United States Government Accountability Office

Testimony before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 9:00 a.m. ET
Thursday, June 9, 2016

INFORMATION TECHNOLOGY

Management of Interdependencies between Programs Supporting 2020 Census

Statement of Carol C. Harris, Director, Information Technology Acquisition Management Issues

GAO-16-723T

June 9, 2016

GAO Highlights

Highlights of GAO-16-723T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

INFORMATION TECHNOLOGY

Management of Interdependencies between Programs Supporting 2020 Census

Why GAO Did This Study

The U.S. Census Bureau (which is part of the Department of Commerce) 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 the Bureau's survey data collection and processing functions.

This statement summarizes preliminary findings from GAO's draft report on, among other things, the Bureau's management of the interdependencies between the CEDCAP and 2020 Census programs, and key information security challenges the Bureau faces in implementing the 2020 Census design. To develop that draft report, GAO 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's draft report includes several recommendations to help the Bureau better manage CEDCAP and 2020 Census program interdependencies related to schedule, risk, and requirements. The draft report is currently with the Department of Commerce and the Bureau for comment.

View GAO-16-723T. For more information, contact Carol C. Harris at (202) 512-4456 or chac@gao.gov.

What GAO Found

The 2020 Census program is heavily dependent upon the Census Enterprise Data Collection and Processing (CEDCAP) program to deliver the key systems needed to support the 2020 Census redesign. However, GAO's preliminary findings showed that 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 less than a year and a half 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 more at 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 who 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.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

I am pleased to be here today to discuss the U.S. Census Bureau's (Bureau) readiness to deliver an enterprise information technology (IT) initiative, referred to as the Census Enterprise Data Collection and Processing (CEDCAP) program, in time to support a significantly redesigned 2020 Census. Specifically, CEDCAP 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.

CEDCAP is particularly important as it is intended to support significant changes for how the Bureau (which is a part of the Department of Commerce) is planning to conduct the 2020 Census. Specifically, the Bureau is aiming to modernize and automate its outdated and inefficient methods of conducting decennial censuses, and to save the government approximately $5.2 billion.[1] This includes 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, enabling a mobile data collection application for field enumerators to use on mobile devices to collect survey data from households, and automating the management of field operations. These new capabilities and supporting systems are expected to be delivered by CEDCAP.

With less than a year and a half 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), this hearing is especially timely. My statement today is based on a draft report, which is currently with Commerce and the Bureau for comment. Specifically, my remarks summarize key preliminary findings from that study, in which we (1) describe the status of the 12 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. We plan to issue this report next month.

[1]Total savings compared to Bureau's projected cost of 2020 Census using traditional approach and methods (in 2020 constant dollars).

Regarding the first objective in our draft report, 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 practices identified 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.

For 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

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

implementing our 2013 information security recommendations.[4] More details on our objectives, scope, and methodology will be provided in the report that we are issuing next month.

We are conducting the work on which this statement is based 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

On October 6, 2015, the 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—and which are expected to dramatically change how the Bureau conducts the Decennial Census. This plan outlines 350 redesign decisions that the Bureau has either made or is planning to make. 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).

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.

[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.

- **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, among other things, identify vacant housing units to remove from enumerators' workloads.[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 Internet response option as well as for non-ID processing with real-time address matching.[8]

[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 Service's Medicare enrollment data.

