United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

October 23, 2019

The Honorable Gene Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street NW
Washington, D.C. 20548

Dear Mr. Dodaro:

The Department of Homeland Security (DHS) is responsible for a wide variety of functions that are critically important to the security of our country and its citizens. To carry out these functions, the department collects and maintains extensive amounts of detailed and sometimes sensitive personally identifiable information (PII). Further, in many cases, DHS leverages the capabilities and expertise of contractors to assist it in its mission, and these contractors also have access to millions of Americans' PII. While the department's functions are essential, it is also essential that it protect the PII that is collected on the department's behalf from improper access or use.

In this regard, three recent DHS data breach incidents are troubling. First, in March 2019, the DHS Office of Inspector General (OIG) announced that the Federal Emergency Management Agency's (FEMA) Transitional Sheltering Assistance (TSA) program had shared too much PII on 2.3 million survivors of hurricanes Harvey, Irma, and Maria and the California wildfires with one of the agency's contractors. The OIG noted that the oversharing of PII increased the risk of identity theft and fraud. Second, in June 2019, U.S. Customs and Border Protection (CBP) officials said that photos of people in vehicles entering and exiting the U.S. through a land border entry port had been stolen by hackers as part of a "malicious cyberattack" on one of CBP's contractors, calling into question the security of the agency's facial recognition technology system. Finally, most recently, DHS announced that sensitive data from a bioterrorism defense program had been stored on an insecure website run by a private contractor. Such lapses in sharing PII with contractors or protecting PII in contractor systems are unacceptable.

Accordingly, we request that GAO conduct a review of the policies and procedures in place at DHS to ensure that PII collected by or shared with contractors is protected from improper access or use. In formulating its specific objectives for this work, we ask that GAO consider these topics:

- What requirements does DHS impose on contractors to protect PII that they receive or collect on behalf of the department?

- What oversight mechanisms are in place at major DHS components to ensure that contractors fully adhere to DHS security and privacy policies?

- When data breaches do occur, what steps does DHS take to ensure that the root causes are identified and remediated in contractor systems and programs?

Please contact Harlan Geer of my staff at (202) 224-1497 to discuss the details and timing of this GAO review.

Sincerely,

Maggie Hassan

Margaret Wood Hassan
Ranking Member
Subcommittee on Federal
Spending Oversight and
Emergency Management