LEADING EDUCATION INNOVATION

State and Federal Education Cybersecurity Policy Developments

2022

(published January 2023)

CoSN's Mission:
CoSN provides current and aspiring K-12 education technology leaders with the community, knowledge and professional development they need to create and grow engaging learning environments.

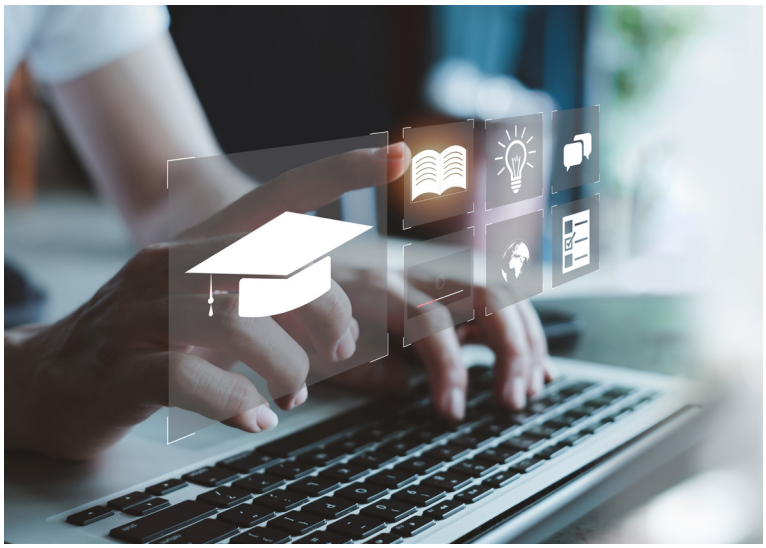
www.cosn.org

For access to this report, please visit www.cosn.org/cybersecurity/2022legislation

This paper was written through funding from the Bill & Melinda Gates Foundation. Views expressed here do not necessarily reflect positions or policies of the foundation.

Introduction

Cyberattacks are among the leading operational and privacy threats facing the nation's schools. Routinely, cyberattacks compromise confidential student and employee information, disrupt classroom instruction and administrative functions, and rob taxpayers. The problem plagues the entire education sector, including schools located in the smallest rural communities and the most sprawling suburban and urban areas. Thus, it was no surprise in September 2022 when the Cybersecurity and Infrastructure Security Agency, again, warned the public and school administrators about the increased risks of ransomware attacks by criminal syndicates targeting kindergarten through twelfth grade schools.[1] A month later, Microsoft Security Intelligence said the education sector continues to be among the industries most affected by malware encounters.[2] Addressing these and other cyber threats will require significant coordination, strong public-private partnerships, and increased government financial and technical assistance, especially for the nation's lowest wealth school districts.



Fortunately, a growing cadre of state and federal policymakers better recognize the serious, and sometimes long term, consequences that cyberattacks can have on students, employees, and schools. The policy response, as measured by bills introduced and laws enacted the past three years, is growing but still insufficient. Government is acting, but many new laws do not address the challenge comprehensively (across all policy needs) or at scale. This year, legislators in 36 states introduced 232 cybersecurity bills with direct or indirect focus on the education sector. CoSN defines a "direct" focus on schools to include bills or new laws that expressly reference schools, school districts, state education agencies or postsecondary entities, while an "indirect" bill or law affects education entities as a component part of state or local government. This year's list of education cybersecurity bills compares to 170 similar bills that were introduced in 2021 and 87 such bills in 2020. At the federal level, legislators introduced 22 cybersecurity bills, including two bills focused on elementary and secondary education and four measures focused on postsecondary institutions. This figure compares to 19 federal bills introduced in 2021 and 10 in 2020.

[1] Cybersecurity & Infrastructure Security Agency. Alert (AA22-249A) #StopRansomware: Vice Society (Sept. 2022). https://www.cisa.gov/uscert/ncas/alerts/aa22-249a

[2] Microsoft Security Intelligence. Global Threat Activity: Most Affected Industries. https://www.microsoft.com/en-us/wdsi/threats (last visited October, 2022)

This year's report inventories the 2022 state and federal education cybersecurity bills and laws that were introduced or adopted. It also highlights policy ideas and trends, with the goal of helping education technology leaders, school administrators, and policymakers identify promising models and strategies. Many resources for school systems can be found at cosn.org/cybersecurity. CoSN encourages leaders tasked with making cybersecurity policy improvements in 2023 to consider the following ideas drawn from our analysis of the changing state policy landscape:

- **Cybersecurity Workforce:** Experts play a central role in ensuring cybersecurity in every sector, including education. If cybersecurity positions are unfilled, schools and institutions will be less secure. Filling workforce gaps was a priority in many states in 2022, but legislators typically proposed to address the problem by funding new higher education degree programs. This "build it and they will come" approach, considered by many states in 2022, is a useful idea but it does not rise to the level of urgency associated with this problem. As described by the CoSN-SETDA cybersecurity staffing report, published in October 2022, a four-year degree focused strategy takes years to yield benefits. Thus, we encourage readers to consider a much more strategic and proactive approach across recruitment, training, and retention with defined goals for building this vitally important workforce, including by emphasizing shorter term credentialing options, and specifying workforce expansion benchmarks with defined timelines. Greater funding will also be needed for compensation to ensure schools and other public entities can compete with the private sector for these highly skilled workers.

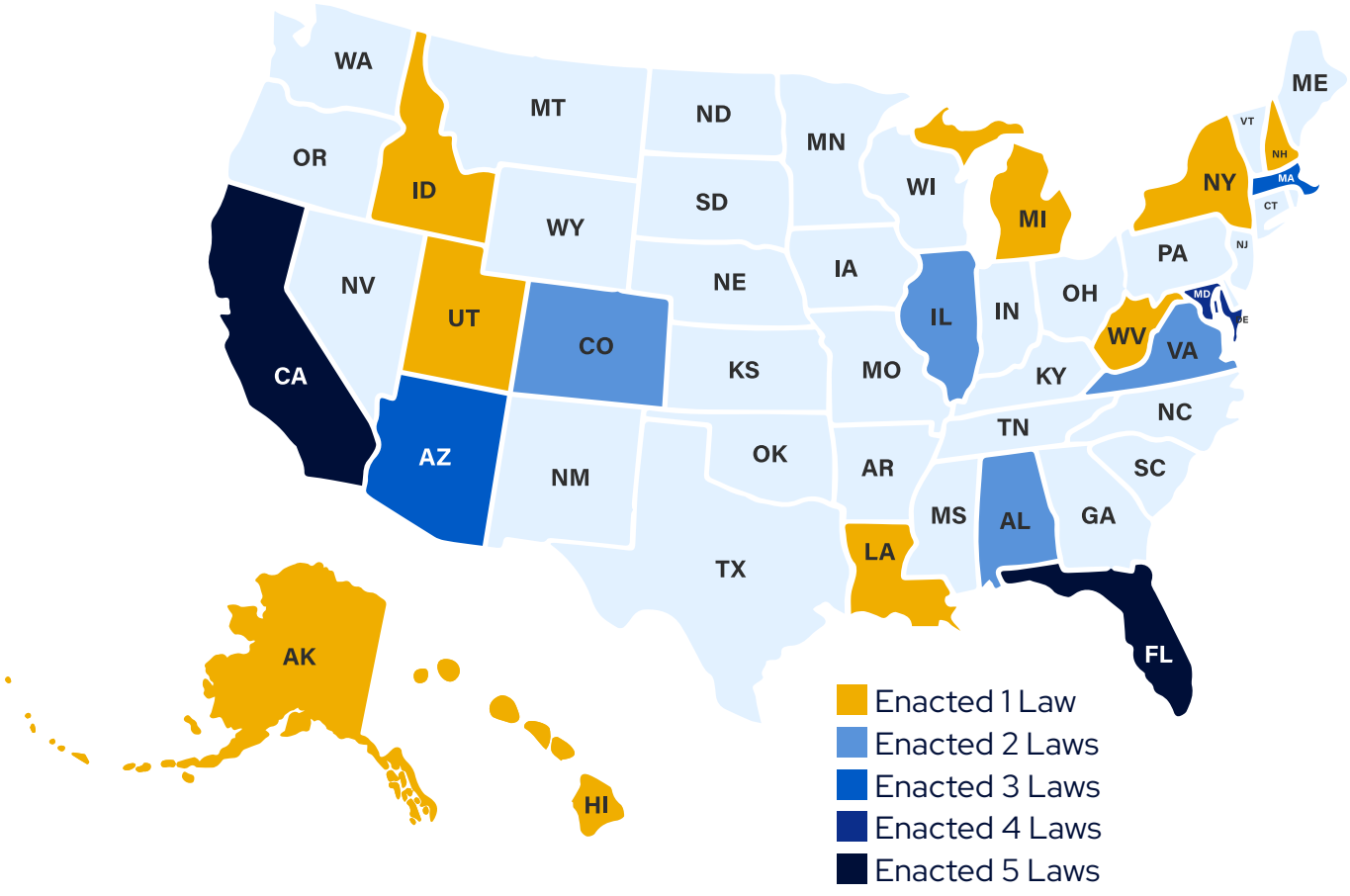
- **Prevention and Planning:** Cyberattacks on the education sector, and other targets, often succeed because users on the systems inadvertently offer "soft" entry points. Government must provide funding for technology to identify and repel attacks, but investments must also focus on continually educating students, staff, families, and the public about how to recognize and avoid attacks. Many states, appropriately, considered this strategy in 2022 but leaders must be bolder and more strategic when designing cybersecurity awareness and prevention campaigns. Limited investments, pilot programs, and vague calls for developing resources and curricula are not sufficient. Legislative prevention strategies must be comprehensive, reflect industry standards and best practice, and include ambitious but realistic timelines for completing required education activities and technology improvements. Many resources for school systems prevention and planning on cosn.org/cybersecurity.

