CENTER FOR DEMOCRACY & TECHNOLOGY

Comments of the Center for Democracy & Technology
Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022
Docket ID No. CISA-2022-0010
November 14, 2022

The Center for Democracy & Technology (CDT) applauds the work of the Cybersecurity and Infrastructure Security Agency (CISA) to protect critical infrastructure from cyber attacks and to solicit[1] public feedback on the implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022.[2] CDT is a 27-year old 501(c)(3) nonpartisan nonprofit organization that fights to put democracy and human rights at the center of the digital revolution. It works to promote democratic values by shaping technology policy and architecture, with a focus on equity and justice.

CDT respectfully submits these comments to highlight the implications of CIRCIA for K-12 schools and other educational institutions such as state educational agencies. K-12 schools have increasingly been victimized by malicious cyber actors through ransomware and other attacks, which have disrupted critical educational services and put students and their personal information at risk. Although the threat to schools is clear, we lack a systematic understanding of its scope at least in part because of the distributed, diverse nature of the K-12 education sector, with more than 13,000 school districts,[3] ranging from a few hundred students to over a million,[4] and data systems spanning across jurisdictions and both private and public entities. Establishing cyber incident reporting requirements will help families, school leaders, and policymakers gain a better understanding of the sector's needs. That reporting will also enable CISA and others to provide the sector with early warnings and guidance about cyber threats as CIRCIA envisions — information that is particularly valuable in this sector, in which schools and other institutions often lack the expertise and resources to engage in cyber threat monitoring or obtain cyber threat intelligence.

To secure these benefits, CISA should:

- include K-12 schools, related educational institutions, and their private contractors in CIRCIA's reporting obligations.
- adopt rules that account for the distributed nature of K-12 data systems.
- coordinate with the U.S. Department of Education to ensure K-12 schools and other educational institutions have the resources they need to meet their reporting obligations.

---

[1] *Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022*, 87 Fed. Reg. 55833 (Sept. 12, 2022).
[2] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-35, div. Y, 136 Stat. 49, 1038 (2022) (codified at 6 U.S.C. § 681–681g).
[3] National Center for Education Statistics, U.S. Department of Education, Digest of Education Statistics tbl. 214.10 (2020), *available at* https://nces.ed.gov/programs/digest/d20/tables/dt20_214.10.asp?current=yes.
[4] *Id.* tbl. 214.20, *available at* https://nces.ed.gov/programs/digest/d21/tables/dt21_214.20.asp?current=yes; *DOE Data at a Glance*, NYC Department of Education, https://www.schools.nyc.gov/about-us/reports/doe-data-at-a-glance (last visited Nov. 10, 2022) ("In 2021-22, there were 1,058,888 students in the NYC school system, the largest school district in the United States.").

1401 K Street NW, Suite 200 Washington, DC 20005

CENTER FOR DEMOCRACY & TECHNOLOGY

I. Include K-12 Schools, Other Educational Institutions, and Their Private Contractors in CIRCIA's Reporting Obligations

Public K-12 schools and related educational institutions such as state educational agencies provide critical services to the public, and the Department of Homeland Security (the Department) has long recognized their importance as "critical infrastructure." In implementing CIRCIA, CISA should (A) continue to recognize K-12 schools, related educational institutions, and their private contractors as critical infrastructure subject to CIRCIA's requirements, and (B) define "substantial cyber incident" to encompass the serious cyber attacks that are increasingly threatening the K-12 sector.

A. Recognize K-12 Schools, Related Educational Institutions, and Their Contractors as Critical Infrastructure Subject to CIRCIA

Public and private K-12 schools, related educational institutions such as state educational agencies,[5] and their contractors should be deemed "covered entities" subject to CIRCIA. CIRCIA applies to "covered entities" engaged in a "critical infrastructure sector," as defined by Presidential Policy Direct 21 (PPD-21).[6] PPD-21 defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, [or] national public health or safety."[7]

The Department has long recognized that schools are critical infrastructure. K-12 schools were included as "critical infrastructure" in the Department's 2009 National Infrastructure Protection Plan (NIPP), with the U.S. Department of Education serving as the Sector-Specific Agency for the Education Facilities Subsector.[8] The Department of Homeland Security elaborated on its position the next year when it published a Sector-Specific Plan for the Education Facilities Subsector.[9] The Subsector Plan noted that although "cyber elements may play a smaller role in the subsector than in other sectors," cyber

