United States Government Accountability Office

Report to Congressional Committees

August 2016

INFORMATION TECHNOLOGY

Better Management of Interdependencies between Programs Supporting 2020 Census Is Needed

GAO-16-623

August 2016

GAO Highlights

Highlights of GAO-16-623, a report to congressional committees

INFORMATION TECHNOLOGY

Better Management of Interdependencies between Programs Supporting 2020 Census Is Needed

Why GAO Did This Study

The Department of Commerce's U.S. Census Bureau plans to significantly change the methods and technology it uses to count the population with the 2020 Decennial Census. The Bureau's redesign of the census relies on the acquisition and development of many new and modified systems. Several of the key systems are to be provided by an enterprise-wide initiative called CEDCAP, which is a large and complex modernization program intended to deliver a system-of-systems for all survey data collection and processing functions.

GAO's objectives for this review included (1) evaluating the extent to which the Bureau is implementing best practices in monitoring and controlling three selected CEDCAP projects, (2) determining the extent to which the Bureau is adequately managing the interdependencies between the CEDCAP and 2020 Census programs, and (3) describing key information security challenges the Bureau faces in implementing the 2020 Census design. GAO selected the three high-priority projects planned for the 2020 design; reviewed Bureau documentation such as project plans and schedules and compared them against relevant guidance; and analyzed information security reports and documents.

What GAO Recommends

GAO is making eight recommendations to the Department of Commerce in the areas of project monitoring and control and in managing interdependencies related to schedule, risk, and requirements. The department agreed with all eight recommendations and indicated that it will be taking actions to address them.

View GAO-16-623. For more information, contact Carol C. Harris at (202) 512-4456 or chac@gao.gov.

What GAO Found

The three selected Census Enterprise Data Collection and Processing (CEDCAP) projects (of 12 total) in GAO's review partially met best practices for monitoring and controlling. For example, the projects fully met the best practice of establishing a process for taking corrective actions if issues are identified, but they did not fully meet the practice of identifying significant performance deviations. Until project officials implement missing practices, they will be limited in their abilities to monitor and control costs, schedules, and performance.

The 2020 Census program is heavily dependent upon CEDCAP to deliver the key systems needed to support the 2020 Census redesign. However, while the two programs have taken steps to coordinate their schedules, risks, and requirements, they lacked effective processes for managing their interdependencies. Specifically:

- Among tens of thousands of schedule activities, the two programs are expected to manually identify activities that are dependent on each other, and rather than establishing one integrated dependency schedule, the programs maintain two separate dependency schedules. This has contributed to misalignment in milestones between the programs.
- The programs do not have an integrated list of interdependent program risks, and thus they do not always recognize the same risks that impact both programs.
- Among other things, key requirements have not been defined for validating responses from individuals who respond to the census using an address instead of a Bureau-assigned identification number, because of the Bureau's limited knowledge and experience in this area. The lack of knowledge and specific requirements related to this critical function is concerning, given that there is about a year remaining before the Census end-to-end test begins in August 2017 (which is intended to test all key systems and operations to ensure readiness for the 2020 Census).

Officials have acknowledged these weaknesses and reported that they are taking, or plan to take, steps to address the issues. However, until these interdependencies are managed more effectively, the Bureau will be limited in understanding the work needed by both programs to meet milestones, mitigate major risks, and ensure that requirements are appropriately identified.

While the large-scale technological changes for the 2020 Decennial Census introduce great potential for efficiency and effectiveness gains, they also introduce many information security challenges. For example, the introduction of an option for households to respond using the Internet puts respondents at greater risk for phishing attacks (requests for information from authentic-looking, but fake, e-mails and websites). In addition, because the Bureau plans to allow its enumerators to use mobile devices to collect information from households that did not self-respond to the survey, it is important that the Bureau ensures that these devices are adequately protected. The Bureau has begun efforts to address many of these challenges; as it begins implementing the 2020 Census design, continued focus on these considerable security challenges will be critical.

Contents

Letter		1
	Background	3
	CEDCAP's 12 Projects Are at Various Stages of Planning and Design	16
	Selected CEDCAP Projects Partially Met Project Monitoring and Control Best Practices	22
	The Bureau Lacks Processes for Effectively Managing Interdependencies between CEDCAP and 2020 Census Programs	26
	Census Bureau Faces Several Information Security Challenges in Implementing the 2020 Census	35
	Conclusions	43
	Recommendations for Executive Action	44
Appendix I	Objectives, Scope, and Methodology	50
Appendix II	Comments from the Department of Commerce	54
Appendix III	GAO Contact and Staff Acknowledgments	59
Tables		
	Table 1: Census Enterprise Data Collection and Processing (CEDCAP) Project Objectives	9
	Table 2: Status of Census Enterprise Data Collection and Processing (CEDCAP) Projects	19
Figures		
	Figure 1: 2020 Census Decision Inventory as of April 2016	4
	Figure 2: Overview of the Census Bureau's Plans and Assumptions for the 2020 Census, as of October 6, 2015	7
	Figure 3: Census Enterprise Data Collection and Processing (CEDCAP) Product Release Schedule – 2020 Decennial Census vs. Other Bureau Surveys	11
	Figure 4: Examples of 2020 Census-related IT Decisions Planned for Later in the Decade that Could Impact the Census	

Enterprise Data Collection and Processing (CEDCAP) Program, as of April 2016 29

Abbreviations

ACS	American Community Survey
Bureau	U.S. Census Bureau
CEDCAP	Census Enterprise Data Collection and Processing
CMMI-ACQ	Capability Maturity Model® Integration for Acquisition
CMMI-DEV	Capability Maturity Model® Integration for Development
COTS	commercial off the shelf
IT	information technology
NIST	National Institute of Standards and Technology
PII	personally identifiable information
US-CERT	U.S. Computer Emergency Readiness Team

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

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

August 9, 2016

Congressional Committees

On October 6, 2015, the U.S. Census Bureau (Bureau) released the first version of its 2020 Census Operational Plan, which is intended to outline the design decisions that drive how the 2020 Decennial Census will be conducted. These design decisions are expected to significantly transform how the Bureau conducts the Decennial Census, in an effort to save approximately $5.2 billion. The redesign largely depends on implementing new technology and systems to modernize and automate many parts of the census. Accordingly, concurrent with the overhaul of the 2020 Census, the Bureau is significantly redesigning the information technology (IT) systems that support each of its surveys, including the 2020 Decennial Census, American Community Survey (ACS), and Economic Census.[1]

Specifically, for the 2020 Decennial Census, the Bureau plans to significantly change the methods and technology it uses to count the population, such as offering an option for households to respond to the survey via the Internet, providing mobile devices for field enumerators to collect survey data from households, and automating the management of field operations. The Bureau's redesign of the census relies on the acquisition and development of many new and modified IT systems. Several of these systems are expected to be provided by an enterprise-wide initiative called Census Enterprise Data Collection and Processing (CEDCAP). This initiative is a large and complex modernization program intended to deliver a system-of-systems for all the Bureau's survey data collection and processing functions, rather than continuing to rely on unique, survey-specific systems with redundant capabilities.

Given CEDCAP's importance to achieving the 2020 Decennial Census redesign, you asked us to review the Bureau's efforts to implement it. The specific objectives of our review were to (1) describe the status of the 12

[1]The ACS collects data on social, demographic, economic, and housing characteristics on a monthly basis and aggregates the results into 1- and 5-year estimates. The Economic Census is conducted every 5 years and provides statistics on all non-farm business establishments in the United States.

CEDCAP projects, (2) evaluate the extent to which the Bureau is implementing best practices in monitoring and controlling selected projects, (3) determine the extent to which the Bureau is adequately managing the interdependencies between the CEDCAP and 2020 Census programs, and (4) describe the key information security challenges the Bureau faces in implementing the 2020 Census design.

To address the first objective, we reviewed relevant CEDCAP program and project documentation, such as the transition plan, segment architecture, project charters, and monthly progress reports, and interviewed Bureau officials on the status and plans of all 12 projects.

To address the second objective, we selected three of the CEDCAP projects based on those that Bureau officials identified as being the highest priority for the 2020 Census—(1) Centralized Operational Analysis and Control Project, (2) Internet and Mobile Data Collection Project, and (3) Survey (and Listing) Interview Operational Control Project. We analyzed project schedules, risk registers, and management reports for these three projects and interviewed Bureau officials on their efforts to manage these projects. We compared the Bureau's approach against best practices for project monitoring and control identified by the Software Engineering Institute's Capability Maturity Model® Integration for Acquisition (CMMI®-ACQ) and for Development (CMMI-DEV).[2]

To address the third objective, we analyzed relevant documentation from the CEDCAP program and the 2020 Census program, such as risk management plans, program-level risk registers, master schedules, program management plans, and requirements management documentation, and compared them against best practices identified in CMMI-ACQ and CMMI-DEV, as well as by GAO for managing interdependencies.[3] We also interviewed Bureau officials from the CEDCAP and 2020 Census programs on their approach to managing interdependencies between the two programs.

[2]Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI®-ACQ), Version 1.3 (Pittsburgh, Pa.: November 2010); CMMI for Development (CMMI-DEV), Version 1.3 (Pittsburgh, Pa.: November 2010).

[3]CMMI-ACQ; CMMI-DEV; and GAO, *Schedule Assessment Guide: Best Practices for Project Schedules,* GAO-16-89G (Washington, D.C.: December 2015).

To address the fourth objective, we reviewed relevant documents, such as CEDCAP and 2020 Census program risk registers and relevant GAO reports on information security challenges. We analyzed and aggregated this information to develop an initial list of information security challenges the Bureau faces in implementing the 2020 Census design. We validated the list of key challenges by obtaining input from internal and external experts in information security and/or Decennial Census operations. We also reviewed documentation regarding the Bureau's progress in implementing our 2013 information security recommendations.[4] Appendix I contains further details on our objectives, scope, and methodology.

We conducted this performance audit from October 2015 to August 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The Bureau's mission is to collect and provide comprehensive data about the nation's people and economy. Its core activities include conducting decennial, economic, and government censuses; conducting demographic and economic surveys; managing international demographic and socioeconomic databases; providing technical advisory services to foreign governments; and performing other activities such as producing official population estimates and projections. One of the Bureau's most important functions and largest undertakings is conducting the Decennial Census, which is mandated by the Constitution and provides data that are vital to the nation. The information collected is used to apportion seats in the House of Representatives, realign the boundaries of legislative districts, and allocate billions of dollars in federal financial assistance.

The Bureau is part of the Department of Commerce and is headed by a Director. It is organized into directorates corresponding to key

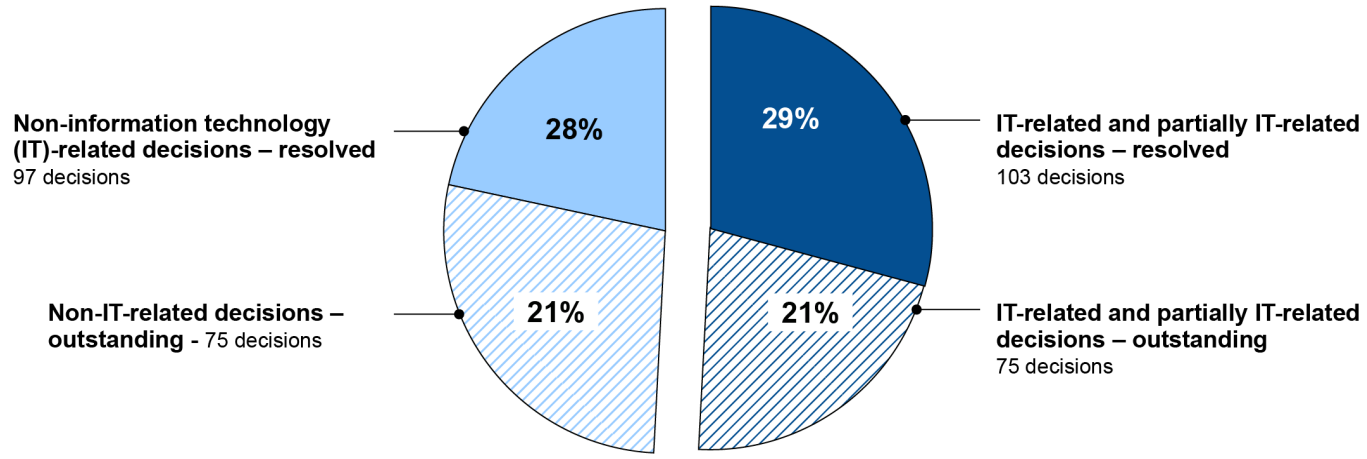
[4]GAO, *Information Security: Actions Needed by Census Bureau to Address Weaknesses*, GAO-13-63 (Washington, D.C.: Jan. 22, 2013). Another version of this report contained sensitive information and, as a result, was issued for limited distribution.

programmatic and administrative functions, including the IT Directorate led by the Associate Director for IT and Chief Information Officer, and the 2020 Census Directorate, led by the Associate Director for Decennial Census Programs.

2020 Census Design Decisions

The Bureau's October 2015 2020 Census Operational Plan outlines 350 redesign decisions that the Bureau has either made or is planning to make largely by 2018. The Bureau has determined that about 51 percent of the design decisions are either IT-related or partially IT-related (84 IT-related and 94 partially IT-related) and the Bureau reported that, as of April 2016, it had made about 58 percent of these decisions (48 IT-related and 55 partially IT-related). (See fig. 1 below.)

Figure 1: 2020 Census Decision Inventory as of April 2016



Source: GAO analysis of Census Bureau data. | GAO-16-623

Note: The percentages in figure 1 do not add up to 100 percent due to rounding.