- **Incident Reporting, Contingency Planning, and Coordination:** Preventing and quickly recovering from cyberattacks benefits from rapid information sharing and other collaboration. Schools and other entities do not face a static cyber enemy. Attackers are constantly changing their tactics and the education sector must be similarly nimble in its collective defense. In 2022, states considered new disclosure requirements, contingency planning obligations, and coordination proposals. These valuable ideas should be embraced not only within states but also on a regional and national level. State and federal policies should encourage greater participation in the collaborative groups that already exist in this space by providing funding and strategic direction. Policy makers should also find ways to remove stigmas associated with reporting attacks so that every attack can be a learning opportunity for other education sector targets.

State Education Cybersecurity Laws Enacted in 2022

This year, 18 states adopted 37 cybersecurity laws with direct or indirect application to the education sector. This number compares to 49 new laws in 2021 and 10 new laws in 2020. The 2022 laws largely focus on policy changes targeted across state and local government, not just on education entities, and they address a range of cybersecurity policy areas and strategies including governance improvements, mandatory incident reporting, required prevention and contingency planning, expanding the available cyber workforce, and security investments targeting state agencies, local agencies, and higher education institutions. Two of the new state laws focus on elementary and secondary education. California adopted Assembly Bill 2355 which requires school districts to report cyberattacks that impact more than 500 students or personnel. The new California law also requires the California Cybersecurity Integration Center to establish a database to track the attacks reported by school districts. Alabama adopted House Bill 135, which provides funding for hiring District Technology Coordinators, "with the qualifications described by the State Board of Education" and providing funding for school districts to improve their cybersecurity. The new district resources must "fund network administration and/or technology that sustains, complements, upgrades, or augments current security measures."

STATES THAT ENACTED CYBERSECURITY LAWS IN 2022



COMMON CYBERSECURITY POLICY STRATEGIES ADOPTED BY STATES IN 2022

	Incident Reporting	State Planning	State Agency Funding	State Governance	K-12 and Higher Ed Funding	Workforce Expansion	Other
Alabama			▯		▯		
Alaska							▯
Arizona		▯	▯	▯			
California	▯	▯		▯	▯	▯	
Colorado				▯			
Florida	▯	▯		▯	▯		
Hawaii				▯			
Idaho							▯
Illinois			▯				
Louisiana							▯
Maryland		▯	▯			▯	
Massachusetts			▯		▯	▯	
Michigan			▯				
New Hampshire	▯						
New York	▯						
Utah		▯		▯			
Virginia	▯			▯			
West Virginia							▯

Summaries of the State Cybersecurity Laws Enacted in 2022

- Alabama (H.B.135) – Provides school districts with funding for a District Technology Coordinator position. Funding must be used by school districts to improve cybersecurity, including protection of data and infrastructure. The Department is required to consult with the Alabama Leaders in Educational Technology to implement this allocation, and to assist school systems' effective use of these funds, including but not limited to, conducting workshops, training, and collaborative support for cybersecurity.

- Alabama (S.B.106) – Provides state level cybersecurity funding for the Alabama Office of Information Technology. Office must report quarterly on the status of updates to the state's cybersecurity system.

- Alaska (H.B.3) – Amends the definition of "disaster" to include a cybersecurity attack that affects critical infrastructure in the state, an information system owned or operated by the state or a political subdivision of the state, information that is stored on, processed by, or transmitted on an information system owned or operated by the state or a political subdivision of the state, or a credible threat of imminent cybersecurity attack or serious cyber incident that the commissioner of administration or commissioner's designee certifies to the governor has a high probability of occurring in the near future.

- Arizona (H.B.2857) – Requires the Arizona Department of Administration to obtain insurance for security system and data breaches and it establishes the Cyber Risk Insurance Fund.

- Arizona (H.B.2862) - Provides funding to the Arizona Department of Homeland Security to acquire cybersecurity software for state agencies and to make statewide cybersecurity grants. The funding for cybersecurity software would be used to procure and implement, through a competitive bidding process, an enterprise license for use by agencies of the state for security software that will integrate security into the development process and scan software code in development, production, and postproduction to detect and improve security threats by using certain testing mechanisms.

- Arizona (S.B.1598) - Requires the Arizona Department of Homeland Security to formulate policies, plans and programs to enhance the ability of the state to prevent and respond to cybersecurity threats. Requires the Department of Administration to develop strategies to protect the information technology infrastructure of the state and the data that is stored on or transmitted by the infrastructure. Further, this bill requires the appointment of a statewide chief information security officer.

- California (A.B.183) – Establishes the Cybersecurity Regional Alliances and Multistakeholder Partnerships Pilot Program to address the cybersecurity workforce gap. California State University campuses may participate in this pilot program.

- California (A.B.2355) – Requires school districts to report any cyberattack impacting more than 500 students or personnel to the California Cybersecurity Integration Center. The California Cybersecurity Integration Center would also be required to establish a database that tracks reports of cyberattacks submitted by LEAs.

- California (A.B.2750) – Requires the Department of Technology, within the Government Operations Agency, to develop a state digital equity plan. This plan must include awareness and use of measures to secure the online privacy and cybersecurity of an individual.

- California (S.B.154) – Provides funding for community college districts to implement technology and data security measures to support improved oversight of fraud mitigation, online learning quality, and cybersecurity efforts. As a condition of receiving funds, community college districts must complete an annual cybersecurity self-assessment and participate in regularly scheduled cybersecurity reporting, which includes reporting of ransomware incidents.

- California (S.B.844) - Existing law, the State and Local Cybersecurity Improvement Act, authorized grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments. The new law requires the California Cybersecurity Integration Center to create four reports, over several fiscal years, that describe all expenditures made by the state within a single fiscal year pursuant to the federal State and Local Cybersecurity Improvement Act.