[5] As described elsewhere in these comments, data systems in the education sector are complex; education data is maintained at the local, state, and federal levels of government, in databases that span across school districts and states, and on services provided by private contractors. The scope of "related educational institutions" should be broadly defined to encompass the full panoply of entities responsible for maintaining educational data.
[6] 6 U.S.C. § 681(5).
[7] Executive Office of the President, Presidential Policy Directive 21 — Critical Infrastructure Security and Resilience (2013), *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[8] U.S. Department of Homeland Security, National Infrastructure Protection Plan 3 n.h, 8, 9 n.3 (2009), *available at* https://www.cisa.gov/publication/nipp-2009-partnering-enhance-protection-resiliency.
[9] U.S. Department of Homeland Security & U.S. Department of Education, Education Facilities Sector-Specific Plan (2010), *available at* https://www.dhs.gov/xlibrary/assets/nipp-ssp-education-facilities-2010.pdf.

remained an important concern given "the increasing use of online student information management systems" and large databases of students' and staff's personal, educational, health, and financial information[10] — a trend that has only accelerated across K-12 schools since 2010.

The latest version of the NIPP, published in 2013 following PPD-21, continues to recognized education facilities as critical infrastructure,[11] and the 2015 Government Facilities Sector Plan interpreted PPD-21 as specifically identifying schools and education facilities as critical infrastructure.[12] CISA's implementation of CIRCIA should align with the Department's longstanding recognition of education facilities as critical infrastructure requiring heightened attention regarding cyber incidents.

Moreover, education facilities also satisfy the criteria for being covered entities under CIRCIA. The statute requires CISA to consider three factors in describing "the types of entities that constitute covered entities":[13]

- the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;
- the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and,
- the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure.

Each of those factors supports a finding that K-12 schools, related educational institutions, and their contractors are covered entities.

1. *Consequences of Disruption or Compromise to National Security, Economic Security, or Public Health or Safety*

The Department's classification of K-12 schools as critical infrastructure reflects the important role they play in protecting national security, economic security, and public health and safety. The pandemic

[10] *Id.* at 7–8.
[11] U.S. Department of Homeland Security, National Infrastructure Protection Plan 43 (2013), *available at* https://www.cisa.gov/national-infrastructure-protection-plan.
[12] U.S. Department of Homeland Security, Government Facilities Sector-Specific Plan ii (2015), *available at* https://www.cisa.gov/publication/nipp-ssp-government-facilities-2015 ("PPD-21 further designated that [] the Education Facilities Subsector, which covers schools, institutions of higher education, and trade schools, with the Department of Education as the Sector-Specific Agency . . . be included as part of the Government Facilities Sector.").
[13] 6 U.S.C. § 681b(c)(1)(A)–(C).

reaffirmed the necessity of providing reliable educational services to students for their continued educational and social development. Congress and the Administration recognized the critical nature of K-12 schools during the course of the pandemic, undertaking unprecedented efforts to ensure that students could continue receiving educational services, even during the height of quarantine orders.[14]

Despite those efforts, and their many successes, disruptions to K-12 schools proved consequential for students and families. In addition, the pandemic disrupted adjacent services provided by schools to support students and families, including nutrition,[15] healthcare, counseling, and mental health supports.[16] The disruption of the education sector had spillover effects into the workforce, as parents struggled to balance work obligations with childcare and newly imposed responsibilities for managing their children's remote learning.[17] Moreover, as discussed below, cyber incidents affecting the educational sector can also result in the theft of personal information affecting millions of people, causing economic harm. All told, significant disruptions of K-12 schools — whether due to a public health emergency or a cyber incident — have debilitating impacts on children, families, and the workforce.

2. Likelihood of Targeting, Including by a Foreign Country

Attacks targeting K-12 schools, related educational institutions, and their private contractors are not just likely to occur, but are occurring and increasing in both number and severity.[18] One K-12 cybersecurity researcher has found that publicly reported incidents increased from less than 100 in

[14] *E.g.*, American Rescue Plan Act of 2021, Pub. L. No. 117-7, tit. VII, sec. 7402, 1345 Stat. 3, 109 (2021) (Emergency Connectivity Fund); *id.*, Pub. L. No. 117-7, tit. II, sec. 2001, 1345 Stat. 3, 19 (Elementary and Secondary School Emergency Relief Fund III); Coronavirus Response and Relief Supplemental Appropriations Act, Pub. L. No. 116-260, tit. III, sec. 313, 134 Stat. 1182, 1929 (2020) (ESSER II); Coronavirus Aid, Relief, and Economic Security (CARES) Act, Pub. L. No. 116-136, div. B, title VIII, sec. 18003, 134 Stat. 281, 565 (2020) (ESSER I).

