

Program / operation	Number of risks
Nonresponse Followup	16
Coverage Measurement Design and Estimation	18
Geographic Programs	22
Census Questionnaire Assistance	25
IT Infrastructure	37
Systems Engineering and Integration	44
Grand Total	330

Data Table for Figure 2: Active Risks to the 2020 Census as of December 2018, by Priority Classification

	Program	Portfolio	Total
High Priority	72	2	74
Medium Priority	148	23	171
Low Priority	110	5	115
Total	330	30	360

Text of Appendix V: Comments from the Department of Commerce

May 20, 2019

Mr. Robert Goldenkoff Director, Strategic Issues

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548 Dear Mr. Goldenkoff:

The U.S. Department of Commerce appreciates the opportunity to comment on the

U.S. Government Accountability Office's (GAO) draft report titled 2020 Census: Additional Actions Needed to Manage Risk (GAO-19-399).

The Department agrees with the GAO's findings. The U.S. Census Bureau is preparing a formal corrective action plan regarding each recommendation, including expected completion dates and our prioritization for each planned action.

Wilber Ross

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 GAO’s website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select “E-mail Updates.”

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 Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail 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/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548