Securing the Nation's Educational Technology

Grace Collins

November 2020

Summary

Never before have so many children in America used so much educational technology, and never before has it been so important to ensure that these technologies are secure. Currently, however, school administrators are overburdened with complex security considerations that make it challenging for them to keep student data secure. The educational technologies now common in America's physical and virtual classrooms should meet security standards designed to protect its students. As a civil rights agency, the Department of Education has a responsibility to lead a coordinated approach to ensuring a baseline of security for all students in the American education system.

This policy initiative will support America's students and schools at a time when educational experiences—and student information—are increasingly online and vulnerable to exploitation. The plan of action outlined below includes a new Department of Education educational technology security rule, training support for schools, a voluntary technology self-certification system, an online registry of certified technologies to help grow a secure educational technology market, and processes for industry support and collaboration in this work. Combined, these efforts will create a safer digital learning environment for the nation's students and a more robust educational technology marketplace.

Challenge and Opportunity

As schools increasingly rely on educational technology (ed tech) and complex modes of online and hybrid education, student safety is at risk without a clear and coordinated approach to security. Insecure technologies can lead to massive student privacy breaches, such as the loss of sensitive student information to malicious actors and foreign-based data collection efforts, as well as damage to school technology and assessment infrastructure necessary for statewide testing.

The Department of Education (ED) has a statutory authority and responsibility to lead on national educational technology issues, including security. In support of its mission of ensuring equal educational access and promoting student achievement, the Department of Education should lead the way in creating a system in which students and parents can be certain that school technology is secure; teachers can quickly identify secure classroom technologies; school administrators can check a trusted website before deploying a new technology to their school or district; schools receive reliable support and training on technology security; and safety-conscious educational technology companies and organizations are supported. This vision can be enacted through a coordinated effort that utilizes resources and authorities already in existence in the Federal Government.

Plan of Action

To meet the challenge of an increasingly complex online educational environment, the Federal Government should utilize the statutory role of the ED's Office of Educational Technology (OET). OET is a statutory office charged with "providing leadership to the Nation in the use of technology." The following five actions will lay the foundation of a comprehensive approach to technology security in education:

Action 1: More Clearly Define the Minimum Standards for School Technology Security: The Securing Educational Technology (SET) Rule

ED provides funding to K-12 schools under the Every Student Succeeds Act (ESSA). ED requested $19.4 billion in 2021 funding[3] for the consolidated Elementary and Secondary Education for the Disadvantaged Block Grant. This formula grant includes funds for Titles I through IV, as well as other programs. These programs require regular academic assessments which can be compromised by insecure technology.

The proposed rule would require that all K-12 schools which receive federal funding from formula grants meet a minimum level of security for technology and data transfer between technologies. Schools will be asked to track and self-assess their security each year. OET will oversee the program and respond to concerns regarding noncompliance. This rule will help protect academic assessments and connected school systems from software exploits, network attacks, and other incidents related to technology security vulnerabilities. This rule will also help ensure that America's educational technology infrastructure better protects student privacy and facilitates secure data transfer and interoperability.

Action 2: Support Technology Security and Safety Training for Schools

In collaboration with the White House and other partners, OET will lead an initiative to support technology security training to schools. This initiative will highlight security as the first step toward increasing digital safety for students. It will also include a focus on commitments from the field to fully invite industry and nonprofits to commit to acting as champions for this effort.

Action 3: Offer Educational Technology Publishers the Opportunity to Certify the Security of their Technology: The Educational Technology Voluntary Self-Certification Process

OET has the statutory responsibility to review programs supported by ED in relation to technology.[4] Under this authority, OET will accept voluntary applications for Educational

[3] U.S. Department of Education, Fiscal Year 2021 Budget Summary, https://www2.ed.gov/about/overview/budget/budget21/summary/21summary.pdf.
[4] GovInfo. 20 U.S. Code § 3425 – Office of Educational Technology. https://www.govinfo.gov/app/details/USCODE-2010-title20/USCODE-2010-title20-chap48-subchapII-sec3425.a

Technology Certifications (ETCs) from technology publishers, nonprofits, and other organizations. Technologies that receive ETCs will be certified to have met all security requirements under the SET rule for a period of one year, or sooner if there has been a major revision to the core technology. The expedited certification process will include a one-page application and will identify the technology's compliance with technology security standards. OET will adopt standards set by industry, nonprofit, and state groups. OET will collect fees through the ETC process to fund the review of applications.

Action 4: Support Schools in More Quickly and Safely Adopting Technologies: The Educational Technology Registry (ETR)

All technologies with an active ETC certificate will be indexed and searchable on the Educational Technology Registry (ETR) website, a public online registry coordinated by OET. The Registry will make it easy and fast for schools to adopt new educational technologies and will support the growth of the educational technology market. This will encourage greater adoption of ed tech and greater trust in the ed tech market. This registry will include the name and publisher of the technology, the status of their certification, and relevant metadata submitted by the publisher. Listings on the ETR will also denote whether the technology has been evaluated by the ED's What Works Clearinghouse, or comparable efficacy studies. Access to data from the Registry will be made available through an open API, allowing other software to access and leverage the ETR's data.

Action 5: Support Industry in Developing a Robust and Trusted Ed Tech Market

In collaboration with the White House Office of Science and Technology Policy, OET will work closely with industry to support their efforts to provide secure technologies to schools and train school personnel. OET will also collaborate with industry on the creation of the ETR and the development of a responsible and secure educational technology market. Dedicated educational technology liaisons at the White House and OET will act as trusted guides for industry on matters relating to federal educational technology requirements.