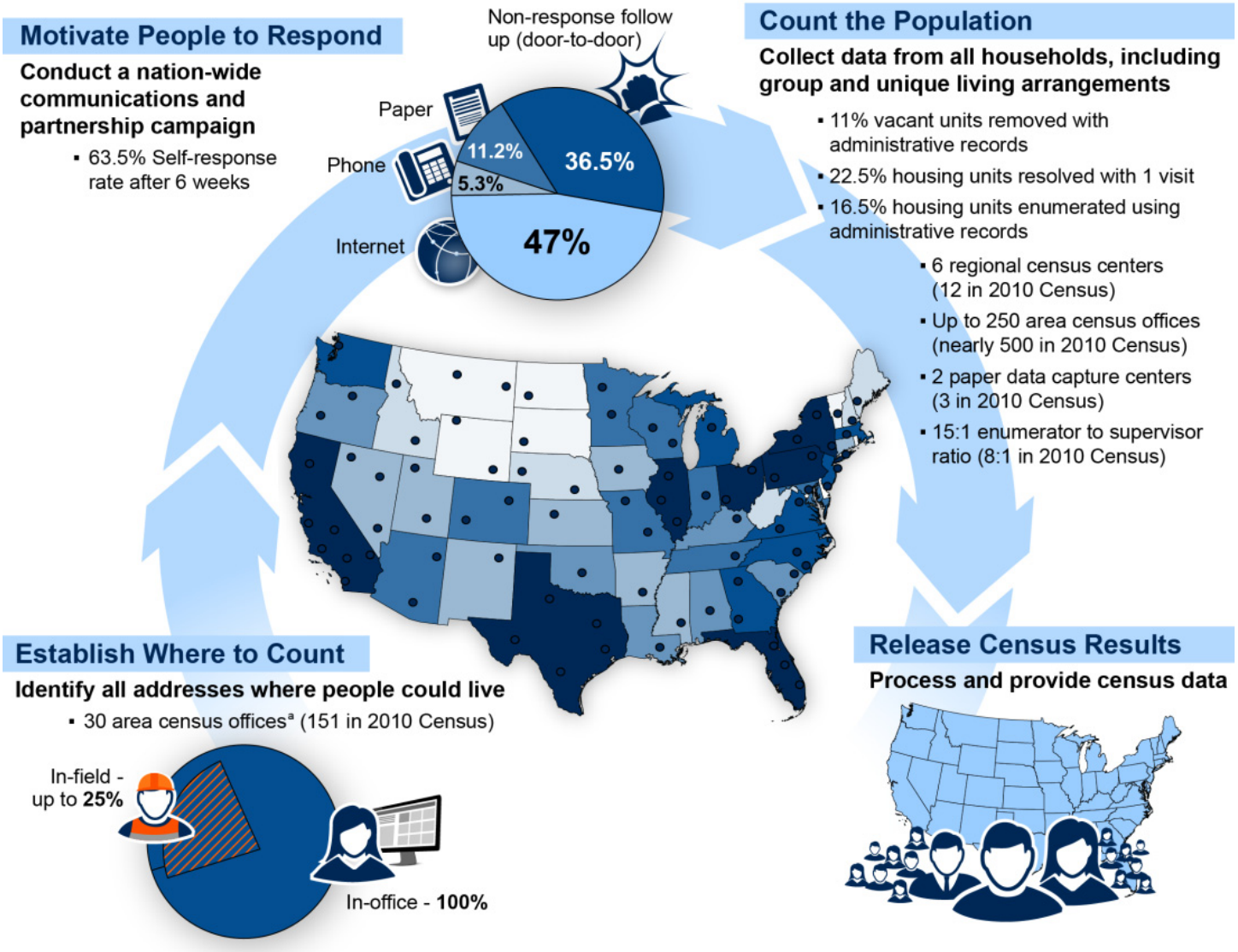
[7]GAO, *2020 Census: Additional Actions Would Help the Bureau Realize Potential Administrative Records Cost Savings,* GAO-16-48 (Washington, D.C.: Oct. 20, 2015).

[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.

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

Figure 1: 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-16-723T

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.

The decisions made to date have been informed by several major field tests, including

- the 2014 Census test, which was conducted in the Maryland and Washington, D.C., areas to test new methods for conducting self-response and non-response follow-up;

- the 2015 Census Test in Arizona, which tested, among other things, the use of a field operations management system to automate data collection operations and provide real-time data and the ability to reduce the non-response follow-up workload using data previously provided to the government, as well as enabling enumerators to use their personally owned mobile devices to collect census data; and

- the 2015 Optimizing Self-Response test in Savannah, Georgia, and the surrounding area, which was intended to explore methods of encouraging households to respond using the Internet, such as using advertising and outreach to motivate respondents, and enabling households to respond without a Bureau-issued identification number.

The following are examples of decisions that had not been finalized as of April 2016:

- **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.

[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

Several of the key systems needed to support the 2020 Census redesign are expected to be provided as CEDCAP enterprise systems under the purview of the Bureau's 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.

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.

