MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Eighteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

January 26, 2023

The Honorable David Pekoske
Administrator
Transportation Security Administration
U.S. Department of Homeland Security
6595 Springfield Center Drive
Springfield, VA 20598-6005

Dear Administrator Pekoske:

We write concerning recent media reporting that a Switzerland-based cyber actor was able to access recent versions of the Federal Terrorist Screening Dataset, as well as a critical derivative of the dataset, the No-Fly List, maintained by the Transportation Security Administration (TSA).[1] Based on this reporting, the Committee understands that as many as 1.5 million data entries, including names, dates of birth, and aliases of individuals prohibited from flying into, out of, within, or over the United States was accessed on an unsecure Amazon Web Services server belonging to CommuteAir, which operates flights exclusively for United Airlines across several major hubs in the United States, including Washington Dulles, Denver, and Houston.[2]

Additionally, the hacker claimed they may have been able to exploit their access to the server to cancel or delay flights and even switch out crew members.[3] If this were to be the case, the national security implications of this are alarming. As you are keenly aware, the transportation systems sector is one of 16 critical infrastructure sectors in the United States, ensuring the free movement of people and goods essential to the American economy and way of life. The notion that such a consequential database be left unsecure is a matter concerning cybersecurity, aviation security, as well as civil rights and liberties.

---

[1] Pandolfo, Chris, "TSA 'No-Fly' List Leaked after being Found on Unsecure Airline Server," Fox Business, 21 January 2023, <https://www.foxbusiness.com/politics/tsa-no-fly-list-discovered-unsecured-airline-server-leaked-trans-lesbian-anarchist-kitten-hacker>.
[2] Pellish, Aaron and Sonnet Swire, "Republican Lawmaker Indicates Congress will Investigate TSA No-Fly List Breach," CNN, 21 January 2023, <https://www.cnn.com/2023/01/21/politics/congress-dan-bishop-investigate-tsa-no-fly-list-breach/index.html>.
[3] Greig, Jonathan, "Congressman 'coming for answers' after 'no-fly list' hack," The Record, 23 January 2023 https://therecord.media/congressman-coming-for-answers-after-no-fly-list-hack/>.

While the Committee has now engaged with TSA to receive additional information related to this incident, concerningly, we were not notified proactively that this breach had occurred. It is incumbent upon the Members of the Committee on Homeland Security to conduct necessary oversight to ensure threats to Americans' transportation systems and civil rights and liberties are taken seriously. To that end, please provide answers to the following questions no later than Wednesday, February 8, 2023:

1. When did TSA first learn of the incident in which this data was accessed by a cyber actor and shared in a public manner?
   a. What actions were taken in coordination with airline partners, to subsequently secure the information?
   b. What steps has TSA taken to ensure this or similar datasets do not exist elsewhere on unsecure systems operated by air carriers?

2. Has TSA identified any deficiencies on the part of United Airlines or CommuteAir which may have led to this information being placed on an unsecure server?

3. What privacy or civil rights and liberties reviews have been conducted in response to this incident by TSA regarding the information of any American citizens that may have been released as part of this breach?

4. What, if any, threat assessments have been conducted in the wake of this incident related to aviation security or cybersecurity of critical transportation infrastructure?

5. Does TSA place any cybersecurity requirements on air carriers related to protecting sensitive information such as the No-Fly list? If so, please list.

6. Is TSA considering any updated or additional guidance or requirements, specifically in TSA's updated aviation Security Directive, to safeguard this sort of data in the future?

7. It has been reported that the revealed list includes Victor Bout, a Russian arms dealer recently released by the Biden administration in relation to a prisoner swap. Can TSA confirm whether Victor Bout remains on the U.S. No-Fly List?

8. Was the ability to switch out pilots, gate attendants, or other security personnel available to those who had access to the documents on this server?
   a. What are the national security implications of an individual being able to cancel flights, delay flights, or switch out crew members—a capability claimed by the cyber actor who accessed the sensitive data?

9. Do airlines have the ability to verify that flight cancellations, flight delays, or alterations to crew assignments are being made by individuals authorized to do so?

10. To the agency's knowledge, have there been any instances of unauthorized individuals cancelling flights, delaying flights, or altering assignments of crew members?

Thank you for your prompt attention to this matter. Should you or your staff have any questions, please contact Eric Heighberger on the Committee staff at (202) 226-8417.

Sincerely,

MARK E. GREEN, MD
Chairman

DAN BISHOP
Member of Congress

cc:
The Honorable Jen Easterly, Director
Cybersecurity and Infrastructure Security Agency