- Colorado (S.B.22-113) - Creates requirements, with limitations, for state agencies that deploy facial recognition services. Specifies that an individual may authorize an agent to access and process the individual's personal data or other information held on a computer, computer network, or computer system and that is otherwise accessible to the individual, and this would not constitute a cybercrime. Temporarily prohibits public schools from entering into new contracts for facial recognition services.

- Colorado (S.B.22-140) – Requires the office of future work in the department and its partners, including the department of education, to create a digital navigation program and employ digital navigators which would, among several things, address digital inequities. Defines "digital inclusion" to include the ability to obtain a "basic awareness of measures to ensure online privacy and cybersecurity."

- Florida (H.B.5001) - Provides funding for certain cybersecurity programs at institutions of higher education.

- Florida (H.B.7055) - Requires political subdivisions, state agencies, and local governments to report cybersecurity and ransomware incidents. Provides for cybersecurity training requirements. Establishes as a crime for willfully, knowingly, and without authorization introducing a computer contaminant that gains unauthorized access to, encrypts, modifies, or otherwise renders unavailable data, programs or support documentation residing or existing within a computer, computer system, computer network, or electronic device owned or operated by a governmental entity and demands a ransom to prevent publication. Governmental entity is defined to include any official, officer, commission, board, authority, council, committee or department of the executive, judicial, or legislative branch of state government and any state university.

- Florida (H.B.7057) – Provides an exemption from public records requirements for certain information related to a cybersecurity incident or ransomware incident held by a state agency and would provide an exemption from public meetings requirements for portions of a meeting that would reveal certain information related to a cybersecurity incident or ransomware incident.

- Florida (S.B.848) – Amends existing cybersecurity law to "facilitate correct interpretation" of the law to say: "Each state agency head shall, at a minimum: (h) Ensure that the cybersecurity requirements in the written specifications for the solicitation, contracts, and service-level agreement of information technology and information technology resources and services meet or exceed the applicable state and federal laws, regulations, and standards for cybersecurity."

- Florida (S.B.2518) – Requires that the Department of Management Services established in existing law would provide operational management and oversight of the state data center. In collaboration with the Department of Law Enforcement and the Florida Digital Service, the Department must develop and implement a process for detecting, reporting, and responding to cybersecurity incidents, breaches, and threats.

- Hawaii (H.B.2171) - Amends existing law relating to the full-time Hawaii cybersecurity, economic, education and infrastructure security coordinator who oversees cybersecurity and cyber resiliency matters for the state. Specifies that the coordinator would be placed with the state department of law enforcement (rather than defense) and selected by the director of law enforcement (rather than state adjutant general).

- Idaho (H.B.621) - Provides that certain cybersecurity records, other than public expenditure records, but including those relating to the nature, location, or function of cybersecurity devices, programs, or systems designed to protect computer, information technology, or communications systems, are exempt from disclosure.

- Illinois (H.B.900) - Provides funding to the Department of Innovation and Technology for all costs associated with cybersecurity training, preparedness, and other related measures.

- Illinois (S.B.3939) – Requires the Secretary of Innovation and Technology to establish a cybersecurity liaison program to advise and assist units of local government and school districts concerning specified cybersecurity issues. Provides for cybersecurity training for employees of counties and municipalities.

- Louisiana SCR14 - Establishes the Cybersecurity Redhibition Task Force, which would be a unified and coordinated body of information technology and security professionals from various branches of federal and state government to consider creating a distinct cause of action for state agencies that respond to cyber incidents as part of the state's emergency support

function to recover qualifying expenses from managed service providers and managed security service providers servicing public bodies and critical infrastructure whose actions or omissions contributed to the cyber incident.

- Maryland (H.B.24)/(S.B.4) – Alters the criteria for the Cybersecurity Public Service Scholarship Program, including increasing the number of years a recipient may hold an award, expanding the qualifying positions for a scholarship recipient to fulfill a work obligation, and establishing criteria for part-time students to be eligible for the scholarship, hold an award, and fulfill a work obligation. This also establishes the Maryland Cybersecurity Loan Assistance Repayment Program.

- Maryland (H.B.1205) - Finances projects related to information technology and cybersecurity-related State government infrastructure. Requires the Department to hire independent contractors to develop a framework for investments in technology and periodically assess the cybersecurity and information technology systems in certain units of State government. Establishes a local cybersecurity support fund.

- Maryland (S.B.754) - This bill requires the Cyber Preparedness Unit to coordinate with the state chief information security officer to support local governments in developing a vulnerability assessment and cyber assessment. This would also require the Unit to develop and update an online database of cybersecurity training resources for local government personnel. Local government is defined to include local school systems and local school boards.

- Maryland (S.B.812) - This bill establishes the Maryland Cybersecurity Coordinating Council and would require the Secretary of Information Technology to develop and maintain a statewide cybersecurity strategy. Further this bill requires certain IT units to certify compliance with certain cybersecurity standards and would require the State Security Operations Center to notify certain agencies of a cybersecurity incident reported in a certain manner.

- Massachusetts (H.4269) - Provides COVID-19 response funding totaling $15,000,000 that would be expended for community colleges to administer a high demand workforce training program for in-demand fields, which would include cybersecurity.

- Massachusetts (H.5050) - Provides funding for the establishment of an information technology audit unit within the office of the state auditor in order to conduct audits of high risk information technology related activities, which includes cybersecurity. Further, this bill provides funding for the operation of the executive office of technology services and security - this bill would require the executive office to submit a report to the secretary of administration and finance, the state auditor and the house and senate committees on ways and means that includes certain topics, including the status of the commonwealth's cybersecurity. Funding is also provided for the

Massachusetts Cybersecurity Innovation Fund to community colleges and state universities to provide regional security operations center services for the monitoring and detection of cyber threat activity.

- Massachusetts (H.5374) – Provides funds for a reserve to support scholarships to Massachusetts students enrolled in pursuing a program of higher education. Scholarship awards would be distributed based on a prioritized process where students enrolled in a course of study aligned to address workforce needs in high-demand fields, including cybersecurity programs. This bill also establishes a cybersecurity center to foster cybersecurity resiliency through work with state agencies, municipalities, educational institutions, and private partners.

- Michigan (S.B.844) – Provides funding for municipal information technology and cybersecurity upgrades.

- New Hampshire (H.B.1277) - Defines "cybersecurity incident" and requires that political subdivisions report such incidents to the department of information technology.

- New York (S.7786) - Amends existing law relating to requiring notice to state entities, including state boards and departments, to be notified within 24 hours of any breach of network security.

- Utah (H.B.280) – Creates a Cybersecurity Commission and directs the Commission to gather information about cybersecurity vulnerabilities and best practices. This bill directs the commission to analyze cybersecurity practices in the private and public sectors.

- Virginia (H.B.1290) - Requires every public body to report to the Chief Information Officer all known incidents that threaten the security of the Commonwealth's data or communications or result in exposure of data and other incidents compromising the security of the public body's information technology systems with the potential to cause major disruption to normal activities of the public body or other public bodies.

- Virginia (H.B.1304)/(S.B.703) - Specifies that the Virginia Information Technologies Agency is tasked with advising the CIO regarding cybersecurity policies, standards, and guidelines for several reasons, but specifically to strengthen the Commonwealth's cybersecurity and to protect against and respond to breaches of information technology security.

- West Virginia (S.B.520) – Increases the financial penalties for any person who introduces ransomware into any computer, computer system or computer network in certain circumstances.

2022 Education Cybersecurity Legislation Trends (All Bills Considered)

Legislators in thirty-six states introduced cybersecurity bills in 2022 with direct or indirect application to the education sector. This section lists these bills, organized into K-12 and postsecondary categories, and highlights common policy strategies suggested across states. The following states did not introduce cybersecurity bills in 2022: Arkansas, Connecticut, Delaware, Kentucky, Maine, Oklahoma, Rhode Island, South Dakota, Tennessee, Wyoming, and Washington, D.C. Further, Montana, Nevada, North Dakota, and Texas did not have sessions in 2022.