Examples of decisions that have been made include the following:

- **Internet response**—For the first time on a nationwide scale, the Bureau will allow individuals/households to respond to the census on the Internet from a computer, mobile device, or other devices that access the Internet.
- **Non-ID processing with real-time address matching**—The Bureau will provide each household with a unique ID by mail. However, users may also respond to the online survey without the unique ID by

entering their address. This operation includes conducting real-time matching of respondent-provided addresses.

- **Non-response follow-up**—If a household does not respond to the census by a certain date, the Bureau will send out employees to visit the home. These enumerators will use a census application, on a mobile device provided by the Bureau, to capture the information given to them by the in-person interviews.[5] The Bureau will also manage the case workload of these enumerators using an operational control system that automatically assigns, updates, and monitors cases during non-response follow-up.
- **Administrative records**—As we reported in October 2015, the Bureau is working on obtaining and using administrative records from other government agencies,[6] state and local governments, and third-party organizations to reduce the workload of enumerators in their non-response follow-up work. For example, the Bureau plans to use administrative records to identify vacant housing units to remove from enumerators' workloads, count households that did not return census questionnaires, predict best times to complete non-response follow-up, and help process responses it receives either on paper or over the Internet that do not have a census ID number on them (non-ID processing).[7]
- **Mobile devices**—The Bureau plans to award a contract that would provide commercially available mobile phones and the accompanying service contract on behalf of the Census Bureau to enumerators, who will use these devices to collect census data. This approach is referred to as the device-as-a-service strategy.
- **Cloud computing**—The Bureau plans to use a hybrid cloud solution where it is feasible, and has decided it will use cloud services for the

[5]The Bureau had been researching an option for enumerators to use their own device for non-response follow-up activities, but has decided not to pursue this option.

[6]The Bureau reported that it plans to obtain information such as the U.S. Postal Service's undeliverable as addressed data, the Internal Revenue Service's individual taxpayer data, and the Centers for Medicare & Medicaid Services' Medicare enrollment data.

[7]GAO, *2020 Census: Additional Actions Would Help the Bureau Realize Potential Administrative Records Cost Savings,* GAO-16-48 (Washington, D.C.: Oct. 20, 2015).

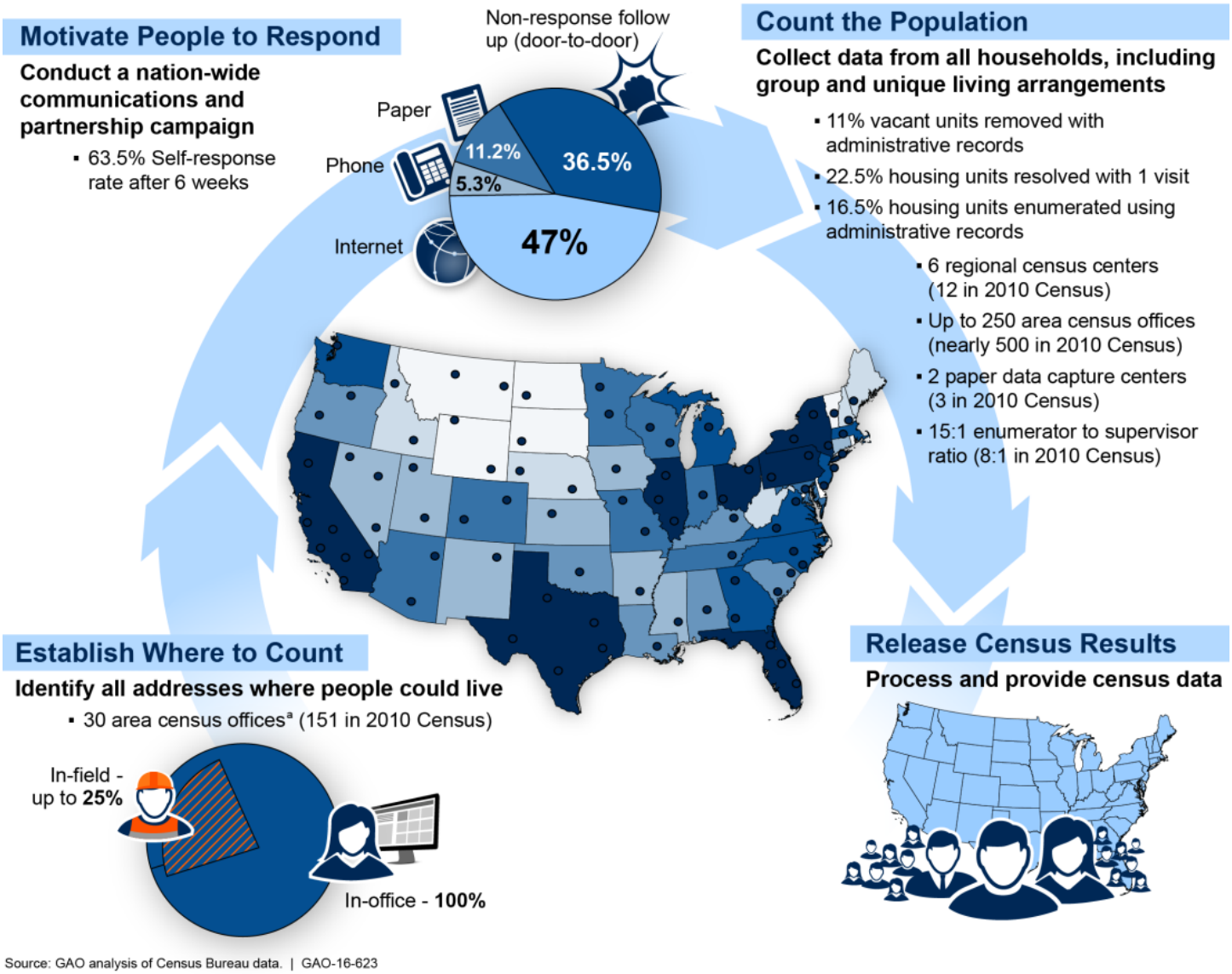
Internet response option as well as for non-ID processing with real-time address matching.[8]

- **Address canvassing**—The Bureau has decided to reengineer its address canvassing process to reduce the need for employing field staff to walk every street in the nation in order to update its address list and maps. For example, the Bureau plans to first conduct in-office address canvassing using aerial imagery, administrative records, and commercial data before sending staff into the field.

Figure 2 provides an overview of additional decisions and assumptions for the 2020 Census, resulting from the October 2015 operational plan.

[8]Cloud computing is a means for delivering computing services via IT networks. A hybrid cloud is one type of deployment model for providing cloud services that combines two or more other deployment models, such as private—set up specifically for one organization—and public—available to the general public and owned and operated by the service provider, and is bound together by standardized or proprietary technology.

Figure 2: Overview of the Census Bureau's Plans and Assumptions for the 2020 Census, as of October 6, 2015



Source: GAO analysis of Census Bureau data. | GAO-16-623

Note: The Bureau continues to refine its assumptions as it conducts further research and testing leading up to the 2020 Census.

[a]The 30 area census offices for identifying addresses where people could live are included in the 250 area census offices planned for the 2020 Census.

Examples of decisions that have not been finalized as of May 2016 include the following.

- **Invalid return detection and non-ID response validation**—The Bureau has not decided on its approach for identifying whether fraudulent returns have been submitted for the 2020 Census or the criteria and thresholds to decide whether further investigation may be needed, such as field follow-up.
- **Solutions architecture**—While the Bureau has established a notional solutions architecture for the 2020 Census, it has not decided on the final design.
- **Internet response for island areas**—The Bureau has not decided on the extent to which the Internet self-response option will be available for island area respondents.[9]
- **Additional uses of cloud**—While Bureau officials have decided on select uses of cloud-based solutions, decisions remain on additional possible uses. For example, the Bureau is exploring whether it will use a cloud service provider to support a tool for assigning, controlling, tracking, and managing enumerators' caseloads in the field.

IT Systems Supporting the 2020 Census

The Bureau's redesign of the census relies on the acquisition and development of many new and modified systems. Several of the key systems are expected to be provided as CEDCAP enterprise systems under the purview of the IT Directorate. According to Bureau officials, the remaining systems (referred to as non-CEDCAP systems) are to be provided by the 2020 Census Directorate's IT Division or other Bureau divisions. The 2020 Census Directorate established a Systems Engineering and Integration program office that is to serve as the technical arm of the 2020 Census program and is responsible for ensuring that all the system capabilities needed for the 2020 Census are developed and delivered, including integration of the CEDCAP and non-CEDCAP systems.

[9]The decennial census island areas include Puerto Rico, U.S. Virgin Islands, Guam, American Samoa, and Commonwealth of the Northern Mariana Islands.

CEDCAP Program Structure and Relationship to the 2020 Census Program

The CEDCAP program is intended to provide data collection and processing solutions, which include systems, interfaces, platforms and environments, to support the Bureau's entire survey life cycle, including survey design; instrument development; sample design and implementation; data collection; and data editing, imputation, and estimation.

The program consists of 12 projects, which have the potential to offer numerous benefits to the Bureau's survey programs, including the 2020 Census program, such as enabling an Internet response option; automating the assignment, controlling, and tracking of enumerator caseloads; and enabling a mobile data collection tool for field work. Eleven of these projects are intended to deliver one or more IT solutions. The twelfth project—IT Infrastructure Scale-Up—is not intended to deliver IT capabilities, solutions, or infrastructure; rather, it is expected to provide funding to the other relevant projects to acquire the necessary hardware and infrastructure to enable 2020 Census systems to scale to accommodate the volume of users. Table 1 describes the objectives of each project.

Table 1: Census Enterprise Data Collection and Processing (CEDCAP) Project Objectives

Project	Objective
Address Listing and Mapping	Provide a multi-platform enterprise solution for field collection of addresses and mapping information.
Dashboard for Monitoring	Provide an interface between the dashboard reporting system that monitors survey cost, progress, and quality and the multi-mode operational control system.
Internet and Mobile Data Collection	Provide two solutions—an Internet self-response option for censuses and surveys and a mobile data collection application for field interviewers to collect survey data from respondents.
Questionnaire Design and Metadata	Provide two solutions—a centralized solution for designing surveys and standardizing input parameters across data collection modes and a paper rendering component.
Survey (and Listing) Interview Operational Control	Provide two solutions—a tool for assigning, controlling, tracking, and managing enumerators' caseloads and a data collection tool to enhance efficiency of field operations.
Centralized Operational Analysis and Control	Provide three solutions—a control system that serves as the operational brain for dynamic caseload management across multiple survey modes and acts as the main interface between multiple other CEDCAP systems, an enterprise modeling platform that stores and uses data to execute statistical models, and a set of application programming interfaces that automate data accessibility to administrative records and previous survey data.
Centralized Development and Test Environment	Provide an integrated environment in which to perform development, integration testing, and pre-production testing.
Electronic Correspondence Portal	Provide census respondents with an electronic assistance portal.
Scanning Data Capture from Paper	Provide an enterprise capability to scan data from paper-based forms.

Project	Objective
Service Oriented Architecture	Provide a platform on which services can be deployed and from which services can be consumed by other applications through an application programming interface that is accessible across the enterprise.
Survey Response Processing	Provide two solutions—a data processing system that performs sample selection and a system to perform response processing.
IT Infrastructure Scale-Up	Provide funding to the other relevant projects to acquire the necessary hardware and infrastructure to enable 2020 Census systems to scale to accommodate the volume of users.

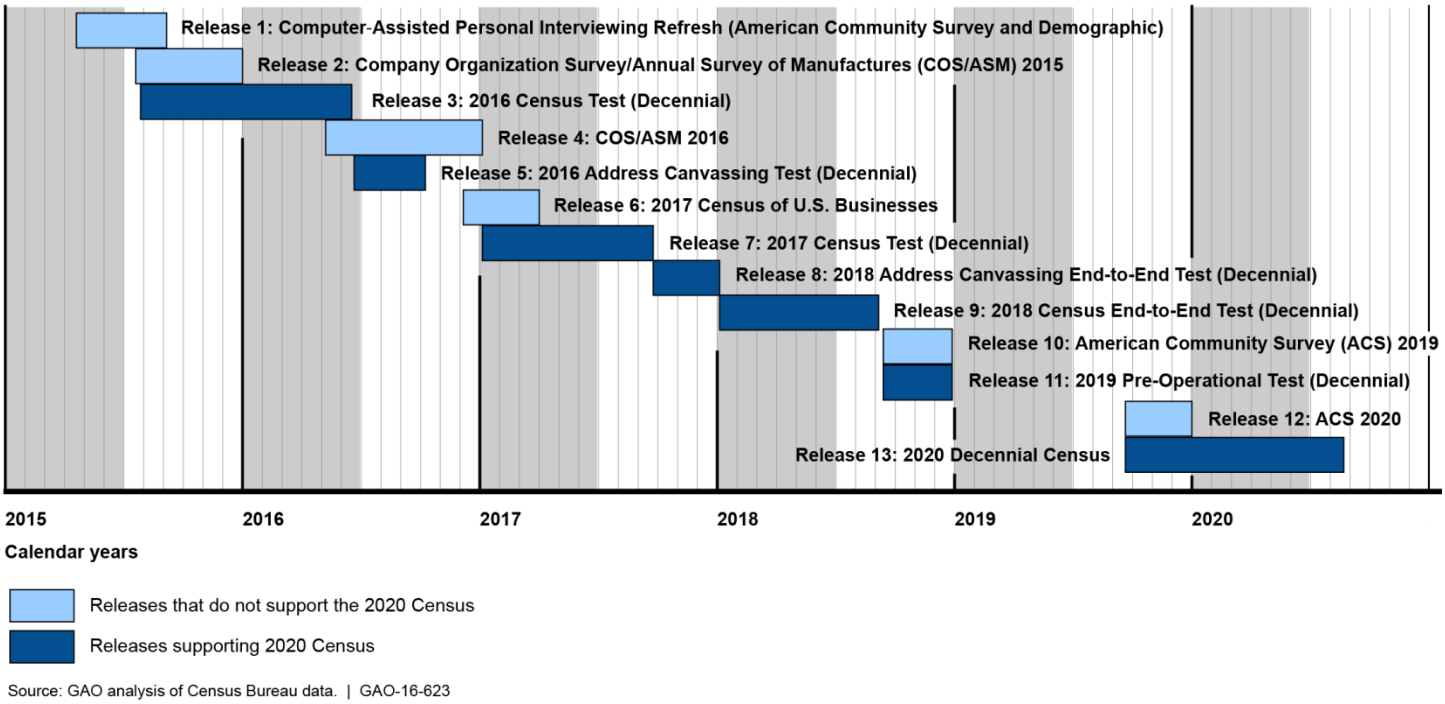
Source: GAO analysis of Bureau documentation. | GAO-16-623

The eleven projects are to provide functionality incrementally over the course of 13 product releases. The product releases are intended to support major tests and surveys at the Bureau through 2020. Of the 13 product releases, 7 are intended to support 6 remaining major tests the 2020 Census program is conducting as it prepares for the 2020 Census,[10] as well as 2020 Census live production. The remaining 6 releases support the other surveys such as the ACS and Economic Census. Most recently, the CEDCAP program had been working on delivering the functionality needed for the third product release which was to support a major census test, referred to as the 2016 Census Test—conducted by the 2020 Census program to inform additional decennial design decisions.

