United States Government Accountability Office

Report to the Chairman
Committee on Homeland Security and Governmental Affairs
U.S. Senate

April 2024

IT MODERNIZATION

Census Bureau Needs Reliable Cost and Schedule Estimates

GAO-24-105979

GAO Highlights

Highlights of GAO-24-105979, a report to the Chairman of the Committee on Homeland Security and Governmental Affairs, U.S. Senate

April 2024

IT MODERNIZATION

Census Bureau Needs Reliable Cost and Schedule Estimates

Why GAO Did This Study

The Census Bureau's IT systems are essential to collecting and providing data about the nation's people and economy. During the run up to the 2020 Census, the Bureau faced challenges in modernizing and consolidating its IT systems. For future surveys, including the 2030 Census, the Bureau has embarked on four modernization programs to collect, process, and disseminate data.

GAO was asked to review the Bureau's implementation of key modernization programs. This report (1) examines the extent to which the Bureau is implementing leading practices related to managing risks, requirements, cost, and schedule for a selected enterprise-wide IT program; and (2) describes the key cybersecurity and privacy challenges the Bureau faces in implementing its IT modernization programs and the extent to which the Bureau has plans to address them.

GAO selected the data dissemination program due to the maturity of its cost and schedule documentation. GAO assessed the program's management of risks, requirements, cost, and schedule against leading practices. In addition, GAO reviewed prior GAO reports and Bureau plans related to cybersecurity and privacy challenges, and interviewed Bureau officials.

What GAO Recommends

GAO is making five recommendations to the Department of Commerce related to managing requirements, estimating cost and schedule, and developing plans and time frames on cybersecurity and privacy challenges. Commerce concurred with the recommendations and stated it would take steps to improve in these areas.

View GAO-24-105979. For more information, contact Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

What GAO Found

The Census Bureau fully implemented selected leading practices for risk management, but it did not fully implement selected leading practices for managing requirements, cost, and schedule for the Center for Enterprise Dissemination Services and Consumer Innovation (an enterprise-wide data dissemination modernization program), as shown in the table.

Extent to Which the Census Bureau Implemented Selected Areas for Managing the Center for Enterprise Dissemination Services and Consumer Innovation Program

Management area	Overall assessment
Risk Management	● Fully implemented
Requirements Management	◕ Substantially implemented
Cost	◐ Partially implemented
Schedule	◔ Minimally implemented

Source: GAO analysis of Census Bureau data. | GAO-24-105979

The Bureau substantially implemented leading practices for requirements management. However, it did not consistently trace requirements forward and backward from their source to the end product. As a result, the program faces challenges in ensuring it adheres to project requirements. Additionally, the program's cost and schedule estimates were unreliable because the Bureau did not substantially or fully implement leading practices. Specifically:

- Although the program substantially met two of the four characteristics of a high-quality, reliable cost estimate (well documented and accurate), it only partially met the remaining two characteristics (credible and comprehensive).
- The program did not substantially meet any of the four characteristics of a reliable schedule: comprehensive, well constructed, credible, and controlled.

Without reliable cost and schedule estimates, the Bureau increases the risk of cost overruns and unmet performance targets.

GAO's prior work identified several cybersecurity and privacy challenges the Bureau faces implementing its IT modernization programs, including

- addressing cybersecurity workforce challenges,
- improving information security initiatives and programs,
- enhancing its detection and response to cyber incidents, and
- ensuring respondent privacy while maintaining the usability of public Census data.

The Bureau has taken steps to address these challenges but lacks detailed plans and strategies. For example, the Bureau drafted a strategy in 2023 to improve the cybersecurity of software development and operations. However, the strategy has not been finalized and does not include specific information (e.g., time frames) for accomplishing its objectives. In addition, the Bureau was unable to provide detailed information about the steps it plans to take to balance the privacy of respondents to the 2025 American Community Survey against the usability of public data. Until the Bureau develops detailed plans and time frames for these activities, it risks not meeting its objectives of effectively securing and protecting its IT systems and data.

Contents

Figures

Abbreviations

CEDCaP	Census Enterprise Data Collection and Processing
CEDSCI	Center for Enterprise Dissemination Services and Consumer Innovation
CMMI	Capability Maturity Model® Integration
DevSecOps	development, security, and operations
DICE	Data Ingest and Collection for the Enterprise
EDL	Enterprise Data Lake
ISACA	Information Systems Audit and Control Association
IT	information technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
WBS	work breakdown structure

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

April 29, 2024

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

Dear Mr. Chairman:

Modern, efficient IT systems are vital to the Census Bureau's mission to collect and provide comprehensive data about the nation's people and economy by conducting censuses and surveys. In the run-up to the 2020 Census, the Bureau attempted to modernize and consolidate its IT systems for data collection and processing into an enterprise-wide modernization program called Census Enterprise Data Collection and Processing (CEDCaP). However, the Bureau faced challenges while implementing CEDCaP, including monitoring risks, controlling IT costs, and managing the schedule for system development and testing. Ultimately, although CEDCaP delivered several systems that were used for the 2020 Census, the Bureau formally closed the program in March 2020 without delivering enterprise-wide data collection and processing capabilities.

The Bureau has begun planning and implementing major enterprise-wide IT programs for the next decade's surveys, including the 2030 Census. In addition to plans to integrate and manage the development of an enterprise-wide program for data collection—similar to CEDCaP—the Bureau also plans to develop and implement other programs for enterprise data storage and processing. In early 2022, we reported that it would be important to obtain early congressional oversight and stakeholder input in the planning for the 2030 Decennial Census.[1]

You asked us to evaluate the Bureau's implementation of the enterprise-wide IT programs for the 2030 Census and other Bureau surveys. This report (1) evaluates the extent to which the Bureau is implementing leading practices in monitoring and controlling risks, requirements, cost, and schedule for a selected enterprise-wide IT program, and (2) describes the key cybersecurity and privacy challenges the Bureau faces

[1]GAO, *2020 Census: Lessons Learned from Planning and Implementing the 2020 Census Offer Insights to Support 2030 Preparations*, GAO-22-104357 (Washington, D.C.: Feb. 11, 2022).

in implementing its IT modernization programs and determines the extent to which the Bureau has plans to address them.

For our first objective, we selected one of the Bureau's four enterprise-wide modernization programs to include in the scope of our review. We selected the Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI) program due to the maturity of its cost and schedule documentation. We determined that the other programs were not far enough along in their development to perform extensive and detailed assessments against the selected criteria. We collected documentation on the CEDSCI program's management of risks, requirements, cost, and schedule. We analyzed this documentation against leading practices from the Information Systems Audit and Control Association's (ISACA) Capability Maturity Model Integration (CMMI),[2] the GAO *Cost Estimating and Assessment Guide*, and the GAO *Schedule Assessment Guide*.[3]

We also interviewed Bureau officials to determine the extent to which they have implemented the leading practices. We corroborated our analyses by interviewing agency officials in the CEDSCI program, especially in cases where they do not appear to have met requirements.

For our second objective, we reviewed (1) prior reports from GAO and the Department of Commerce's Office of Inspector General, and (2) Bureau documentation on lessons learned from the 2020 Census. This enabled us to identify the key cybersecurity and privacy areas that pose significant challenges for the Bureau's IT modernization efforts. We reviewed documentation regarding activities the Bureau plans to take to address the identified cybersecurity and privacy challenges. We also interviewed Bureau officials to understand their plans to address the challenges. Additional details on our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from April 2022 to April 2024 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

[2]ISACA, *CMMI Model V2.2* (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

[3]GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, GAO-20-195G (Washington, D.C.: Mar. 12, 2020); *GAO Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The Census Bureau's mission is to collect and provide comprehensive data about the nation's people and economy. The data that the Bureau collects are essential to government functions, including apportioning seats in the House of Representatives, determining federal and state funding needs, and identifying how the COVID-19 pandemic affected education and employment. To collect these data, the Bureau conducts various censuses and surveys, including the decennial census, the Economic Census, and the American Community Survey.

Censuses and Surveys

The Census Bureau conducts over 100 different censuses and surveys, including the

- Decennial Census, used to apportion the seats of the House of Representatives and allocate billions of dollars each year in federal financial assistance;
- Economic Census, which serves as the benchmark for current economic activity, such as the gross domestic product; and
- American Community Survey, which is a source of social, demographic, economic, and housing information for the nation, states, counties, cities, and towns.

Source: GAO summary of Census Bureau information. | GAO-24-105979

Because of the importance of the data, IT systems and infrastructure that support data collection, processing, and dissemination are foundational to the Bureau's censuses and surveys. For example, for the 2020 Census, the Bureau developed and deployed 52 IT systems to support operations. These operations included internet self-response data collection, nonresponse follow-up, and data processing.

However, the Bureau's censuses and surveys have largely relied on survey-specific IT systems to perform similar functions, which has resulted in many systems performing duplicative activities. Before the 2020 Census, the Bureau attempted to modernize and consolidate its survey data collection and processing systems through an enterprise-wide modernization program, known as CEDCaP. The Bureau intended this program to deliver a system-of-systems to support all the Bureau's survey data collection and processing functions, rather than continuing to develop survey-specific systems.

As we reported over the last decade, the Bureau struggled to implement CEDCaP.[4] For example, in the run-up to the 2020 Census, the Bureau faced significant challenges in managing the schedule for developing and

[4]See GAO, *2020 Census: Bureau Released Apportionment and Redistricting Data, but Needs to Finalize Plans for Future Data Products*, GAO-22-105324 (Washington, D.C.: Mar. 14, 2022); GAO-22-104357; *2020 Census: Innovations Helped with Implementation, but Bureau Can Do More to Realize Future Benefits*, GAO-21-478 (Washington, D.C.: June 14, 2021); *2020 Census: Census Bureau Needs to Assess Data Quality Concerns Stemming from Recent Design Changes*, GAO-21-142 (Washington, D.C.: Dec. 3, 2020); *2020 Census: Census Bureau Improved the Quality of Its Cost Estimation but Additional Steps Are Needed to Ensure Reliability*, GAO-18-635 (Washington, D.C.: Aug. 17, 2018); and *Information Technology: Better Management of Interdependencies between Programs Supporting 2020 Census Is Needed*, GAO-16-623 (Washington, D.C.: Aug. 9, 2016).

testing IT systems—including systems developed as part of CEDCaP—due to issues experienced during systems development. The agency also struggled to control IT costs, which stemmed, in part, from late decisions on IT capabilities and contractors. The Bureau reduced the scope of CEDCaP due to these challenges. Although the program delivered several systems that were used for the 2020 Census, the Bureau formally closed it in March 2020 without delivering enterprise-wide data collection and processing capabilities.