Elementary and Secondary Schools Focused Legislation (34 bills in 18 states)

Legislators in 18 states introduced thirty-four cybersecurity bills[3] focused directly on elementary and secondary schools. This total is four fewer bills than legislators introduced in 2021 (38 bills in 16 states in 2021); but significantly more than the 19 bills in 13 states that policymakers introduced in 2020.

Many of the education cybersecurity bills introduced in 2022 focused on preventing attacks. These prevention models typically called on districts to educate students, staff, and the public about cyberthreats and safety, call for the development of model curriculum or training guides and courses. Some of the prevention strategy bills provided funding to schools and districts to pay for these activities. Several states considered legislation designed to expand the available cybersecurity workforce through work-based learning or career pathways systems that would include a cybersecurity option. As described in the section above, only two of the K-12 focused proposals became law: California's incident reporting requirement and Alabama's district technology coordinator and funding strategy.

[3] This number also includes study orders in Massachusetts.

COMMON CYBERSECURITY POLICY STRATEGIES INTRODUCED IN STATES IN 2022

	Prevention and Safety	Workforce Expansion	K-12 Funding	Incident Reporting
Alabama			▯	
California	▯			▯
Georgia		▯		
Hawaii		▯		
Illinois				▯
Iowa	▯			
Maryland	▯			
Massachusetts	▯			
Michigan	▯			
Minnesota			▯	
Mississippi	▯			
Missouri	▯			
New Jersey		▯		
New Mexico			▯	
New York	▯			
South Carolina		▯		
Virginia		▯		
Washington	▯			

List of 2022 K-12 Focused Cybersecurity Bills

- Alabama H.B.135 (enacted, appropriations for District Technology Coordinator position – funding must also be used to improve cybersecurity)
- Alabama S.B.151 (appropriations for District Technology Coordinator position – funding must also be used to improve cybersecurity)
- California A.B.2355 (enacted, LEAs must report cyberattack impacting more than 500 students or personnel and tracking of these reports required)
- California S.B.767 (creation of educational technology plan, includes training and support for educators on cybersecurity and online safety)
- Georgia H.R.877 (encourages department to provide funds for outreach efforts to promote and

improve cybersecurity education, training, and workforce development)

- Hawaii H.B.1222 (increases computer science education offerings at public schools) [companion to S.B.242 (signed into law in 2021; H.B.1222 carried over to 2022)]
- Illinois H.B.4152 (requires districts to report cyber security attacks to SBE)
- Iowa H.F.2461 (prohibits ransomware re: schools, community colleges, education agencies; exception for ransomware for research purposes)
- Maryland H.B.1163 (vetoed, virtual schools must provide parents/guardians with informational materials on cybersecurity policy and best practices)
- Maryland H.B.1410 (publish cyber safety guide and training course to be implemented in public schools) [cross-filed with S.B.162]
- Maryland S.B.162 (publish cyber safety guide and training course to be implemented in public schools) [cross-filed with H.B.1410]
- Massachusetts H.106 (limit screen time and digital tech in early education; requires early education certification and re-cert re: relevant education on cybersecurity)
- Massachusetts H.5040 (study order of H.106)
- Massachusetts H.107 (enact and enforce policy directive on cybersecurity)
- Massachusetts H.5040 (study order of H.107)
- Massachusetts H.112 (plan to hard-wire public education facilities; facilitate statewide PD plan and education materials to support cybersecurity)
- Massachusetts H.5040 (study order of H.112)
- Massachusetts H.127 (regulations to establish data security and privacy responsibilities of the

department of education - must consult with experts in cybersecurity)

- Massachusetts S.55 (creates school district cybercrime prevention program to provide info on strategies, best practices, and programs relating to prevention of cybercrimes)
- Massachusetts S.2683 (study order for S.55)
- Michigan H.B.5036 (Department to create materials, resources, model curricula, and lesson plans concerning digital literacy and cyber safety)
- Michigan S.B.520 (Department to create materials, resources, model curricula, and lesson plans concerning digital literacy and cyber safety)
- Minnesota H.F.4005 (appropriations to pay for costs of enhancing cybersecurity in the district's information systems) [companion to S.F.3380]
- Minnesota S.F.627 (appropriations to pay for costs of enhancing cybersecurity in the district's information systems)
- Minnesota S.F.3380 (appropriations to pay for costs of enhancing cybersecurity in the district's information systems) [companion to H.F.4005]
- Mississippi H.B.818 (encouraged to designate central location within district which may be used to provide courses and instruction to students; including courses in cybersecurity)
- Missouri H.B.1585 (curriculum re: social media, including cyber safety, cybersecurity, and ethics)
- New Jersey A.1982 (required instruction on cybersecurity; model curricula; loan redemption programs in certain cybersecurity occupations)
- New Mexico H.B.122 (funding to develop cybersecurity program for all schools/districts)
- New York A.4567 (cyber crime prevention services program to provide districts with info on strategies, best practices and programs re: prevention of cyber crimes in schools) [same as S.349]
- New York S.349 (cyber crime prevention services program to provide districts with info on strategies, best practices and programs re: prevention of cyber crimes in schools) [same as A.4567]
- New York A.4640 (annual notifications re: combatting cyber crime, including reminder of strategies and best practices most effective at combatting) [same as S.348]
- New York S.348 (annual notifications re: combatting cyber crime, including reminder of strategies and best practices most effective at combatting) [same as A.4640]
- South Carolina H.3612 (expansion of computer science education; creation of career pathways including in high demand career fields, such as cybersecurity)
- Virginia H.B.466 (establishes register of cybersecurity professionals to assist IHEs, work-based learning programs, and school divisions in addressing IT and cybersecurity challenges)
- Washington H.B.1450 (relates to procuring computers and devices, which must allow for cybersecurity protection in the process of procurement)

Postsecondary Focused State Cybersecurity Legislation (35 bills in 12 states)

Legislators' focus on postsecondary cybersecurity increased in 2022. Policymakers in twelve states introduced 35 bills in 2022, compared to 6 bills in 4 states in 2020 and 2021. Most bills provided funding for cybersecurity programs aimed at building the cyber workforce, while a smaller number of bills proposed investments to secure campus networks. Other bills provided an affirmative defense for covered entities that have written cybersecurity programs (IL); required incident reporting (IL); established a new prohibition on ransomware, except for research (IA); and planning for cyberattacks (NJ).

COMMON POSTSECONDARY CYBERSECURITY POLICY STRATEGIES INTRODUCED IN STATES IN 2022

	Workforce Expansion	IT Funding	Safe Harbor Defense	Incident Reporting
California	▯	▯		
Florida	▯			
Illinois	▯		▯	▯
Maryland	▯			
Massachusetts	▯	▯		
Minnesota	▯			
Nebraska		▯		
New York	▯			
North Carolina	▯	▯		
Washington	▯			

Complete List of 2022 Postsecondary Focused Cybersecurity Bills

- California A.B.154 (funding for community college districts to implement measures relating to cybersecurity)
- California A.B.183 (enacted, establishes pilot program through California State University campuses to address cybersecurity workforce gap)
- California A.B.2695 (establishes pilot program through California State University campuses to address cybersecurity workforce gap)
- California S.B.154 (enacted, funding for community college districts to implement measures relating to cybersecurity)