The 2018 Census End-to-End Test, noted below, is critical to testing all production-level systems and operations in a census-like environment to ensure readiness for the 2020 Census. The 2020 Census program plans to begin this test in August 2017. Figure 3 identifies which of the 13 CEDCAP product releases support the 2020 Census versus other surveys, as of May 2016.

[10]Beginning in 2013, the Bureau conducted several major field tests to examine possible redesign options, including the 2013 Census test, 2014 Census test, and the 2015 Census test. These tests were used to inform design decisions that were identified in Bureau's 2020 Census Operational Plan. As of March 2016, the Bureau planned to conduct four more major tests to further refine the design through 2018, as well as defect resolution and post end-to-end performance testing in 2019. According to Bureau officials, they planned to also conduct defect resolution and post-end-to-end performance testing, although time frames for those tests have not yet been established.

Figure 3: Census Enterprise Data Collection and Processing (CEDCAP) Product Release Schedule – 2020 Decennial Census vs. Other Bureau Surveys, as of May 2016



Source: GAO analysis of Census Bureau data. | GAO-16-623

Note: In June 2016, Bureau officials provided us with updated program documentation, which they indicated includes changes to their product release schedule. We have not reviewed this new documentation to verify the changes.

Each product release is decomposed into increments which follow a 40-day delivery schedule. Each of these 40-day increments focuses on a subset of functionality to deliver at the end of the increment. The Bureau determined that iterative deliveries of increments of functionality would best suit the CEDCAP program, instead of a “big bang” delivery approach for all solutions across all census and survey operations. Officials reported that such an approach would be impractical given the complexity of the program.

To manage this complex program, the CEDCAP Program Management Office consists of three distinct functions:

- **Program Governance, Planning, and Execution:** This function is led by the Program Manager and is responsible for strategically leading, integrating, and managing the 12 projects.

- **Business Operations:** Led by the Assistant Chief of Business Operations, this function is responsible for project management, risk, issue, schedule, and budget activities. It focuses on the processes that are critical to ensuring seamless integration across projects.
- **Technical Integration:** This function is led by the Chief Program Architect, Chief Program Engineer, and Chief Security Engineer, and is responsible for supporting integration and execution of projects, participating in technical reviews, and establishing technical processes related to design, development, testing, integration, and IT security.

In addition to the Program Management Office, the Bureau established the Office of Innovation and Implementation to articulate the overall business needs across the enterprise and ensure they are fulfilled by the capabilities to be delivered by CEDCAP. The Office of Innovation and Implementation is responsible for gathering and synthesizing business requirements across the Bureau, including for the 2020 Census Directorate, and delivering them to CEDCAP.

Prior Related GAO Reports Identified IT Management Challenges

Our prior work has identified the importance of having sound management processes in place to help the Bureau as it manages the multimillion dollar investments needed for its decennial census. For the last decennial, we issued multiple reports and testimonies from 2005 through 2010 on weaknesses in the Bureau's acquisition, management, and testing of key 2010 census IT systems.

For example, we reported on significant issues with the Census Bureau's Field Data Collection Automation program, which was intended to develop custom handheld mobile devices to support field data collection for the census, including in-person follow-up with those who did not return their census questionnaires (nonresponse follow-up). However, as we testified in March 2008, the program was experiencing significant problems, including schedule delays and cost increases from changes in requirements. Due in part to these technology issues the Bureau was facing, we designated the 2010 Census a high-risk area in March 2008.[11]

[11]GAO, *Information Technology: Significant Problems of Critical Automation Program Contribute to Risks Facing 2010 Census*, GAO-08-550T (Washington, D.C.: Mar. 5, 2008).

In April 2008, the Bureau decided not to use the handheld devices for nonresponse follow-up. Dropping the use of handheld devices for nonresponse follow-up and replacing them with a paper-based system increased the cost of the census by up to $3 billion. Although the Bureau worked aggressively to improve the paper-based system that replaced the handheld computers, we reported in December 2010 that the paper-based system also experienced significant issues when it was put in operation.[12]

Since the 2010 Census, we have issued additional reports and testimonies on weaknesses in the Bureau's efforts to institutionalize IT and program management controls for the 2020 Census. Relevant reports include the following:

- In September 2012, we reported that the Bureau had taken steps to draft new processes to improve its ability to manage IT investments and system development, and to improve its IT workforce planning.[13] However, we found that additional work was needed to ensure that these processes were effective and successfully implemented across the Bureau, such as finalizing plans for implementing its new investment management and systems development processes across the Bureau, conducting an IT skills assessment and gap analysis, and establishing a process for directorates to coordinate on IT workforce planning. The Bureau has fully addressed our recommendations to address these weaknesses by, for example, finalizing its investment management process, conducting an enterprise-wide IT competency assessment and gap analysis, and developing action plans to address the identified gaps.
- As we reported in November 2013, the Bureau was not producing reliable schedules for two efforts related to the 2020 Census: (1) building a master address file and (2) 2020 Census research and

[12]GAO, *2010 Census: Data Collection Operations Were Generally Completed As Planned, but Long-Standing Challenges Suggest Need for Fundamental Reforms*, GAO-11-193 (Washington, D.C.: Dec. 14, 2010).

[13]GAO, *Information Technology: Census Bureau Needs to Implement Key Management Practices,* GAO-12-915 (Washington, D.C.: Sept. 18, 2012).

testing.[14] For example, the Bureau did not include all activities and required resources in its schedules, or logically link a number of the activities in a sequence. We recommended that the Bureau take actions to improve the reliability of its schedules, including ensuring that all relevant activities are included in the schedules, complete scheduling logic is in place, and a quantitative risk assessment is conducted. We also recommended that the Bureau undertake a robust workforce planning effort to identify and address gaps in scheduling skills for staff that work on schedules. The Bureau has taken steps to implement these recommendations, but has not fully implemented them.

- In April 2014 and February 2015 we reported on the Bureau's lack of prioritization of IT decisions related to the 2020 Census. Specifically, in April 2014, we reported that the Bureau had not prioritized key IT research and testing needed for its 2020 Census design decisions.[15] Accordingly, we recommended that the Bureau prioritize its IT-related research and testing projects. The Bureau had taken steps to address this recommendation, such as releasing a plan in September 2014 that identified research questions intended to inform the 2020 Census operational design decisions. In February 2015, however, we reported that the Bureau had not determined how key IT research questions that were identified in the September 2014 plan would be answered—such as the expected rate of respondents using its Internet response option or the IT infrastructure that would be needed to support this option.[16] We recommended that the Bureau, among other things, develop methodologies and plans for answering key IT-related research questions in time to inform design decisions. The Bureau has taken steps to implement the recommendations, such as releasing a preliminary 2020 Census Operational Plan that documents many key IT-related decisions; however, many other IT-related questions, including the ones that were identified in our report, are to remain unanswered until 2016 through 2018.

[14]GAO, *2020 Census: Bureau Needs to Improve Scheduling Practices to Enhance Ability to Meet Address List Development Deadlines,* GAO-14-59 (Washington, D.C.: Nov. 21, 2013).

[15]GAO, *2020 Census: Prioritized Information Technology Research and Testing Is Needed for Census Design Decisions,* GAO-14-389 (Washington, D.C.: Apr. 3, 2014).

[16]GAO, *2020 Census: Key Challenges Need to Be Addressed to Successfully Enable Internet Response,* GAO-15-225 (Washington, D.C.: Feb. 5, 2015).

- As a result of the Bureau's challenges in key IT internal controls and its looming deadline, we identified CEDCAP as an IT investment in need of attention in our February 2015 High-Risk report.[17]
- Further, we testified in November 2015, that key IT decisions needed to be made soon because the Bureau was less than 2 years away from end-to-end testing of all systems and operations to ensure readiness for the 2020 Census and there was limited time to implement it.[18] We emphasized that that Bureau had deferred key IT-related decisions, and that it was running out of time to develop, acquire, and implement the systems it will need to deliver the redesign and achieve its projected $5.2 billion in cost savings. In addition, we stated that while the Bureau had made improvements in some key IT management areas, it still faced challenges in the areas of workforce planning and information security because it had yet to fill key positions—most concerning was the lack of a permanent chief information officer.

We have also reported extensively on the increasing security risks facing federal agencies' systems and data.[19] These risks were recently illustrated by the data breaches at the Office of Personnel Management, which affected millions of current and former federal employees. As we have reported, protecting the information systems and the information

[17]Every 2 years at the start of a new Congress, GAO calls attention to agencies and program areas that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation. As part of a new entry into the February 2015 update to our High-Risk Series focused on improving the management of IT acquisitions and operations, CEDCAP was identified as an IT investment—among others across the federal government—in need of the most attention. See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[18]GAO, *2020 Census: Key Information Technology Decisions Must Be Made Soon,* GAO-16-205T (Washington, D.C.: Nov. 3, 2015).

[19]See, for example, GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15-714 (Washington, D.C.: Sept. 29, 2015); *Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*, GAO-15-758T (Washington, D.C.: July 8, 2015); *Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies*, GAO-15-725T (Washington, D.C.: June 24, 2015); *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013); and *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged*, GAO-12-757 (Washington, D.C.: Sept. 18, 2012).

that resides on them and effectively responding to cyber-incidents is critical to federal agencies because the unauthorized disclosure, alteration, and destruction of the information on those systems can result in great harm to those involved.

Since 1997, we have designated federal information security as a government-wide high-risk area. In the February 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information that is collected, maintained, and shared by both federal and nonfederal entities.[20] The data collected from the Census Bureau, or shared with the Bureau from other federal agencies, contains personally identifiable information and is protected by federal law.[21] The wrongful disclosure of confidential census information could lead to criminal penalties.[22]

CEDCAP's 12 Projects Are at Various Stages of Planning and Design

The 12 CEDCAP projects are at varying stages of planning and design. Nine of the projects began when the program was initiated in October 2014, two of the projects began later in June 2015, and the twelfth project—IT Infrastructure Scale-Up[23]—has not yet started. The 11 ongoing projects have efforts under way to deliver 17 solutions, which are in different phases of planning and design.

- For 8 of the 17 solutions, the Bureau recently completed an analysis of alternatives to determine whether it will acquire commercial-off-the-

[20]GAO-15-290.

[21]For example, 13 U.S.C. § 9 provides that all information collected from the public by the Census Bureau be maintained as confidential. The data may be seen only by persons sworn to uphold the confidentiality of Census Bureau's information, and may be used only for statistical purposes. The Internal Revenue Service is required to keep tax return information confidential but the Census Bureau may access that data pursuant to an exception in 26 U.S.C. § 6103(j) that permits the Internal Revenue Service to share it with the Census Bureau for statistical purposes only. These data must be protected against unauthorized disclosure.

[22]A prison term of up to 5 years and fines of up to $250,000 may be imposed for violations under 13 U.S.C. § 214 and 18 U.S.C. §§ 3559 and 3571.

[23]The twelfth project, according to Bureau officials, is to provide funding to enable 2020 Census systems to scale-up to accommodate the increased volume of users, rather than to deliver an IT capability or solution.

shelf (COTS) solutions or whether they will be built in-house in order to deliver the needed capabilities. On May 25, 2016, the Bureau issued a memorandum documenting its decision to acquire the capabilities using a COTS product. The memorandum also described the process used to select the commercial vendor. Prior to this decision, the Bureau had developed several pilot systems to provide functionality to support the ongoing survey tests, such as the 2016 Census test. For example, the Survey (and Listing) Interview Operational Control project has been developing a pilot system referred to as Mojo that serves as an operational control system for field operations that assigns, controls, tracks, and manages cases. The Mojo pilot was used in the field in the 2015 Census Test and the 2016 Census Test.

- For the remaining 9 IT solutions, the Bureau has identified the sourcing approach (e.g., buy, build, or use/modify existing system) and has either identified the solution to be implemented or is in the process of evaluating potential solutions. For example, the Electronic Correspondence Portal project is working on combining an existing government-off-the-shelf product with an existing COTS product.

According to program officials, these projects are expected to deliver their final production solutions in support of the 2020 Census from March 2019 to March 2020, except for the Centralized Development and Test Environment project, which has not yet determined when it will deliver the final production solution for the 2020 Census. All projects are scheduled to end by September 2020 (see table 2 for more detail).[24]

In 2013, the CEDCAP program office estimated that the program would cost about $548 million to deliver its projects from 2015 to 2020. In July 2015, the Bureau's Office of Cost Estimation, Analysis, and Assessment completed an independent cost estimate for CEDCAP that projected the projects to cost about $1.14 billion from 2015 to 2020 ($1.26 billion through 2024).