[15] Cory Turner, *'Children Are Going Hungry': Why Schools Are Struggling to Feed Students*, NPR (Sept. 8, 2020), https://www.npr.org/2020/09/08/908442609/children-are-going-hungry-why-schools-are-struggling-to-feed-students.

[16] *Telehealth: Virtual Service Delivery Updated Recommendations*, National Association of School Psychologists, https://www.nasponline.org/resources-and-publications/resources-and-podcasts/covid-19-resource-center/special-education-resources/telehealth-virtual-service-delivery-updated-recommendations (last visited Oct. 27, 2022); Tim Walker, *Student Trauma Won't Just Disappear In the Fall, Counselors Warn*, neaToday (May 20, 2020), http://neatoday.org/2020/05/20/student-trauma-wont-just-disappear-when-schools-reopen.

[17] *E.g.*, Laura Howells, *'Felt Like Crying': Parents and Teacher Struggle to Balance Work and Online School*, CBC (Jan. 9, 2021), https://www.cbc.ca/news/canada/hamilton/ontario-online-learning-january-1.5862211; Ashley Stahl, *Struggles For Working Parents Are Likely to Remain Post-Pandemic*, Forbes (Apr. 2, 2021), https://www.forbes.com/sites/ashleystahl/2021/04/02/struggles-for-working-parents-are-likely-to-remain-post-pandemic; *The Impact of Covid-19 on Working Parents*, Catalyst (Sept. 29, 2020), https://www.catalyst.org/research/impact-covid-working-parents.

[18] K12 SIX, State of K-12 Cybersecurity 3 (2022), *available at* https://www.k12six.org/the-report.

2016 to more than 300 in 2019 and more than 400 in 2020.[19] And publicly reported incidents no doubt are only a subset of the total number of incidents. Although the number of incidents decreased with schools returning to in-person learning in 2021,[20] high-profile incidents targeted at large school districts and large contractors have continued to affect millions of students.[21] Schools have also been targeted by foreign actors, as demonstrated by the recent release of 500 GB of data stolen from Los Angeles Unified School District by the Russian-speaking "ransomware gang" Vice Society.[22]

3. Likelihood of Disruption of Critical Infrastructure

Because the education sector relies heavily on information systems and data, successful cyber attacks are highly likely to disrupt the operation of schools. As one cybersecurity researcher observed, "[S]chool systems rely on a disproportionately large number of IT assets and systems, are responsible for managing significant quantities of personally identifiable student and educator data, and face significant risks to public confidence should they experience a cybersecurity incident."[23] Consequently, cyber incidents in the education sector directly impact educational services, resulting in lost learning time ranging "from 3 days to 3 weeks."[24]

Those incidents affect far more than academic records such as grades or test results; the Government Accountability Office reports that cyber incidents have compromised students' names, birthdates, Social Security numbers, medical records, counseling records, insurance information, schedules, gender, race, and housing status.[25] Other education databases might include a student's eligibility for

[19] K12 SIX, State of K-12 Cybersecurity 1 (2021), *available at* https://www.k12six.org/the-report.
[20] K12 SIX, State of K-12 Cybersecurity 3 (2022), *available at* https://www.k12six.org/the-report.
[21] Howard Blume & Alejandra Reyes-Velarde, *Student Information Remains at Risk After Massive Cyberattack on Los Angeles Unified*, Los Angeles Times (Sept. 7, 2022), https://www.latimes.com/california/story/2022-09-07/ los-angeles-unified-schools-cyberattack; Mark Keierleber, *After Huge Illuminate Data Breach, Ed Tech's 'Student Privacy Pledge' Under Fire*, The 74 (July 24, 2022), https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-techs-student-privacy-pledge-under-fire.
[22] Joshua Bay, *LA Parents Sound Off After Cyberattack Leaves Students Vulnerable*, The 74 (Oct. 7, 2022), https://www.the74million.org/article/la-parents-sound-off-after-cyberattack- leaves-students-vulnerable.
[23] K12 SIX, Cybersecurity Frameworks: What K-12 Leaders Need to Know 3–4 (2022), *available at* https://www.k12six.org/news/k12-six-and-setda-collaborate-to-promote-cybersecurity-best-practices-for-school-districts.
[24] U.S. Government Accountability Office, Critical Infrastructure: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity 13–14 (2022), *available at* https://www.gao.gov/products/gao-23-105480.
[25] U.S. Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 12 (2020), *available at* https://www.gao.gov/products/gao-20-644.

free or reduced price meals,[26] migrant status,[27] and languages spoken by the student and at home.[28] Further, as described above, disruption of K-12 data systems can also have spillover effects in nutrition, health care, and the workforce. The incapacity or destruction of education data systems can have a debilitating impact on the security, economic security, health, and safety of students, families, and school employees.