- California S.B.183 (establishes pilot program through California State University campuses to address cybersecurity workforce gap)
- Florida H.B.3273 (appropriations for college re: database and cybersecurity programs)
- Florida H.B.5001 (enacted, appropriations for cybersecurity programs at IHEs)
- Florida S.B.2500 (appropriations for cybersecurity programs at IHEs)
- Illinois H.B.3030 (creates Cybersecurity Compliance Act – affirmative defense for covered entity where maintains written cybersecurity program)
- Illinois H.B.4152 (universities and community college districts must report cybersecurity attacks)
- Illinois H.B.5243 (creates Cybersecurity Compliance Act – affirmative defense for covered entity where maintains written cybersecurity program)
- Illinois H.B.5561 (funding for Institute of Technology Cybersecurity Bootcamp program)
- Iowa H.F.2461 (prohibits ransomware re: schools, community colleges, education agencies; exception for ransomware for research purposes)
- Maryland H.B.24 (enacted, scholarship program and creates cybersecurity loan assistance repayment program) [cross-filed with S.B.4]
- Maryland S.B.4 (enacted, scholarship program and creates cybersecurity loan assistance repayment program) [cross-filed with H.B.24]
- Massachusetts H.4219 (COVID19 funding – may use funds for high demand workforce training program for in-demand fields, including cybersecurity) [published as H.4234]
- Massachusetts H.4234 (COVID19 funding – may use funds for high demand workforce training program for in-demand fields, including cybersecurity) [reported by H.4269]
- Massachusetts H.4269 (enacted, COVID19 funding – may use funds for high demand workforce training program for in-demand fields, including cybersecurity) [signed bill of H.4219 and H.4234]
- Massachusetts H.4720 (appropriations for institutions re: technology and innovation fields, including cybersecurity) [new draft is H.4864]
- Massachusetts H.4864 (appropriations for institutions re: technology and innovation fields, including cybersecurity) [new draft of H.4720]
- Massachusetts H.4977 (appropriations for institutions re: technology and innovation fields, including cybersecurity) [new draft of H.4864]
- Massachusetts H.5007 (appropriations for institutions re: technology and innovation fields, including cybersecurity) [published as H.5034]
- Massachusetts H.5034 (appropriations for institutions re: technology and innovation fields, including cybersecurity) [bill H.5007 published as amended]

- Massachusetts S.3030 (amendment to H.5034)
- Massachusetts H.5374 (enacted, provides funds for scholarships for students enrolled in programs focused on high-demand fields such as cybersecurity)
- Minnesota H.F.3362 (appropriations for cybersecurity program at Metropolitan State University) [companion to S.F.3109]
- Minnesota S.F.3109 (appropriations for cybersecurity program at Metropolitan State University) [companion to H.F.3362]
- Nebraska L.B.904 (funding for U of Nebraska to establish Artificial Intelligence, Cybersecurity, and Holland Computer Center facility)
- Nebraska L.B.1206 (funding for Neb. State Colleges to improve information technology infrastructure and cybersecurity)
- New Jersey A.3379 (IHEs must establish plans re: cyber security and prevention of cyberattacks)
- New Mexico S.B.48 (vetoed, funding for cybersecurity education at NM Institute of Mining and Technology)
- North Carolina H.B.1132 (appropriations for cybersecurity improvements at certain institutions)
- North Carolina H.B.1154 (funding to support workforce development programs at colleges related to critical technologies, including cybersecurity)
- North Carolina H.B.1156 (funding to support resource of critical technologies, including cybersecurity, available to colleges and universities)
- Virginia H.B.466 (establishes register of cybersecurity professionals to assist IHEs, work-based learning programs, and school divisions in addressing IT and cybersecurity challenges)

2022 General Government State Cybersecurity Bills that reference K-12 (27 bills in 12 states)

Legislators in 12 states introduced 27 cybersecurity bills that focused generally on government agencies but also reference K-12 schools. For comparison, in 2021 legislators introduced 16 bills in 11 states, and in 2020 legislators in four states introduced 9 such bills.

Common legislative themes included educating employees and students about cyber risks and safety, governance changes and security standards, and incident reporting. Other measures proposed to prohibit ransomware payments (AZ); establish facial recognition services requirements (CO); provide cybersecurity assistance for government agencies (IL, MD, NM); establish a cybersecurity simulation training center (IA); and require multifactor authentication (NY).

COMMON GENERAL GOVERNMENT WITH K-12 CYBERSECURITY POLICY STRATEGIES INTRODUCED IN STATES IN 2022

	Prevention and Safety Training	Governance and Standards	Incident Reporting	Prohibit Ransom Payments
Arizona				▯
Colorado		▯		
Georgia	▯	▯		
Florida			▯	
Illinois	▯			
Iowa	▯			
Maryland	▯			
Mississippi			▯	
New Jersey		▯	▯	
New Mexico		▯		
New York			▯	

Complete List of 2022 General Government Cybersecurity Bills with a K-12 Focus

- Arizona H.B.2145 (prohibits payments to remove or decrypt ransomware, refers to schools districts and community college districts)
- Colorado S.B.22-113 (enacted, facial recognition services requirements)
- Colorado S.B.22-140 (enacted, digital navigation program)
- Florida H.B.7055 (enacted, relates to reporting ransomware and cybersecurity incidents and training requirements)
- Florida S.B.1670 (mandatory reporting of attack, cybersecurity standards adopted)
- Georgia H.B.1217 (compliance standards for tech protection measures, includes development of guidelines for training of school personnel)
- Illinois H.B.5165 (establishes cybersecurity liaison program to assist local govt units and school districts; also provides training for employees and school districts)
- Illinois S.B.3939 (enacted, establishes cybersecurity liaison program to assist local govt units and school districts; also provides training for employees and school districts)
- Iowa H.F.2361 (establishes cybersecurity simulation training center – may be used by students and educators, in addition to business and state entities)
- Iowa H.F.2555 (establishes cybersecurity simulation training center – may be used by students and educators, in addition to business and state entities)

- Iowa H.S.B.669 - (establishes cybersecurity simulation training center – may be used by students and educators, in addition to business and state entities) [renumbered as H.F.2361]
- Maryland H.B.5 (creation of training program, will be required of certain employees in govt, higher education, and education) [cross-filed with S.B.107]
- Maryland H.B.1202 (vetoed, develop cyber assessments and develop online database of cybersecurity training resources for local govt. personnel – defined to include local school systems and local school boards) [cross-filed with S.B.754]
- Maryland H.B.1205 (enacted, financing of cybersecurity-related govt infrastructure) [cross-filed with S.B.811]
- Maryland S.B.107 (creation of training program, will be required of certain employees in govt, higher education, and education) [cross-filed with H.B.5]
- Maryland S.B.754 (enacted, develop cyber assessment and develop an online database of cybersecurity training resources for local govt. personnel – defined to include local school systems and local school boards) [cross-filed with H.B.1202]
- Maryland S.B.780 (office established to implement cybersecurity best practices and overall cybersecurity preparedness for units of local govt and local school boards)
- Maryland S.B.811 (financing of cybersecurity-related govt infrastructure) [cross-filed with H.B.1205]
- Mississippi S.B.2530 (vetoed, expands enterprise security program and coordinated oversight of cybersecurity efforts; requires reporting of ransomware)
- New Jersey A.1450 (required information security standards to be used by state agencies; boards of education must follow guidelines to protect information)
- New Jersey A.1671 (state, county, and other employees to complete cybersecurity awareness training)
- New Jersey A.1983 (reporting requirements for govt and school districts re: cybersecurity incidents)
- New Mexico S.B.98 (Cybersecurity Act, establishes office and committee, and state chief of information security; assessment of cybersecurity services for govt agencies, including schools and districts and postsecondary institutions)
- New York A.8793 (notice within 24 hours of breach of network security to state agencies, including state boards and departments) [substituted by S.7786]
- New York S.7786 (enacted, notice within 24 hours of breach of network security to state agencies, including state boards and departments) [substituted for A.8793]
- New York S.2652 (multifactor authentication required for all govt. entities, including school districts)
- North Carolina S.B.792 (appropriations bill for cyber-related activities; includes funding for work-based learning opportunities for students, including in high-demand fields such as cybersecurity)

General Government State Cybersecurity Bills that Reference Postsecondary Institutions (21 bills in 11 states)

There was also a notable increase in state legislation focused on general government state cybersecurity that includes a reference on postsecondary institutions. Legislators introduced 21 bills in 11 states in 2022, compared to 4 bills in 2 states in 2021.