Bureau officials reported that as of March 2016, the projects have collectively spent approximately $92.1 million—17 percent of the total program office estimate and 8 percent of the independent cost estimate. According to Bureau officials, the CEDCAP program is currently

[24]According to Bureau officials, the CEDCAP program will continue beyond 2020.

budgeting its projects to the 2013 program office estimate. Table 2 summarizes the status of the 12 CEDCAP projects and their associated actual or potential IT solutions, and provides the cost estimates for each project, as well as the amount project officials reported spending as of March 2016.

Table 2: Status of Census Enterprise Data Collection and Processing (CEDCAP) Projects

Project	Start and completion dates	Actual or potential solution	Final delivery of production solution for 2020 Census	Status of sourcing decisions by solution	Estimated cost (in millions) from 2015 to 2020[b]		Amount spent (in millions) as of March 2016
					Program office estimate	Independent cost estimate	
Address Listing and Mapping	October 2014 to September 2020	Listing and Mapping	March 2019[a]	In May 2016, the Bureau decided to acquire Listing and Mapping capabilities from a commercial vendor.	$29	$30	$16.0
Dashboard for Monitoring	October 2014 to September 2020	Unified Tracking System-Multi-Mode Operational Control System Integration	March 2019[a]	In May 2016, the Bureau decided to acquire Unified Tracking System-Multi-Mode Operational Control System Integration capabilities from a commercial vendor.	$17	$41	$2.6
Internet and Mobile Data Collection	June 2015 to September 2020	Primus (pilot)	March 2019[a]	In May 2016, the Bureau decided to acquire Primus capabilities from a commercial vendor, while continuing to test the in-house developed Primus pilot alongside the commercial system to determine which scales the most efficiently to meet the needs of the 2020 Census before making a final decision on the Internet self-response option.	$40	$18	$6.5
		Enumeration application (pilot)[c]	March 2019[a]	The Bureau also decided to acquire Enumeration Application capabilities from a commercial vendor and plans to transition from the Enumeration Application pilot to the commercial solution.			
Questionnaire Design and Metadata	October 2014 to September 2020	Content Metadata (pilot)	September 2019[a]	In May 2016, the Bureau decided to acquire Content Metadata capabilities from a commercial vendor and plans to transition from the Content Metadata pilot to the commercial solution.	$25	$12	$6.2
		Census Automated Forms Engine	September 2019	Working to update an existing commercial-off-the-shelf (COTS) solution for Census Automated Form Engine, which is a sub-system of Content Metadata.			

Project	Start and completion dates	Actual or potential solution	Final delivery of production solution for 2020 Census	Status of sourcing decisions by solution	Estimated cost (in millions) from 2015 to 2020[b]		Amount spent (in millions) as of March 2016
					Program office estimate	Independent cost estimate	
Survey (and Listing) Interview Operational Control	June 2015 to September 2020	Mojo (pilot)	March 2019[a]	In May 2016, the Bureau decided to acquire Mojo and Mobile Case Management capabilities from a commercial vendor and plans to transition from the Mojo and Mobile Case Management pilots to the commercial solutions. Within Mojo, the Bureau has decided to use the optimization/routing engine component that was developed in-house as a pilot because it demonstrated superior capabilities to the COTS product.	$71	$193	$10.1
		Mobile Case Management (pilot)	March 2019[a]				
Centralized Operational Analysis and Control	October 2014 to September 2020	Multi-Mode Operational Control System (pilot)	March 2019[a]	In May 2016, the Bureau decided to acquire Multi-Mode Operational Control System capabilities from a commercial vendor and plans to transition from the Multi-Mode Operational Control System pilot to the commercial solution.	$64	$214	$9.2
		Current Analysis and Estimation System	March 2020	Working on in-house development of Current Analysis and Estimation System.			
		Administrative Records and Response Data-Data Access Layer	March 2020	Evaluating a COTS solution for Administrative Records and Response Data–Data Access Layer.			
Centralized Development and Test Environment	October 2014 to September 2020	Enterprise Development, Integration, and Test Environment	To be determined	Working to consolidate existing development and testing environments for the Enterprise Development, Integration, and Test Environment.	$15	$35	$3.1
Electronic Correspondence Portal	October 2014 to September 2020	eCorrespon-dence	March 2020	Working to update an existing COTS solution and combine it with a government-off-the-shelf portal for eCorrespondence.	$14	$26	$4.2

Project	Start and completion dates	Actual or potential solution	Final delivery of production solution for 2020 Census	Status of sourcing decisions by solution	Estimated cost (in millions) from 2015 to 2020[b]		Amount spent (in millions) as of March 2016
					Program office estimate	Independent cost estimate	
Scanning Data Capture from Paper	October 2014 to September 2020	Integrated Computer Assisted Data Entry	March 2020	Working to update the existing Integrated Computer Assisted Data Entry system and evaluate whether it can meet Decennial availability and disaster recovery needs.	$45	$63	$10.5
Service Oriented Architecture	October 2014 to September 2020	Application Programming Interface Infrastructure	March 2019	Working to update existing COTS product for the Application Programming Interface Infrastructure.	$63	$74	$12.9
Survey Response Processing	October 2014 to September 2020	Control and Response Data System	March 2020	Working on in-house, custom development of Control and Response Data System.	$47	$91	$10.8
		Standard Economic Processing System II	Not a solution for the 2020 Census	Working on in-house, custom development with COTS component for Standard Economic Processing System II.			
IT Infrastructure Scale-Up	October 2016 to September 2020	Not applicable	Not applicable	This project was intended to conduct analysis and provide funding beginning in fiscal year 2017 for the IT infrastructure scale-up needed for the 2020 Census. In January 2016, the Bureau decided to move the analysis work under the responsibility of the 2020 Census program's Decennial IT Architecture and Roadmap project.	$119	$282	Not yet started

Source: Data reported by Census Bureau officials. | GAO-16-623

[a]These IT solutions are those for which the Bureau has recently decided to acquire the solutions from a commercial vendor. According to Bureau officials in June 2016, the implementation schedule is being negotiated with the selected vendor and is subject to change.

[b]The cost estimates represent the Bureau's reported estimates for delivering the capabilities associated with each project.

[c]The current pilot, referred to as Census Operations Mobile Platform for Adaptive Services and Solutions (COMPASS), which was used in the 2014, 2015, and 2016 Census Tests, was developed by the 2020 Census program and is not currently considered part of the CEDCAP program. However, CEDCAP is expected to provide the enterprise solution for enumeration application capability, and the recently completed build or buy assessment included COMPASS as a potential alternative.

Selected CEDCAP Projects Partially Met Project Monitoring and Control Best Practices

According to CMMI-ACQ and CMMI-DEV, an effective project monitoring and control process provides oversight of the program's performance, in order to allow appropriate corrective actions if actual performance deviates significantly from planned performance.[25] Key activities in project monitoring and control include

- determining progress against the plan by comparing actual cost and schedule against the documented plan for the full scope of the project and communicating the results;
- identifying and documenting when significant deviations in cost and schedule performance (i.e., deviations from planned cost and schedule that, when left unresolved, preclude the project from meeting its objectives) have occurred;
- taking timely corrective actions, such as revising the original plan, establishing new agreements, or including additional mitigation activities in the current plan, to address issues when performance deviates significantly from the plan;
- monitoring the status of risks periodically, which can result in the discovery of new risks, revisions to existing risks, or the need to implement a risk mitigation plan; and
- implementing risk mitigation plans that include sufficient detail such as start and completion dates and trigger events and dates, which provide early warning that a risk is about to occur or has just occurred and are valuable in assessing risk urgency.

However, the three selected CEDCAP projects—Centralized Operational Analysis and Control project, Internet and Mobile Data Collection project, and Survey (and Listing) Interview Operational Control project—did not fully implement these practices. Specifically, the Centralized Operational Analysis and Control project fully met two of the practices in monitoring and controlling but did not meet the three other practices. The Internet and Mobile Data Collection project and Survey (and Listing) Interview Operational Control project fully met one of the best practices in monitoring and controlling, but partially met the other four best practices.

[25]CMMI-ACQ and CMMI-DEV, Project Monitoring and Control Process Area.

- **Determining progress against the plan—**Each of the three projects partially met this practice. Specifically, the three projects meet weekly to monitor the current status of each project and produce monthly reports that document cost and schedule progress. However, the projects' planning documents lacked sufficient detail against which to monitor progress because their plans did not include details about the full scope of their projects for their entire life cycles. For example, while project officials have provided key information, such as when build-or-buy decisions were to be made, when the production systems are to be initially released, and when the final systems are to be released to support the 2020 Census, project planning documents for the three projects do not consistently include this information. This is especially problematic when the production systems that these projects are expected to produce need to be implemented in time for the 2018 end-to-end system integration test, which is to begin in August 2017 (in about a year).

  Bureau officials agreed with our concerns and in June 2016 they stated that they were in the process of updating the project plans and expect to be done by August 2016. It will be important that these plans include the full scope of these projects to enable the project managers and the CEDCAP program manager to determine progress relative to the full scope of the projects.

- **Document significant deviations in performance—**Each of the three selected projects partially met this practice. Specifically, the Bureau's monthly progress reports capture schedule and cost variances and document when these variances exceed the threshold for significant deviation, which is 8 percent. For example, the Internet and Mobile data collection project had a cost variance of 20 percent in September 2015 and the Survey (and Listing) Interview Operational Control project had a cost variance of 25 percent in September 2015, which were flagged by the projects as exceeding the significant deviation threshold.

  However, the projects do not have up-to-date cost estimates with which to accurately identify significant deviations in cost performance. Specifically, the projects are measuring whether there are significant deviations in costs against their budgeted amounts, which are based on a 2013 CEDCAP program office estimate. This estimate was prepared well before the program began in October 2014 and, according to program officials, is out of date and was developed based on very early assumptions and limited details about the projects. For example, key information such as program requirements

was not available when the 2013 program cost estimate was prepared. However, since then more information about the program has become available. For example, program requirements were finalized in May 2015.

Program officials recognized that the program office estimate needs to be updated and stated that they planned to update their estimate once the program and its projects are better understood and more complete information is available, including the recently completed build-versus-buy decisions. However, until the program cost estimate is updated, the program lacks a basis for monitoring true cost variances for these three projects.

- **Taking corrective actions to address issues when necessary—** Each of the three selected projects met this practice. Specifically, the CEDCAP program has established a process for taking corrective actions to address issues when needed and, as of April 2016, Bureau officials stated they have not needed to take any corrective actions to address CEDCAP program issues. For example, while we found several significant deviations in cost and schedule for the three projects in the monthly progress reports, these did not require corrective actions because they were due to, for example, delays in contract payments, contract awards, and other obligations for hardware and software outside the control of the CEDCAP program office.
- **Monitoring the status of risks periodically—**One project (the Centralized Operational Analysis and Control project) fully met this practice and the other two projects partially met this practice. Specifically, the three projects monitor the status of their risks in bi-weekly project status meetings and monthly risk review board meetings, have established risk registers, and regularly update the status of risks in their registers. However, while according to Bureau officials the projects are to document updates on the status of their risks in their respective risk registers, the Internet and Mobile Data Collection and Survey (and Listing) Interview Operational Control projects do not consistently document status updates. For example as of April 2016, all four of the Internet and Mobile Data Collection project's medium-probability, medium-impact risks had not been updated in its risk register in 9 months. Also as of April 2016, two of five of the Survey (and Listing) Interview Operational Control project's medium-probability, medium-impact risks had not been updated in the risk register in 4 months.

Bureau officials recognized the need to document updates in the risk registers more consistently and stated that efforts were under way to address this. In May 2016, Bureau officials provided updates on the Internet and Mobile Data Collection project risk list that showed improvement in documenting the status of risks for that project for 1 month. In June 2016, Bureau officials stated that they had taken additional steps to improve how risk registers are updated by, for example, conducting training sessions for project managers on the CEDCAP program's expectations for monitoring and updating the status of risks, and reviewing project risk registers monthly to ensure compliance. Bureau officials also stated that they planned to release an updated version of the CEDCAP Risk Management Plan that more clearly outlines the process and expectations for monitoring and updating project risk registers by the end of August 2016. While the officials have taken positive steps, until actions are fully implemented to ensure that the projects are consistently documenting updates to the status of risks in a repeatable and ongoing manner, they will not have comprehensive information on how risks are being managed.

- **Implementing risk mitigation plans—**Each of the three selected projects partially met this practice. As of October 2015, the three projects had developed basic risk mitigation steps for each of the risks associated with the projects that required a mitigation plan. However, contrary to industry best practices and the Bureau's risk management guidance, these risk mitigation plans lacked important details. Specifically, none of the mitigation plans for the three projects contained start or completion dates. Additionally, the Centralized Operational Analysis and Control and the Internet and Mobile Data Collection projects did not have any trigger events for their risks that require risk triggers (e.g., those risks that exceed a predefined exposure threshold). For example, the Centralized Operational Analysis and Control project had an active issue in March 2016 that if late requirements were given to the project, it would face delays in delivering for the 2016 Census test. This risk did not contain a detailed risk mitigation plan or a trigger date or description.

  In February 2016, Bureau officials recognized that there were issues with their risk management process and stated that they were working on addressing them. In April 2016, Bureau officials stated that they had revised their risk management process to increase the threshold for requiring risk mitigation plans and trigger events. However, the April 2016 risk registers did not contain any risks that exceeded the new risk threshold and, therefore, none of the risks required risk mitigation plans and trigger events. As a result, it is unclear to what

extent the Bureau has improved its practices in developing detailed risk mitigation plans and assigning trigger events when required. Until the three projects establish detailed risk mitigation plans and trigger events for all of their risks that require both, they will not be able to identify potential problems before they occur and mitigate adverse impacts to project objectives.

