# Report in Brief

June 19, 2019

## Background

The U.S. Census Bureau (the Bureau) is responsible for conducting a decennial census to ensure an accurate count of the U.S. population. During the 2020 decennial census (the 2020 Census), the Bureau will use the Internet to collect sensitive data of U.S. individuals and businesses protected under U.S. Code Title 13. These protected Title 13 data include personally identifiable information, such as names, addresses, dates of birth, and telephone numbers. The far-reaching consequences of altered, lost, or stolen Title 13 data emphasize the necessity to safeguard the Bureau information technology (IT) systems that will support the 2020 Census.

Every aspect of the 2020 Census related to Title 13 data collection and storage will rely upon commercial cloud services for its primary means, and will therefore require unique security precautions.

As part of the preparation for the 2020 Census, the Bureau conducted the 2018 End-to-End (E2E) Test to assess and validate the 2020 Census operations, procedures, systems, and infrastructure. To execute an effective test of the IT systems that will support the 2020 Census, Title 13 data were collected and stored within the Bureau's 2020 Census cloud environments.

## Why We Did This Review

The objective of this audit was to determine the effectiveness of security processes and controls for select cloud-based IT systems supporting the 2020 Census.

U.S. CENSUS BUREAU

## The Census Bureau Must Correct Fundamental Cloud Security Deficiencies in Order to Better Safeguard the 2020 Decennial Census

OIG-19-015-A

## WHAT WE FOUND

We found that the Bureau's cloud-based IT systems—which will support the 2020 Census—contained fundamental security deficiencies that violated federal standards and U.S. Department of Commerce policies. Many of these deficiencies indicate that the Bureau was behind schedule and rushed to deploy its systems to support the 2018 E2E Test and the 2020 Census. Specifically, we found that (1) unsecured GovCloud root user keys caused severe risks to 2020 Census cloud environments; (2) unimplemented security baselines that document system settings and configurations left critical systems vulnerable; and (3) basic security practices were not fully implemented to protect Title 13 data hosted in the cloud.

Throughout this audit, we worked closely with Bureau system administrators, security staff, and senior leadership so that the security issues we identified could be addressed. This coordination allowed the Bureau to remediate some of these issues before the conclusion of our audit. However, these findings demonstrate that the Bureau did not securely use commercial cloud services to host its cloud environments during 2020 Census preparations, which placed the sensitive Title 13 data collected by the Bureau during the 2018 E2E Test at increased risk of potential misuse or loss. Our recommendations, if fully implemented, will help the Bureau manage its cloud environments in a more secure manner.

## WHAT WE RECOMMEND

We recommend that the Chief Information Officer of the U.S. Census Bureau do the following:

1. Manage the GovCloud root user account according to federal and Departmental requirements. This must include a standardized, documented process to disable the use of all GovCloud root user accounts during the environment creation process for any new GovCloud environments.
2. Assess all Amazon Web Services user accounts in accordance with National Institute of Standards and Technology (NIST) account management requirements and conduct periodic reviews as part of Office of Information Security assessments.
3. Reassess, implement, and continuously monitor security baselines within all cloud environments.
4. Perform technical assessments to validate implementation of security baselines as part of the Bureau's cloud systems' initial and ongoing assessments.
5. Track all Title 13 data that are stored and processed in Bureau cloud environments. This must include coordination between cloud administrators, operational staff, and Office of Information Security personnel.
6. Expedite the implementation of the backup solution in progress and ensure it is operating in accordance with NIST guidance.
7. Formally document and ensure the implementation of controls compensating for lack of disaster recovery planning or engage in disaster recovery planning if the Bureau is unable to meet its obligation to compensate for the lack of disaster recovery planning.
8. Develop and approve an exit strategy for all Bureau cloud systems, including details for completely and securely removing data from the cloud service provider.