The Bureau's Current Efforts to Modernize and Consolidate IT Systems

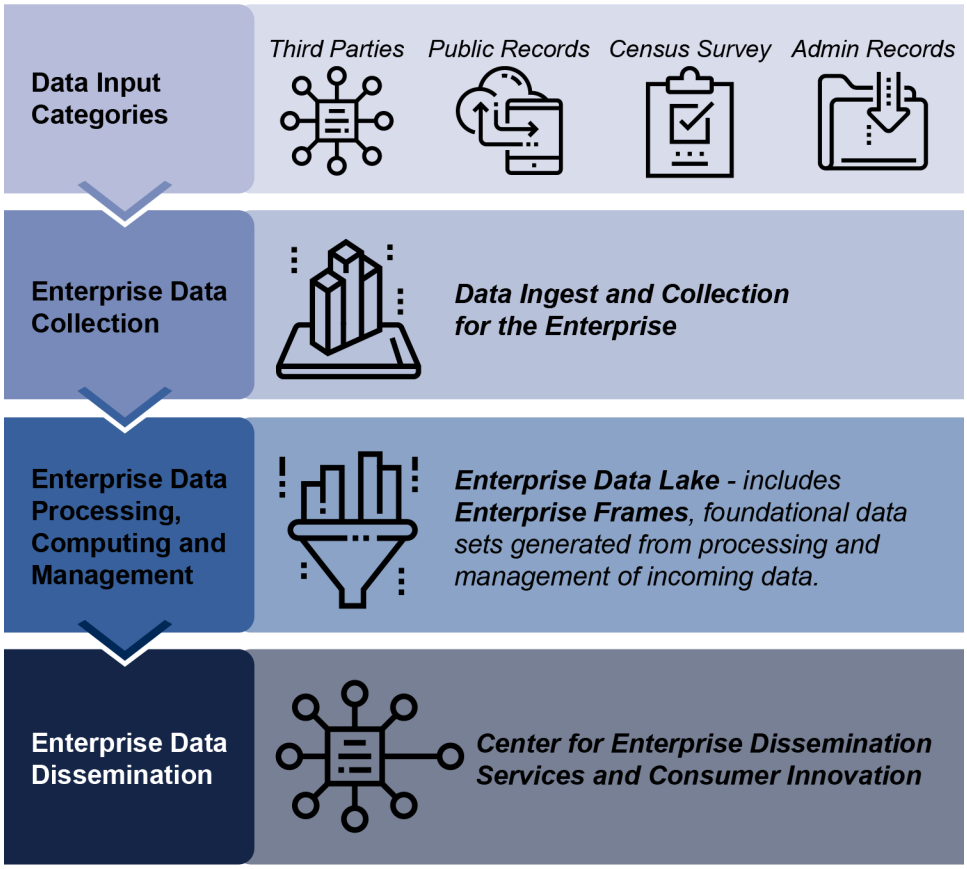
After the 2020 Census, the Bureau embarked on a large-scale effort to modernize and consolidate the Bureau's data collection, storage, and dissemination systems for its censuses and surveys. This effort, called the Business Ecosystem, consists of four integrated, enterprise-wide IT modernization programs:

1. **Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI),** aimed at modernizing data dissemination systems;
2. **Data Ingest and Collection for the Enterprise (DICE),** focused on data collection systems;
3. **Enterprise Data Lake (EDL),** intended to modernize data processing and storage systems; and
4. **Frames**, expected to link data sets.

The aim of these programs is to create an integrated and data-centric ecosystem for Bureau activities.

Figure 1 provides additional information about the Business Ecosystem effort, each of the four enterprise-wide IT modernization programs, and how they interface with each other.

Figure 1: Census Bureau's Business Ecosystem Enterprise-Wide IT Modernization Programs



Sources: GAO analysis of Census Bureau data; palau83/stock.adobe.com (icons). | GAO-24-105979

Table 1 provides more information about each of the four programs within the Bureau's Business Ecosystem effort.

Table 1: Census Bureau Business Ecosystem Program Descriptions and Life Cycle Cost Estimates

Modernization program	Description	Initiation date[a]	Life cycle cost estimate[b] (dollars in millions)
Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI)	This program is intended to be the Bureau's primary platform for data dissemination and the public gateway to Bureau information. According to officials, the Bureau designed the program to improve users' experience by providing tools and data visualizations to allow users to better find, access, connect, and use data. CEDSCI systems were used during the 2020 Census and is the follow-on effort of the Bureau's American FactFinder program.	2017	753
Data Ingest and Collection for the Enterprise (DICE)	This program is expected to develop, integrate, and manage an enterprise "system of systems" that facilitates collecting data from respondents as well as gathering data from third party/administrative sources (such as the Internal Revenue Service, Social Security Administration, and local governments). This is expected to reduce the Bureau's IT footprint by consolidating redundant systems and retiring legacy solutions. DICE is the follow-on effort of the Census Enterprise Data Collection and Processing (CEDCaP) program.	2021	1,423.8
Enterprise Data Lake (EDL)	This program is intended to modernize data storage and data analysis capabilities across all the Bureau's directorates with appropriate role-based access control. The EDL is expected to be the Census Bureau's primary location for collected and ingested data and is to be used to analyze and store data.	2021	337
Frames	This program is expected to allow disparate census datasets to be linked, which is intended to improve research, reduce administrative burden, and increase productivity. In other words, instead of having the datasets serve as standalone entities, such as the master address file and business register, Frames is expected to gather datasets and provide an easy and efficient way to link them for purposes that are useful to the Bureau. These datasets are intended to be linked within the EDL.	2021	Not applicable[c]

Source: GAO analysis of Census Bureau data. | GAO-24-105979

[a]Initiation date is the year the program was funded.

[b]The life cycle cost estimate is based on data reported in the most recent program office estimate of the programs' life cycle duration for the following fiscal years: CEDSCI—2020–2030; DICE—2021–2033; and EDL—2021–2033. As of February 2024, the Bureau planned to baseline the DICE life cycle cost estimate in early 2024.

[c]According to the Bureau, the Frames program is an ongoing research project that has a fixed annual budget of about $12 million, as part of the appropriated Geographic Support Program.

Leading Practices to Guide Organizations' IT Modernization

We and ISACA have identified practices to assist in ensuring the proper management of IT modernization initiatives. The following guides and model outline these practices:

ISACA's CMMI. The CMMI provides an organized collection of leading practices for business and performance improvement.[5] The current version, Model 2.2, includes a set of practice areas that can provide improved performance in the skills and activities of an organization or project. Each practice area is organized into levels that build on the previous level to increase the capability of the organization to implement that practice. For example, at level 2, the CMMI includes two practices related to risk and opportunity management that are used to identify and mitigate potential negative impacts that may make it difficult to meet objectives (see table 2).

Table 2: Selected Leading Practices for Risk and Opportunity Management within the Capability Maturity Model Integration

Selected practices	Example activities
Analyze identified risks or opportunities	Analyze the identified risks to understand their effect on achieving the work's objectives.
	Identify the impact of each risk.
	Identify the probability of occurrence for each risk.
	Assign priorities to each risk based on the impact and probability of occurrence.
Monitor identified risk or opportunities and communicate status to affected stakeholders	Periodically review risks or opportunities in the context of status, circumstance, and past or planned activities.
	Update risks or opportunities as additional information becomes available, such as when new risks are identified, or corrective actions are taken.
	Communicate the risk or opportunity status to affected stakeholders.

Source: GAO analysis of Information Systems Audit and Control Association, Capability Maturity Model Integration, Model V2.2. | GAO-24-105979

Similarly, at level 2, the CMMI includes five practices within the requirements development and management practice area. These practices and their associated activities, as described in table 3, are used to address the needs of stakeholders.

[5]ISACA, CMMI Model V2.2 (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

Table 3: Selected Leading Practices for Requirements Development and Management within the Capability Maturity Model Integration

Selected practices	Description and example activities
Elicit stakeholder needs, expectations, constraints, and interfaces or connections	Additional requirements that are not explicitly provided by stakeholders should be identified. These requirements could be collected from sources such as questionnaires, interviews, use cases, and observation of existing solutions.
Transform stakeholder needs, expectations, constraints, and interfaces or connections into prioritized customer requirements	An organization should consolidate and prioritize inputs from customers and stakeholders, obtain missing information, and resolve conflicts. Sources for requirements include customer and stakeholder provided input, previous efforts, existing solution systems, laws and regulations, standards, and business policies.
Develop an understanding with the requirements providers on the meaning of the requirements	An organization should ensure that it has a shared understanding of the meaning of requirements. To do this, an organization may develop criteria for requirements evaluation and acceptance, analyze requirements to ensure that established criteria are met, reach an understanding of requirements with the requirements providers and the project participants, and record needed changes to requirements.
Obtain commitment from project participants that they can implement the requirements	As requirements are developed, an organization should ensure that project participants commit to requirements and any resulting changes in plans and work products. This may include assessing the impact of requirements on existing commitments, negotiating and recording commitments, developing impact assessments, and recording commitments that requirements can be met.
Develop, record, and maintain bidirectional traceability among requirements and activities or work products	Bidirectional traceability includes tracing requirements from their source, through work products, to the final deliverable to ensure that all requirements are implemented. For projects using agile development methodology (like the CEDSCI program), this can be implemented by tracing requirements from user stories to final work products.

Source: GAO analysis of Information Systems Audit and Control Association, Capability Maturity Model Integration, Model V2.2. | GAO-24-105979

GAO's *Cost Estimating and Assessment Guide*. Reliable cost estimates are critical for successfully delivering IT programs. Such estimates provide the basis for informed decision-making, realistic budget formulation, meaningful progress measurement, and accountability for results. GAO's *Cost Estimating and Assessment Gu*ide outlines best practices for developing reliable cost estimates that management can use to make informed decisions.[6] These practices can be organized into four characteristics—well documented, accurate, comprehensive, and credible. In addition, for the estimate to be considered reliable, an organization must meet or substantially meet each characteristic. Table 4 summarizes the four characteristics and corresponding best practices of a reliable cost estimate identified in the cost guide.

[6]GAO-20-195G.