The CEDCAP program, which began in October 2014, is intended to provide data collection and processing solutions (including 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.
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-16-723T

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

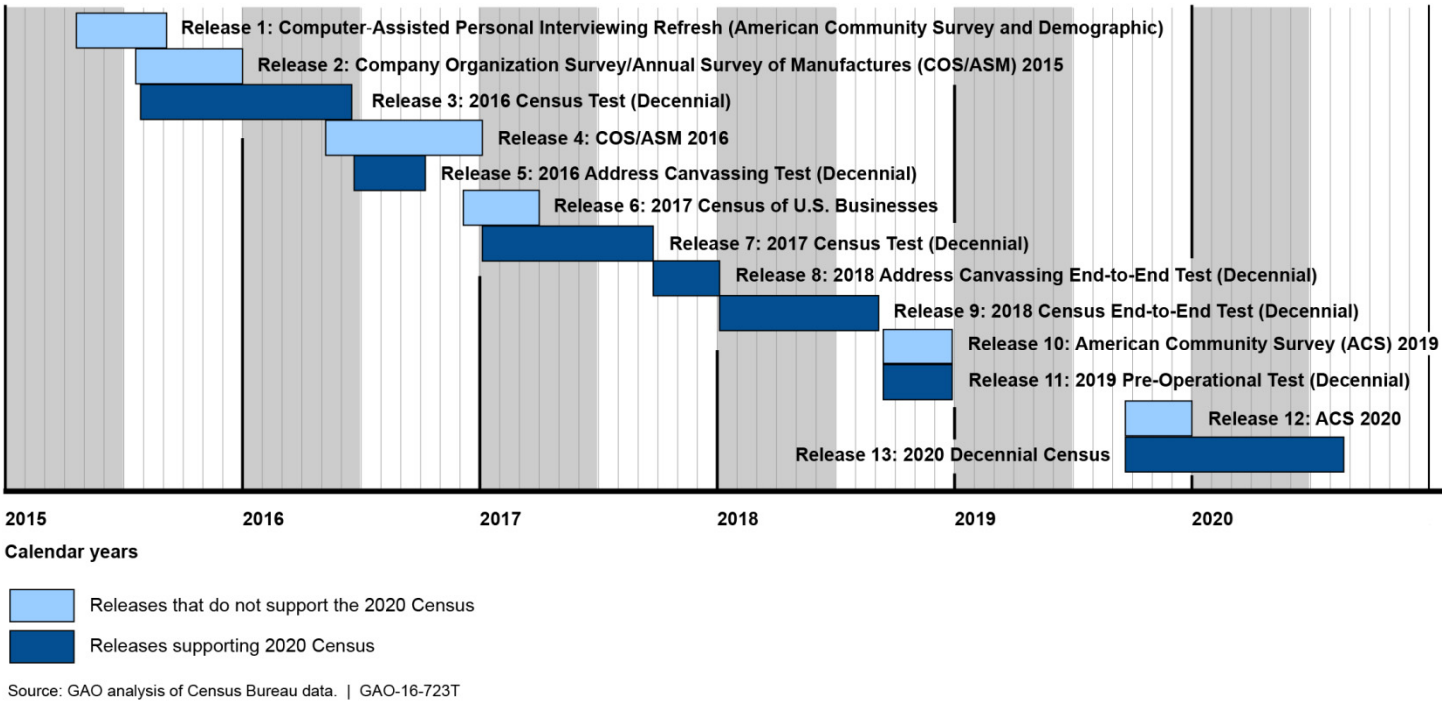
2020 Census program is conducting as it prepares for the 2020 Census,[10] as well as 2020 Census live production. The remaining 6 releases support the other surveys such as the American Community Survey (ACS) and Economic Census.[11] Most recently, the CEDCAP program has been working on delivering the functionality needed for the third product release, which is 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 (mentioned previously) 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 2 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 with the support of CEDCAP, including the ongoing 2016 Census Test, 2016 Address Canvassing Test, 2017 Census Test, and 2018 Census End-to-End test. 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.

[11]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.

Figure 2: 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-16-723T

Note: On June 2, 2016, Bureau officials provided us with updated program documentation, which they indicated includes changes to their release schedule. We have not reviewed this new documentation to verify the changes.