* * *

K-12 schools satisfy the three factors enumerated in CIRCIA for identifying critical infrastructure. However, because of the complexity of educational data systems, it is important that CISA not limit CIRCIA's reporting obligations to K-12 schools but also include related educational institutions and their private contractors. "Related educational institutions" should include, at minimum, local educational agencies, state educational agencies, the U.S. Department of Education, and databases of students' personal information that they maintain. CIRCIA's reporting obligations should similarly reach contractors, researchers, and other entities that retain students' personal information to provide services to schools — namely entities that receive student data under exceptions to the parental consent requirement of the Family Educational Rights and Privacy Act (FERPA):

- school officials, including contractors and vendors;[29]
- authorized representatives conducting audits or evaluations for certain governmental entities;[30]
- organizations determining eligibility for financial aid;[31]

[26] Food and Nutrition Service, U.S. Department of Agriculture, Eligibility Manual for School Meals 35–42 (2017), *available at* https://www.fns.usda.gov/cn/eligibility-manual-school-meals. Students may be eligible for free or reduced price meals based on enrollment in other assistance programs, and most states have implemented a state-level system that automatically matches students with children enrolled in assistance programs based on information in state-level student information systems. *See, e.g.*, Wisconsin Department of Public Instruction, DC User Guide 5 (2021), *available at* https://dpi.wi.gov/school-nutrition/program-requirements/direct-certification; New York State Education Department, NYSIS State Match System User Guide 3–6 (2018), *available at* http://www.cn.nysed.gov/file/nyssis-state-match-system-user-guide.

[27] States are required to upload federally prescribed "minimum data elements" on migrant students to a centralized database known as the Migrant Student Information Exchange, maintained by Deloitte Consulting and Amazon Web Services on behalf of the U.S. Department of Education. System of Records Notice, 84 Fed. Reg. 32895, 32897 (July 10, 2019); U.S. Department of Education, Privacy Impact Assessment (PIA) for Migrant Student Information Exchange 8 (2021), *available at* https://www2.ed.gov/notices/pia/index.html.

[28] Office of English Language Acquisition, U.S. Department of Education, English Learner Toolkit ch. 1, at 4 (2017), *available at* https://ncela.ed.gov/english-learner-toolkit.

[29] 34 C.F.R. § 99.31(a)(1).

[30] 34 C.F.R. § 99.31(a)(3).

[31] 34 C.F.R. § 99.31(a)(4).

- organizations conducting studies;[32] and,
- accrediting organizations.[33]

Including these entities as critical infrastructure will help ensure that cyber incidents are reported, no matter where students' data is shared.

B. Many Cyber Incidents in the K-12 Sector Qualify as "Substantial Cyber Incidents" Subject to CIRCIA

Many cyber incidents in the education sector qualify as "significant cyber incidents" subject to CIRCIA's requirements, as demonstrated by the escalating series of attacks on schools and their contractors over recent years.

CIRCIA defines both an "incident" and a "cyber incident" by incorporating[34] the existing definition of "incident."[35] The existing definition is an "occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system."[36] CIRCIA, however, limits the scope of that definition, including only occurrences that "actually" threaten information or an information system.[37] CIRCIA requires CISA to consider two groups of factors in describing "the types of substantial cyber incidents that constitute covered cyber incidents":[38]

- "at minimum," the occurrence of (i) a cyber incident that results in the "substantial loss of confidentiality, integrity, or availability" of an information system, (ii) "a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability" against an information system or network; or (iii) "unauthorized access or disruption of business or industrial operations due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise"; and,

[32] 34 C.F.R. § 99.31(a)(6).
[33] 34 C.F.R. § 99.31(a)(7). FERPA's remaining exceptions to parental consent apply to disclosures of students' personal information to other schools, *id.* § 99.31(a)(2), which would be covered by CIRCIA, or to entities outside the school system, *id.* § 99.31(a)(5), (8)–(16), which are beyond the scope of these comments.
[34] 6 U.S.C. § 681(6), (9).
[35] 6 U.S.C. § 659(a)(5).
[36] *Id.*
[37] 6 U.S.C. § 681(6)(B).
[38] 6 U.S.C. § 681b(c)(2)(A).

