EDUCAUSE News Bulletin

Greetings,

As the Chief Information Officer (CIO) at the U.S. Department of Education, I am responsible for ensuring that the Department’s Information systems are well protected. I also work closely with our staff to promote cybersecurity awareness and best practices. We are all responsible for protecting the information entrusted to us by students and the public.

When educational institutions and their students are attacked by cyber threats or experience system failures due to poor resilience, it’s often the student who suffers. For example, if a phishing student unknowingly pays tuition to a fraudster the consequence may mean a missed semester or the potential derailment of an entire academic career. Like EDUCAUSE and other similar organizations in the Educational community, we share a common cybersecurity goal to protect students’ educational journeys.

To respond to the growing cyber-attacks against our educational information systems, the Department is working to improve information sharing and strengthen communications with our partners and customers. While the Department has had a substantial relationship with higher education through our Office of Federal Student Aid (FSA), we’d like to expand our outreach to the entire education IT and cybersecurity community. I believe there are opportunities at three levels for the Department to contribute to educational cybersecurity:

- **Operational** - The Department of Education and our federal partners, such as the Department of Homeland Security (DHS) and the Federal Bureau of Investigation, can be of enormous assistance to the educational community. As a cabinet-level agency, we have access to unique intelligence, risk, threat and vulnerability information that, combined with information many organizations receive from the commercial sector, can offer substantial insights. Working with our civilian partners, such as EDUCAUSE and the Research and Education Networks Information Sharing and Analysis Center (REN-ISAC), and Federal partners like DHS, we can build capabilities that enable greater sharing of this unique blend of information.

- **Tactical** - In the near term we have opportunities to share best practices for building and maintaining secure and resilient systems. We have extensive experience in contracting, cloud, workforce development, and several complementary disciplines necessary to help protect an organization’s IT systems. Our goal is expanded partnerships for sharing best practices.

- **Strategic** - As the Department’s programs change, we need to understand how those changes affect our educational institutions. For example, if we implement new cybersecurity requirements for the protection of Education Department data, there will be consequences for all institutions that use that data. Frank conversations with our Federal and civilian partners about IT or cybersecurity requirements help everyone understand the potential impacts. Effects of changing technologies and policies, both positive and negative, can inform strategic planning efforts within the Department and across the educational community.

400 MARYLAND AVE. S.W., WASHINGTON, DC 20202

www.ed.gov

The Department of Education’s mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.
Working together we can look five to ten years in the future. Cooperation began earlier this year with a joint meeting between the Department and EDUCAUSE during which we discussed how we can engage with the educational community to learn and grow from each other’s experiences and to build a stronger culture of sharing. By working with EDUCAUSE, I’m optimistic that doors have opened to better collaboration, understanding and communication. Together we can help protect students, save taxpayer dollars, and build better systems. I’m excited about this new partnership and hope you’ll be a part of our journey forward.

Sincerely,

Jason Gray
Chief Information Officer
U.S. Department of Education