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

May 12, 2026

VIA ELECTRONIC TRANSMISSION

Steve Daly
Chief Executive Officer
Instructure
6330 S 3000, Suite 700
Salt Lake City, UT 84121

Dear Mr. Daly:

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 Instructure and its learning management system (LMS), Canvas, highlights the impact these growing threats have on disrupting our educational system.[1] Canvas, the most widely used LMS in the United States, is used by approximately 30 million individuals, including for course management, communication with students, and administrative functions.[2] This disruption comes at the end of the school year, creating numerous complications around finals and end-of-year functions for students. Instructure has thus far stated that compromised "data fields involved include information like usernames, email addresses, course names, enrollment information and messages."[3] Estimates thus far indicate that this incident has affected the data of over 275 million individuals and over 8,000 school districts, universities, and other educational stakeholders.[4]

---

[1] Hannah Ziegler, *Canvas Online Learning Platform Shut Down for Hours After Cyberattack*, The New York Times (May 7, 2026), https://www.nytimes.com/2026/05/07/education/canvas-hacked-down-data-breach.html.
[2] Rachel Treisman, *Canvas is Back Online, but Questions – and Final Exam Disruptions – Linger*, NPR (May 8, 2026), https://www.npr.org/2026/05/08/nx-s1-5815956/canvas-data-breach-school-finals.
[3] *Security Incident Update & FAQs*, Instructure (May 9, 2026), https://www.instructure.com/incident_update.
[4] Jason Koebler, *'The Biggest Student Data Privacy Disaster in History': Canvas Hack Shows the Danger of Centralized EdTech*, 404 Media (May 8, 2026), https://www.404media.co/the-biggest-student-data-privacy-disaster-in-history-canvas-hack-shows-the-danger-of-centralized-edtech/; Lawrence Abrams, *Instructure Hacker Claims Data Theft from 8,800 Schools, Universities*, Bleeping Computer (May 5, 2026),

This is not the first time Instructure has experienced a cybersecurity incident. In fact, Instructure was previously the victim of a cybersecurity incident in 2025, and recent reporting indicates that the ongoing incident stems from two separate attacks on Instructure's systems.[5] Additional transparency is needed regarding what information hostile actors accessed, what measures Instructure 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.[6] To that end, we request answers to the following questions by May 28, 2026:

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

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

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

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

5. Instructure has stated that "data fields involved include information like usernames, email addresses, course names, enrollment information and messages.[7]
    a. Has Instructure determined if this information contained any personally identifiable information?
    b. What steps is Instructure taking to identify any additional information that may have been accessed?
    c. How is Instructure proactively communicating with potentially impacted individuals and entities, including the parents or guardians of potentially impacted children under age 18?

6. Many of Instructure's customers have been the victim of defacement attacks where hostile actors have publicized the list of affected schools.
    a. How many customers has Instructure identified as potentially affected by the cybersecurity incident?

---

https://www.bleepingcomputer.com/news/security/instructure-hacker-claims-data-theft-from-8-800-schools-universities/.

[5] *Instructure Canvas Cybersecurity Incidents: Analysis of 2025 Salesforce Breach and 2026 Canvas Data 2 & Beta Security Event*, Rescana (May 3, 2026), https://www.rescana.com/post/instructure-canvas-cybersecurity-incidents-analysis-of-2025-salesforce-breach-and-2026-canvas-data-2-beta-security-event/.

[6] *See* note 3.

[7] *Id*.

b. What steps has Instructure taken to support customers to regain access to Canvas or affected systems?

7. Instructure was the victim of a previous cybersecurity incident in September 2025.
    a. What remedial steps did Instructure take to improve its security protocols after that incident?
    b. What remedial steps has Instructure taken, or does it intend to take, to improve its security protocols in response to the ongoing incident?

8. Instructure recently stated that it "reached an agreement with the unauthorized actor involved in this incident," including the return of all exfiltrated data and the "digital confirmation of data destruction."[8]
    a. What were the specific terms associated with this agreement?
    b. What data was included in this agreement?
    c. Has Instructure determined whether the hostile actor exfiltrated data not covered by this agreement?

Sincerely,

Bill Cassidy, M.D.
Chairman
U.S. Senate Committee on Health, Education, Labor, and Pensions

Tommy Tuberville
Chairman
Subcommittee on Education and the American Family

[8] *See* note 3.