Table 4: Four Characteristics and Best Practices of a Reliable Cost Estimate According to GAO's Cost Estimating and Assessment Guide

Characteristic	Corresponding best practices
Well documented	• The documentation should show the source data used, the reliability of the data, and the estimating methodology used to derive each element's cost. • The documentation describes how the estimate was developed so that a cost analyst unfamiliar with the program could understand what was done and replicate it. • The documentation discusses the technical baseline description and the data in the technical baseline are consistent with the cost estimate. • The documentation provides evidence that the cost estimate is reviewed and accepted by management.
Accurate	• The cost model was developed by estimating each work breakdown structure element using the best methodology from the data collected. • The estimate has been adjusted properly for inflation. • The estimate contains few, if any, minor mistakes. • The estimate is regularly updated to ensure it reflects program changes and actual costs. • The estimate is based on a historical record of cost estimating and actual experiences from other comparable programs.
Comprehensive	• The estimate includes all life cycle costs. • The technical baseline description completely defines the program, reflects the current schedule, and is technically reasonable. • The estimate is based on a work breakdown structure that is product-oriented, traceable to the statement of work, and at an appropriate level of detail to ensure that cost elements are neither omitted nor double-counted. • The estimate documents all cost-influencing ground rules and assumptions.
Credible	• The estimate includes a sensitivity analysis that identifies a range of possible costs based on varying major assumptions, parameters, and data inputs. • A risk and uncertainty analysis is conducted that quantifies the imperfectly understood risks and identifies the effects of changing key cost driver assumptions and factors. • Major cost elements are cross-checked to see if results are similar. • An independent cost estimate is conducted by a group outside the acquiring organization to determine whether other estimating methods produce similar results.

Source: GAO analysis. | GAO-24-105979

GAO's *Schedule Assessment Guide*. The success of a project depends, in part, on having an integrated and reliable master schedule that defines when and how long work will occur, and how each activity is related to the others. A project's schedule provides not only a road map for systematic project execution, but also the means by which to gauge progress, identify and resolve potential problems, and promote accountability at all levels of the project. GAO's *Schedule Assessment Guide* identifies best practices for developing and maintaining reliable project schedules.[7] The best practices are grouped into four characteristics of a reliable schedule: comprehensive, well constructed,

[7]GAO-16-89G.

credible, and controlled. Table 5 summarizes the four characteristics and corresponding best practices of a reliable cost estimate identified in the cost guide.

Table 5: Four Characteristics and Best Practices of a Reliable Schedule According to GAO's Schedule Assessment Guide

Characteristic	Corresponding best practices
Comprehensive	**Capturing all activities:** The schedule should reflect all activities as defined in the program's work breakdown structure (WBS), which defines in detail the work necessary to accomplish a project's objectives, including activities both the owner and the contractors are to perform. **Assigning resources to all activities:** The schedule should reflect the resources (labor, materials, travel, facilities, equipment, and the like) needed to do the work, whether they will be available when needed, and any constraints on funding or time. **Establishing the duration of all activities:** The schedule should realistically reflect how long each activity is expected to take. When the duration of each activity is determined, the same rationale, historical data, and assumptions used for cost estimating should be used. Durations should be reasonably short and meaningful and should allow for discrete progress measurement. Schedules that contain planning and summary planning packages as activities will normally reflect longer durations until broken into work packages or specific activities.
Well constructed	**Sequencing all activities:** The schedule should be planned so that critical program dates can be met. To do this, activities must be logically sequenced and linked (i.e., listed in the order in which they are to be carried out and joined with logic). In particular, a predecessor activity must start or finish before its successor. Date constraints and lags should be minimized and justified. This helps ensure that the interdependence of activities that collectively lead to the completion of activities or milestones can be established and used to guide work and measure progress. **Confirming that the critical path is valid:** The schedule should identify the program's critical path—the path of longest duration through the sequence of activities. Establishing a valid critical path is necessary for examining the effects of any activity's slipping along this path. The program's critical path determines the program's earliest completion date and focuses the team's energy and management's attention on the activities that will lead to the project's success. **Ensuring reasonable total float:** The schedule should identify reasonable total float (or slack)—the amount of time a predecessor activity can slip before the delay affects the program's estimated finish date—so that the schedule's flexibility can be determined. The length of delay that can be accommodated without the finish date's slipping depends on the number of date constraints within the schedule and the degree of uncertainty in the duration estimates, among other factors. However, the activity's total float provides a reasonable estimate of this value. As a general rule, activities along the critical path have the least total float. Unreasonably high total float on an activity or path indicates that schedule logic might be missing or invalid.
Credible	**Verifying that the schedule can be traced horizontally and vertically:** The schedule should be horizontally traceable, meaning that it should link products and outcomes associated with other sequenced activities. Such links are commonly referred to as "hand-offs" and serve to verify that activities are arranged in the right order for achieving aggregated products or outcomes. The schedule should also be vertically traceable—that is, data should be consistent between different levels of a schedule. When schedules are vertically traceable, lower-level schedules are clearly consistent with upper-level schedule milestones, allowing for total schedule integrity and enabling different teams to work to the same schedule expectations. **Conducting a schedule risk analysis:** A schedule risk analysis should start with a good critical path method schedule. Data about program schedule risks are to be incorporated into a statistical simulation to (1) predict the level of confidence in meeting a program's completion date; (2) determine the contingency, or reserve of time, needed for a level of confidence; and (3) identify high-priority risks. Programs should include the results of the schedule risk analysis in constructing an executable baseline schedule.

Characteristic	Corresponding best practices
Controlled	**Updating the schedule using actual progress and logic:** Progress updates and logic should provide a realistic forecast of start and completion dates for program activities. Maintaining the integrity of the schedule logic is necessary to reflect the true status of the program. To ensure that the schedule is properly updated, people responsible for the updating should be trained in critical path method scheduling. **Maintaining a baseline schedule:** A baseline schedule is the basis for managing the program scope, the time period for accomplishing it, and the required resources. The baseline schedule should be designated as the target schedule and subjected to a configuration management control process. Program performance is to be measured, monitored, and reported against the baseline schedule. The schedule should be continually monitored so as to reveal when forecasted completion dates differ from baseline dates and whether schedule variances affect downstream work. A corresponding basis document should (1) explain the overall approach to the program, (2) define custom fields in the schedule file, (3) detail ground rules and assumptions used in developing the schedule, and (4) justify constraints, lags, long activity durations, and any other unique features of the schedule.

Source: GAO analysis. | GAO-24-105979

Cybersecurity is a High-Risk Area for Federal Agencies

Federal agencies like the Bureau are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and national security, prosperity, and well-being. Many of these systems contain vast amounts of personally identifiable information, thus making it imperative to protect the confidentiality, integrity, and availability of this information and effectively respond to data breaches and security incidents when they occur.[8]

The risks to IT systems supporting the federal government are increasing as security threats continue to evolve and become more sophisticated. These risks include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks.

Compounding these risks, IT systems are often riddled with security vulnerabilities—both known and unknown. These vulnerabilities can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety.

[8]In general, personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security number, or that otherwise can be linked to an individual. The Bureau may collect personally identifiable information when it obtains individual survey responses.

To highlight the importance of these issues, we have designated information security as a government-wide high-risk area since 1997.[9] In 2015, we added protecting the privacy of personally identifiable information to this high-risk area.[10] Since then, advances in technology have enhanced the ability of government and private sector entities to collect and process extensive amounts of personally identifiable information, which has posed challenges to ensuring the privacy of such information.

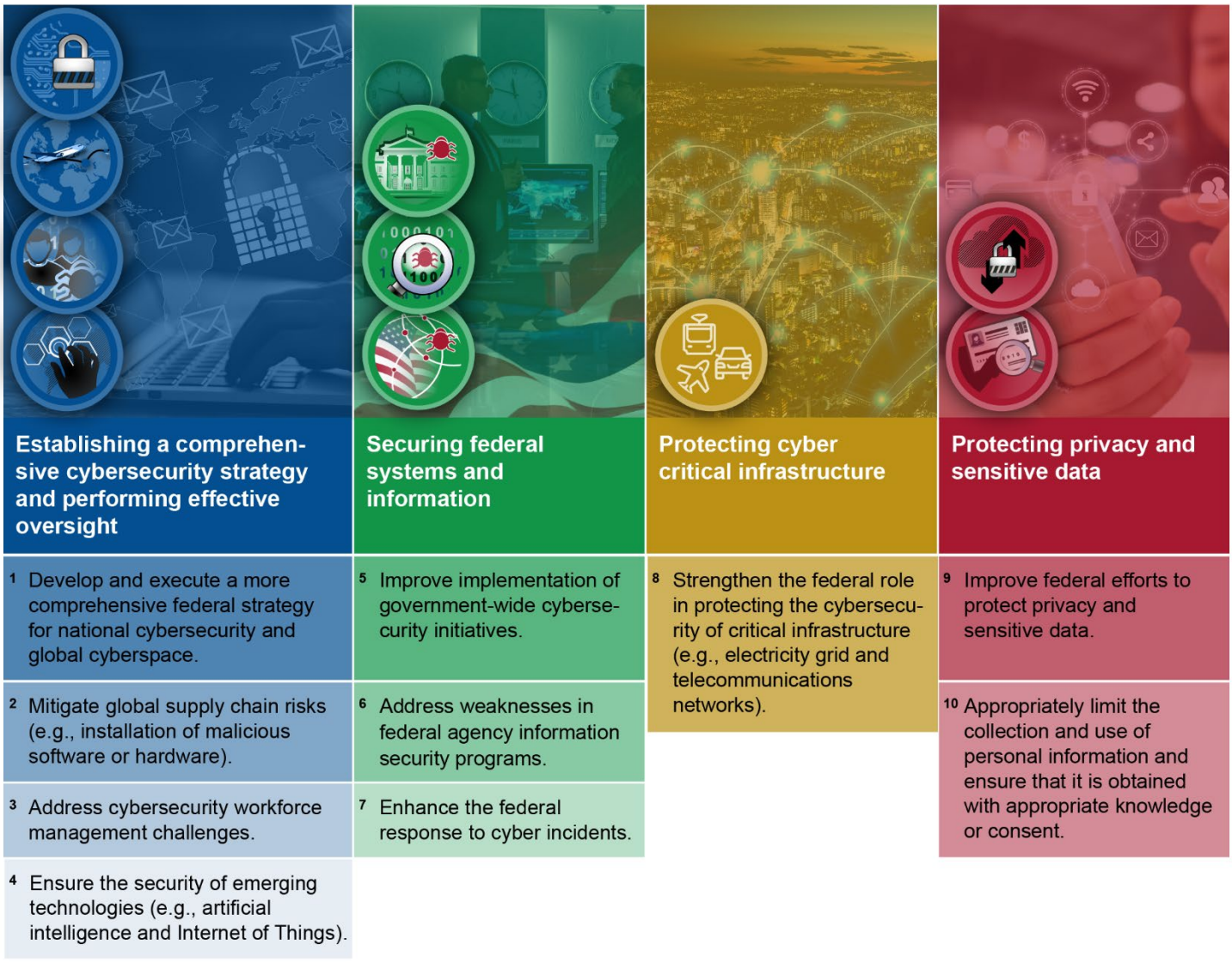
In our high-risk updates from September 2018 and March 2023, we emphasized the critical need for the federal government to take 10 specific actions to address four major cybersecurity challenges that the federal government faces.[11] These challenges are (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. These challenges and action items are shown in figure 2.