- consideration of "the sophistication or novelty of the tactics used, as well as the type, volume, and sensitivity of the data at issue," "the number of individuals directly or indirectly affected or potentially affected," and "potential impacts on industrial control systems."

Sufficiently severe cyber incidents in the education sector meet that definition and should be subject to CIRCIA's requirements.

1. *Substantial Loss of Confidentiality, Integrity, or Availability of an Information System, Disruption of Operations, or Unauthorized Access*

Cyber incidents affecting K-12 schools can result in a loss of confidentiality and the availability of information systems, disruptions to the sector's operations, and unauthorized access.

K-12 cyber incidents have exposed confidential information of millions of individuals. For example, one edtech vendor suffered a cyber incident that resulted in the disclosure of 3 million current and former students' information,[39] including 820,000 in New York City alone.[40] That loss of confidentiality extends beyond academic data, putting students', families', and employees' financial and physical wellbeing at risk. As the Government Accountability Office has described, student data "can be sold on the black market and can cause significant financial harm to students who typically have clean credit histories and often do not inquire about their financial status until adulthood."[41] One breach included the personal information of students who completed surveys on bullying, and another included students' phone numbers, which "were used to send text messages that threatened physical violence."[42]

Incidents can also disrupt operations in the sector, resulting in lost learning time ranging from a few days to several weeks.[43] Ransomware attacks, for example, may result in canceled classes or even district-wide closures; one Missouri school district resorted to closing down its IT systems and internet

[39] Mark Keierleber, *After Huge Illuminate Data Breach, Ed Tech's 'Student Privacy Pledge' Under Fire*, The 74 (July 24, 2022), https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-techs-student-privacy-pledge-under-fire.
[40] Ashlyn Eperjesi, *The Top Data Breaches of 2022 So Far*, Security Boulevard (Nov. 3, 2022), https://securityboulevard.com/2022/11/the-top-data-breaches-of-2022-so-far.
[41] U.S. Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 13 (2020), *available at* https://www.gao.gov/products/gao-20-644.
[42] *Id.*
[43] U.S. Government Accountability Office, Critical Infrastructure: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity 13–14 (2022), *available at* https://www.gao.gov/products/gao-23-105480.

altogether to address a ransomware attack.[44] Another district was forced to use "activity packets" after an incident left its ordinary systems inaccessible.[45]

2. *Sophistication of Tactics, Volume and Sensitivity of Data, Number of Individuals Affected, and Impacts on Industrial Control Systems*

Cyber incidents affecting K-12 systems are employing increasingly sophisticated tactics. While ransomware attacks once constituted only nine percent of publicly reported cyber incidents in the K-12 education sector,[46] they were the most common type of publicly reported cyber incident in 2021.[47] Moreover, ransomware attackers have increasingly started leveraging "double extortion" tactics by demanding payments both to decrypt school networks and to *not* release the victims' data.[48] CISA and the Federal Bureau of Investigation warned schools that ransomware attackers may be expressly targeting the "data-rich environment of student information in schools and education technology (edtech) services."[49] As described above, the data rich environments include not just academic information, but also birthdates, Social Security numbers, medical records, counseling records, insurance information, schedules, gender, race, housing status, socioeconomic status, migrant status, and language spoken at home.[50]

In addition to increasing sophistication, cyber attacks on schools are also affecting increasing numbers of students. As noted above, one recent incident involved a contractor serving schools in six states, affecting over three million current and former students.[51] Similarly, a recent ransomware attack on Los Angeles Unified School District has resulted in the release of 500 GB of data, including students' personal information, which was posted online when the school district declined to pay a ransom.[52]

---

[44] Karl Wehmhoener, *Eldon School District Canceled Classes Tuesday due to Ransomware Attack*, ABC 17 (Dec. 7, 2021), https://abc17news.com/news/2021/12/07/eldon-school-district-cancels-classes-due-to-ransomware.
[45] Rob Manning, *Instruction Halted as East Multnomah Co. School District Suffers Apparent Cyberattack*, OPB (Apr. 24, 2021), https://www.opb.org/article/2021/04/27/instruction-halted-as-east-multnomah-co-school-district-suffers-apparent-cyberattack.
[46] K12 SIX, State of K-12 Cybersecurity 6 (2019), *available at* https://www.k12six.org/the-report.
[47] K12 SIX, State of K-12 Cybersecurity 7 (2022), *available at* https://www.k12six.org/the-report.
[48] K12 SIX, State of K-12 Cybersecurity 9 (2022), *available at* https://www.k12six.org/the-report.
[49] CISA & FBI, *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data*, CISA.gov (Dec. 10, 2020), https://www.cisa.gov/uscert/ncas/alerts/aa20-345a.
[50] U.S. Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 12 (2020), *available at* https://www.gao.gov/products/gao-20-644.
[51] Mark Keierleber, *After Huge Illuminate Data Breach, Ed Tech's 'Student Privacy Pledge' Under Fire*, The 74 (July 24, 2022), https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-techs-student-privacy-pledge-under-fire.
[52] Howard Blume & Alejandra Reyes-Velarde, *Student Information Remains at Risk After Massive Cyberattack on Los Angeles Unified*, Los Angeles Times (Sept. 7, 2022), https://www.latimes.com/california/story/2022-09-07/ los-angeles-unified-