The Bureau's past efforts to implement new approaches and systems have not always gone as planned. As one example, during the 2010 Census, the Bureau planned to use handheld mobile devices to support field data collection for the census, including following up with nonrespondents. However, due to significant problems identified during testing of the devices, cost overruns, and schedule slippages, the Bureau decided not to use the handheld devices for non-response follow-up and reverted to paper-based processing, which increased the cost of the 2010 Census by up to $3 billion and significantly increased its risk as it had to

switch its operations to paper-based operations as a backup.[12] Due in part to these technology issues the Bureau was facing, we designated the 2010 Census a high-risk area in March 2008.[13]

We have also identified and reported on numerous occasions concerns about the Bureau's IT internal control, its IT preparations for the 2020 Census, and its looming deadline.[14] Accordingly, we identified CEDCAP as an IT investment in need of attention in our February 2015 High-Risk report.[15]

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.[16] We emphasized that the 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 to the IT issues I am testifying on today, there are other risks and uncertainties facing a successful headcount that we are monitoring at

[12]GAO, *2010 Census: Preliminary Lessons Learned Highlight the Need for Fundamental Reforms*, GAO-11-496T (Washington, D.C.: Apr. 6, 2011); and *Information Technology: Census Bureau Testing of 2010 Decennial Systems Can Be Strengthened*, GAO-09-262 (Washington, D.C.: Mar. 5, 2009).

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

[14]GAO, *Information Technology: Census Bureau Needs to Implement Key Management Practices,* GAO-12-915 (Washington, D.C.: Sept. 18, 2012); *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.); *2020 Census: Prioritized Information Technology Research and Testing Is Needed for Census Design Decisions,* GAO-14-389 (Washington, D.C.: Apr. 3, 2014); and *2020 Census: Key Challenges Need to Be Addressed to Successfully Enable Internet Response,* GAO-15-225 (Washington, D.C.: Feb. 5, 2015).

[15]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).

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

the request of Congress. For example, in October 2015, we reported on actions the Bureau needs to take in order to ensure it fully realizes potential cost-savings associated with its planned use of administrative records. Likewise, we are assessing the reliability of the Bureau's estimate of the cost of the 2020 Census and anticipate issuing that report to Congress later this month. We also have ongoing work evaluating the 2016 Census Test, which is currently taking place in Harris County, Texas, and Los Angeles County, California.

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

As part of our ongoing work, we determined that 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[17]—has not 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-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.
- 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 are 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.

All projects are scheduled to end by September 2020.[18]

[17]The twelfth project, according to Bureau officials, is to provide the 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.

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

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 program 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 program used the 2013 program cost estimate to establish its current budget and to track project costs.

Selected CEDCAP Projects Partially Met Project Monitoring and Control Best Practices

We determined that the three selected CEDCAP projects we reviewed—the Centralized Operational Analysis and Control project, Internet and Mobile Data Collection project, and Survey (and Listing) Interview Operational Control project— did not fully implement best practices for project monitoring and control, which are critical for making sure that projects are meeting their goals and that action can be taken to correct problems in a timely fashion.[19]

- **Determining progress against the plan.** This involves comparing actual cost and schedule against the documented plan for the full scope of the project and communicating the results. While the three projects meet weekly to monitor the current status of each project and produce monthly reports that document cost and schedule progress, their plans did not include sufficient detail against which to monitor progress. For example, project planning documents for the three projects did not include key information, such as when build-or-buy decisions were to be made or when final systems are to be released. 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 begins in August 2017 (in less than a year and a half). Bureau officials agreed with our concerns and in June 2016 they stated that they are in the process of

[19]These practices have been identified in the Software Engineering Institute's CMMI-ACQ and CMMI-DEV.

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.** Projects should identify and document when deviations from planned cost and schedule occur that, if left unresolved, would preclude the project from meeting its objectives. 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 are measuring deviations against their budgeted amounts, which are based on the 2013 CEDCAP program office cost estimate. This estimate was developed based on very early assumptions and limited details about the program and is thus out-of-date. In the absence of an up-to-date cost estimate, the program lacks a basis for monitoring true deviations in performance. Accordingly, our draft report includes a recommendation that the Bureau update the CEDCAP program office cost estimate to reflect the current status of the program as soon as appropriate information becomes available.