[9]GAO, *High-Risk Series: Information Management and Technology*, HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: An Overview*, HR-97-1 (Washington, D.C.: February 1997).

[10]GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[11]GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Washington, D.C.: Apr. 20, 2023), and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

Figure 2: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges



Sources: GAO (analysis and icons), Who is Danny (blue image); Gorodenkoff/stock.adobe.com (green image); metamorworks/stock.adobe.com (yellow image); Monster Ztudio/stock.adobe.com (red image); motorama/stock.adobe.com (icons); https://www.whitehouse.gov (logo). | GAO-24-105979

The Bureau Did Not Fully Implement All Selected Leading IT Management Practices for the CEDSCI Program

The Bureau fully implemented leading practices for risk management for its CEDSCI modernization program. However, it had not fully implemented leading practices related to managing the program's requirements, cost, and schedule. Specifically, while the Bureau had substantially implemented leading practices for requirements, it did not document requirements consistently. In addition, although the program's cost estimate substantially met two of the four characteristics of a high-quality, reliable cost estimate (well documented and accurate), it only partially met the remaining two characteristics (credible and comprehensive). The schedule did not substantially or fully meet any of the four characteristics of a reliable schedule: comprehensive, well constructed, credible, and controlled. Because the Bureau had not fully or substantially implemented all leading practices related to the cost estimate and schedule, both were unreliable.

The Bureau Fully Implemented Leading Practices for Risk Management

Leading practices for risk management, as outlined in CMMI Model 2.2, emphasize establishing a risk management plan with activities that include helping organizations identify potential problems and plan risk-handling activities across the life of the program.[12]

The Census Bureau established a risk management plan for the CEDSCI program that described activities that the program will undertake to identify, assess, plan responses for, and control or monitor risks and issues. This risk management plan described the steps the program takes to manage risks, including

- documenting risks and issues through risk and issue logs and escalating enterprise-wide risks and issues to the relevant Bureau risk and issue logs,
- updating the status of its risks and issues on a monthly basis,
- documenting risk mitigation plans that describe strategies in place and actionable steps, and
- documenting the risk owner, mitigation plan, date identified, impact, and a risk category for each risk.

The risk management plan fully met selected practices for analyzing and monitoring risks, as shown in table 6.

[12]ISACA, *CMMI Model V2.2* (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

Table 6: Extent to Which the Census Bureau Met Selected Practices for Risk Management for the CEDSCI Program

Selected practice	Assessment	Example activities	Summary of assessment
Analyze identified risks or opportunities	●	Analyze the identified risks	CEDSCI's risk management plan calls for all identified risks to be assessed to identify the range of possible project outcomes. According to the plan, Bureau officials are to assess the likelihood an identified risk will occur, the potential severity of the impact if the risk occurs, the time frame in which the event would occur, and the priority of the risk relative to other risks. As of March 2024, the Bureau had documented the results of this analysis in the risk register and identified the risk with a title, risk identification number, and a description of the risk. This documentation included the status, probability, and impact of the risk.
		Identify the impact of each risk	According to CEDSCI officials, the program identified new and emerging risks as early as possible to proactively implement effective mitigation strategies, preventing risks from becoming issues. In the program's risk registers, each identified risk included an impact rating.
		Identify the probability of occurrence for each risk	According to the program's risk management plan, risk owners are to perform both a qualitative and quantitative analysis of risks. This should include an assessment of the likelihood that an identified risk would occur. As of February 2024, each risk identified in the program's monthly risk registers included a rating for the probability that the risk would occur.
		Assign priorities to each risk based on the impact and probability of occurrence	As directed in the risk management plan, risk owners are to provide subject matter expertise and develop and manage risk and issue statements, risk probability and impact ratings, issue priority and impact, as well as other necessary risk and issue fields. In the program's risk register, each risk included an exposure rating, which was a calculation based on the probability of the risk occurring, and the impact if the risk did occur. The exposure rating influenced how the Bureau determines its response to the risk.
Monitor identified risk or opportunities and communicate status	●	Periodically review risks or opportunities	According to the risk management plan, the Risk Review Board's responsibilities include providing status updates on program risks and issues and reviewing mitigation and contingency plans. For example, the program held several risk management meetings, including quarterly Risk Review Board meetings and monthly program-level risk meetings, where program risks were discussed. In addition, in 2022 and 2023, the program's risk registers included monthly updates on risks, as applicable.
		Update risks or opportunities as additional information becomes available	According to the risk management plan, the Risk Review Board is expected to review status updates on program risks and issues and provide input. As described above, risks are expected to be discussed at quarterly Risk Review Board meetings and monthly risk meetings. As of March 2024, the program had documented all changes and updates to the risks in monthly risk registers.
		Communicate the risk or opportunity status to affected stakeholders	According to the program's risk management plan, mitigation controls must be communicated to stakeholders, team members, and the Risk Review Board as appropriate. As of February 2024, the program recorded changes and updates to risks in the risk registers on a monthly basis and shared with the affected parties.

Legend: ● – Met; ◕ - Substantially met; ◐ - Partially met; ◔ - Minimally met; O – Not met

Source: GAO analysis of Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI) information. | GAO-24-105979

Officials in the CEDSCI program noted that they hold regular meetings with Bureau areas to align with enterprise risk management and strong communication between stakeholders in the Bureau. By continuing to use leading practices for risk management, the Bureau is better able mitigate and address uncertainties that could have a negative impact on meeting objectives.

The Bureau Fully or Substantially Implemented Leading Practices for Requirements Management

CMMI Model 2.2 outlines leading practices for managing requirements.[13] Project requirements are the basis for developing the right solutions to support mission needs.

The Bureau established a requirements management plan for the CEDSCI program according to leading practices. Specifically, the program fully met four of the selected practices and substantially met one practice, as shown in table 7.

Table 7: Extent to Which the Census Bureau Met Selected Practices for Requirements Development and Management of the CEDSCI Program

Selected practices	Assessment	Summary of assessment
Elicit stakeholder needs, expectations, constraints, and interfaces or connections	●	New requirements for the CEDSCI program originated from multiple sources, including from members of the program team, Bureau data providers, Bureau directorates, and system users. For example, the program elicited stakeholder needs from data owners in data release plans, which identified their needs, requirements, and preferences. Additionally, data owners provided requirements in feature scope analyses or—for work that affects the architecture—in architectural enabling scope documents. Feature scope analyses included a description of the feature, acceptance criteria for the feature, and any dependencies. Architecture enablement specifications included information on success criteria and described any impacts to existing requirements.
Transform stakeholder needs, expectations, constraints, and interfaces or connections into prioritized customer requirements.	●	The Bureau leveraged existing requirements from the predecessor to CEDSCI (known as the American FactFinder) as the basis for developing the technical platform for data dissemination. Program officials collected the original requirements and data release plans from the American FactFinder program and shared them with relevant staff. It also consolidated and transformed stakeholder needs into customer requirements and prioritized and stored those requirements. It collected feedback from its technical reviews and the first release and analyzed their findings to ensure that the requirements were complete.
Develop an understanding with the requirements providers on the meaning of the requirements	●	The requirements management plan included criteria for evaluation and acceptance of requirements that are received. According to the plan, when the program determines a requirement is critical to meeting the customer need, the technical managers are to perform an analysis to further define and prioritize the requirement and document their results in a requirements library. Program officials performed analyses of each requirement to further define and prioritize the requirement and documented their results in a requirements library.

[13]ISACA, *CMMI Model V2.2* (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

Selected practices	Assessment	Summary of assessment
Obtain commitment from project participants that they can implement the requirements	●	The program managed its requirements by using (1) the requirements library to store all of the requirements; (2) the project schedule, which included specific details about the program's requirements and when they are to be implemented; and (3) outputs from program development increments describing what was actually developed. The program broke down requirements into user stories and tasks that were then scheduled in a 2-week program development increment to ensure that they could be implemented. The program also used a requirements traceability and verification matrix to ensure that requirements were met.
Develop, record, and maintain bidirectional traceability among requirements and activities or work products	◕	As described above, the program broke down requirements into user stories, which were further defined into tasks that could be completed during a 2-week development program increment. The program developed requirements documents—that is, feature scope analyses and, if applicable, architecture enablement specifications for its requirements. However, not all user stories reviewed demonstrated bidirectional traceability (e.g., the ability to trace forward and backward from requirements to the end product). Specifically, these stories did not consistently provide detailed support for their respective feature scope analysis or architecture enablement specification. For example, in certain user stories, the information provided was not always consistent with the corresponding feature scope analysis.

Legend: ● – Met; ◕ - Substantially met; ◐ - Partially met; ◔ - Minimally met; O – Not met

Source: GAO analysis of Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI) information. | GAO-24-105979

As described above, the CEDSCI program did not fully demonstrate that it maintained traceability from requirements to user stories and other work products like the feature scope analyses and architecture enablement specifications. Bureau officials acknowledged that the information in the user stories was not always consistent with the other work products (i.e., the feature scope analyses and architecture enablement specifications). They stated this was because the work products are less formal than the requirements documents they are based on. Additionally, the work products are expected to be living documents that explain how features work. Ensuring that requirements can be traced through the work products would help ensure consistency between the requirements and the final solution, which increases the likelihood that the solution will meet user needs. Until the Bureau implements leading practices for ensuring bidirectional traceability for requirements, it will face challenges in effectively managing how the program adheres to project requirements.

The Bureau's Cost Estimate for CEDSCI Was Not Reliable

GAO's *Cost Estimating and Assessment Guide* outlines best practices associated with developing a reliable, high-quality cost estimate to enable government programs to better estimate and manage their costs to improve program management and execution.[14] According to this guide, the four characteristics of a high-quality, reliable cost estimate are that it is well documented, accurate, comprehensive, and credible. The

[14]GAO-20-195G.

guidance considers an estimate reliable if it substantially or fully meets each of the characteristics of a reliable cost estimate.

The Bureau's cost estimate for CEDSCI was unreliable. Although it substantially met two of the four characteristics of a high-quality, reliable cost estimate (well documented and accurate), it only partially met the remaining two characteristics (credible and comprehensive). Table 8 summarizes our assessment of the program's cost estimate compared to best practices.