Finally, cyber incidents strain the resources of schools. For example, a ransomware attack on a Texas school district cost more than a half million dollars to mitigate, and attacks in Baltimore and Buffalo cost in excess of $9 million each.[53]

* * *

CISA should ensure that CIRCIA applies to such significant incidents. At minimum, CISA should ensure that its definition of a "substantial" cyber incident encompasses occurrences that disrupt the provision of educational services or jeopardize significant numbers of students' privacy or safety. Several states have passed legislation regarding cyber incident reporting or data breach notifications, and CISA may look to those laws as models for the scope of "substantial":

- Some state cyber incident reporting laws focus on the effects of a cyber incident on the provision of governmental services. For example, West Virginia requires reporting of "qualified cyber incidents," which means the "ability of the entity that experienced the incident to conduct business is substantially affected."[54] Similarly, Virginia requires "public bodies" to report incidents "with the potential to cause major disruption to normal activities of the public body."[55]
- Other state laws focus on the number of impacted individuals or students. California's new cyberattack reporting law requires local educational agencies to report any "cyberattack impacting more than 500 pupils or personnel."[56] Florida's general data breach notification law imposes a similar reporting threshold.[57]

CISA could incorporate each of those approaches, defining a "substantial" cyber incident for the education sector as a cyber incident that:

- materially and adversely impacts the delivery of educational or related services; or,

---

schools-cyberattack; Joshua Bay, *LA Parents Sound Off After Cyberattack Leaves Students Vulnerable*, The 74 (Oct. 7, 2022), *https://www.the74million.org/article/la-parents-sound-off-after-cyberattack- leaves-students-vulnerable*.

[53] K12 SIX, State of K-12 Cybersecurity 8 (2022), *available at* https://www.k12six.org/the-report; *see also* McKenna Oxenden, *Baltimore County Schools Suffered a Ransomware Attack. Here's What You Need to Know*, Baltimore Sun (Nov. 30, 2020), https://www.baltimoresun.com/maryland/baltimore-county/bs-md-co-what-to-know-schools-ransomware-attack-20201130-2j3ws6yffzcrrkfzzf3m43zxma-story.html.

[54] W. Va. Code § 5A-6C-3(b)(2).

[55] Va. Code Ann. § 2.2-5514(C).

[56] Cal. Code Educ. § 35265.

[57] Fla. Stat. § 501.171(3)(a).

- otherwise impacts 500 or more students or staff members, or the entire student body of a school, whichever is less,[58] such as due to the unauthorized disclosure of students' or staff members' personal information.[59]

These two prongs encompass the considerations required by CIRCIA: the substantial loss of the confidentiality, integrity, or availability of information systems, a disruption to operations, unauthorized access, and the number of individuals affected.

CISA should avoid adopting definitions of a "substantial" cyber incident that are premised on the costs to harmed individuals or costs to remediate the incident. The costs of a breach may be difficult to ascertain with any degree of certainty until weeks or months after the breach, potentially delaying reporting.

* * *

Ensuring that CIRCIA's reporting requirements apply to the escalating cyber attacks on schools will provide important protections to students, families, and school staff. Doing so will also ensure that K-12 schools are on the same accountability footing as other operators of critical infrastructure. Laws regarding data, privacy, and cybersecurity in the education sector often lack a cyber incident or data breach reporting requirement, especially as applied to K-12 schools.[60] FERPA, for example, only requires educational institutions to record unauthorized disclosures in students' education records; it does not require notice to be provided directly to students and families.[61] The Children's Online Privacy Protection Act similarly lacks a cyber incident reporting requirement.[62] Consequently, there is no unified or consistent reporting of K-12 cyber incidents, and reporters have found that schools and districts often fail to report incidents, sometimes intentionally obfuscating that an incident has occurred.[63] The lack of reliable data on cyber incidents in K-12 education makes it difficult for