The Bureau Lacks Processes for Effectively Managing Interdependencies between CEDCAP and 2020 Census Programs

The CEDCAP and 2020 Census programs are intended to be on parallel implementation tracks and have major interdependencies; however, the interdependencies between these two programs have not always been effectively managed. Specifically, CEDCAP relies on 2020 Census to be one of the biggest consumers of its enterprise systems, and 2020 Census relies heavily on CEDCAP to deliver key systems to support its redesign. Thus, CEDCAP is integral to helping the 2020 Census program achieve its estimated $5.2 billion cost savings goal. Accordingly, as reported in the President's Budget for Fiscal Year 2017, over 50 percent of CEDCAP's funding for fiscal year 2017 ($57.5 million of the requested $104 million) is expected to come from the 2020 Census program.

Nevertheless, while both programs have taken a number of steps to coordinate, such as holding weekly schedule coordination meetings and participating in each other's risk review board meetings, the two programs lack processes for effectively integrating their schedule dependencies, integrating the management of interrelated risks, and managing requirements. Without effective processes for managing these interdependencies, the Bureau is limited in its ability to understand the work needed by both programs to meet agreed upon milestones, mitigate major risks, and ensure that requirements are appropriately identified.

CEDCAP and 2020 Census Programs Do Not Have an Effective Process for Integrating Schedule Dependencies

According to GAO's Schedule Assessment Guide, major handoffs between programs should be discussed and agreed upon and all interdependencies in the programs' schedules should be clearly identified and logically linked so that dates can be properly calculated. The guide also specifies that changes in linked activities can automatically reforecast future dates, resulting in a dynamic schedule, and that attempting to manually resolve incompatible schedules in different software can become time-consuming and expensive, and thus should be avoided. Moreover, constantly updating a schedule manually defeats the purpose of a dynamic schedule and can make the schedule particularly prone to error. According to best practices, if manual schedule reconciliation cannot be avoided, the parties should define a process to

preserve integrity between the different schedule formats and to verify and validate the converted data whenever the schedules are updated.[26]

About half of CEDCAP's major product releases (7 of 13) are intended to align with and support the major tests and operations of the 2020 Census. Accordingly, the CEDCAP and 2020 Census programs have both established master schedules that contain thousands of milestones and tens of thousands of activities through 2020 Census production and have identified major milestones within each program that are intended to align with each other. In addition, both program management offices have established processes for managing their respective master schedules.

However, the CEDCAP and 2020 Census programs maintain their master schedules using different software where dependencies between the two programs are not automatically linked and are not dynamically responsive to change. Consequently, the two programs have been manually identifying activities within their master schedules that are dependent on each other, and rather than establishing one dependency schedule, as best practices dictate, the programs have each developed their own dependency schedule and meet weekly with the intent of coordinating these two schedules. In addition, the programs' dependency schedules only include near-term schedule dependencies, and not future milestones through 2020 Census production. For example, as of February 2016, the dependency schedules only included tasks associated with the CEDCAP product release in support of the 2020 Census program's 2016 Census Test through July 2016. According to Bureau officials, they are currently working to incorporate activities for the next set of near-term milestones in the dependency schedules, which are to support the 2016 Address Canvassing Test.

Nonetheless, this process has proven to be ineffective, as it has contributed to the misalignment between the programs' schedules. For example:

- The CEDCAP program originally planned to complete build-or-buy decisions for several capabilities by October 2016, while the 2020 Census timeline specified that these decisions would be ready by

[26]GAO-16-89G.

June 2016. In November 2015, CEDCAP officials stated that they recognized this misalignment and decided to accelerate certain build-or-buy decisions to align with 2020 Census needs.

- As of April 2016, while CEDCAP's major product releases need to be developed and deployed to support the delivery of major 2020 Census tests, CEDCAP's releases and 2020 Census major test milestones were not always aligned to ensure CEDCAP releases would be available in time. For example, development of CEDCAP release 7, which was intended to support the 2017 Census Test, was not scheduled to begin until almost a month after the 2017 Census Test was expected to begin (December 2016), and was not planned to be completed until about 2 months after the 2017 Census Test was expected to end (July 2017). Bureau officials acknowledged that CEDCAP release dates needed to be revised to accurately reflect the program's current planned time frames and to appropriately align with 2020 Census time frames. Officials provided updated documentation in June 2016 which was intended to better align CEDCAP and 2020 Census time frames.[27] However, officials also stated in June that following the May 2016 decision to acquire many of the CEDCAP solutions, the implementation schedule is being negotiated with the selected vendor and is subject to change.

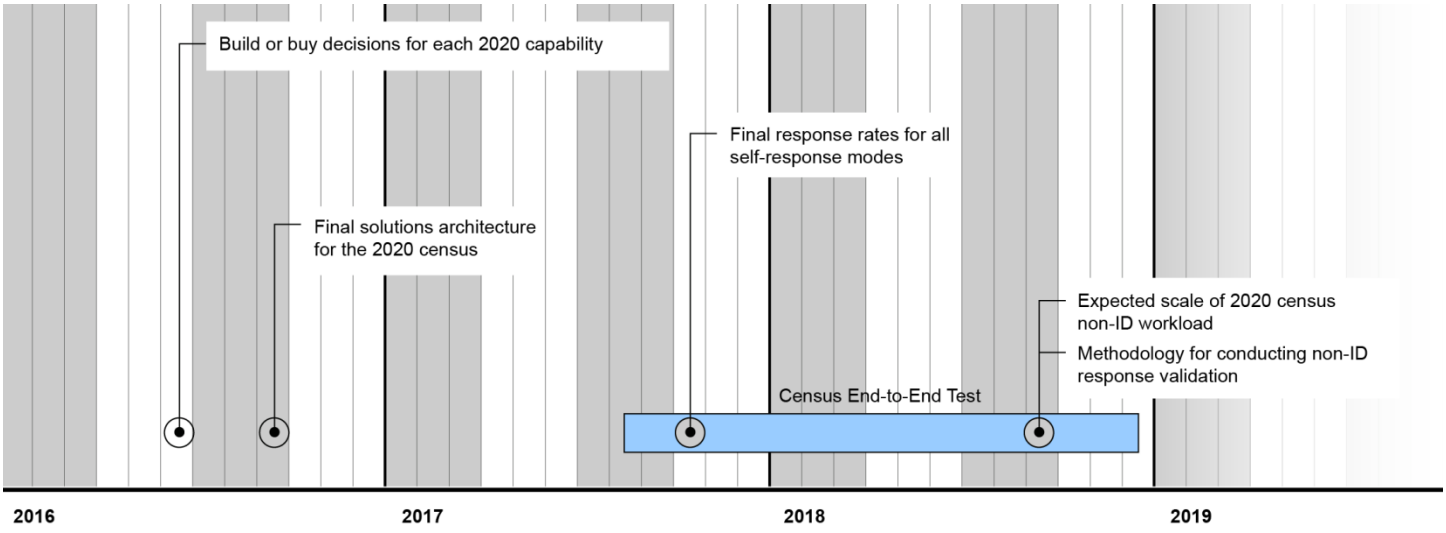
Adding to the complexity of coordinating the two programs' schedules, as we testified in November 2015, several key decisions by the 2020 Census program are not planned to be made until later in the decade, which may impact CEDCAP's ability to deliver those future requirements and have production-ready systems in place in time to conduct end-to-end testing, which is to begin in August 2017.[28] For example, the Bureau does not plan to decide on the full complement of applications, data, infrastructure, security, monitoring, and service management for the 2020 Census—referred to as the solutions architecture—until September 2016. The Bureau also does not plan to finalize the expected response rates for all self-response modes, including how many households it estimates will respond to the 2020 survey using the Internet, telephone, and paper, until October 2017.

[27]We have not reviewed this new documentation to verify the changes.

[28]GAO-16-205T.

Figure 4 illustrates several IT-related decisions which are not scheduled to be made until later in the decade and may impact CEDCAP's ability to prepare for the end-to-end test and 2020 Census.

Figure 4: Examples of 2020 Census-related IT Decisions Planned for Later in the Decade that Could Impact the Census Enterprise Data Collection and Processing (CEDCAP) Program, as of April 2016



Source: GAO analysis of Census Bureau data. | GAO-16-623

Note: These reflect when final design decisions are to be made. The Bureau plans to make some preliminary design decisions earlier, such as in the areas of solutions architecture, self-response rates, and non-ID workload.

Further exacerbating the difficulties with the two programs managing separate dependency schedules is that, as of May 2016 (a year and a half into the CEDCAP program), their process for managing the dependencies had not been documented. In response to our draft report, program officials provided documentation of this process. However, as previously mentioned, the current process is ineffective, thus documenting the as-is process does not help the Bureau. Further, while the programs intend to revise their respective schedules to correct the existing misalignments identified in this report, continuing to rely on an ineffective process for manually aligning their milestones will likely lead to future misalignment as changes occur.

Thus, until the Bureau modifies its current process to ensure complete alignment between the 2020 and CEDCAP programs by, for example, maintaining a single dependency schedule, it will be limited in its ability to ensure that both programs are planning and measuring their activities

according to the same agreed upon time frames. Moreover, until program officials document the modified process for managing the schedule dependencies, the Bureau cannot ensure that it has a repeatable process and that an integrated dependency schedule (if established) will stay current and help avoid future misalignments.

CEDCAP and 2020 Census Programs Do Not Have an Integrated List of Risks Facing Both Programs

According to GAO best practices on enhancing and sustaining collaboration among federal agencies, to achieve a common outcome, stakeholders should work together to jointly define and agree on their respective roles and responsibilities, and establish strategies that work in concert with each other or are joint in nature.[29] Additionally, according to CMMI-ACQ and CMMI-DEV, effective risk management calls for stakeholder collaboration on identifying and mitigating risks that could negatively affect their efforts.[30]

Both the CEDCAP and 2020 Census programs have taken steps to collaborate on identifying and mitigating risks. For example, both programs have processes in place for identifying and mitigating risks that affect their respective programs, facilitate risk review boards, and have representatives attend each other's risk review board meetings to help promote consistency. However, these programs do not have an integrated list of risks (referred to as a risk register) with agreed-upon roles and responsibilities to jointly track risks that heavily impact them and instead separately track these risks. This decentralized approach introduces two key problems.

First, there are inconsistencies in tracking and managing interdependent risks. Specifically, selected risks were recognized by one program's risk management process and not the other. This included the following examples as of March 2016:

- The CEDCAP program identified the lack of real-time schedule linkages as a high probability, high-impact risk in its risk register,

[29]GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies,* GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

[30]CMMI-ACQ and CMMI-DEV, Integrated Project Management and Risk Management Process Areas.

which as of March 2016 had been realized and was considered an issue for the program. However, the 2020 Census program had not recognized this as a risk in its risk register.

- While CEDCAP had identified the ability to scale systems to meet the needs of the Decennial Census as a medium-probability, high-impact risk in its risk register, the 2020 Census program had not recognized this as a risk in its risk register.
- The CEDCAP program had identified the need to define how the Bureau will manage and use cloud services to ensure successful integration of cloud services with existing infrastructure as a low probability, high-impact risk in its risk register; however, the 2020 Census program had not recognized the adoption of cloud services as a formal risk in its risk register. This is especially problematic as the 2020 Census program recently experienced a notable setback regarding cloud implementation. Specifically, the 2020 Census program was originally planning to use a commercial cloud environment in the 2016 Census Test, which would have been the first time the Bureau used a cloud service in a major census test to collect census data from residents in parts of the country. However, leading up to the 2016 Census Test, the program experienced stability issues with the cloud environment. Accordingly, in March 2016, the 2020 Census program decided to cancel its plans to use the cloud environment in the 2016 Census Test. Officials stated that they plan to use the cloud in future census tests.

According to 2020 Census program officials, they did not consider the lack of real-time schedule linkages to be a risk because they were conducting weekly integration meetings and coordinating with CEDCAP on their schedules to ensure proper alignment. However, as stated previously, attempting to manually resolve incompatible schedules in different software can be time-consuming, expensive, and prone to errors, and the Bureau's process for managing schedule dependencies between the CEDCAP and 2020 Census programs is ineffective. Regarding the lack of scalability and cloud services risks in the 2020 Census risk log, 2020 Census program officials acknowledged that it was an oversight and that they should have been recognized by the program as formal risks.

The second problem of not having an integrated risk register is that tracking risks in two different registers can result in redundant efforts and potentially conflicting mitigation efforts. For example, both programs have identified in their separate risk registers several common risks, such as risks related to late changes in requirements, integration of systems, human resources, build-or-buy decisions, and cybersecurity. These

interdependent risks found in both risk registers can introduce the potential for duplicative or inefficient risk mitigation efforts and the need for additional reconciliation efforts.

Until the Bureau establishes a comprehensive list of risks facing both the CEDCAP and 2020 Census programs, and agrees on their respective roles and responsibilities for jointly managing this list, it will continue to have multiple sets of inconsistent risk data and will be limited in its ability to effectively monitor and mitigate the major risks facing both programs.