Table 8: Extent to Which the CEDSCI Program's September 2022 Cost Estimate Met Best Practices for Cost Estimating

Characteristic	Assessment	Best practices	Summary of assessment
Well documented	◕	Shows the source data used, the reliability of the data, and the estimating methodology used to derive each element's cost	The basis of estimate document provided a thorough description of the methods and approaches. This documentation was adequate for updating the estimate. The documentation also identified methodologies, normalized data, and documented inflation. However, certain key data elements lacked detailed documentation of the associated scope, which made it difficult to ensure that the data can be effective for accurately estimating future costs. For example, costs were extrapolated from actual contract values. However, the basis of estimate did not describe the scope and productivity of the historical effort and how it applied to future efforts.
		Describes how the estimate was developed so that a cost analyst unfamiliar with the program could understand what was done and replicate it	The basis of estimate provided narratives and cost tables at a summarized level. It also described the guidance used to develop the estimate, the approach to risk and uncertainty, and electronic copies of the model and documentation are available to authorized personnel. However, the Bureau did not address some elements that are best practices. For example, methodology descriptions were not at the cost element level.
		Discusses the technical baseline description; the data in the technical baseline are consistent with the cost estimate	The estimate discussed the technical baseline description, and the data in the technical baseline were consistent with the cost estimate.
		Provides evidence that the cost estimate was reviewed and accepted by management	The Bureau reviewed the estimate at a Cost Review Board meeting and a cost acceptance meeting. However, the Bureau did not discuss certain key elements of the cost estimate, such as ground rules and assumptions, as well as data sources.
Accurate	◕	Is developed by estimating each WBS element using the best methodology from the data collected	The estimate employed generally accepted methodologies. However, it lacked sufficient justification for many of the methods used. For example, the American FactFinder contract—which is the predecessor of CEDSCI—was used as a basis for the cost of data onboarding. However, it did not include a discussion of how American FactFinder data onboarding efforts compared to the expected CEDSCI data onboarding efforts.
		Is adjusted properly for inflation	The estimate properly adjusted for inflation.
		Contains few, if any, minor mistakes	The estimate was largely error free.

Characteristic	Assessment	Best practices	Summary of assessment
		Is regularly updated to reflect program changes and actual costs	According to CEDSCI program officials, the current program office estimate did not track variances. The program did report monthly planned versus actual budget variances, but at a very high level, rather than at the detailed WBS level. Unless the cost estimate is properly updated on a regular basis, it cannot provide decision-makers with accurate information for assessing alternative decisions.
		Is based on a historical record of cost estimating and actual experiences from other comparable programs	The estimate was overly reliant on subject matter expert opinion and lacked detail about similar programs used as the estimating basis. While the documentation provided significant evidence of the use of historical data, it did not contain sufficient detail to assess the reliability of the historical data. Unless cost estimators know the factors that influenced a program's cost, they may not capture the right data.
Comprehensive	◐	Includes all life-cycle costs	The estimate covered all life cycle costs. The estimate time frame was documented and justified, and government and contractor costs were included. Costs included all life cycle costs except disposal costs, and this choice was documented as well.
		Completely defines the program and reflects the current schedule and technical baseline	The estimate lacked detail on the technical solution to be implemented. For example, while the estimate described desired capabilities at a summary level, it did not describe specific solutions for achieving the capabilities. Without an adequate understanding of the acquisition program—such as the acquisition strategy, technical definition, characteristics, system design features, and included technologies—the cost estimator would not be able to identify the technical and program parameters that underpin the cost estimate. Consequently, the quality of the cost estimate could be compromised.
		Incorporates a WBS with sufficient detail to ensure that cost elements are neither omitted nor double-counted	The program used a standard WBS and WBS dictionary that had not been tailored to the program. The WBS and WBS dictionary lacked the detail necessary to fully outline the end products or the work to be done. While the level of detail in a WBS depends on a program's complexity and risk, the WBS should contain a level of detail that is sufficient for planning and successfully managing the full scope of work. Also, if a cost estimate does not include an associated WBS dictionary, one cannot ensure that the estimate includes all relevant costs.
		Ensures that cost-influencing assumptions and ground rules on which the estimate is based are identified and documented	The program included detailed ground rules and assumptions that were developed by the cost-estimating team with input from technical experts. Additionally, many of the WBS-level assumptions were tied to the risk and uncertainty and sensitivity analyses that were conducted.
Credible	◐	Includes a sensitivity analysis that identifies a range of possible costs based on varying major assumptions, parameters, and data inputs	The Bureau incompletely documented the sensitivity analysis. The program office estimate and basis of estimate reflected sensitivity on a single element: cloud costs. Other documentation showed that the Bureau conducted further sensitivity analysis but did not provide details. Carefully assessing the underlying risks and supporting data, and documenting the sources of variation, is necessary for a sensitivity analysis to be useful in making informed decisions.

Characteristic	Assessment	Best practices	Summary of assessment
		Includes a risk and uncertainty analysis to quantify the imperfectly understood risks and identify the effects of changing key cost driver assumptions and factors	The program employed a solid approach to risk and uncertainty analysis and conducted an independent cost estimate. However, the Bureau did not apply risk and uncertainty analysis to all key cost elements. If the Bureau does not apply risk and uncertainty analysis to all key cost elements, it may not be able to update progress and changes to risk.
		Cross-checks major costs to see if results are similar	The basis of estimate document pointed to the independent cost estimate and quality assurance reviews. While both are important parts of a reliable cost estimate, they do not take the place of cross-checks, particularly of high-cost elements. Unless an estimate employs cross-checks, the estimate will have less credibility because stakeholders will have no assurance that alternative estimating methodologies produce similar results.
		Includes an independent cost estimate by a group outside the acquiring organization to determine whether other estimating methods produce similar results	The program provided an independent cost estimate by a group outside the organization.

Legend: ● – Met; ◕ - Substantially met; ◐ - Partially met; ◔ - Minimally met; O – Not met

CEDSCI— The Census Bureau's Center for Enterprise Dissemination Services and Consumer Innovation

WBS—work-breakdown structure

Source: GAO analysis of CEDSCI information. | GAO-24-105979

CEDSCI officials acknowledged that their cost estimate could be more mature and provided several reasons for the deficiencies in the cost estimate described above. For example, CEDSCI officials explained that they lost key personnel with experience in developing and updating the cost estimate in fiscal year 2023. They are also establishing a development roadmap that is expected to detail a technical solution and improve both the cost and schedule estimates. In February 2024, the CEDSCI program manager noted that they have updated the cost estimate to better meet the best practices. For example, they reported that they have updated the work breakdown structure and incorporated it into the program office estimate along with suggestions from subject matter experts. Bureau officials in the CEDSCI program noted that they plan to revise the program office estimate in March 2024 and update it on a quarterly basis thereafter.

Adhering to the cost estimate best practices identified in our cost guide could help the Bureau effectively plan, manage, and oversee its modernization efforts. By implementing a cost estimate that does not reflect the four characteristics of a high-quality, reliable estimate, the Bureau is making decisions based on potentially inaccurate data. As a

result, management faces increased risk of cost overruns and unmet performance targets.

The Bureau's Schedule for CEDSCI Was Not Reliable

GAO's *Schedule Assessment Guide* identifies best practices for developing and maintaining reliable project schedules.[15] According to this guide, a schedule estimate must substantially or fully meet four characteristics—comprehensive, well constructed, credible, and controlled—to be considered reliable.

The Bureau uses an integrated master schedule to manage CEDSCI activities, and has a WBS, among other tools, that details its activities. However, the Bureau's schedule for the program was not reliable because it did not substantially or fully meet any of the four characteristics of a reliable schedule. Table 9 summarizes our assessment of the program's schedule compared to leading practices for reliable schedules.

Table 9: Extent to Which the Census Bureau's September 2022 Schedule for the CEDSCI Program Met Best Practices for Reliable Project Schedules

Characteristic	Assessment	Best practices	Summary of assessment
Comprehensive	◔	Captures all activities	The schedule included plans through January 11, 2024, and did not show the required effort to accomplish four major milestones that were defined in the program management office's Fiscal Year 2020 strategy to be completed by 2030. Therefore, the schedule did not show the required effort to accomplish the four major milestones by 2030 in CEDSCI's vision statement or the effort to accomplish the costs assigned in the August 2022 program office estimate. If all activities are not accounted for, it is uncertain whether all activities are scheduled in the correct order, resources are properly allocated, or a schedule risk analysis can account for all risk.
		Assigns resources to all activities	Less than 1 percent of remaining scheduled activities had resource assignments. Information on resource needs and availability in each work period assists the program office in forecasting the likelihood of completing activities as scheduled. If the current schedule does not allow insight into the current or projected allocation of resources, then the program's risk of slipping is significantly increased.
		Establishes durations of all activities	While activities were generally short enough in duration to be consistent with effective planning and program execution, longer-duration activities that appeared to be level-of-effort were not clearly labeled as such. Additionally, nonwork holidays did not appear to have been accounted for in the schedule calendars. Task or resource calendars that are improperly defined will not accurately represent the forecasted start, finish, and durations of planned activities. Ensuring calendars are realistic provides for more accurate dates and may reveal opportunities to advance the work.

[15]GAO-16-89G.

Characteristic	Assessment	Best practices	Summary of assessment
Well constructed	◔	Sequences all activities	The schedule network had instances of sequencing issues, including missing logic and the use of unjustified date constraints, dangling logic (a form of incomplete logic), lags, and leads. If logic among activities is missing, program team members could misunderstand one another, especially regarding receivables and deliverables. Additionally, date constraints may prevent activities from taking advantage of time savings, dangling logic can interfere with the valid forecasting of scheduled activities, and lags may delay a successor activity with no effort or resources associated with this passage of time.
		Confirms that the critical path is valid	The scheduling software could not produce a valid critical path (the path of longest duration through the sequence of activities). Bureau officials reported that they do not use critical path method scheduling. Without a valid critical path, management cannot focus on activities that will detrimentally affect the key program milestones and deliveries if they are delayed. Unless the schedule can produce a true critical path, the program office will not be able to provide reliable time line estimates or identify when problems or changes may occur and their effects on subsequent work.
		Ensures reasonable total float	The float (i.e., the amount of time a predecessor activity can slip before the delay affects the program's estimated finish date) did not reflect accurate flexibility due to sequencing issues and date anomalies. As such, the schedule cannot identify activities that could be delayed by reallocating resources to other more urgent activities. Further, incorrect float estimates may result in an inaccurate assessment of program status and completion dates, leading to decisions that may jeopardize the program.
Credible	◔	Can be horizontally and vertically traced[a]	While officials reported that dissemination of survey datasets were not required to be linked, the schedule did not achieve horizontal traceability because the schedule network did not respond appropriately to delays in activity durations. This was due to the sequencing issues in the schedule. As reported, logic issues prevented the schedule from transmitting delays to activities that should depend on them. Additionally, the major milestones between the schedule and management documents could not be mapped. Without vertical traceability, the Bureau cannot be confident that all consumers of the schedule are getting the same correct schedule information.
		Conducts a schedule risk analysis	While the Bureau managed risks in the program's risk register with the program's Risk Review Board, it did not conduct a formal schedule risk analysis. If a schedule risk analysis is not conducted, the following cannot be determined: the likelihood of the program's completion date, how much schedule risk contingency is needed to provide an acceptable level of certainty for completion by a specific date, risks most likely to delay the program, or the paths or activities most likely to delay the program.

