BILL CASSIDY, OF LOUISIANA, CHAIRMAN

RAND PAUL, OF KENTUCKY
SUSAN M. COLLINS, OF MAINE
LISA MURKOWSKI, OF ALASKA
ROGER MARSHALL, OF KANSAS
TIM SCOTT, OF SOUTH CAROLINA
JOSH HAWLEY, OF MISSOURI
TOMMY TUBERVILLE, OF ALABAMA
JIM BANKS, OF INDIANA
JON HUSTED, OF OHIO
ASHLEY MOODY, OF FLORIDA
ALAN ARMSTRONG, OF OKLAHOMA

BERNARD SANDERS, OF VERMONT
PATTY MURRAY, OF WASHINGTON
TAMMY BALDWIN, OF WISCONSIN
CHRISTOPHER MURPHY, OF CONNECTICUT
TIM KAINE, OF VIRGINIA
MARGARET WOOD HASSAN, OF NEW HAMPSHIRE
JOHN W. HICKENLOOPER, OF COLORADO
EDWARD J. MARKEY, OF MASSACHUSETTS
ANDY KIM, OF NEW JERSEY
LISA BLUNT ROCHESTER, OF DELAWARE
ANGELA D. ALSOBROOKS, OF MARYLAND

MATT GALLIVAN, MAJORITY STAFF DIRECTOR
WARREN GUNNELS, MINORITY STAFF DIRECTOR

www.help.senate.gov

United States Senate
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS
WASHINGTON, DC 20510–6300

October 28, 2026

Amit Sevak
Chief Executive Officer
660 Rosedale Road
Princeton, NJ 08541

Dear Mr. Sevak,

Cybersecurity threats are one of the most significant risks currently affecting the safety and security of our most sensitive information. At a time when hostile actors are increasingly using sophisticated tactics leveraging artificial intelligence, it is essential for the education technology sector to take meaningful steps to safeguard student and consumer information.

The recent cybersecurity incident affecting Educational Testing Service (ETS) highlights the impact these growing threats have on disrupting our educational system. ETS provides assessment tools for approximately 50 million individuals annually across a student's educational career.[1] The current investigation thus far indicates millions of current and former California students' information was accessed and copied, including "student names, dates of birth, residential addresses… demographic information… [and] disability [status]."[2] The California Department of Education (CDE) oversees the largest public education system in the United States, managing over 5.7 million K-12 students.[3]

Additional transparency is needed regarding what information threat actors accessed, what measures ETS had implemented prior to the incident to protect sensitive information, and what steps the company intends to take going forward to address vulnerabilities and improve its security infrastructure. To that end, I request answers to the following questions by November 12, 2026:

[1] *U.S. Workers Know They Must Adapt but Action is Stalling, New ETS Report Reveals*, Educational Testing Service (Jul. 13, 2026), https://www.ets.org/newsroom/ets-launches-human-progress-report-50-states-edition.html.
[2] *Educational Testing Service (ETS) Incident*, California Department of Education (Oct. 16, 2026), https://www.cde.ca.gov/nr/in/ets-incident.asp#whathappened.
[3] Fingertip Facts on Education in California, California Department of Education (Oct. 15, 2026), https://www.cde.ca.gov/ds/ad/ceffingertipfacts.asp?utm_source=chatgpt.com.

1. What security protocols, both cyber and physical, does ETS have in place to protect against a cyberattack?

2. How does ETS incorporate cybersecurity best practices implemented by other critical infrastructure sectors?

3. When did ETS first become aware of a cyber incident affecting its systems?

4. When did ETS notify federal agencies of a cyber incident, and which agencies did ETS notify?

5. ETS has stated that "Affected individuals include current and former students enrolled in California public schools between 2023 and the current school year, as well as students who left a California school since 2006 and did not confirm transfer to another school with the CDE."[4]
    a. What steps is ETS taking to fully identify what individuals were potentially impacted?
    b. How is ETS proactively communicating with potentially impacted individuals and entities, including the parents or guardians of potentially impacted children under age 18?

6. ETS thus far has indicated that "student demographic, program participation, and assessment data that ETS maintains in connection with California's statewide assessment programs" was accessed and copied.[5]
    a. What steps is ETS taking to identify any additional information that may have been accessed?

[4] *Id.*
[5] *Id.*

7. ETS has stated that it "has taken steps to reduce the potential risk of the data being made publicly accessible."
    a. What steps has ETS taken to reduce the potential risk of data being made publicly available?
    b. Has ETS had any communications with the threat actor who accessed and copied the impacted information?

Sincerely,

Bill Cassidy, M.D.

Bill Cassidy, M.D.
Chairman
U.S. Senate Committee on Health,