Processes for Managing Requirements between CEDCAP and 2020 Census Have Not Been Finalized

According to CMMI-ACQ and CMMI-DEV, requirements management processes are important for enabling programs to ensure that its set of approved requirements is managed to support the planning and execution needs of the program. Such a process should include steps to review and obtain commitment to the requirements from stakeholders and manage changes to requirements as customer needs evolve.[31]

The Bureau's Office of Innovation and Implementation serves as the link in managing requirements between the 2020 Census and CEDCAP programs. This office is responsible for gathering and synthesizing business requirements across the Bureau, including from the 2020 Census program, and delivering them to CEDCAP. Additionally, for the 2020 Census program, the Bureau established the 2020 Census Systems Engineering and Integration program office, which is responsible for delivering 2020 Census business requirements to the Office of Innovation and Implementation. CEDCAP receives the requirements on an incremental basis, and as mentioned previously, CEDCAP builds functionality containing subsets of the requirements in the 40-day cycles. CEDCAP has delivered 12 increments of system functionality to support the first three releases.

However, as of April 2016, the Office of Innovation and Implementation's process for collecting and synthesizing requirements, obtaining commitment to those requirements from stakeholders, and managing changes to the requirements had been drafted, but not yet finalized. In July 2016, Bureau officials stated that due to the recent selection of a

[31]CMMI-ACQ and CMMI-DEV, Requirements Management Process Area.

commercial vendor to deliver many of the CEDCAP capabilities, they do not plan to finalize this process until January 2017. Additionally, as of April 2016, the 2020 Census Systems Engineering and Integration program had not yet finalized its program management plan, which outlines, among other things, how it is to establish requirements to be delivered to the Office of Innovation and Implementation, which are then to be delivered to CEDCAP. According to program officials, they have been working on a draft of this plan and expect it to be finalized by the end of August 2016. As a result, the Bureau has developed three CEDCAP releases without having a fully documented and institutionalized process for collecting those requirements.

In addition, the 2020 Census program identified about 2,500 capability requirements needed for the 2020 Census; however, there are gaps in these requirements. Specifically, we determined that of the 2,500 capability requirements, 86 should be assigned to a test prior to the 2020 Census, but were not. These included 64 requirements related to redistricting data program, 10 requirements related to data products and dissemination, and 12 requirements related to non-ID response validation. Bureau officials stated that the 74 redistricting data program and data products and dissemination requirements have not yet been assigned to a Census test because they have not yet gone through the Bureau's quality control process, which is planned for later this calendar year.

Regarding the 12 non-ID response validation requirements, Bureau officials stated that once this area is better understood, a more complete set of requirements will be established, and then they will assign the requirements to particular tests, as appropriate. As of April 2016, the Bureau was in the early stages of conducting research in this area. Thus, it has not tested non-ID response validation in the 2013, 2014, or 2015 Census tests. These tests were intended to, among other things, help define requirements around critical functions.

With about a year remaining before the 2018 Census end-to-end test begins, the lack of experience and specific requirements related to non-ID response validation is especially concerning, as incomplete and late definition of requirements proved to be serious issues for the 2010 Census. Specifically, leading up to the 2010 Census, we reported in

October 2007 that not fully defining requirements had contributed to both cost increases and schedule delays experienced by the failed program to deliver handheld computers for field data collection—contributing to an up to $3 billion overrun.[32] Increases in the number of requirements led to the need for additional work and staffing. Moreover, we reported in 2009 and 2010 that the Bureau's late development of an operational control system to manage its paper-based census collection operations resulted in system outages and slow performance during the 2010 Census.[33] The Bureau attributed these issues, in part, to the compressed development and testing schedule.

As the 2020 Census continues to make future design decisions and CEDCAP continues to deliver incremental functionality, it is critical to have a fully documented and institutionalized process for managing requirements. Additionally, until measures are taken to identify when the 74 requirements related to the redistricting data program and data products and dissemination will be tested, and to make developing a better understanding of, and identifying requirements related to, non-ID response validation a high and immediate priority, or to consider alternatives to avoid late definition of such requirements, the Bureau is at risk of experiencing issues similar to those it experienced during the 2010 Census.

[32]GAO, *Information Technology: Census Bureau Needs to Improve Its Risk Management of Decennial Systems,* GAO-08-79 (Washington, D.C.: Oct. 5, 2007).

[33]GAO, *2010 Census: Data Collection Operations Were Generally Completed as Planned, but Long-standing Challenges Suggest Need for Fundamental Reforms,* GAO-11-193 (Washington, D.C.: Dec. 14, 2010); *2010 Census: Data Collection Is Under Way, but Reliability of Key Information Technology Systems Remains a Risk*, GAO-10-567T (Washington, D.C.: Mar. 25, 2010); *2010 Census: Key Enumeration Activities Are Moving Forward, but Information Technology Systems Remain a Concern,* GAO-10-430T (Washington, D.C.: Feb. 23, 2010); and *2010 Census: Census Bureau Continues to Make Progress in Mitigating Risks to a Successful Enumeration, but Still Faces Various Challenges*, GAO-10-132T (Washington, D.C.: Oct. 7, 2009).

Census Bureau Faces Several Information Security Challenges in Implementing the 2020 Census

While the Bureau plans to extensively use IT systems to support the 2020 Census redesign in an effort to realize potentially significant efficiency gains and cost savings, this redesign introduces numerous critical information security challenges.

- **Developing policies and procedures to minimize the threat of phishing—**Phishing is a digital form of social engineering that uses authentic-looking, but fake, e-mails, websites, or instant messages to get users to download malware, open malicious attachments, or open links that direct them to a website that requests information or executes malicious code. Phishing attacks could target respondents, as well as Census employees and contractors. The 2020 Census will be the first one in which respondents will be heavily encouraged to respond via the Internet. The Bureau plans to highly promote the use of the Internet self-response option throughout the nation and expects, based on preliminary research, that approximately 50 percent of U.S. households will use this option. This will likely increase the risk that cyber criminals will use phishing in an attempt to steal personal information. A report developed by a contractor for the Bureau noted that criminals may pretend to be a census worker, caller, or website, to phish for personal information such as Social Security numbers and bank information.

  Further, phishing attacks directed at Census employees, including approximately 300,000 temporary employees, could have serious effects. The U.S. Computer Emergency Readiness Team (US-CERT) has recently reported on phishing campaigns targeting federal government agencies that are intended to install malware on government computer systems. These could act as an entry point for attackers to spread throughout an organization's entire enterprise, steal sensitive personal information, or disrupt business operations.

  To minimize the threat of phishing, organizations such as US-CERT and the National Institute of Standards and Technology (NIST) recommend several actions for organizations, including communicating with users.[34] Additionally, as we previously reported, in 2015 the White House and the Office of Management and Budget

[34]National Institute of Standards and Technology, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, SP 800-83 Revision 1 (Gaithersburg, Md.: July 2013).

identified anti-phishing as a key area for federal agencies to focus on in enhancing their information security practices.[35]

- **Ensuring that individuals gain only limited and appropriate access to 2020 Census data—**The Decennial Census plans to enable a public-facing website and mobile devices to collect personally identifiable information (PII) (e.g., name, address, and date of birth) from the nation's entire population—estimated to be over 300 million. In addition, the Bureau is planning to obtain and store administrative records containing PII from other government agencies to help augment information that enumerators did not collect. Further, the 2020 Census will be highly promoted and visible throughout the nation, which could increase its appeal to malicious actors. Specifically, cyber criminals may attempt to steal personal information collected during and for the 2020 Decennial Census, through techniques such as social engineering, sniffing of unprotected traffic, and malware installed on vulnerable machines.[36]

  We have reported on challenges to the federal government and the private sector in ensuring the privacy of personal information posed by advances in technology. For example, in our 2015 High Risk List, we expanded one of our high-risk areas—ensuring the security of federal information systems and cyber critical infrastructure—to include protecting the privacy of PII.[37] Technological advances have allowed both government and private sector entities to collect and process extensive amounts of PII more effectively.

  However, the number of reported security incidents involving PII at federal agencies has increased dramatically in recent years. Because

[35]GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15-714 (Washington, D.C.: Sept. 29, 2015).

[36]Sniffing occurs when data are sent to or from a device over an unsecured (i.e., not encrypted) network connection, allowing an eavesdropper to "listen to" and record the information that is exchanged. Malware is malicious software (including spyware and viruses) that is often disguised as a game, patch, utility, or other useful third-party software application.

[37]GAO-15-290. We designated the security of our federal cyber assets as a high-risk area in 1997. In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure, and in 2015 we expanded it again, to include risks to personally identifiable information.

of these challenges, we have recommended, among other things, that federal agencies improve their response to information security incidents and data breaches involving PII, and consistently develop and implement privacy policies and procedures. Accordingly, it will be important for the Bureau to ensure that only respondents and Bureau officials are able to gain access to this information, and that enumerators and other employees only have access to the information needed to perform their jobs.

- **Adequately protecting mobile devices—**The 2020 Census will be the first one in which the Census Bureau will provide mobile devices to enumerators to collect PII from households who did not self-respond to the survey. The Bureau plans to use a contractor to provide approximately 300,000 census-taking-ready mobile devices to enumerators. The contractor will be responsible for, among other things, the provisioning, shipping, storage, and decommissioning of the devices. The enumerators will use the mobile devices to collect data from non-response follow-up activities.

  Many threats to mobile devices are similar to those for traditional computing devices; however, the threats and attacks to mobile devices are facilitated by vulnerabilities in the design and configuration of mobile devices, as well as the ways consumers use them. Common vulnerabilities include a failure to enable password protection and operating systems that are not kept up to date with the latest security patches.[38] In addition, because of their small size and use outside an office setting, mobile devices are easier to misplace or steal, leaving their sensitive information at risk of unauthorized use or theft.

  In 2012 we reported on key security controls and practices to reduce vulnerabilities in mobile devices, protect proprietary and other confidential business data that could be stolen from mobile devices, and ensure that mobile devices connected to the organization's network do not threaten the security of the network itself.[39] For example, we reported that organizations can require that devices meet government specifications before they are deployed, limit

[38]GAO-12-757.

[39]GAO-12-757.

storage on mobile devices, and ensure that all data on the device are cleared before the device is disposed of. Doing so can help protect against inappropriate disclosure of sensitive information that is collected on the mobile devices. Accordingly, we recommended, among other things, that the Department of Homeland Security, in collaboration with the Department of Commerce, establish measures about consumer awareness of mobile security. In September 2013, the Department of Homeland Security addressed this recommendation by developing a public awareness campaign with performance measures related to mobile security.

- **Ensuring adequate control in a cloud environment—**The Bureau has decided to use cloud solutions whenever possible for the 2020 Census; however, as stated previously, it has not yet determined all of the needed cloud capabilities. In September 2014, we reported that cloud computing has both positive and negative information security implications for federal agencies.[40] Potential information security benefits include the use of automation to expedite the implementation of secure configurations on devices, reduced need to carry data on removable media because of broad network access, and low-cost disaster recovery and data storage. However, the use of cloud computing can also create numerous information security risks for federal agencies, including that cloud service vendors may not be familiar with security requirements that are unique to government agencies, such as continuous monitoring and maintaining an inventory of systems. Thus, we reported that, to reduce the risks, it is important for federal agencies to examine the specific security controls of the provider the agency is evaluating when considering the use of cloud computing.

  In addition, in April 2016, we reported that agencies should develop service-level agreements with cloud providers that specify, among other things, the security performance requirements—including data reliability, preservation, privacy, and access rights—that the service provider is to meet.[41] Without these safeguards, computer systems

[40]GAO, *Cloud Computing: Additional Opportunities and Savings Need to Be Pursued*, GAO-14-753 (Washington, D.C.: Sept. 25, 2014).

[41]GAO, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*, GAO-16-325 (Washington, D.C.: Apr. 7, 2016).

and networks, as well as the critical operations and key infrastructures they support, may be lost; information—including sensitive personal information—may be compromised; and the agency's operations could be disrupted.

- **Adequately considering information security when making decisions about the IT solutions and infrastructure supporting the 2020 Census—**Design decisions related to the 2020 Census will have security implications that need to be considered when making decisions about future 2020 Census design features. As described previously, as of April, the Census Bureau still had to make 350 decisions about the 2020 Census, and half of those have an IT component. For example, the Bureau has not yet made decisions about key aspects of its IT infrastructure to be used for the 2020 Census, including defining all of the components of the solution architecture (applications, data, infrastructure, security, monitoring, and service management), deciding whether it will develop a mobile application to enable respondents to submit their survey responses on their mobile devices, and deciding how it plans to use cloud providers.

  We have previously reported on challenges that the Bureau has had in making decisions in a timely manner. Specifically, in April 2014, and again in April 2015, we noted that key decisions had yet to be made about the 2020 Census, and noted that as momentum builds toward Census Day 2020, the margin for schedule slippages is getting increasingly slim. The Chief Information Security Officer echoed these concerns, stating that any schedule slippage can affect the time needed to conduct a comprehensive security assessment. As key design decisions are deferred and the time to make such decisions becomes more compressed, it is important for the Bureau to ensure that information security is adequately considered and assessed when making design decisions about the IT solutions and infrastructure to be used for the 2020 Census.

- **Making certain key IT positions are filled and have appropriate information security knowledge and expertise—**As our prior work and leading guidance recognize, having the right knowledge and skills is critical to the success of a program, and mission-critical skills gaps in such occupations as cybersecurity pose a high-risk to the nation. Whether within specific federal agencies or across the federal workforce, these skills gaps impede federal agencies in cost-effectively serving the public and achieving results. Because of this, we added strategic human capital management, including cybersecurity human capital, to our High Risk List in 2001, and it

remains on that list today.[42] These skills gaps are also a key contributing factor to our high-risk area of ensuring the security of federal information systems. As we reported in February 2015, although steps have been taken to close critical skills gaps in the cybersecurity area, it remains an ongoing problem and additional efforts are needed to address this issue government-wide.