[58] Cal. Code Educ. § 35265; Fla. Stat. § 501.171(3)(a).
[59] *See* Cal. Civ. Code §§ 1798.29(a), (f), 1798.82(a), (g); N.Y. Gen. Bus. Law § 899-aa(2); N.Y. State Tech. § 208(2); Tex. Bus. Orgs. Code Ann. § 521.053(a), (b). CIRCIA requires CISA to exclude "any event where the cyber incident is perpetrated in good faith" from the scope of substantial cyber events requiring reporting. 6 U.S.C. § 681(c)(2(C)(i).
[60] K12 SIX, State of K-12 Cybersecurity 5 (2022), *available at* https://www.k12six.org/the-report.
[61] 73 Fed. Reg. 74805, 74843 (Dec. 9, 2008).
[62] *Cf.* 16 C.F.R. § 312.8 (requiring "reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children," without reference to cyber incidents or reporting requirements).
[63] Scott Travis, *Investigation: Broward Schools Took Extraordinary Steps to Hide Key Details of Massive Data Breach*, South Florida Sun-Sentinel (Feb. 17, 2022), https://www.sun-sentinel.com/news/education/fl-ne-broward-schools-hacker-investigation-report-20220217-6jy2t5rzrzbjxn63oyq5wwuyb4-story.html; Julie Watts, *Schools Aren't Required to Report Increasing Cyber Attacks: Kids at Risk, Parents in The Dark*, CBS Sacramento (Sept. 29, 2021), https://www.cbsnews.com/sacramento/news/school-report-increasing-cyber-attacks-kids-risk-parents; Brian New, *Has Your Kid's Texas School District Been Hammered By Cyberattacks? I-Team Investigation*, CBS DFW (Aug. 16, 2021),

policymakers, schools, students, and families to make informed decisions regarding cybersecurity and technology use.[64] CIRCIA would help fill that gap and provide valuable information to students, families, school leaders, and policymakers.

II. Adopt Rules that Account for the Distributed Nature of the K-12 School System

CISA should ensure that CIRCIA's reporting rules account for schools' complex data structures that span private and public entities, include multiple layers of government, and cross jurisdictional lines, as well as schools' relatively limited resources.

Private contractors play an important role in maintaining educational data. For example, at the school district level, many school information technology (IT) services are contracted to "off-premises" third party contractors, such as cloud computing, telecommunications, remote learning systems, or student information systems. Those privately maintained systems have increasingly become the target of cyberattacks,[65] and attacks against them can affect multiple school districts and "thousands of students" simultaneously.[66] One recent high-profile breach involved attacks on a private contractor that served districts in six states, affecting millions of students.[67]

Further, educational data is often maintained by government agencies other than schools or school districts. Many state educational agencies maintain statewide longitudinal databases that track students from preschool through postsecondary education, and sometimes into graduate school or the workforce.[68] Other databases may span across levels of government; for example, the Migrant Student Information Exchange (MSIX) is maintained by a contractor for the U.S. Department of Education and is composed of data submitted to state level databases that are then linked with MSIX.[69] Similarly,

---

https://www.cbsnews.com/dfw/news/dozens-texas-school-districts-hammered-cyberatacks- ransomware ("Mesquite ISD and Fort Worth ISD did not report their recent ransomware attacks to the Texas Education Agency.").

[64] U.S. Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 2 (2020), *available at* https://www.gao.gov/products/gao-20-644 (noting that comprehensive data on cyber incidents at K-12 schools had to be determined from public reports and that incidents were likely under-reported).

[65] K12 SIX, State of K-12 Cybersecurity 10 (2022), *available at* https://www.k12six.org/the-report.

[66] U.S. Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 17 (2020), *available at* https://www.gao.gov/products/gao-20-644.

[67] Mark Keierleber, *After Huge Illuminate Data Breach, Ed Tech's 'Student Privacy Pledge' Under Fire*, The 74 (July 24, 2022), https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-techs-student-privacy-pledge-under-fire.

[68] 76 Fed. Reg. 75603, 75609–10 (Dec. 2, 2011); *From Education to Workforce*, Data Quality Campaign, https://dataqualitycampaign.org/our-work/policy-areas/from-education-to-workforce (last visited Oct. 27, 2022).

