Cybersecurity Experts Warn: Student Privacy at Risk if Department of Education Is Eliminated

Loss of Federal Oversight Could Leave FERPA Unenforced and Student Data Unprotected

COLUMBUS, OH, UNITED STATES, March 20, 2025 /EINPresswire.com/ -- The potential elimination of the U.S. Department of Education has raised urgent concerns about the future of cybersecurity and data privacy in higher education. While much of the public focus has centered on the loss of federal student aid programs, cybersecurity professionals warn of another looming crisis: the collapse of federal enforcement mechanisms protecting student data.

“As a former full Pell Grant recipient, my first thought was about less fortunate students who may lose access to education,” says Matt Santill, former Chief Information Security Officer (CISO) in higher education and CEO of Cyber Security Services. “But I’m also deeply concerned about the impact on cybersecurity and student data privacy—particularly when it comes to FERPA.”

The Family Educational Rights and Privacy Act (FERPA) is a federal law that governs access to student education records and ensures their privacy. However, enforcement of FERPA relies on the Department of Education, which oversees compliance, investigates violations, and can impose corrective actions tied to federal funding.

If the Department is eliminated, several consequences are likely to follow:

1. No enforcement body. The Department of Education currently serves as the primary enforcer of FERPA.

2. No audits or compliance reviews. The Department ensures institutions follow the law through oversight activities.

3. No funding leverage. Corrective action plans and the threat of losing federal funding have historically been powerful tools to drive compliance—these could disappear entirely.

“FERPA has always relied on the presence of a federal agency to ensure compliance,” Santill explains. “Without oversight, we risk creating a patchwork of state regulations—or worse, no regulation at all. That’s a dangerous place for student data privacy to be.”

As policymakers debate the future of the Department of Education, cybersecurity experts like Santill are calling for clarity on how student privacy protections will be maintained.

“We need a clear strategy for who will protect student privacy in the absence of the Department of Education,” Santill adds. “If not, institutions will be left to navigate this gap on their own, and students’ data could be at serious risk.”

For further insights or to schedule an interview with Matt Santill, contact Cyber Security Services at the details below.

About Matt Santill and Cyber Security Services
Matt Santill is a former Chief Information Security Officer for one of the largest colleges by student body in the United States and the CEO of Cyber Security Services, a cybersecurity consulting firm focused on risk management, privacy, and information security for higher education institutions. He was an original contributor to the NIST Cybersecurity Framework and performs penetration testing for some of the world’s largest organizations. Learn more at cybersecurityservices.com.

Matt Santill
Cyber Security Services
+1 786-266-7388
matt.santill@cybersecurityservices.com
Visit us on social media:
LinkedIn