We also reported in February 2015, that the Bureau continues to have critical skills gaps, such as in cloud computing, security integration and engineering, enterprise/mission engineering life-cycle, requirements development, and internet data collection.[43] The Bureau has made some progress in addressing its skills gaps and continues to work toward ensuring that key information security skills are in place. However, it has faced longstanding vacancies in key IT positions, such as the Chief Information Officer (vacant from July 2015 to June 2016) and the CEDCAP Chief Security Engineer (vacant since October 2015). Ensuring that key positions are filled with staff who have the appropriate expertise will be important to ensure that security controls are adequately designed in the systems used to collect and store census data.

- **Ensuring that contingency and incident response plans are in place that encompass all of the IT systems to be used to support the 2020 Census—**Because of the brief time frame for collecting data during the Decennial Census, it is especially important that systems are available for respondents to ensure a high response rate. 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. Implementing important security controls including policies, procedures, and techniques for contingency planning and incident response helps to ensure the confidentiality, integrity, and availability of information and systems, even during disruptions of service.

  However, we have reported on weaknesses across the federal government in these areas. Specifically, in April 2014 we estimated

[42]GAO-15-290.

[43]GAO-15-225.

that federal agencies (including the Department of Commerce) had not completely documented actions taken in response to detected incidents reported in fiscal year 2012 in about 65 percent of cases.[44] We made a number of recommendations to improve agencies' cyber incident response practices, such as developing incident response plans and procedures and testing them.

- **Adequately training Bureau employees, including its massive temporary workforce, in information security awareness—**The Census Bureau plans to hire an enormous temporary workforce during the 2020 Census activities, including about 300,000 temporary employees to, among other things, use contractor-furnished mobile devices to collect personal information from households that have not yet responded to the Census. Because uninformed people can be one of the weakest links when securing systems and networks, information security awareness training is intended to inform agency personnel of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. However, ensuring that every one of the approximately 300,000 temporary enumerators is sufficiently trained in information security will be challenging. Providing training to agency personnel, such as this new and temporary staff, will be critical to securing information and systems.
- **Making certain security assessments are completed in a timely manner and that risks are at an acceptable level—**According to guidance from NIST, after testing an information system, authorizing officials determine whether the risks (e.g., unaddressed vulnerabilities) are acceptable and issue an authorization to operate. Each of the systems that the 2020 Census IT architecture plans to rely on will need to undergo a security assessment and obtain authorization to operate before it can be used for the 2020 Census.
- **Properly configuring and patching systems supporting the 2020 Census—**Configuration management controls ensure that only authorized and fully tested software is placed in operation, software and hardware are updated, information systems are monitored, patches are applied to these systems to protect against known

[44]GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 30, 2014).

vulnerabilities, and emergency changes are documented and approved. We reported in September 2015 that for fiscal year 2014, 22 of the 24 agencies in our review (including the Department of Commerce) had weaknesses in configuration management controls.[45] Moreover, in April 2015, US-CERT issued an alert stating that cyber threat adversaries continue to exploit common, but unpatched, software products from vendors such as Adobe, Microsoft, and Oracle. Without strong configuration and patch management, an attacker may exploit a vulnerability not yet mitigated, enabling unauthorized access to information systems or enabling users to have access to greater privileges than authorized.

The Bureau's acting Chief Information Officer and its Chief Information Security Officer have acknowledged these challenges and described the Bureau's plans to address them. For example, the Bureau has developed a risk management framework, which is intended to ensure that proper security controls are in place and provide authorizing officials with details on residual risk and progress to address those risks. In addition, the Bureau has also embedded three security engineers in the 2020 Census program to provide assistance and guidance to project teams. Bureau officials also stated that they are in the process of filling—or plan to fill—vacancies in key positions and intend to hire staff with expertise in key areas, such as cloud computing. To minimize the risk of phishing, Bureau officials note that they plan to contract with a company to monitor the Internet for fraudulent sites pretending to be the Census Bureau. Continued focus on these considerable challenges will be important as the Bureau begins to develop and/or acquire systems and implement the 2020 design.

We have previously reported on Census Bureau weaknesses that are related to many of these information security challenges. Specifically, we reported in January 2013 that the Bureau had a number of weaknesses in its information security controls due, in part, to the fact that it had not fully implemented a comprehensive information security program.[46] Thus, we

[45]GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15-714 (Washington, D.C.: Sept. 29, 2015).

[46]GAO, *Information Security: Actions Needed by Census Bureau to Address Weaknesses,* GAO-13-63 (Washington, D.C.: Jan. 22, 2013). Another version of this report was issued for limited distribution.

made 13 public recommendations in areas such as security awareness training, incident response, and security assessments. We also made 102 recommendations to address technical weaknesses we identified related to access controls, configuration management, and contingency planning.[47]

As of June 2016, the Bureau had made significant progress in addressing these recommendations. Specifically, it had implemented all 13 public recommendations and 92 of 102 technical recommendations. For example, the Bureau developed and implemented a risk management framework with a goal of better management visibility of information security risks; this framework addressed a recommendation to document acceptance of risks for management review.

We have work under way to evaluate whether the 10 remaining recommendations have been fully addressed. These recommendations pertain to access controls and configuration management, and are related to two of the security challenges we previously mentioned—ensuring individuals gain only limited and appropriate access, and properly configuring and patching systems. The Bureau's progress toward addressing our recommendations is encouraging; however, completing this effort is necessary to ensure that sensitive information is adequately protected and that the challenges we outline in this report are overcome.

Conclusions

The CEDCAP program's 12 projects have the potential to offer numerous benefits to the Bureau's survey programs, including the 2020 Census program, such as enabling an Internet response option; automating the assignment, controlling, and tracking of enumerator caseloads; and enabling a mobile data collection tool for field work. While the Bureau has taken steps to implement these projects, considerable work remains between now and when its production systems need to be in place to support the 2020 Census end-to-end system integration test—in about a year.

[47]These recommendations were included in a separate report with limited distribution due to the sensitive nature of the information it contained.

Although the three selected CEDCAP projects had key project monitoring and controlling practices in place or planned, such as producing monthly progress reports, gaps exist in other important ways to monitor and control projects, such as the lack of detailed project plans, documentation of risk status updates, and complete risk mitigation plans. While officials plan to update the project plans with more detail, until the program and the selected projects address these other gaps, they are at risk of not adequately monitoring these projects.

Given the numerous and critical dependencies between the CEDCAP and 2020 Census programs, their parallel implementation tracks, and the 2020 Census' immovable deadline, it is imperative that the interdependencies between these programs are effectively managed. However, this has not always been the case. While actions such as weekly meetings to discuss the programs' respective schedules demonstrate that the programs are trying to coordinate, additional actions would help better align the programs. Specifically, until the two programs establish schedules that are completely aligned, develop an integrated list of all interdependent risks, and finalize processes for managing requirements, both programs are at risk of not delivering their programs as expected.

Finally, while the large-scale technological changes for the 2020 Decennial Census introduce great potential for efficiency and effectiveness gains, it also introduces many information security challenges, including educating the public to offset inevitable phishing scams. Continued focus on these considerable security challenges and remaining open recommendations will be important as the Bureau begins to develop and/or acquire systems and implement the 2020 Census design.

Recommendations for Executive Action

To ensure that the Bureau is better positioned to deliver CEDCAP, we are recommending that the Secretary of Commerce direct the Director of the Census Bureau to take the following eight actions:

- Update the CEDCAP program office cost estimate to reflect the current status of the program as soon as appropriate information becomes available.
- Ensure that updates to the status of risks are consistently documented for CEDCAP's Internet and Mobile Data Collection and Survey (and Listing) Interview Operational Control projects.

- Ensure that CEDCAP's Internet and Mobile Data Collection, Survey (and Listing) Interview Operational Control, and Centralized Operational Analysis and Control projects establish detailed risk mitigation plans on a consistent basis and that the Internet and Mobile Data Collection and Centralized Operational Analysis and Control projects establish trigger events for all relevant risks.
- Define, document, and implement a repeatable process to establish complete alignment between CEDCAP and 2020 Census programs by, for example, maintaining a single dependency schedule.
- Establish a comprehensive and integrated list of all interdependent risks facing the CEDCAP and 2020 Census programs, and clearly identify roles and responsibilities for managing this list.
- Finalize documentation of processes for managing requirements for CEDCAP.
- Identify when the 74 requirements related to redistricting data program and data products and dissemination will be tested.
- Make developing a better understanding of and identifying requirements related to non-ID response validation a high and immediate priority, or consider alternatives to avoid late definition of such requirements.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Department of Commerce, which are reprinted in appendix II. In its comments, the department agreed with all eight of our recommendations and indicated that it will be taking actions in response to our recommendations. The department also stated that for several of the recommendations it believed that some additional context should be included in our report, which we discuss below.

First, the department reported that the Census Bureau decided on May 25, 2016, to use a commercial off-the-shelf solution in combination with in-house solutions for the data collection component of the 2020 Census, which is to be delivered by the CEDCAP program. We updated relevant statements in our report to reflect this recent decision.

In response to our first recommendation to update the CEDCAP program office cost estimate to reflect the current status of the program as soon as appropriate information becomes available, the department agreed and noted that with the recent May 2016 decision, the Bureau has begun work on new program life cycle cost estimates. This is a positive step forward,

and it will be important that the Bureau prepares a reliable estimate in a timely manner in order to have a basis for monitoring true cost variances for the three selected CEDCAP projects we reviewed.

The department agreed with our fourth recommendation to define, document, and implement a repeatable process to establish complete alignment between CEDCAP and the 2020 Census program by, for example, maintaining a single dependency schedule. Specifically, the department stated that the Bureau must maintain schedule alignment between the 2020 Census and CEDCAP programs through a single integrated schedule. The department further stated that the 2020 Census is the program of interest and, as such, it must and will drive the schedule for all solutions that support it, including CEDCAP solutions. The department also stated that the 2020 Census manages its master schedule through the Primavera software package, as recommended earlier in the decade by GAO.

However, GAO does not make recommendations on the use of specific software packages, and thus did not make such a recommendation to the Bureau. The Bureau's selection of a software tool should have been based on an assessment of the costs, benefits, and risks associated with alternative solutions. Regardless of the software packages used, the 2020 Census schedule is dependent on the delivery of CEDCAP solutions and, as we state in the report, the process for integrating the schedule dependencies between these two programs is ineffective. Thus, we maintain that until the Bureau modifies its current process to ensure complete alignment between the 2020 Census and CEDCAP programs by, for example, maintaining a single dependency schedule, it will be limited in its ability to ensure that both programs are planning and measuring their activities according to the same agreed-upon time frames.

In response to our fifth recommendation to establish a comprehensive and integrated list of all interdependent risks facing the CEDCAP and 2020 Census programs, the department agreed and stated that the 2020 Census program should better monitor interdependent risks through an integrated risk register. The department further stated that it uses an enterprise risk management tool to enable access to an integrated list of all active risks, including interdependent risks. It also stated that linkages between the two programs' risk registers can be flagged and tracked using these processes and then used to ensure the same process for responding to emerging risks are followed. However, although the Bureau's comments discuss capabilities of its enterprise risk

management tool that could help address our recommendation, during our review the two programs' interdependent risks were not being linked or tracked in an integrated manner, and we have not received additional evidence to demonstrate that further actions had been taken by the Bureau to address this.

The department agreed with our seventh recommendation to identify when the 74 requirements related to redistricting data program and data products and dissemination will be tested. In its letter, the department stated that the Bureau had been conducting research on the highest-priority areas and activities relative to core operational and cost-efficiency requirements due to budget limitations this decade, but that planning and requirements development for these two areas are now under way. The Bureau intends to ensure that any testing needs are prioritized for inclusion in the 2018 end-to-end census test. Full implementation of our recommendation should help ensure that the requirements are sufficiently tested prior to the 2020 Census.

In response to our eighth recommendation to make identifying requirements related to non-ID response validation a high and immediate priority, or consider alternatives to avoid late definition of such requirements, the department agreed that non-ID response requirements should continue to receive attention and priority. The department also noted that non-ID response validation operations have been conducted for several censuses, using a paper process, and that they validated these responses prior to tabulating the data to ensure that the response was legitimate and not duplicative.

However, while the Bureau has prior experience conducting non-ID response validation operations in a controlled, small-scale paper-based environment, 2020 will be the first decennial census that the Bureau introduces an Internet response option on a wide scale, as well as the first time the Bureau attempts non-ID response collection via the Internet. According to Bureau officials, the use of the Internet to collect non-ID responses introduces the potential for a much higher volume of responses that will need to be validated than if the Bureau were to use a paper-based non-ID approach. The Bureau has also reported that Internet-based non-ID response collection increases the likelihood of fraudulent responses. Given that the Bureau is in the early stages of conducting research and developing requirements in this area and there is only a year remaining before the 2018 Census end-to-end test begins, we maintain that the lack of experience and specific requirements related to non-ID response validation is highly concerning, and our

recommendation to make this a high and immediate priority or consider alternative approaches needs to be implemented.

The department also stated that the Bureau has a long history of and demonstrated commitment to ensuring the confidentiality of the information provided by the public. It stated that implementing strong protections for all of its solutions and conforming to leading cybersecurity and fraud prevention best practices will be paramount for the self-response and field data collection operations. We agree and are encouraged by the significant progress the Bureau has made in addressing our prior recommendations on information security weaknesses.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Secretary of Commerce, the Director of the U.S. Census Bureau, and interested congressional committees. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-4456 or Chac@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.

Carol C. Harris
Director
Information Technology Acquisition Management Issues

List of Committees

The Honorable Ron Johnson
Chairman
The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jason Chaffetz
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

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

The Honorable Will Hurd
Chairman
The Honorable Robin L. Kelly
Ranking Member
Subcommittee on Information Technology
Committee on Oversight and Government Reform
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the status of the 12 Census Enterprise Data Collection and Processing (CEDCAP) projects, (2) evaluate the extent to which the U.S. Census Bureau (Bureau) is implementing best practices in monitoring and controlling selected CEDCAP projects, (3) determine the extent to which the Bureau is adequately managing the interdependencies between the CEDCAP and 2020 Census programs, and (4) describe the key information security challenges the Bureau faces in implementing the 2020 Census design.