[69] System of Records Notice, 84 Fed. Reg. 32895, 32897 (July 10, 2019); U.S. Department of Education, Privacy Impact Assessment (PIA) for Migrant Student Information Exchange 8 (2021), *available at* https://www2.ed.gov/notices/pia/index.html.

researchers[70] and nonprofit community organizations[71] may also maintain student data. These are important databases and critical infrastructure for providing students with key services, but schools or school districts would not be well positioned to report cyber incidents that affect them.

The complexities of policing this structure — spanning private and public entities and multiple levels of government — can be compounded by schools' relatively limited resources. Many school districts do not have dedicated privacy or cybersecurity personnel; even schools or districts that do have privacy and cybersecurity personnel may assign them multiple responsibilities or share them among multiple entities.[72] Further, school district IT leaders noted in interviews with CDT that while they seek to hold contractors accountable for cybersecurity through contractual mechanisms, they often lack the resources to audit or monitor contractors' compliance with those contractual requirements.[73]

CISA can adopt rules that account for the distributed nature of the K-12 school system by ensuring that reporting obligations are not imposed solely on schools or school districts, but the entities best positioned to detect and report the incident. To help provide this flexibility, CISA should consider:

- assigning reporting obligations by default to the party maintaining the IT systems subject to a reportable cyber incident, including third party contractors providing services to schools; and,
- permitting K-12 schools, related educational institutions, and contractors to contractually assign responsibility and establish procedures for filing reports under CIRCIA.

III. Coordinate with the U.S. Department of Education to Ensure K-12 Schools and Other Educational Institutions Have Necessary Resources to Meet Their Reporting Obligations

Finally, CISA should coordinate closely with the U.S. Department of Education in developing the cyber incident reporting requirements for the education sector. K-12 institutions have traditionally turned to the Department of Education for guidance on privacy and security, with resources provided by its Student Privacy Policy Office, Privacy Technical Assistance Center, and its Readiness and Emergency

[70] *See* 76 Fed. Reg. 75603, 75615–26 (Dec. 2, 2011) (requirements under FERPA for disclosures to "authorized representatives" of state educational authorities for an audit or evaluation, including outcome data on high school graduates); 73 Fed. Reg. 74805, 74824–29 (Dec. 9, 2008) (requirements under FERPA for studies).
[71] *See* U.S. Department of Education, Data-Sharing Tool Kit for Communities (2016), *available at* https://www2.ed.gov/programs/promiseneighborhoods/datasharingtool.pdf.
[72] Elizabeth Laird, Center for Democracy & Technology, Chief Privacy Officers: Who They Are and Why Education Leaders Need Them 5–6 (2019), *available at* https://cdt.org/insights/chief-privacy-officers-who-they-are-and-why-education-leaders-need-them.
[73] DeVan Hankerson Madrigal et al., Center for Democracy & Technology, Online and Observed 16 (2021), *available at* https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software.

Management for Schools Technical Assistance Center. Moreover, the U.S. Department of Education is the Sector Risk Management Agency for the Education Facilities Subsector, with the role implemented by the Office of Safe and Supportive Schools (OSSS).[74] OSSS is consequently responsible for coordinating not only among federal agencies, but also non-federal stakeholders.

However, the Government Accountability Office has found that a lack of coordination between CISA and the Department of Education has hampered a unified response to K-12 cyber incidents. Thus, CISA should coordinate with ED in publicizing and supporting schools in meeting CIRCIA's reporting requirements.

We applaud CISA and the Department of Homeland Security for their work to protect critical infrastructure, including schools, from cyber attacks. To ensure that students, families, and schools may reap the full benefits of CIRCIA, CISA should ensure that it includes K-12 schools, other educational institutions, and their private contractors in CIRCIA's reporting obligations, provide K-12 schools and other educational institutions with flexibility where possible, and coordinate with the U.S. Department of Education to support schools in meeting their reporting obligations.

Please feel free to contact us if we can support CISA's critical work.

Sincerely,

Elizabeth Laird
Director, Equity in Civic Technology

Cody Venzke
Senior Counsel, Equity in Civic Technology

[74] U.S. Government Accountability Office, Critical Infrastructure: Additional Federal Coordination Is Needed to Enhance K-12 Cybersecurity 6 (2022), *available at* https://www.gao.gov/products/gao-23-105480. The 2015 Government Facilities Sector-Specific Plan identifies OSSS's predecessor, the Office of Safe and Drug Free Schools, as the Sector Risk Management Agency (then known as a Sector-Specific Agency). U.S. Department of Homeland Security, Government Facilities Sector-Specific Plan 10 (2015), *available at* https:// www.cisa.gov/publication/nipp-ssp-government-facilities-2015.