

United States Senate

WASHINGTON, DC 20510-0803

August 28, 2019

The Honorable Christopher C. Krebs
Director of the Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
Washington, D.C. 20528

The Honorable Steven Dillingham, PH.D.
Director of the U.S. Census Bureau
U.S. Department of Commerce
Washington, D.C. 20233

Dear Director Krebs and Dr. Dillingham:

I write to request information relating to the Department of Homeland Security's (DHS) involvement in assisting the United States Census Bureau ("the Bureau") in its constitutional requirement to conduct a count of the country's population in 2020. The Cybersecurity and Infrastructure Security Agency (CISA), an agency within DHS, is tasked with defending against cyber-attacks by providing the federal government with tools, incident response services, and assessment capabilities to safeguard the '.gov' networks.¹

As you know, the Census Bureau is responsible for carrying out the 2020 Decennial Census, from which the data is used, among other purposes, "to apportion the seats of the U.S. House of Representatives; redraw congressional districts in each state; and allocate billions of dollars each year in federal financial assistance."² The 2020 Census is the first to be conducted electronically. As such, measures must be taken to ensure the cybersecurity of personally identifiable information collected, stored, and used by the Bureau. It is critical that the information systems and networks that hold this data be continuously monitored for vulnerabilities, and that any discovered vulnerabilities be quickly remediated.

In testimony provided by the Government Accountability Office (GAO) before the Subcommittee on Commerce, Justice, Science, and Related Agencies for the House Committee on Appropriations in April 2019, the Bureau was stated to be working with DHS in supporting its cybersecurity efforts to ensure a scalable and secure network, and to strengthen cybersecurity posture and response to threats.³ In a letter addressed to Secretary Wilbur Ross and then-Acting

¹ *About CISA*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, <https://www.dhs.gov/cisa/about-cisa>.

² U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-157SP, SUBSTANTIAL EFFORTS NEEDED TO ACHIEVE GREATER PROGRESS ON HIGH RISK (2019), <https://www.gao.gov/assets/700/697245.pdf>.

³ *Oversight Hearing: 2020 Census Preparation Before the Subcomm. on Commerce, Justice, Science, and Related Agencies, H. Comm. on Appropriations*, 116th Cong. 23 (2019) (statements of Robert Goldenkoff, Director of Strategic Issues, GAO, and Nick Marinos, Director, Information Technology, GAO), <https://www.gao.gov/assets/700/698794.pdf>.

Director of the Census Bureau Dr. Ron Jarmin, cybersecurity experts, including former senior government officials from the White House National Security Council, the Office of the Director of National Intelligence, the Department of Justice, the National Security Agency, the Department of State, the Department of Homeland Security, and the Federal Bureau of Investigation, expressed concerns over how the Department of Commerce will be securing and storing the collection of information.⁴

With the census less than a year away, I turn to CISA and the Bureau for answers on how the agencies are working together to ensure that personally identifiable information will be secured. I ask that you provide this information as soon as possible, but no later than September 27, 2019.

1. Has an outside auditor validated the sufficiency of the Census Bureau's encryption strength?
 - a. Are the responses from the 2020 Census going to be stored on a separate Census Bureau network dedicated solely to handling census data, or the Department of Commerce's preexisting network?
 - i. Will the information be stored or reviewable by any other Agency?
 - b. Aside from the two-factor authentication, will other security protections and tools be in place to protect the information and manage risks, and if so, what are those other security protections and tools?
 - i. What are CISA and the Bureau assessing the highest risks to be, and what is being done to mitigate those risks specifically?
 - c. Will the information collected be stored in a segmented way to create boundaries in accessing the information already in the system?
 - d. Please explain how the Census Bureau would be able to determine if data integrity was compromised and data was inappropriately manipulated – either during collection, or while in storage. What processes are in place to understand 'ground truth' and react swiftly and appropriately to any concerns identified?
2. In written testimony by GAO witnesses before a Homeland Security and Governmental Affairs Committee hearing on the 2020 Census, GAO stated that in the last two years, DHS provided the Bureau with 42 recommendations in strengthening its cybersecurity

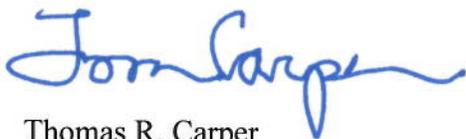
⁴ Letter from J. Michael Daniel, Joshua A. Geltzer, Dipayan Ghosh, Robert Litt, Alexander Macgillivray, Mary B. McCord, Matthew G. Olsen, Christopher Painter, Daniel J. Rosenthal, Paul Rosenzweig, James C. Trainor, to The Honorable Wilbur L. Ross, Secretary of the U.S. DEP'T. OF COMMERCE and Dr. Ron S. Jarmin, then-Acting Director of the U.S. CENSUS BUREAU (July 16, 2018) (on file with the Institute for Constitutional Advocacy and Protection at Georgetown University Law Center), <https://www.law.georgetown.edu/icap/wp-content/uploads/sites/32/2018/07/Census-Cybersecurity-Letter.pdf>.

efforts.⁵ Of the 42 recommendations, 10 are considered “mandatory services” for the Bureau and include risk management and vulnerability assessments for high value assets.⁶ The other 32 recommendations are “voluntary services.”⁷

- a. Have any of the 10 “mandatory services” recommendations been implemented?
 - i. How many is the Bureau planning to implement and when does it expect them to be completed?
 - b. Please provide the 42 recommendations from DHS to the Bureau. This information can be provided in the text of your letter, or in a classified annex, as necessary.
 - c. Please describe the Census Bureau’s process and procedures for tracking receipt and implementation of DHS recommendations related to cybersecurity.
3. Please describe what steps, if any, are being taken by DHS or the Bureau, to identify and combat potential social engineering efforts by malicious actors to obtain and exploit Americans’ personally identifiable information by fraudulently claiming to be associated with the Census.
 4. To what extent, if at all, are other Federal agencies such as the National Security Agency, U.S. Cyber Command, and the Office of the Director of National Intelligence, involved in working with DHS or the Bureau in addressing potential cyber threats, and what will that involvement be as the census begins in earnest in April 2020?

Thank you for your attention to this matter. Please contact Saadia Khan or Abby Shenkle on my staff at (202) 224-2441 with any questions.

Sincerely,



Thomas R. Carper
United States Senator

⁵ *2020 Census: Conducting a Secure and Accurate Count Before the S. Comm. on Homeland Security and Governmental Affairs*, 116th Cong. 29 (2019) (statements of Robert Goldenkoff, Director of Strategic Issues, GAO, and Nick Marinos, Director, Information Technology and Cybersecurity, GAO), <https://www.hsgac.senate.gov/imo/media/doc/Testimony-Goldenkoff%20and%20Marinos-2019-07-161.pdf>.

⁶ *Id.*

⁷ *Id.*

CC: The Honorable Russell T. Vought
Acting Director of the Office of Management and Budget
Washington, D.C. 20503