# Report in Brief

November 22, 2022

## Background

One of the U.S. Census Bureau's (the Bureau's) well-known functions is the decennial census which, among other things, dictates the apportionment of congressional lawmakers in the U.S. House of Representatives. These data are also used to define congressional districts and distribute billions of dollars in federal funds for infrastructure and public services, such as highways, hospitals, and schools. More broadly, the Bureau collects, analyzes, and publishes demographic and economic statistics which can include sensitive financial and personal information on U.S. residents and businesses.

The Bureau uses an information technology enterprise network to store, process, and transmit data.

In January 2020, hackers were able to successfully exploit a security weakness in the Bureau's virtual desktop infrastructure just prior to the official start of the 2020 Census. The hackers' success came from exploiting a known vulnerability, and our office reported on this incident in an August 2021 report. In light of that incident, we launched a cyber red team to provide a realistic assessment of the Bureau's susceptibility to advanced cyber threats. A cyber "red team" is the deliberate use of an emulated threat against organizational assets to test the defenses of an organization.

## Why We Did This Review

Our audit objective was to determine the effectiveness of the Bureau's cybersecurity posture against a simulated real-world attack.

## U.S. Census Bureau

## Simulated Internal Cyber Attack Gained Control of Critical Census Bureau Systems

OIG-23-004-I

## WHAT WE FOUND

We determined that the Bureau did not have an effective cybersecurity posture in place to protect against a simulated real-world attack. Specifically, we found that the red team:

I. Gained unauthorized and undetected access to a Bureau domain administrator account.

II. Gained unauthorized and undetected access to personally identifiable information (PII) of Bureau employees.

III. Reduced the Bureau's defensive options by CUI [redacted]

IV. Used insecure programs on [redacted] to send fake emails.

V. Carried out several malicious actions that identified 11 security weaknesses.

## 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. Implement a process to periodically review and verify that Active Directory permissions are protected from common attacks, are aligned to least privilege principles, and that configurations adhere to least functionality principles.

2. Implement advanced authentication security controls and verify proper protection against the discovered vulnerabilities.

3. Develop alerts that align with common detection methods for known attacks and periodically verify that these detection methods remain current and effective.

4. Verify that file shares containing PII have (a) proper permissions that follow least privilege principles and (b) permissions are periodically reviewed.

5. Implement a control for sensitive data CUI [redacted]

6. Update logging configuration requirements to collect information necessary for reporting breaches related to sensitive PII.

7. CUI [redacted]

8. Establish a process to periodically test and inspect Bureau websites and web applications for vulnerabilities and susceptibility of malicious input.

9. Formalize and continue to perform a process of cleaning and removing legacy code in Bureau systems.

10. Conduct a full after-action review on the detailed red team report and develop a corrective action plan to resolve specific issues identified by the red team, as appropriate, and based on risk.

~~**Controlled by: U.S. Department of Commerce, Office of Inspector General**~~
~~**1401 Constitution Avenue NW, Washington, DC 20230**~~