# Report in Brief

January 7, 2021

## Background

The U.S. Census Bureau (the Bureau) is responsible for conducting a decennial census as mandated by the United States Constitution to ensure an accurate count of the U.S. population. Data collected during a decennial census are used to determine the number of seats each state will be apportioned in the U.S. House of Representatives, define congressional districts, and distribute billions of dollars in federal funds for infrastructure and public services, such as highways, hospitals, and schools.

During the 2020 decennial census (the 2020 Census), the Bureau used the Internet to collect sensitive data of U.S. individuals and businesses protected under Title 13 of the U.S. Code. These protected Title 13 data include PII (personally identifiable information), such as names, addresses (including GPS coordinates), 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 support the 2020 Census.

## Why We Did This Review

The objective of this audit was to determine the effectiveness of security measures for select IT systems that support the 2020 Census. Our audit scope included the Bureau's risk management program, security operations center (SOC) capabilities, security of Active Directory, and implementation of multi-factor authentication.

## U.S. CENSUS BUREAU

# Fundamental Security Safeguards Were Not In Place to Adequately Protect the IT Systems Supporting the 2020 Census

OIG-21-018-A

## WHAT WE FOUND

We found that fundamental security safeguards were not in place to adequately protect the Bureau's IT systems supporting 2020 Census operations. Specifically, the Bureau's inadequate risk management program left significant risks present in decennial IT systems, some of which were identified in our previous audit report. We also found that the Bureau's Decennial SOC lacked fundamental capabilities during the 2018 End-to-End Census Test and address canvassing campaign, which included the collection of Title 13 protected data.

Furthermore, the Bureau inadequately managed its Active Directory that supports decennial operations by allowing excessive access rights and not properly managing user accounts. In addition, the Bureau had not enforced personal identity verification (PIV) in accordance with federal and Departmental requirements.

## WHAT WE RECOMMEND

We recommend that the Director of the U.S. Census Bureau ensure that the Bureau's Chief Information Officer does the following:

1. Develop and adhere to risk acceptance policies and procedures in accordance with the National Institute of Standards and Technology risk management framework (NIST SP 800-37).
2. Reassess all instances of security risks on the decennial IT infrastructure that were accepted without mitigation and ensure correct actions are taken to minimize existing security risks.
3. Ensure critical SOC capabilities are in place and operating as intended by immediately verifying (a) the implementation and operation of a file level encryption for all required resources; (b) the implementation of a technical solution for data loss prevention is fully functional; and (c) the implementation and complete vulnerability scanning coverage of all required databases.
4. Regularly perform a thorough review of Active Directory configurations and ensure that all active accounts have the minimum access rights to fulfill operational requirements. Consider the feasibility of using specialized software tools to augment the Bureau's review of Active Directory configurations.
5. Prioritize the enforcement of PIV and other forms of multi-factor authentication (MFA) by (a) establishing a process to validate the enforcement of federal PIV requirements for all users accessing Bureau resources via government-owned computers and (b) regularly verifying that all privileged access to the Bureau network or its resources for contractors working on-site at the Bowie Computer Center or Bureau headquarters in Suitland, Maryland, is protected with MFA in accordance with federal and Department requirements.