Characteristic	Assessment	Best practices	Summary of assessment
Controlled	◔	Is updated using actual progress and logic	While progress was recorded regularly, the program did not produce a schedule narrative document describing the status of key milestone dates; explanations for any changes in key dates after each status update; changes in network logic; a description of the critical paths; and a description of any significant scheduling software options that changed between update periods. Also, CEDSCI did not provide evidence of schedule health metrics performed. The schedule's status update process was questionable due to date anomalies such as start dates and finish dates in the past that had not been actualized through the February 1, 2023, status date. Good documentation helps with analyzing changes in the program schedule and identifying the reasons for variances between estimates and actual results, thereby contributing to the collection of cost, schedule, and technical data that can be used to support future estimates. Further, if unfinished work remains in the past, the schedule no longer represents a realistic plan to complete the program, and team members will lose confidence in the model.
		Maintains a baseline schedule	The Bureau did not provide a schedule basis document explaining the overall approach to the program, defining custom fields in the schedule file, detailing ground rules and assumptions used in developing the schedule, and justifying constraints, lags, long activity durations, and any other unique features of the schedule. In addition, the trend analysis provided did not trace back to the schedule. The schedule's baseline was questionable due to the number of activities that had the current start and finish dates equal to the baselined start and finish dates. In addition, the baseline appeared to be set 6 days after the schedule's last status date, or date of the last update. Without a formally established baseline schedule to measure performance against, management cannot identify or mitigate the effect of unfavorable performance.

Legend: ● – Met; ◕ - Substantially met; ◐ - Partially met; ◔ - Minimally met; O – Not met

CEDSCI—Center for Enterprise Dissemination Services and Consumer Innovation

Source: GAO analysis of Census Bureau data. | GAO-24-105979

[a]A schedule should be horizontally traceable, meaning that it should link products and outcomes associated with other sequenced activities. schedule should also be vertically traceable—that is, varying levels of activities and supporting subactivities can be traced.

CEDSCI officials provided several reasons for the deficiencies in the schedule. For example, they noted that the schedule did not reflect concrete activities in future years, as the activities assigned to the 2030 Decennial Census are still in formulation and will continue to be matured throughout the remainder of the decade. They also noted the program's current dissemination activities would be executed throughout the decade but were intentionally omitted to allow for efficiency in schedule management. In addition, they stated that the program's various schedules have different updating cadences, due to the nature and content included in each schedule, and that multiple schedule reports are generated on a weekly basis where program resources can review them. Further, they stated the program was in the process of establishing a

high-level roadmap to incorporate into the schedule to increase vertical traceability.

By implementing a program schedule that does not fully and accurately reflect the four characteristics of a high quality, reliable estimate, the Bureau faces an increased risk of schedule uncertainty. This may result in unreliable completion dates, time extension requests, and delays in the CEDSCI program. Further, if unfinished work remains, the schedule no longer represents a realistic plan for completing the project, and team members will lose confidence in the model. Without a formally established baseline schedule to measure performance against, management cannot identify or mitigate the effect of unfavorable performance. In addition, employing an unreliable schedule may hinder management's ability to make informed decisions related to possible sequences of activities and the flexibility of the schedule according to available resources, among other things. Such uncertainty can cause schedule slippages and increased project costs.

The Bureau Lacks Detailed Plans to Fully Address Key Cybersecurity and Privacy Challenges

We and the Department of Commerce Office of Inspector General have issued several reports over the last decade that identified cybersecurity and privacy challenges the Bureau faced in implementing its previous IT modernization efforts and developing systems for the 2020 Census.[16] These align with major cybersecurity challenges in our High Risk report.[17] As the Bureau undertakes its new IT modernization efforts and prepares for future surveys such as the 2030 Census, it will continue to face key cybersecurity and privacy challenges related to, among other things:

[16]See, for example, GAO-22-104357; 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); GAO-16-623; and Department of Commerce, Office of Inspector General, *Simulated Internal Cyber Attack Gained Control of Critical Census Bureau System*, OIG-23-004-1 (Washington, D.C.: Nov. 22, 2022).

[17]Our 2021 High-Risk Report emphasized the critical need for the federal government to undertake specific actions to meet four major challenges in cybersecurity: establishing a comprehensive cybersecurity strategy and performing effective oversight; securing federal systems and information; protecting cyber critical infrastructure; and protecting privacy and sensitive data. As part of the challenge related to establishing a comprehensive cybersecurity strategy, agencies are expected to address cybersecurity workforce challenges. GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

- addressing cybersecurity workforce challenges by ensuring key IT positions are filled,
- improving information security initiatives and programs,
- enhancing the detection and response to cybersecurity incidents, and
- ensuring respondent privacy while maintaining the usability of public data.

Leading practices for project planning note that plans for addressing challenges should describe what is needed to accomplish the work within the standards and constraints of the organization.[18] Planning documents should describe, among other things, who is responsible for accomplishing the steps in the plan and the time frames for doing so.

The Bureau has taken steps to address key cybersecurity and privacy challenges but lacks detailed plans to fully address two of them. For example, the agency has developed workforce plans and filled many key IT positions. In addition, they have taken steps to address recommendations from the Department of Commerce's OIG related to responding to cybersecurity incidents. However, an implementation strategy related to securing the Bureau's systems, and its plans for protecting respondent data, have not been finalized and lack important details (such as time frames). Specifically:

The Bureau has developed plans to address cybersecurity workforce challenges and ensured key IT positions are filled. Having personnel with the right knowledge and skills is critical to the success of a program, and we have previously reported that mission-critical skills gaps in such occupations as cybersecurity pose a high-risk to the nation.[19] Because the appropriate skills are crucial to the success of a program, we added strategic human capital management, including cybersecurity human capital, to our High-Risk List in 2001, and it remains on our most recent High-Risk List.[20]

[18]SACA, *CMMI Model V2.2* (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

[19]GAO, *Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight*, GAO-23-106415 (Washington, D.C.: Jan. 19, 2023).

[20]GAO-23-106203.

The Bureau has had challenges in the past with filling key IT positions. In 2016, we reported that the Bureau struggled to fill critical skills gaps for the 2020 Census, such as those in cloud computing and security integration and engineering.[21] However, the Bureau was able to make progress in addressing its skills gaps before the 2020 Census and continued to work toward ensuring that key information security skills are in place.

The Bureau's Chief Information Security Officer noted that hiring and retaining a cybersecurity workforce is an industry-wide challenge. To address challenges in planning for the cybersecurity and IT workforce in the Office of the Chief Information Officer (OCIO), Bureau officials stated that they have implemented workforce planning activities, including

- collaborating with stakeholders at the Bureau—such as its Human Resources Division—to plan, develop, analyze, and evaluate the OCIO's workforce;
- developing cybersecurity immersion programs, cloud and IT training programs along with staff development opportunities; and
- implementing strategic workforce training activities to enhance the knowledge and skills for employees along with training and staff development programs.

Bureau officials reported that these workforce planning activities have allowed the OCIO to recruit and retain a diverse staff. Specifically, Bureau officials reported that as of November 2023, they had filled 90 percent of the positions in the OCIO and were actively recruiting for several vacancies.

Because the four modernization programs require significant IT and cybersecurity-related knowledge, they also face similar challenges in hiring and recruiting IT staff. According to Bureau officials, each program identifies staff needs and works with human resources staff to fill those positions. For example, the CEDSCI program tracked hiring as a risk in its risk register in fiscal year 2023. Because the program was able to fill 25 of the 29 open positions, this risk was closed in October 2023.

The Bureau's efforts in hiring IT and cybersecurity staff will be important to its success in meeting its workforce planning goals. With plans in place to hire and train cybersecurity and IT personnel, the Bureau is better able

[21]GAO-16-623.

to ensure that it has the personnel with knowledge and experience to implement security controls in the systems used to collect, store, process, and disseminate data.

The Bureau's plans to improve its information security initiatives and programs lack details. We previously reported on challenges that the Bureau faced in securing systems for the 2020 Census.[22] For example, in 2018 we reported that the Bureau accepted cybersecurity risks because delays in system development compressed the time available for security assessments.[23] In addition, the Bureau struggled to complete cybersecurity corrective actions identified in these security assessments in a timely manner.

To its credit, for the 2020 Census the Bureau took steps to protect its systems and data by working with federal partners such as the Department of Homeland Security for cybersecurity assistance.[24] Among other things, DHS provided threat intelligence and information sharing, and provided assessments on topics including incident response and vulnerabilities. According to Census Bureau officials, the Bureau continues to receive cybersecurity threat information from DHS as appropriate, and while it no longer has a formal relationship with DHS following the 2020 Census, Bureau officials would consider leveraging its expertise in the future.

In response to the challenges faced during the 2020 Census, in September 2021, the Bureau identified several IT- and cybersecurity-related lessons learned. Among other things, Bureau officials noted that cybersecurity should be better integrated into the planning and development of systems from the outset, instead of after a system is developed. Officials also stated that the Bureau should implement principles of development, security, and operations (DevSecOps).[25] In September 2022, the Bureau reported that, among other things, it

[22]GAO, *2020 Census: Actions Needed to Address Key Risks to a Successful Enumeration*, GAO-19-588T (Washington D.C.: July 16, 2019).

[23]GAO, *2020 Census: Actions Needed to Mitigate Key Risks Jeopardizing a Cost-Effective and Secure Enumeration*, GAO-18-543T (Washington, D.C.: May 8, 2018).

[24]GAO-21-478.

[25]This model combines "development," "security," and "operations," and emphasizes communication, collaboration, and continuous integration between software developers and users.

planned to implement a DevSecOps strategy as part of its approach to secure systems and data for the four modernization initiatives.

