RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224–5244

United States Senate
WASHINGTON, DC 20510–3703

COMMITTEES:

COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

February 21, 2020

Andre McGregor
Chief Security Officer
ShiftState Security
2826 Hudson Street
Denver, CO 80207

Dear Mr. McGregor:

I write to seek information about ShiftState Security's cybersecurity audit of the mobile voting app Voatz.

Cybersecurity experts have warned for decades that internet voting is dangerous and should not be used. In spite of these clear warnings, officials in West Virginia, Utah, Colorado and Oregon have, in recent elections, piloted Voatz, a mobile voting app. To convince state and local officials to take a chance on Voatz's controversial technology, Voatz touted an audit conducted by ShiftState Security. ShiftState and Voatz have not published the audit, and Voatz has refused to provide me with a copy. However, in a press interview last year, you declared that Voatz "did very well" in the full security review that you and your team conducted.

Voatz's high marks from ShiftState stand in sharp contrast to the failing grade it received in a recent audit by cybersecurity researchers at the Massachusetts Institute of Technology (MIT). The MIT team found that any adversary that controls a voter's internet connection, like their internet provider or employer, can determine the candidates for whom that person voted. They also found that the PIN the Voatz app uses to protect Americans' votes is far too short, enabling anyone with access to a voter's phone to discover how they voted in previous elections. Finally, the MIT researchers discovered that Voatz's much-hyped use of a blockchain technology does not, in fact, prevent an attacker with control of Voatz's servers from modifying, fabricating or exposing a user's vote.

In recent months, several state officials have cited your company's audit in response to my office's inquiries about Voatz's security or lack thereof. These officials believe, reasonably so, that Voatz's technology passed a comprehensive audit. However, any comprehensive audit should have found the alarming flaws discovered by the MIT team. Indeed, the MIT researchers note in their report that the significant flaws they discovered are not "novel," that many are simply the result of poor design, and that the flaws should have been "easily recognizable." Elections officials and voters have a right to know why ShiftState did not uncover these flaws, and the extent to which federal, state, and local officials may have been misled by Voatz. Accordingly, please provide me with answers to the following questions by March 9, 2020:

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326–7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431–0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962–7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858–5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330–9142

707 13TH ST, SE
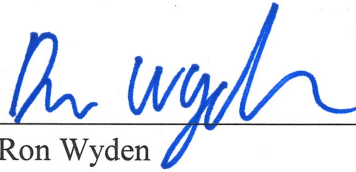SUITE 285
SALEM, OR 97301
(503) 589–4555

HTTPS://WYDEN.SENATE.GOV
PRINTED ON RECYCLED PAPER

1. Please identify the number of people on the ShiftState team that audited Voatz who have experience in:
   a. Election security.
   b. Cryptographic protocol design and analysis.
   c. Side channel analysis.
   d. Blockchain security.
2. Did ShiftState's security audit discover the same issues discovered by the MIT team? If no, please explain why. If yes, please explain why you still told the press that Voatz did "very well" on their audit.
3. Do you disagree with the findings of the MIT team? If yes, please explain.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden
United States Senator