Frequently Asked Questions

School Self-Assessments

What process will be required for school self -assessments?

The annual school self-assessment process will be conducted internally at each school under guidance provided by ED. Schools will be asked to maintain a list of certified technologies in use, security configurations, security trainings, and relevant staffing. This data need not be reported to the ED, only recorded and kept on file at the school.

What technologies will be considered secure?

All technologies listed in the Educational Technology Registry (ETR) will be considered secure for the purposes of the self-assessment. If a school is using a technology that has not received an Educational Technology Certificate (ETC), they must submit a justification document for that specific technology to the Department of Education that includes the relevant security standards in use, the technology's scope of use, connection to testing systems, and other considerations.

How will schools find new secure technologies to adopt?

The ETR will provide a trusted source for identifying secure educational technologies.

How will the Securing Educational Technology (SET) policies be enforced at the K-12 level?

ED's Office of Educational Technology (OET) will provide guidance on SET policies. OET will also receive and investigate concerns and complaints related to security in schools. The goal of the complaint process will be to support schools' compliance with security requirements. Similar to FERPA, violations may trigger consequences such as liability to third party actors or loss of federal funding. Schools found not to be in compliance with security standards will be indexed and searchable by the public.

Voluntary Technology Self-Certifications

What are the benefits of the certification process?

Certified technologies will be listed in the Educational Technology Registry (ETR), a trusted source for schools to identify school-appropriate technology. Schools will be able to rely on these baseline security certifications. This will reduce costs and increase trust between schools and technology providers.

How long is the self-certification process?

Organizations submitting a technology to be certified can expect an expedited online application of approximately one page. This application will collect, at a minimum, the name of the technology and the approved security standard(s) with which it aligns. Organizations may also provide optional metadata to make the technology more discoverable by schools in the ETR.

What security standards are approved?

ED will work with states, industry groups, and nonprofits each year to develop a continually updated list of approved security standards. ED will also encourage and support existing nonprofits to continue developing appropriate standards.

How will the Department of Education ensure that organizations do not provide false information on ETC applications?

It is a felony to make false statements to the Federal Government in connection with a federal matter, including on federal forms. OET may request additional information from organizations submitting certification applications to verify the veracity of the information provided. If an organization is found to have provided misleading information, the organization will be flagged in the ETR to encourage schools to exercise additional caution when considering their technology.

What information will be searchable in the ETR?

Required information—including the name, type, and description of the technology, as well as its aligned security standards—will be searchable for all technologies. Additionally, optional searchable metadata will include privacy, interoperability, licensing, and educational standards with which the technology is aligned, as well as accessibility and efficacy information.

Supporting the Ed Tech Marketplace

How will this policy program develop a more secure ed tech marketplace?

Schools face two immediate challenges when adopting ed tech: finding a relevant technology solution and identifying whether that technology is safe. This policy addresses both challenges. The ETR will assemble a trusted group of certified technologies for schools searching for new technology solutions. The certification process, registry listings, school training programs, and industry outreach program will support schools in understanding security in technology.

Will this process support organizations creating new ed tech?

The ETC process will be simple and quick for ed tech organizations whose technologies already align to industry-wide security standards. This process will support those organizations in gaining visibility and trust from schools. Technologies that have not been created in alignment with security standards (including some technologies created by schools and districts) must improve their security before being certified. This process will provide guidance and support to those organizations in creating more secure ed tech.

Will this impact experimental or test versions of ed tech?

A safe harbor provision will allow schools to test non-certified ed tech in schools in accordance with size and impact limitations.

Additional Questions

How will this policy program increase security for assessments?

This policy program -- including its requirements, support, and guidance -- will reduce security and privacy vulnerabilities in networked school systems that may impact state assessments. Consistent and comprehensive school-focused security standards will reduce the prevalence and impact of malicious attacks, harmful data exposure, and systemwide outages that currently impact K12 systems.

What is the rollout process for this policy program?

A two-year rollout process is envisioned for this set of policies. The first year will include an opt-in process for a cohort of schools and targeted industry groups. The second year will include an opt-in process for all schools and open the ETC and ETR programs to all educational technology organizations. The third year will begin mandatory self-assessment requirements for all schools.

Are these requirements best enacted at the federal level?

Most online ed tech are inherently interstate and require a coordinated, national approach to security. For states that have already established sufficient security standards in ed tech, those standards will qualify when listed on ETC applications.

Does this policy program cover student privacy/data interoperability as well?

Security is a prerequisite for privacy. This policy program is foundational in the creation of an educational technology landscape that supports robust student privacy and data interoperability in the future, along with broader federal and ED priorities.

About the Author

Grace Collins is the CEO and founder of games and education research firm Liminal Esports and Snowbright Studio, a game and educational tech development studio. Previously, Grace led game-based education policy for the U.S. Department of Education and coordinated the Federal Games Working Group across the executive branch under the Obama and Trump administrations. Grace is a former educator and was recognized for their work as an educator with a 2020 Educator Award from the National Center for Women & Information Technology and for their advocacy work as a finalist for the 2020 international "Breakthrough of the Year" award in Digital Education from the Falling Walls Foundation. Grace is also an outspoken LGBTQ+ and gender equity advocate who served as a 2019 LGBTQIA+ Fellow for the Union for Reform Judaism. Grace holds two undergraduate degrees in Computer Science fields and a Juris Doctor from Washington & Lee University. The author gives special thanks to the students from Hathaway Brown School for their guidance in supporting the proposal.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of a future presidential term. For more about the Day One Project, visit dayoneproject.org.