To describe the status of the 12 CEDCAP projects, we reviewed relevant CEDCAP program and project documentation, such as the transition plan, segment architecture, project charters, monthly progress reports, and the program office cost estimate and independent cost estimate. We used the information in this documentation to summarize the 12 projects in terms of project objectives, overall time frames, estimated costs, and amount spent to date, among other things. We also interviewed Bureau officials, including the CEDCAP program manager, on the status and plans of all 12 projects.

To evaluate the extent to which the Bureau is implementing best practices in monitoring and controlling selected CEDCAP projects, we selected three projects based on those that Bureau officials identified as being the highest priority for the 2020 Census—(1) Centralized Operational Analysis and Control Project, (2) Internet and Mobile Data Collection Project, and (3) Survey (and Listing) Interview Operational Control Project. We reviewed program management documentation for the selected projects against project monitoring and controlling best practices identified by the Software Engineering Institute's Capability Maturity Model® Integration for Acquisition (CMMI®-ACQ) and for Development (CMMI-DEV).[1] These key practices included

- determining progress against the plan,
- documenting significant deviations in performance,
- taking corrective actions to address issues when necessary,

[1]Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI®-ACQ), Version 1.3 (Pittsburgh, Pa.: November 2010); CMMI for Development (CMMI-DEV), Version 1.3 (Pittsburgh, Pa.: November 2010), Project Monitoring and Control Process Area.

- monitoring the status of risks periodically, and
- implementing the risk mitigation plan.

Specifically, we analyzed program management documentation, including the program management plan, schedule management plan, risk management plan, transition plan, and segment architecture. We also analyzed documentation for each of the three selected projects, including project charters, schedules, risk registers, and monthly progress reports. Further, we interviewed Bureau officials, including the CEDCAP program manager and the project managers for each of the selected projects, on their efforts to manage these projects. We assessed the evidence against the best practices to determine whether each project fully, partially, or did not meet the best practices. Specifically, "met" means that the Bureau provided complete evidence that satisfies the entire criterion, "partially met" means the Bureau provided evidence that satisfies some but not all of the criterion, and "not met" means the Bureau provided no evidence that satisfies any of the criterion.

To determine the extent to which the Bureau is adequately managing the interdependencies between the CEDCAP and 2020 Census programs, we compared program documentation related to managing interdependencies against best practices identified in CMMI-ACQ and CMMI-DEV, as well as by GAO.[2] Specifically, we analyzed relevant documentation from both programs, such as risk management plans, program-level risk registers, master schedules, dependency schedules, program management plans, and requirements management documentation. We also reviewed the 2020 Census Operational Plan, artifacts from meetings of the CEDCAP and 2020 Census Executive Steering Committees, and presentations from the 2020 Census Program Management Review meetings. For assessing schedule dependencies between the CEDCAP and 2020 Census programs, we reviewed both programs' master schedules and other program planning documents that contained major milestones and compared the dates against each other. We identified any potential misalignment in major milestones between the

[2]CMMI-ACQ; CMMI-DEV, Integrated Project Management, Risk Management, and Requirements Management Process Areas; GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005); and *Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: December 2015).

two programs and discussed these with CEDCAP and 2020 Census program officials. We summarize these misalignments in our report. We also interviewed Bureau officials from the CEDCAP and 2020 Census programs, including the CEDCAP program manager, Associate Director of Decennial Census Programs, the Chief of the Bureau's Office of Innovation and Implementation, and the Bureau's acting Chief Information Officer, on their approach to managing schedule, risk, and requirement interdependencies between the two programs.

To describe the key information security challenges the Bureau faces in implementing the 2020 Census design, we reviewed documentation on the 2020 Census design—including the 2020 Census Operational Plan, CEDCAP and 2020 Census program risk registers, and a report developed by a contractor for the 2020 Census—and interviewed staff within the Bureau's Office of the Chief Information Security Officer. We developed a list of key assumptions on the design of the 2020 Census based on the documentation and input from Bureau officials. We also reviewed reports by GAO and others on information security challenges faced across the federal government. We synthesized the information in these reports to determine which security practices were most important given the design assumptions of the 2020 Census, to develop an initial list of key challenges.

We then obtained input on our initial list of challenges from relevant experts and the Census Bureau. Specifically, we identified relevant experts within two of the Bureau's key advisory groups—the National Academy of Sciences and Census Scientific Advisory Committee. These advisory groups consist of academic and industry experts from various fields, including information technology, and they meet with the Bureau regularly to provide feedback on various areas, including the 2020 Census program. We also identified relevant experts within the information security field on GAO's Executive Council on Information Management and Technology, including the Chair of the Association for Computing Machinery's Committee on Computers and Public Policy; the Executive Director for the National Association of State Chief Information Officers; and the Executive Director of the Center for Education and Research in Information Assurance and Security. We provided our list of key information security challenges to these experts, and obtained their perspectives. Finally, we provided the list to the Census Bureau's Acting Chief Information Officer and the Chief Information Security Officer, to gain their feedback on our list and allow them the opportunity to respond with the Bureau's plans for the challenges.

We also determined the Bureau's progress in addressing recommendations from our 2013 public and limited official use only reports by reviewing Bureau documentation, such as the Bureau's Risk Management Framework, IT Security Program Policy, and guidelines and procedures for incident response plan tests.[3] We compared the agency documentation to the relevant information security best practices for each of the recommendations, to determine how many recommendations had been implemented.

We conducted this performance audit from October 2015 to August 2016 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.

[3]GAO, *Information Security: Actions Needed by Census Bureau to Address Weaknesses*, GAO-13-63 (Washington, D.C.: Jan. 22, 2013). Another version of this report contained sensitive information and, as a result, was issued for limited distribution.

Appendix II: Comments from the U.S. Department of Commerce

THE DEPUTY SECRETARY OF COMMERCE
Washington, D.C. 20230

June 24, 2016

Ms. Carol Cha
Director
Information Technology Acquisition Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Cha:

The Department of Commerce appreciates the opportunity to comment on the Government Accountability Office's draft report entitled *Information Technology: Better Management of Interdependencies between Programs Supporting 2020 Census is Needed* (GAO-16-623). The Department's comments on this report are enclosed.

Sincerely,

Bruce H. Andrews

Enclosure

Department of Commerce
Census Bureau's Comments on the
Government Accountability Office Draft Report
Entitled *Information Technology: Better Management of Interdependencies between Programs Supporting 2020 Census is Needed* (GAO-16-623), July 2016

The Department of Commerce appreciates the opportunity to review this draft report. We agree with the report's recommendations; however, for several of the recommendations, we believe some additional context should be included in the report. Once the Government Accountability Office (GAO) issues the final version of this report, the Department will prepare an action plan to document the steps we will take regarding the final recommendations.

In that regard, we are pleased to report the Census Bureau's May 25, 2016, decision to use a Commercial Off-the-Shelf (COTS) platform in combination with in-house solutions for the data collection component of the 2020 Census. In identifying the requirements for the COTS solution, the Census Bureau focused on many of the same areas suggested in this GAO report, and we now expect that we will be able to expediently address many of the recommendations made by GAO. We recognize this decision was not made until after GAO completed their audit work, so it could not be reflected in the draft report. We would also note that this recent decision relates to several statements in the draft report, including statements on page 10, page 18, and Table 2.

The decision memorandum and report are available at the following URLs:

- 2020 Census Program Memorandum Series 2016.06 on "2020 Census Business Solution Architecture": http://www2.census.gov/programs-surveys/decennial/2020/program-management/memo-series/2020-memo-2016_06.pdf

- Report on "Census Enterprise Data Collection and Processing (CEDCaP) COTS Capability Assessment & Analysis": http://www2.census.gov/about/policies/cedcap/cedcap-report-final.pdf

The recommendations concern our need to:

1. Update the Census Enterprise Data Collection and Processing (CEDCaP) program office cost estimate to reflect the current status of the program as soon as appropriate information becomes available.
2. Ensure that updates to the status of risks are consistently documented for CEDCaP's Internet and Mobile Data Collection and Survey (and Listing) Interview Operational Control projects.
3. Ensure that, on a consistent basis, CEDCaP's Internet and Mobile Data Collection and Survey (and Listing) Interview Operational Control and Centralized Operational Analysis and Control projects establish detailed risk mitigation plans and that the Internet and Mobile Data Collection and Centralized Operational Analysis and Control projects establish trigger events for all relevant risks.

1

4. Define, document, and implement a repeatable process to establish complete alignment between CEDCaP and the 2020 Census program by, for example, maintaining a single dependency schedule.
5. Establish a comprehensive and integrated list of all interdependent risks facing the CEDCaP and 2020 Census programs, and clearly identify roles and responsibilities for managing this list.
6. Finalize documentation of processes for managing requirements for CEDCaP.
7. Identify when the 74 requirements related to the redistricting data program as well as data products and dissemination will be tested.
8. Make developing a better understanding of and identifying requirements related to non-ID respondent validation a high and immediate priority, or consider alternatives to avoid late definition of such requirements.

Below are the Department's comments on recommendations 1, 4, 5, 7, and 8. We had no substantive comments on recommendations 2, 3, and 6.

Recommendation 1:

We agree with this recommendation. We do note that, with the decision made on May 25 to use a COTS solution, combined with some in-house elements to deliver the CEDCaP capabilities for the 2020 Census, the Census Bureau has already begun work on new program lifecycle cost estimates.

Recommendation 4:

We agree that the Census Bureau must maintain schedule alignment between the 2020 Census and CEDCaP through a single integrated schedule. The 2020 Census is the program of interest, and as such, it must and will drive the schedule for all solutions that support it, including CEDCaP. The key milestones of the 2020 Census, therefore, become key milestones for CEDCaP. The 2020 Census integrated master schedule already in place is the single schedule with which all dependent projects must coordinate their status. As GAO recommended earlier in the decade, the 2020 Census manages its integrated master schedule through the Primavera software package, as is necessary for a program of its complexity. The 2020 Census integrated master schedule status process requires all dependent projects, including but not limited to CEDCaP projects, to update their status on a weekly basis. Individual dependent projects and solutions may have their own detailed schedules to support day-to-day tasks, specifically those tasks too detailed for the integrated master schedule, in order to support the timelines necessary to meet the 2020 Census milestones. As such, the CEDCaP schedule is a solution of the 2020 Census and will continue to be a dependent schedule of the 2020 Census integrated master schedule, which remains the scheduling tool of record for the management of the 2020 Census.

Recommendation 5:

We agree that the 2020 Census program should continue to enhance its strategies to better monitor interdependent risks with all of its dependent solutions, and it should do so through an integrated risk register.

The Census Bureau already maintains comprehensive risk registers for the 2020 Census and its dependent project-level solutions, including CEDCaP. Risk information maintained in all 2020-related risk registers includes triggers, mitigation strategies, and contingency plans for risks with the highest exposure level. Quarterly reviews by Census Bureau senior leadership are held to examine and monitor the highest-level, crosscutting risks.

The 2020 Census and all of its project-level solutions utilize the Census Bureau's Enterprise Risk Management (ERM) tool to enable access, visibility, integration, and management of active risks. The ERM database enables integration of the 2020 Census and all related risk registers, thereby enabling access to an integrated list of all active risks, including interdependent risks. Additionally, for large solutions supporting the 2020 Census, like CEDCaP, there is a cross-staff presence on the risk review boards to actively monitor risks with the potential to impact both program and project. Linkages between the two program risk registers can be flagged and tracked using these processes and then used to ensure that the same procedures for responding to emerging risks are followed.

We continue to work to improve our risk management process and further improve the integration of the risk register for the 2020 Census and its dependent project-level solutions. In recognition of the GAO findings, we have added a risk into the 2020 Census risk register that acknowledges that some CEDCaP risks are not formal 2020 Census risks and that has documented mitigation strategies, including holding weekly meetings to discuss interdependent risks and maintaining open risk registers at the enterprise level.

Recommendation 7:

The Department agrees with the recommendation to identify and document the testing plan for the few remaining requirements for two program areas (the redistricting data program and 2020 Census data products). It is important to note that, due to budget limitations this decade, the Census Bureau has had to conduct research on the highest priority areas and activities relative to core operational and cost-efficiency requirements needed to conduct a successful 2020 Census. Planning and requirements development for these two areas is well underway, and we will ensure that any testing needs are prioritized for inclusion in the 2018 End-to-End Census Test.

Recommendation 8:

We agree that non-ID response requirements should continue to receive attention and priority. The non-ID response validation operation is one that the Census Bureau has conducted for several censuses, but with the use of an Internet response option, the volume of such cases and the risk of duplicate returns from the same person will be larger. In past decennial censuses, we have enabled individuals to respond on a paper "Be Counted" form without requiring a census-

assigned identifier. We validated these responses prior to tabulating the data to ensure that the response was legitimate and not duplicative.

The Census Bureau has a long history and demonstrated commitment to ensuring the confidentiality of the information the public provides to us. We are bound to this by law, and anyone with access to such data is sworn for life to protect the individual response data. For all of our solutions, we are implementing strong protections on both the front-end as well as the back-end to catch any fraudulent submissions. These solutions, conforming with leading cybersecurity and fraud prevention best practices, will be paramount for our self-response and field data collection operations in our tests as well as in the 2020 Census.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris at (202) 512-4456 or chac@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Shannin G. O'Neill (Assistant Director), Jeanne Sung (Analyst in Charge), Andrew Beggs, Chris Businsky, Juana Collymore, Lee McCracken, and Kate Sharkey.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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

Please Print on Recycled Paper.