These general government bills did not overlap with much consistency other than a theme that emerged around governance, audits, and contract requirements. Other discrete topics included facial recognition services requirements (CO); critical infrastructure contract requirements (FL); administration of state cybersecurity programs (HI); establishing a cybersecurity simulation training centers (IA); training programs and requirements (MD); direct funding (MA); and assessments and reviews of cybersecurity infrastructure (NJ, NM).

COMMON GENERAL GOVERNMENT WITH POSTSECONDARY CYBERSECURITY POLICY STRATEGIES INTRODUCED IN STATES IN 2022

	Governance, Audit, Contract Requirements	Prevention and Safety Training
Florida	▯	
Illinois	▯	
Iowa		▯
Massachusetts	▯	
Maryland		▯
New Jersey	▯	
New Mexico	▯	
New York	▯	

Complete List of 2022 General Government Cybersecurity Bills that Reference Postsecondary Education

- Arizona H.B.2145 (prohibits payments to remove or decrypt ransomware, refers to school districts and community college districts)
- Colorado S.B.22-113 (enacted, facial recognition services requirements)
- Colorado S.B.22-140 (enacted, digital navigation program)
- Florida H.B.1147 (critical infrastructure contract requirements, including all assets, systems, and networks vulnerable to cybersecurity attacks)

- Florida H.B.7055 (enacted, relates to reporting ransomware and cybersecurity incidents and training requirements)
- Florida S.B.828 (critical infrastructure contract requirements, including all assets, systems, and networks vulnerable to cybersecurity attacks)
- Hawaii H.B.2118 (amends existing law relating to state cybersecurity program, administered in partnership with govt agencies and IHEs) [companion to S.B.3086]
- Hawaii S.B.3086 (amends existing law relating to state cybersecurity program, administered in partnership with govt agencies and IHEs) [companion to H.B.2118]
- Illinois H.B.4285 (allows state agencies and public institutions of higher education to purchase cybersecurity products that are included in Authorized Product List)
- Iowa H.F.2361 (establishes cybersecurity simulation training center – may be used by students and educators, in addition to business and state entities)
- Iowa H.F.2555 (establishes cybersecurity simulation training center – may be used by students and educators, in addition to business and state entities)
- Iowa H.S.B.669 (establishes cybersecurity simulation training center – may be used by students and educators, in addition to business and state entities) [renumbered as H.F.2361]
- Maryland H.B.5 (creation of training program, will be required of certain employees in govt, higher education, and education) [cross-filed in S.B.107]
- Maryland S.B.107 (creation of training program, will be required of certain employees in govt, higher education, and education) [cross-filed in H.B.5]
- Massachusetts H.4701 (appropriations and reporting re: status of cybersecurity; funding for colleges/universities for monitoring and detection of cyber threat activity) [identical to S.2915]
- Massachusetts H.5050 (enacted, appropriations re: audit of high risk information technology and funding for colleges/universities for monitoring and detection of cyber threat activity)
- Massachusetts S.2915 (appropriations and reporting re: status of cybersecurity; funding for colleges/universities for monitoring and detection of cyber threat activity) [identical to H.4701]
- New Jersey A.4013 (govt and state college conduct review of department's or college's cybersecurity infrastructure and make recommendations to improve) [identical to S.484]
- New Jersey S.484 (govt and state college conduct review of department's or college's cybersecurity infrastructure and make recommendations to improve) [identical to A.4013]
- New Mexico S.B.98 (Cybersecurity Act, establishes office and committee, and state chief of information security; assessment of cybersecurity services for govt agencies, including schools and districts and postsecondary institutions)
- New York S.7312 (critical infrastructure review to determine if vulnerable to cybersecurity attacks)

General State Government Cybersecurity Bills (120 bills in 31 states)

In 2022 state legislators introduced a greater number and wider variety of general government cybersecurity bills compared to 2021. Policymakers introduced 120 bills[4] in 31 states, compared to 96 bills in 33 states in 2021 and 55 bills introduced in 21 states in 2020. Bills proposing to require governance improvements, audits of cyber readiness, contracting improvements and technical standards adoption were among the most common approaches. Funding for information technology improvements also factored high on policymakers' priorities, followed closely by an emphasis on supporting internal preventative measures like awareness building and safety training.

COMMON GENERAL CYBERSECURITY POLICY STRATEGIES INTRODUCED IN STATES IN 2022

	Governance, Audit, Contract Requirements	IT Funding	Prevention and Safety Training, Response	Incident Reporting	Open Records Exception
Alabama				▯	
Arizona	▯				
California	▯	▯			
Colorado				▯	
Florida		▯			▯
Georgia	▯	▯			
Hawaii		▯		▯	
Idaho					▯
Illinois		▯	▯		
Iowa	▯		▯		
Kansas			▯		▯
Maryland	▯	▯	▯		
Massachusetts	▯	▯			
Michigan		▯			
Minnesota		▯			
New Jersey			▯		
New York	▯	▯			
North Carolina				▯	

[4] This number also includes study orders in Massachusetts.

	Governance, Audit, Contract Requirements	IT Funding	Prevention and Safety Training, Response	Incident Reporting	Open Records Exception
Ohio	▯				
Pennsylvania		▯			
Utah	▯				
Vermont				▯	
Virginia				▯	
Wisconsin	▯				

Complete List of 2022 General Government Cybersecurity Bills

- Alabama S.B.106 (enacted, appropriations for cybersecurity and reporting)
- Alaska H.B.3 (enacted, amends definition of "disaster" to include cybersecurity attack)
- Arizona H.B.2584 (requirements for cybersecurity software bids)
- Arizona H.B.2690 (requires insurance for security system and data breaches)
- Arizona H.B.2857 (enacted, requires insurance for security system and data breaches)
- Arizona H.B.2862 (enacted, requirements for cybersecurity software bids)
- Arizona S.B.1598 (enacted, enhance response to cybersecurity threats)
- Arizona S.B.1724 (requires insurance for security system and data breaches)
- Arizona S.B.1729 (requirements for cybersecurity software bids)
- California A.B.214 (appropriations for Cybersecurity Integration Center)
- California A.B.581 (state agencies must use NIST guidelines)
- California A.B.809 (Office of Information Security to ensure integrity of state systems)
- California A.B.2190 (Office of Information Security to ensure integrity of state systems)
- California A.B.2750 (enacted, state digital equity plan)
- California A.B.2826 (privacy and cybersecurity safeguards for platform for researchers)
- California S.B.112 (appropriations for Cybersecurity Integration Center)
- California S.B.844 (enacted, grants to address cybersecurity risks and threats to information systems)
- California S.B.1018 (vetoed, requirements for operators that collect PII, reasonable privacy, and cybersecurity safeguards)
- Colorado H.B.22-1404 (analysis of current cyber incident response capabilities in state)
- Florida H.B.1287 (confidential local govt information including records of cybersecurity incidents)