In June 2023, the Bureau provided a draft DevSecOps implementation strategy, which is intended to integrate cybersecurity and IT operations requirements into software development and operations. This draft strategy includes a list of objectives and a high-level roadmap of tasks to achieve them. The objectives of the strategy include continuous collaboration and communication among development, operations, and security teams and ensuring that cybersecurity requirements, including principles related to zero trust, are defined prior to launching software.[26] The key steps to achieve those goals include assessing the current state of requirements definition and risk analysis, refining policies and procedures, and training staff on DevSecOps principles.

However, the draft implementation strategy has not been finalized and does not include key elements that would increase the likelihood that the Bureau is able to achieve those objectives. Specifically, it does not include time frames for any of the identified key steps. It also does not identify the officials responsible for accomplishing these steps. Bureau officials reported that they are currently revising the strategy and intend to finalize it in early 2024.

The steps noted in the DevSecOps strategy are important to addressing key cybersecurity lessons learned from the 2020 Census. Without details such as time frames for completing the steps, the Bureau is less likely to meet the goals and objectives laid out in their DevSecOps strategy.

The Bureau is in the process of enhancing its detection and response to cybersecurity incidents. Contingency planning and incident response help ensure that if normal operations are interrupted, network managers are able to detect, mitigate, and recover from a service disruption while preserving access to vital information.

To better enhance its response to potential incidents, the Bureau has developed policies and procedures for detecting and responding to

[26]Zero trust architecture is a cybersecurity approach that authenticates and authorizes every interaction between a network and a user or device—in contrast to traditional cybersecurity models that allow users or devices to move freely within the network once they are granted access. The Bureau's DevSecOps strategy is intended to be consistent with Office of Management and Budget's memorandum on zero trust: *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,* M-22-9 (Jan. 26, 2022).

potential incidents and data breaches and conducted related training, including the following:

- *Incident response policies and procedures:* The Bureau's incident response plan defines the processes and procedures for rapid incident response led by the Bureau's cybersecurity center. The plan addresses, among other things, the reporting of incidents, and the proper and timely escalation path for communicating risks to Bureau management, Department of Commerce, and federal authorities as appropriate.
- *Data breach policies and procedures:* The Census Bureau has a data breach policy implementation guide, which assists the data breach team in appropriately responding to data breaches based on the specific characteristics of the incident. The purpose of the policy is to help improve the Census Bureau's procedures for handling moderate and high-level breaches of personally identifiable information. It clarifies the responsibilities of division chiefs and department heads, and coordinates communications among the Bureau's data breach response committee, senior managers, the Associate Directors, the Chief Operating Officer, and the Department of Commerce's Chief Privacy Officer.
- *Incident response training:* To test the effectiveness of their incident response capability, the Census Bureau's Security Operations Center and Office of the Information Systems Security Officer conduct monthly tabletop exercises that document lessons learned after the exercise. The tabletop exercises deliver critical information, such as the definition of the incident, examples of real incidents that have occurred at Census, where to report incidents, and the incident response process.

However, the Bureau has struggled to implement incident detection and reporting procedures. In November 2022, the Department of Commerce OIG reported that the Bureau had insufficient incident detection and alerting, and made several recommendations to the Bureau to improve its incident response program.[27] For example, the OIG found that the Bureau (1) missed opportunities to mitigate a critical vulnerability, which resulted in exploitation of vital servers, (2) did not discover and report the incident in a timely manner, and (3) did not maintain sufficient logs, which hindered the incident investigation. Thus, the OIG made a series of recommendations, such as for the Bureau to frequently review and update vulnerability scanning lists, document all exceptions as part of this

[27]Department of Commerce, Office of Inspector General, OIG-23-004-1.

process, and periodically review system logs. As of December 2023, the Bureau was working to address these recommendations.

The Bureau's continuing efforts to enhance its detection and response to cybersecurity incidents will help ensure that the Bureau is better able to detect, mitigate, and recover from potential disruptions while preserving access to vital information.

The Bureau has not finalized plans to ensure respondent privacy while maintaining the usability of public data. Federal law requires agencies to have policies in place to address data privacy, and to protect personally identifiable information.[28] For example, the Bureau is prohibited from making any publication whereby the data furnished by a particular establishment or individual can be identified.[29] Faced with rising privacy threats, the Bureau has taken steps to identify, research, and strengthen methods to protect respondent privacy.

Bureau officials have reported that security, privacy, and confidentiality are paramount, and they are committed to having robust safeguards in place to protect data. However, they noted that publishing high-quality statistical products derived from information collected during censuses and surveys, such as the Decennial Census and the American Community Survey, is a challenge. Thus, navigating the balance between confidentiality protections and data utility is likely to be an ongoing concern for both privacy advocates and data users.

We have previously reported on the Bureau's efforts to address this challenge and the struggle to determine which privacy protections should be used on its publicly released data.[30] Specifically, two years before data collection began for the 2020 Census, the Bureau determined that it was not able to use the same privacy protections that it had used in prior decennials. The agency found that, using advances in technology, it was able to reconstruct sex, age, race, and ethnicity information for the enumerated population using data that had been published from the 2010 Census. To protect the confidentiality of respondents and their data, the

[28]In general, personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and Social Security number; or that otherwise can be linked to an individual. The Bureau may collect personally identifiable information when it obtains individual survey responses.

[29]13 U.S.C. § 9(a)(2).

[30]GAO-22-105324.

Bureau decided to use a new technique known as differential privacy on its publicly released statistical products.

The Bureau faced issues in implementing differential privacy for the 2020 Census. Among other things, the Bureau, its advisory committees, and its data users raised concerns about the Bureau's communication to users about its privacy protections (and any resulting impacts to the accuracy of the publicly available data). We also found that the Bureau's schedule to protect respondent privacy in 2020 Census data products lacked specificity. Thus, we recommended that the Bureau update its schedule for privacy-related activities for the 2020 Census, to include specific time frames for all related activities. As of February 2024, this recommendation has not yet been implemented.

Differential Privacy

Differential privacy is a type of formal privacy or disclosure avoidance technique aimed at limiting statistical disclosure and controlling privacy risk. According to the Bureau, the technique functions by including some statistical noise (i.e., data inaccuracies) using algorithms. These algorithms allow policy makers to determine the trade-off between the accuracy of data in Census products and the privacy of respondents.

Source: GAO summary of Census Bureau information. | GAO-24-105979

The Bureau has taken steps to evaluate the methods it will use to protect respondent data in future surveys. For example, in 2019 the Bureau reported that it was evaluating whether and how to use differential privacy (or a technique similar to it) to protect respondent data for the 2025 release of the American Community Survey. In December 2022, Bureau officials stated that it was taking the time to carefully research options and engage with the data user community about the confidentiality protections for the American Community Survey, and that differential privacy may not be the best fit to protect the data.

However, Bureau officials were not able to provide a plan with specific information about the steps they intend to take, and, importantly, the time frames for taking them, to determine the best methods to protect respondent privacy for the American Community Survey. These officials reported that the research into privacy methods is ongoing and slow moving, and the science does not yet exist to implement certain privacy techniques on surveys as complex as the American Community Survey. As of February 2024, Bureau officials reported that it had not decided on what privacy methods it will use for the 2025 American Community Survey but were planning to use prior methods while continuing to evaluate other options. Bureau officials indicated that a decision regarding privacy implementation for the data to be released in 2026 would need to be made no later than March 1, 2025. They also reported that this deadline is highly dependent on the scope of the solution and the necessary time to develop and test the systems used in the production environment to accommodate that solution.

Without identifying specific steps, including time frames, that it plans to take to identify and evaluate privacy methods, the Bureau is at increased

risk that it will not have enough information to make to make decisions about the implementation of privacy protections on future data products, and that the selected privacy implementation may not meet objectives.

Conclusions

The data that the Bureau collects are vital to government functions, and the associated IT systems are critical to secure, efficient, and effective operations. However, the Bureau's past attempt to modernize and consolidate IT systems did not deliver expected results.

The Bureau is now undertaking a new, large-scale modernization initiative but has had mixed results in managing the portion known as CEDSCI. While the Bureau has largely implemented leading practices related to managing risks and requirements, it has not yet developed a reliable cost estimate or a reliable schedule. Accordingly, the agency lacks assurance that it can effectively manage CEDSCI's cost and schedule and that decision-makers have the information needed to monitor the program.

The Bureau has taken steps to establish plans for addressing many of the cybersecurity and privacy challenges experienced during the prior Census. However, the Bureau has not yet committed to time frames for all of its efforts—specifically those in its DevSecOps plan and those aimed at protecting respondent privacy for the American Community Survey. Continued focus on these key cybersecurity challenges will be important as the Bureau develops systems and implements the IT modernization programs.

Recommendations for Executive Action

We are making the following five recommendations to the Department of Commerce:

The Secretary of Commerce should direct the Director of the Census Bureau to ensure that the CEDSCI program consistently documents user stories to ensure bidirectional traceability with requirements. (Recommendation 1)

The Secretary of Commerce should direct the Director of the Census Bureau to ensure that the CEDSCI program develops reliable cost estimates using best practices described in GAO's *Cost Estimating and Assessment Guide*, in particular those practices related to the comprehensive and credible characteristics. (Recommendation 2)

The Secretary of Commerce should direct the Director of the Census Bureau to ensure that the CEDSCI program develops its schedule using

the best practices described in GAO's *Schedule Assessment Guide*. (Recommendation 3)

The Secretary of Commerce should direct the Director of the Census Bureau to ensure that the OCIO incorporates key elements, such as time frames, into its DevSecOps strategy and finalizes it in a timely manner. (Recommendation 4)

The Secretary of Commerce should direct the Director of the Census Bureau to ensure that the American Community Survey program develops a plan, including time frames, for the steps they intend to take to determine the most appropriate methods to protect respondent privacy in the publicly available data releases. (Recommendation 5)

Agency Comments

We provided a draft of this report to the Department of Commerce for review and comment. Commerce concurred with all five of our recommendations and stated that it will take steps to improve in the areas of requirements management, cost estimating, and schedule management associated with our IT modernization efforts. It also noted that, related to confidentiality and the American Community Survey, the Census Bureau is committed to thoroughly protecting respondent data. Commerce's comments are reproduced in appendix II.

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

If you have any questions about this report, please contact me at (202) 512-6151 or walshk@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 III.

Sincerely,

Kevin Walsh
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) evaluate the extent to which the Bureau is implementing leading practices in monitoring and controlling risks, requirements, cost, and schedule for a selected enterprise-wide IT program, and (2) describe the key cybersecurity and privacy challenges the Bureau faces in implementing its IT modernization programs and determine the extent to which the Bureau has plans to address them.