- **Taking corrective actions to address issues when necessary.** Projects should take 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 cost or schedule deviates significantly from the plan. 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.** This practice can result in the discovery of new risks, revisions to existing risks, or the need to

implement a risk mitigation plan. 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, these programs had not updated the status of medium-probability, medium-impact risks for several months. Bureau officials recognized the need to document updates in the risk registers more consistently and stated that efforts are under way to address this, but they did not have an estimated completion date. Until these efforts are complete, the Bureau will not have comprehensive information on how risks are being managed. Accordingly, our draft report includes a recommendation that the Bureau 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.

- **Implementing risk mitigation plans.** Risk mitigation plans that include sufficient detail—such as start and completion dates and trigger events and dates—provide early warning that a risk is about to occur or has just occurred and are valuable in assessing risk urgency. 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, these risk mitigation plans lacked important details such as start or completion dates. Additionally, two projects did not have any trigger events for their risks that exceed a predefined exposure threshold. Bureau officials recognized that there were issues with their risk management process and stated that they were working on addressing them. Bureau officials told us they had revised their risk management process to address these weaknesses, but it was unclear to what extent this process has been implemented. Without detailed risk mitigation plans and trigger events, officials will be hindered in their ability to identify potential problems and mitigate their impacts. Therefore, our draft report includes a recommendation that the Bureau consistently implement detailed risk mitigation plans for the three projects.

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

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

Despite significant interdependencies between the CEDCAP and 2020 Census Programs, our ongoing audit work determined that the Bureau is not effectively managing these interdependencies. About half of CEDCAP's major product releases (7 of 13 total), are to align with and support the remaining 6 major 2020 Census tests, as well as the 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, as called for by best practices identified in our Schedule Assessment Guide.[20] 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 developed two separate dependency schedules for each program, and meet weekly with the intent of coordinating these two schedules. Our schedule guide also indicates that constantly updating a schedule manually defeats the purpose of a dynamic schedule and can make the schedule particularly prone to error.

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

[20]GAO-16-89G.

working to incorporate activities for the next set of near-term milestones, which are to support the 2016 Address Canvassing Test.

This practice of maintaining separate dependency schedules which must be manually reconciled 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 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 2020 Census' major tests, CEDCAP's releases and 2020 Census' major tests milestones were not always aligned to ensure CEDCAP releases would be available in time. For example, development of the seventh CEDCAP release, which is intended to support the 2017 Census Test, is not scheduled to begin until almost a month after the 2017 Census Test is expected to begin (December 2016), and is not planned to be completed until about 2 months after the 2017 Census Test ends (July 2017). Bureau officials acknowledged that CEDCAP release dates need to be revised to accurately reflect the program's current planned time frames and to appropriately align with 2020 Census time frames. Officials stated that these changes will be made by the end of May 2016.