- Florida H.B.7057 (enacted, public records requirements related to cybersecurity/ransomware)
- Florida H.B.9241 (funding for Cyber Florida – infrastructure and technical assistance program)
- Florida S.B.1694 (public records requirements related to cybersecurity/ransomware)
- Florida S.B.2518 (enacted, process to detect, report, and respond to cybersecurity incidents)
- Georgia H.B.159 (creates State Cybersecurity Review Board)
- Georgia S.B.596 (creates Georgia Cyberforce to protect citizens and assets from cyberattacks)
- Georgia S.R.741 (creates Study Committee on creation of Cybersecurity Force)
- Hawaii H.B.957 (establishes joint integration center to integrate information technology, cybersecurity, and cybercrime prevention) [companion to S.B.1111]
- Hawaii H.B.2052 (prohibits govt agencies from paying ransom related to cyber incident)
- Hawaii H.B.2171 (enacted, places cybersecurity, economic, education, and infrastructure security coordinator in the state department of law enforcement) [companion to S.B.3139]
- Hawaii S.B.1111 (establishes joint integration center to integrate information technology, cybersecurity, and cybercrime prevention) [companion to H.B.957]
- Hawaii S.B.3139 (places cybersecurity, economic, education, and infrastructure security coordinator in the state department of law enforcement) [companion to H.B.2171]
- Idaho H.B.621 (enacted, certain cybersecurity records are exempt from disclosure)
- Illinois H.B.900 (enacted, appropriations for costs associated with cybersecurity training)
- Illinois H.B.969 (appropriations for costs associated with cybersecurity training)
- Illinois H.B.2869 (unit of local govt may use technologies to execute duties where it utilizes accepted methods of data storage and cybersecurity)
- Illinois H.B.5615 (appropriations for cybersecurity risks and threats)
- Illinois H.B.5679 (appropriations for cybersecurity training and preparedness)
- Illinois S.B.2506 (unit of local govt may use technologies to execute duties where it utilizes accepted methods of data storage and cybersecurity)
- Illinois S.B.4074 (appropriations for cybersecurity training and preparedness)
- Illinois S.B.4087 (appropriations for cybersecurity risks and threats)
- Indiana H.B.1274 (establishes volunteer cyber civilian corps)
- Iowa H.F.2288 (modifies "essential county purpose" to include cybersecurity purposes – may act without approval by voters at election)
- Iowa H.S.B.670 (creates cybersecurity unit within office of chief information officer)
- Iowa H.S.B.691 (prohibits state or political subdivision from paying for ransomware attack)
- Iowa S.F.2207 (prohibits state or political subdivision from paying for ransomware attack)

- Iowa S.S.B.3068 (modifies "essential county purpose" to include cybersecurity purposes – may act without approval by voters at election)
- Kansas H.B.2292 (exemptions in open records act for cybersecurity assessments, plans, and vulnerabilities)
- Kansas H.B.2548 (cybersecurity awareness training program for all state agencies)
- Kansas H.B.2744 (sunset advisory committee – cybersecurity practices is considered as part of need determination for continuation of agency)
- Kansas S.B.250 (cybersecurity awareness training for all state agencies)
- Louisiana S.C.R.14 (enacted, creates task force to create distinct cause of action for state agencies that respond to cyber incidents to recover expenses in certain circumstances)
- Maryland H.B.419 (codifies offices focused on cybersecurity strategy and policy) [cross-filed with S.B.390]
- Maryland H.B.1339 (grant program for cybersecurity improvements to critical infrastructure) [cross-filed with S.B.810]
- Maryland H.B.1346 (vetoed, establishes Council in order to develop cybersecurity strategy) [cross-filed with S.B.812]
- Maryland S.B.390 (codifies offices focused on cybersecurity strategy and policy) [cross-filed with H.B.419]
- Maryland S.B.810 (grant program for cybersecurity improvements to critical infrastructure) [cross-filed with H.B.1339]
- Maryland S.B.812 (enacted, establishes Council in order to develop cybersecurity strategy) [cross-filed with H.B.1346]
- Massachusetts H.122 (state agencies that procure IT goods or services must give preference to vendors with cybersecurity insurance)
- Massachusetts H.5040 (study order of H.122)
- Massachusetts H.3132 (task force re: need for increased cybersecurity in govt agencies and offices)
- Massachusetts H.4858 (study order for H.3132)
- Massachusetts H.3133 (contracts involving tech component must comply with cybersecurity standards, if over $1,000,000)
- Massachusetts H.4910 (study order for H.3133)
- Massachusetts H.5260 (funding for infrastructure and improve cybersecurity)
- Massachusetts S.51 (office of data protection, cybersecurity and privacy)
- Massachusetts H.4892 (study order for S.51)

- Massachusetts S.2088 (Cybersecurity Control and Review Commission to recommend standards for interagency cybersecurity data collaboration)
- Massachusetts S.2564 (COVID19 funding for cybersecurity workforce and infrastructure) [substituted for H.4234 and reported as text of S.2580]
- Massachusetts S.2580 (COVID19 funding for cybersecurity workforce and infrastructure) [text of S.2564]
- Massachusetts S.D.2645 (funding for tech upgrades and information tech modernization projects)
- Michigan H.B.4373 (appropriations for modernization of state information tech systems)
- Michigan S.B.844 (enacted, appropriations for municipal information technology and cybersecurity upgrades)
- Minnesota H.F.1776 (appropriations to enhance cybersecurity across state govt) [companion to S.F.1875]
- Minnesota H.F.4125 (appropriations for grants to address cybersecurity risks and threats) [companion to S.F.4002]
- Minnesota H.F.4293 (appropriations for cybersecurity-related programs) [companion to S.F.3975]
- Minnesota H.F.4568 (Governor may declare emergency when actions endanger life and property and local govt resources cannot handle situation – this incudes cyberattacks) [companion to S.F.4388]
- Minnesota S.F.3975 (appropriations for cybersecurity-related programs) [companion to H.F.4293]

- Minnesota S.F.4002 (appropriations for grants to address cybersecurity risks and threats) [companion to H.F.4125]
- Minnesota S.F.4388 (Governor may declare emergency when actions endanger life and property and local govt resources cannot handle situation – this incudes cyberattacks) [companion to H.F.4568]
- Missouri H.B.2436 (Dept of Economic Development may provide grants to employers to enhance cybersecurity)
- Missouri S.B.674 (Dept of Economic Development may provide grants to employers to enhance cybersecurity)
- New Hampshire H.B.1277 (enacted, defines "cybersecurity incident")
- New Jersey A.493 (public agency reporting requirements re: cybersecurity incidents) [identical to S.297]
- New Jersey A.1848 (employees with access to state agency computers must receive training in cybersecurity best practices)
- New Jersey A.1962 (creation of cyberinfrastructure strategic plan) [identical to S.423]
- New Jersey A.4184 (hiring of cyber security professionals) [identical to S.2827]
- New Jersey S.297 (public agency reporting requirements re: cybersecurity incidents) [identical to A.493]
- New Jersey S.423 (creation of cyberinfrastructure strategic plan) [identical to A.1962]
- New Jersey S.2827 (hiring of cybersecurity professionals) [identical to A.4184]
- New Jersey A.J.R.66 (task force to make recommendations to government on cybersecurity threats) [identical to S.J.R.12]
- New Jersey S.J.R.12 (task force to make recommendations to government on cybersecurity threats) [identical to A.J.R.66]
- New York A.3900 (Commission to study EU's general protection data regulation and current state of cybersecurity in state) [same as S.6068]
- New York A.3904 (relating to assessments of vulnerability of critical infrastructure to cyberattacks) [substitute for S.5579]
- New York A.6984 (civilian cyber security reserve forces to educate and protect state against cyberattacks)
- New York A.9995 (cybersecurity enhancement funds to upgrade local govts) [same as S.6154]
- New York S.3213 (state agencies required to meet NIST Cybersecurity framework standards when procuring end point devices)
- New York S.5579 (relating to assessments of vulnerability of critical infrastructure to cyberattacks) [substituted by A.3904]