For the first objective, we reviewed documentation describing the four programs that Bureau officials identified as their enterprise-wide modernization initiatives. We analyzed Bureau program management documentation, including program management plans, operational plans, strategic plans, risk management plans, requirements management plans, budget plans, and schedule management plans. Of the four modernization programs, we selected the Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI) program for our review, due to the maturity of its cost and schedule estimates. To properly assess the cost and schedule for the modernization programs, it was necessary that they had baseline costs and schedules to evaluate. We determined that the other programs were not far enough along in their development to perform extensive and detailed assessments against the selected criteria.

- To determine the extent to which the Bureau implemented leading practices for risk management, we selected two risk management leading practices identified by the Information Systems Audit and Control Association's (ISACA) Capability Maturity Model Integration (CMMI).[1] These leading practices map to the managed practices of risk management, where projects are planned, performed, measured, and controlled. These selected practices were (1) analyzing identified risks or opportunities and (2) monitoring identified risk or opportunities and communicate status to affected stakeholders. We then evaluated CEDSCI program documentation against the selected practices. Specifically, we reviewed the program's risk management plan, monthly risk registers, and mitigation and contingency plans for risks identified as "high" in the risk registers.

  To assess the reliability of data from CEDSCI's risk register, we interviewed knowledgeable Bureau officials, such as the CEDSCI program manager, about the accuracy and completeness of the data. We also compared the data to other relevant program documentation

[1]ISACA, *CMMI Model V2.2* (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

on requirements and risk management, such as the department's risk management plan. We determined that the data used were sufficiently reliable for the purpose of evaluating the department's practices for managing risk.

- To determine the extent to which the Bureau had implemented leading practices for requirements management, we selected five requirements management leading practices identified in the ISACA's CMMI.[2] These leading practices map to the managed practices of requirements development and management, where projects are planned, performed, measured, and controlled to identify and monitor progress towards project performance objectives. The selected practices were (1) eliciting stakeholder needs, (2) transforming stakeholder needs into prioritized customer requirements and consolidating and prioritizing various inputs from customers and stakeholders, (3) developing an understanding with the requirements providers on the meaning of the requirements, (4) obtaining commitment from project participants that they can implement the requirements, and (5) developing, recording, and maintaining bidirectional traceability among requirements and activities or work products, among others. We then evaluated CEDSCI program documentation against the selected practices. Specifically, we reviewed the program's requirements management plan, the documentation of stakeholder needs, user stories, feature scope analyses, and architectural enablement specifications.

  To assess the reliability of the program's requirements data, we interviewed knowledgeable Bureau officials (such as the CEDSCI program manager) about the procedures used by the program to assure accuracy and completeness of the data. We also compared the data to other relevant requirements documentation, such as user stories and feature scope analyses. We determined that the data used were sufficiently reliable for the purpose of evaluating the department's practices for managing IT requirements.

- To analyze the Bureau's progress in monitoring and controlling cost for the CEDSCI program, we compared cost documentation against cost best practices identified by our *Cost Estimating and Assessment*

[2]ISACA, *CMMI Model V2.2* (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

Guide.[3] These best practices map to the four characteristics of a high-quality, reliable cost estimate—comprehensive, well documented, accurate, and credible. Specifically, we analyzed cost documentation supporting the CEDSCI lifecycle cost estimate from September 2022. This documentation included the basis of estimate and other program office estimate documentation, independent cost estimate documentation, work breakdown structures, and documentation, such as meeting minutes, from Cost Review Board meetings.

To assess the reliability of the CEDSCI cost estimate data that we used to support findings in this report, we evaluated relevant program documentation, such as cost estimating models, as available, to substantiate evidence obtained from interviews with knowledgeable agency officials. We found the data we used to be sufficiently reliable for the purposes of our report.

- To determine the extent to which the Bureau implemented schedule estimation best practices, we compared schedule documentation for the CEDSCI program against schedule best practices identified by our *Schedule Assessment Guide*.[4] These best practices map to the four characteristics of a high-quality, reliable schedule estimate—comprehensive, well constructed, credible, and controlled. Specifically, we analyzed documentation from the CEDSCI program's schedule from September 2022, including the integrated master schedule, backlogs, trend analysis documentation, and program board documents for the budget year.

  To assess the reliability of the CEDSCI schedule, we evaluated documentation supporting the schedule, such as the integrated master schedule. We found the data we used to be sufficiently reliable for the purposes of our report.

For each of the four areas, we assessed the evidence against the best and leading practices to determine whether each project fully met, substantially met, partially met, minimally met, or did not meet the best practices. Specifically, "met" means that the Bureau provided complete evidence that satisfies the entire criterion, "substantially met" means the Bureau provided evidence that satisfies most but not all of the criterion, "partially met" means the Bureau provided evidence that satisfies some

[3]GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, GAO-20-195G (Washington, D.C.: Mar. 12, 2020).

[4]GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: Dec. 22, 2015).

but not all of the criterion, “minimally met” means the Bureau provided evidence that satisfies a small portion of the criterion, and “not met” means the Bureau provided no evidence that satisfies any of the criterion.

We also interviewed Bureau officials to determine the extent to which they have implemented the selected leading practices. We corroborated our analyses by interviewing agency officials in the CEDSCI program, especially in cases where they do not appear to have met the selected practices. Specifically, we interviewed Bureau officials from the CEDSCI program and the Decennial Census Directorate, including the CEDSCI program manager, Associate Director of Decennial Census Programs, and the Bureau’s Chief Information Security Officer, on their approach to managing risks, requirements, cost, and schedule for the program.

For the second objective, we reviewed prior reports by GAO and the Department of Commerce’s Office of the Inspector General that identified cybersecurity and privacy challenges the Bureau faced during the 2020 Census.[5] We also reviewed reports, such as GAO’s *Cybersecurity High-Risk Series*, that describe the major cybersecurity challenges across the federal government and summarize suggested actions for each of these challenges.[6] We reviewed documentation summarizing the Bureau’s lessons learned from the 2020 Census—which included actions related to cybersecurity and privacy protection—and interviewed staff within the Bureau’s Office of the Chief Information Officer. We also reviewed reports

[5]See, for example, GAO, *2020 Census: Lessons Learned from Planning and Implementing the 2020 Census Offer Insights to Support 2030 Preparations*, GAO-22-104357 (Washington, D.C.: Feb. 11, 2022); *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); *Information Technology: Better Management of Interdependencies between Programs Supporting 2020 Census Is Needed*, GAO-16-623 (Washington, D.C.: Aug. 9, 2016); and Department of Commerce, Office of Inspector General, *Simulated Internal Cyber Attack Gained Control of Critical Census Bureau System*, OIG-23-004-1 (Washington, D.C.: Nov. 22, 2022).

[6]GAO, *Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data*, GAO-23-106443 (Washington, D.C.: Feb. 14, 2023); *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure*, GAO-23-106441 (Washington, D.C.: Feb. 7, 2023); *Cybersecurity High-Risk Series: Challenges in Securing Federal Systems and Information*, GAO-23-106428 (Washington, D.C.: Jan. 31, 2023); *Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight*, GAO-23-106415 (Washington, D.C.: Jan. 19, 2023). The four major cybersecurity challenges identified in GAO’s 2023 High Risk Report were (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.

by GAO and others on information security challenges faced across the federal government. We synthesized the information from these reports to identify common themes of potential challenges. Based on this analysis, we developed an initial list of potential cybersecurity and privacy challenges that the Bureau may face in implementing its IT modernization initiatives.

To determine which of the identified challenges were key for the Bureau to address, we compared our initial list against Bureau documentation of cybersecurity and privacy challenges and risks. Specifically, we reviewed Bureau documentation related to (1) cybersecurity and privacy challenges faced during the Bureau's prior IT modernization activities; (2) the Bureau's lessons learned from the 2020 Census, which included actions related to cybersecurity and privacy protections; and (3) cybersecurity and privacy risks described in risk registers for the four modernization programs. In addition, we interviewed Bureau officials in the Office of the Chief Information Officer to confirm which challenges they considered the most critical. As part of this comparison, as well as to keep the list manageable, we selected the ones that, based on our judgement, posed the most significant challenges to the Bureau at the time of our review. This resulted in the four key challenges described in this report:

- addressing cybersecurity workforce challenges by ensuring key IT positions are filled,
- improving information security initiatives and programs,
- enhancing the detection and response to cybersecurity incidents, and
- ensuring respondent privacy while maintaining the usability of public data.

To determine the Bureau's plans to address each of the key challenges, we analyzed documentation regarding activities the Bureau plans to take to address the identified cybersecurity and privacy challenges, including hiring goals; the draft development, security, and operations strategy; the integration plan for the Bureau's four enterprise-wide modernization programs; the Bureau's incident response plan; and the Bureau's policies related to safeguarding and managing information. We also interviewed Bureau officials, such as the Chief Information Officer and the Chief Information Security Officer.

We conducted this performance audit from April 2022 to April 2024 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: Comments from the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
Office of the Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

April 3, 2024

Mr. Kevin Walsh
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Walsh:

The U.S. Census Bureau appreciates the opportunity to comment on the U.S. Government Accountability Office (GAO) draft report entitled, "IT MODERNIZATION: Census Bureau Needs Reliable Cost and Schedule Estimates" (GAO-24-105979).

The Census Bureau agrees with the draft report related to Census Bureau technology modernization. The Census Bureau appreciates the GAO's recognition of our risk management practices, concurs with the five recommendations, and will take steps to improve our requirements management, cost estimating, and schedule management associated with our IT modernization efforts. In relation to confidentiality and the American Community Survey, the Census Bureau is committed to thoroughly protecting respondent data and we currently support this effort robustly in planning for our yearly releases and continuing our research into alternative privacy frameworks to ensure this confidentiality. The Census Bureau will prepare a formal action plan addressing these recommendations upon GAO's issuance of the final report.

Thank you for your continued interest in and efforts toward increasing the benefits of the Census Bureau's IT modernization programs.

Sincerely,

JEREMY PELTER Digitally signed by JEREMY PELTER Date: 2024.04.03 17:43:53 -04'00'

Jeremy Pelter
Deputy Assistant Secretary for Administration,
Performing the Non-Exclusive Functions and
Duties of the Chief Financial Officer and Assistant
Secretary for Administration

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Kevin Walsh, (202) 512-6151, or walshk@gao.gov

Staff Acknowledgments

In addition to the contact named above, Kate Sharkey (Assistant Director), Lisa Hardman (Analyst-in-Charge), Amanda Andrade, Lauri Barnes, Chris Businsky, Juana Collymore, Matthew Gray, Angel Green, William Laing IV, Carlton Maynard, Ty Mitchell, Bradley Pedone, Christeena Saji, Dwayne Staten, Walter Vance, and Adam Vodraska made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

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