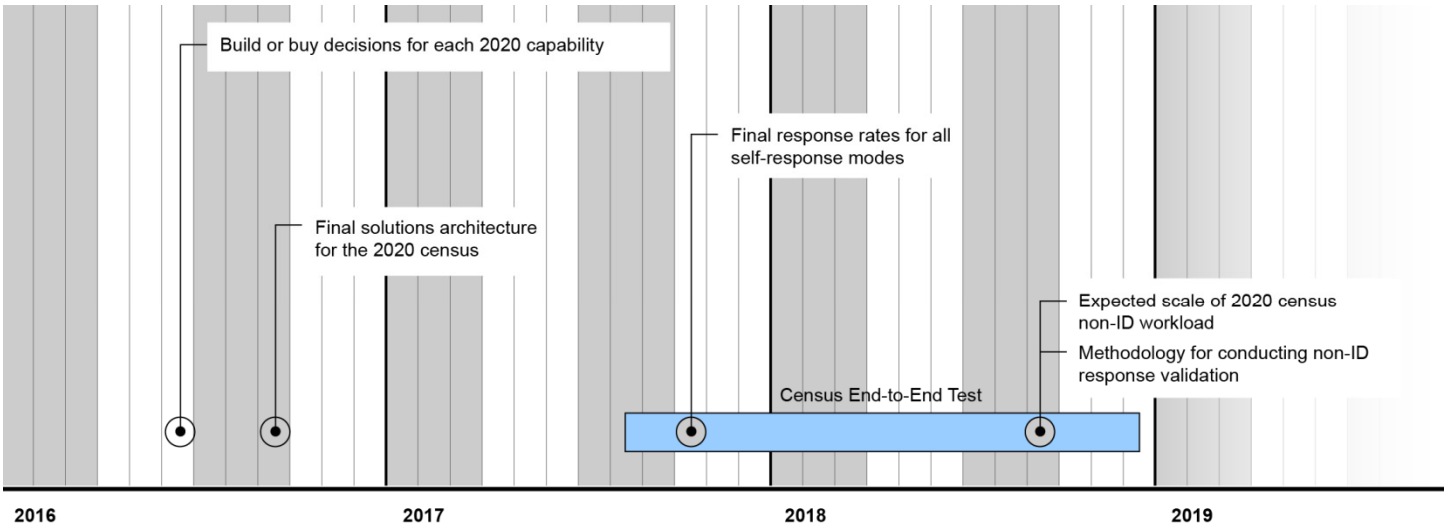
Adding to the complexity of coordinating the two programs' schedules, several key decisions by the 2020 Census program are not planned to be made until later in the decade, as we testified in November 2015.[21] This may impact CEDCAP's ability to deliver those future requirements and have production-ready systems in place in time to conduct end-to-end testing, which is to begin in August 2017. 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

[21]GAO-16-205T.

respond to the 2020 survey using the Internet, telephone, and paper, until October 2017.

Figure 3 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 3: Examples of 2020 Census-related IT Decisions Planned for Later in the Decade that Could Impact CEDCAP, as of April 2016



Source: GAO analysis of Census Bureau data. | GAO-16-723T

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 these difficulties, as of April 2016 (a year and a half into the CEDCAP program), the programs have not documented their process for managing the dependencies, contrary to our schedule guide which indicates that 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.[22] Program officials stated that they aim to document this process by June 2016, but this would at best

[22]GAO-16-89G.

document a process that has not been effective, likely leading to additional misalignment in the future.

We concluded in our draft report that without an effective process for ensuring alignment between the two programs, the Bureau faces increased risk that capabilities for carrying out the 2020 Census will not be delivered as intended. Thus, our draft report (which is with Commerce and the Bureau for comment) includes a recommendation that the Bureau 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.

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

The CEDCAP and 2020 Census programs were also not effectively managing risks common to the two programs. 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, our preliminary findings indicate that these programs do not have an integrated list of risks (referred to as a risk register) with agreed-upon roles and responsibilities for tracking them, as called for by best practices identified by GAO for collaboration and leading practices in risk management.[23] 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, including 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, which as of March 2016 had been realized and was considered an

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

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, manually resolving incompatible schedules in different software can be time-consuming, expensive, and prone to errors. And, as noted above, the Bureau's process for managing schedule dependencies between the two programs has not been effective. 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.

Thus we concluded in our draft report that until it 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, the Bureau is in danger of not fully addressing risks facing the programs. Accordingly, in our draft report we include a recommendation that the Bureau 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.

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

Lastly, despite their significant interdependencies, a process for managing requirements for the two programs has not been finalized. The Bureau's Office of Innovation and Implementation 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 builds functionality containing subsets of the requirements in the 40-day cycles.

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—as recommended by best practices[24]—had not been finalized. According to Bureau officials, they have drafted the process and are working on incorporating feedback from customers. Office officials stated that they plan to finalize this documentation by June 2016. 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

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

expect it to be finalized by June 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 less than a year and a half 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.

Failure to fully define requirements has been a problem for the Bureau in the past. 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.[25] 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

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

system outages and slow performance during the 2010 Census.[26] 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, we concluded in our draft report that 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 similar issues that it experienced during the 2010 Census. Thus, our draft report includes the following recommendations:

- 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; and
- 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.

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

[26]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).

gains and cost savings, this redesign introduces the following 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.[27] Additionally, as we previously reported, in 2015 the White House and the Office of Management and Budget identified anti-phishing as a key area for federal agencies to focus on in enhancing their information security practices.[28]

[27]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).

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

- **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. Additionally, 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.[29]

  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.[30] 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 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 ensure that only respondents and Bureau officials are able to gain access to this information and that

[29]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.

[30]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.

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 personally identifiable information 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 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.[31] 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.[32] For example, we reported that organizations can require that devices meet government specifications before they are deployed, limit 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,

[31]GAO-12-757.

[32]GAO-12-757.

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.[33] 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.[34] Without these safeguards, computer systems and networks, as well as the critical operations and key infrastructures they support, may be lost, and 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 to be considered when making decisions

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

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

about future 2020 Census design features. As described previously, as of April, the Census Bureau still had yet 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 that the Bureau ensures 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.[35] 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.

[35]GAO-15-290.

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.[36] 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, the Bureau 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 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.[37] We made a number of recommendations to improve agencies' cyber incident response practices, such as developing incident response plans and procedures and testing them.

[36]GAO-15-225.

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

- **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 they 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 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.[38] 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

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

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.[39] Thus, we 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.[40]

As of May 2016, the Bureau had made significant progress in addressing these recommendations. Specifically, it had implemented all 13 public recommendations and 88 of 102 technical recommendations. For example, the Bureau developed and implemented a risk management

[39]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.

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

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.

Of the remaining 14 open recommendations, we have determined that 3 require additional actions by the Bureau, and for the other 11 we have work under way to evaluate if they 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.

In conclusion, our ongoing audit work determined that the CEDCAP program has the potential to offer numerous benefits to the Bureau's survey programs, including the 2020 Census program. 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 less than a year and a half. Moreover, although the three selected CEDCAP projects had key project monitoring and controlling practices in place or planned, the gaps we identified in our draft report are impacting the Bureau's ability to effectively monitor and control 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, and additional actions would help align the programs.

Additionally, 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.

Our draft report, which is currently with Commerce and the Bureau for comment, includes several recommendations that, if implemented, will help address the issues we identified and improve the management of the interdependencies between the CEDCAP and 2020 Census programs.

In addition, prior to today's hearing we discussed the preliminary findings from our draft report with Bureau officials, including the Decennial Census Programs' Associate Director, and incorporated their technical comments, as appropriate. According to the officials, they have actions under way to address some of the issues we identified, such as those related to improving risk management for CEDCAP projects. Regarding our finding that the CEDCAP and 2020 programs lack an effective process for integrating schedule dependencies, Bureau officials stated that they believe that they are in compliance with GAO's schedule guide. However, we maintain that the Bureau is not in compliance with the GAO schedule guide because it has not documented an effective process for managing the dependencies. Regarding our finding that the two programs do not have an integrated list of risks facing both programs, Bureau officials stated that they have an enterprise-wide risk management program, in which the Deputy Director has visibility into risks affecting both programs. While we agree that the Deputy Director has visibility into the CEDCAP and 2020 Census risks, documentation of joint management of key program risks does not exist. Therefore, we maintain our position that it is important that the programs establish a comprehensive list of risks facing both programs and agree on their respective roles and responsibilities for jointly managing the list.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

Contact and Acknowledgments

If you have any questions concerning this statement, please contact Carol C. Harris, Director, Information Technology Acquisition Management Issues, at (202) 512-4456 or chac@gao.gov. GAO staff who made key contributions to this testimony are Shannin G. O'Neill (Assistant Director), Jeanne Sung (Analyst in Charge), Andrew Beggs, Chris Businsky, Juana Collymore, Lee McCracken, and Kate Sharkey.

Carol (Cha) Harris

Mrs. Harris is the Director for Information Technology Acquisition Management Issues at the U.S. Government Accountability Office. In this position, she has responsibility for GAO's evaluations of information technology across the federal government. Specific responsibilities include government-wide and agency-specific assessments of system and software development and acquisition; cost and schedule estimation; enterprise architectures; technology investment management; and telecommunications.

Since joining GAO in 2002, Mrs. Harris has led numerous reviews of information technology systems and management at a wide array of federal agencies, including the Departments of Commerce, Defense, and Homeland Security, as well as the Federal Aviation Administration. She is also the co-author of GAO's first best practice guide for developing and managing capital program costs.

Mrs. Harris has a B.S. in Business Information Technology from Virginia Tech.