- New York S.6068 (Commission to study EU's general protection data regulation and current state of cybersecurity in state) [same as A.3900]
- New York S.6154 (cyber security enhancement funds to upgrade local govts) [same as A.9995]
- New York S.6806 (prohibits govt agencies from paying ransom in event of cyber incident)
- New York S.9005 (relates to state entities preparing for ransomware attack)
- North Carolina H.B.813 (prohibits state entities from paying ransom in connection with cybersecurity attack; attack must be reported)
- Ohio H.B.230 (cybersecurity and fraud advisory board to adopt best practices in cybersecurity)
- Oregon H.B.4155 (provides Oregon Cybersecurity Center of Excellence oversees providing education, awareness, and training for public and private sectors, cybersecurity workforce development)
- Pennsylvania H.B.40 (Office of Information Technology created to strengthen cybersecurity posture)
- Pennsylvania H.B.433 (appropriations for information technology cybersecurity)
- Pennsylvania H.B.1362 (Cybersecurity Coordination Board created)
- Pennsylvania H.B.2220 (appropriations for cybersecurity)
- Pennsylvania S.B.171 (appropriations for information technology cybersecurity)
- Pennsylvania S.B.482 (Office of Information Technology created to strengthen cybersecurity posture)
- Utah H.B.280 (enacted, creates Cybersecurity Commission to gather info on cybersecurity vulnerabilities and best practices for the state)
- Vermont H.304 (creates crime of intent to extort by introducing ransomware; creates Cybercrime Study Committee)
- Virginia H.B.1290 (enacted, reporting requirements relating to incidents that threaten security of data, including compromises to information technology systems)
- Virginia H.B.1304 (enacted, Virginia Information Technologies Agency tasked with advising CIO regarding cybersecurity policies, standards, and guidelines)
- Virginia S.B.703 (enacted, Virginia Information Technologies Agency tasked with advising CIO regarding cybersecurity policies, standards, and guidelines)
- West Virginia H.B.4498 (increases financial penalties for ransomware crimes)
- West Virginia S.B.520 (enacted, increases financial penalties for ransomware crimes)
- Wisconsin A.B.818 (requires admin rules promulgation relating to cybersecurity standards for state agencies and authorities)
- Wisconsin S.B.786 (requires admin rules promulgation relating to cybersecurity standards for state agencies and authorities)

Ransomware Focused Legislation (18 bills in 10 states)

In 2022, legislators in ten states introduced 18 bills related to payments and reporting of ransomware incidents. This list compares to 7 ransomware bills that were introduced in 6 states in 2021.

- Arizona H.B.2145 (prohibits payments to remove or decrypt ransomware, refers to schools districts and community college districts)
- California A.B.154 (requires reporting of cybersecurity incidents, including ransomware attacks, as condition of receiving funding)
- California S.B.154 (requires reporting of cybersecurity incidents, including ransomware attacks, as condition of receiving funding)
- Florida H.B.7055 (enacted, relates to reporting ransomware and cybersecurity incidents and training requirements)
- Florida H.B.7057 (enacted, public records requirements related to cybersecurity/ransomware)
- Florida S.B.1670 (mandatory reporting of attack, cybersecurity standards adopted)
- Florida S.B.1694 (public records requirements related to cybersecurity/ransomware)
- Hawaii H.B.2052 (prohibits govt agencies from paying ransom related to cyber incident)
- Iowa H.F.2461 (prohibits ransomware re: schools, community colleges, education agencies; exception for ransomware for research purposes)
- Iowa H.S.B.691 (prohibits state or political subdivision from paying for ransomware attack)
- Iowa S.F.2207 (prohibits state or political subdivision from paying for ransomware attack)
- Mississippi S.B.2530 (vetoed, expands enterprise security program and coordinated oversight of cybersecurity efforts; requires reporting of ransomware)
- New York S.6806 (prohibits govt agencies from paying ransom in event of cyber incident)
- New York S.9005 (relates to state entities preparing for ransomware attack)
- North Carolina H.B.813 (prohibits state entities from paying ransom in connection with cybersecurity attack; attack must be reported)
- Vermont H.304 (creates crime of intent to extort by introducing ransomware; creates Cybercrime Study Committee)
- West Virginia H.B.4498 (increases financial penalties for ransomware crimes)
- West Virginia S.B.520 (enacted, increases financial penalties for ransomware crimes)

Creation of Task Force, Commission, or Office Related to Cybersecurity (30 bills in 15 states)

In 2022, state legislators in 15 states introduced 30 bills[5] that proposed to create a task force, commission, or office of cybersecurity. This list compares to 28 such bills introduced in 14 states in 2021.

- Georgia H.B.159 (creates State Cybersecurity Review Board)
- Georgia S.B.596 (creates Georgia Cyberforce to protect citizens and assets from cyberattacks)
- Georgia S.R.741 (creates Study Committee on creation of Cybersecurity Force)
- Hawaii H.B.957 (establishes joint integration center to integrate information technology, cybersecurity, and cybercrime prevention) [companion to S.B.1111]
- Hawaii S.B.1111 (establishes joint integration center to integrate information technology, cybersecurity, and cybercrime prevention) [companion to H.B.957]
- Indiana H.B.1274 (establishes volunteer cyber civilian corps)
- Iowa H.S.B.670 (creates cybersecurity unit within office of chief information officer)
- Louisiana S.C.R.14 (enacted, creates task force to create distinct cause of action for state agencies that respond to cyber incidents to recover expenses in certain circumstances)
- Maryland H.B.419 (codifies offices focused on cybersecurity strategy and policy) [cross-filed with S.B.390]
- Maryland H.B.1346 (vetoed, establishes Council in order to develop cybersecurity strategy) [cross-filed with S.B.812]
- Maryland S.B.390 (codifies offices focused on cybersecurity strategy and policy) [cross-filed with H.B.419]
- Maryland S.B.812 (enacted, establishes Council in order to develop cybersecurity strategy) [cross-filed with H.B.1346]
- Massachusetts H.3132 (task force re: need for increased cybersecurity in govt agencies and offices)
- Massachusetts H.4858 (study order for H.3132)
- Massachusetts H.5374 (enacted, establishes cybersecurity center to foster cybersecurity resiliency with state agencies, municipalities, educational institutions, and private partners)
- Massachusetts S.51 (office of data protection, cybersecurity and privacy)
- Massachusetts H.4892 (study order for S.51)
- Massachusetts S.2088 (Cybersecurity Control and Review Commission to recommend standards for interagency cybersecurity data collaboration)

[5] This number also includes study orders in Massachusetts.

- New Jersey A.J.R.66 (task force to make recommendations to govt on cybersecurity threats) [identical to S.J.R.12]
- New Jersey S.J.R.12 (task force to make recommendations to govt on cybersecurity threats) [identical to A.J.R.66]
- New Mexico S.B.98 (Cybersecurity Act, establishes office and committee, and state chief of information security; assessment of cybersecurity services for govt agencies, including schools and districts and postsecondary institutions)
- New York A.3900 (Commission to study EU's general protection data regulation and current state of cybersecurity in state) [same as S.6068]
- New York S.6068 (Commission to study EU's general protection data regulation and current state of cybersecurity in state) [same as A.3900]
- Ohio H.B.230 (cybersecurity and fraud advisory board to adopt best practices in cybersecurity)
- Oregon H.B.4155 (provides Oregon Cybersecurity Center of Excellence oversees providing education, awareness, and training for public and private sectors, cybersecurity workforce development)
- Pennsylvania H.B.40 (Office of Information Technology created to strengthen cybersecurity posture)
- Pennsylvania H.B.1362 (Cybersecurity Coordination Board created)
- Pennsylvania S.B.482 (Office of Information Technology created to strengthen cybersecurity posture)
- Utah H.B.280 (enacted, creates Cybersecurity Commission to gather info on cybersecurity vulnerabilities and best practices for the state)
- Vermont H.304 (creates crime of intent to extort by introducing ransomware; creates CyberCrime Study Committee)

Cybersecurity Training Requirements (27 bills in 9 states)

In 2022, legislators in nine states introduced 27 bills[6] focused on cybersecurity training requirements. This list compared to 15 such bills that were introduced in 7 states in 2021.

- California S.B.767 (creation of educational technology plan, includes training and support for educators on cybersecurity and online safety)
- Georgia H.B.1217 (compliance standards for tech protection measures, includes development of guidelines for training of school personnel)
- Georgia H.R.877 (encourages department to provide funds for outreach efforts to promote and improve cybersecurity education, training, and workforce development)

[6] This number also includes study orders in Massachusetts.

- Georgia S.R.741 (creates Study Committee on creation of Cybersecurity Force)
- Illinois H.B.900 (enacted, appropriations for costs associated with cybersecurity training)
- Illinois H.B.969 (appropriations for costs associated with cybersecurity training)
- Illinois H.B.5165 (establishes cybersecurity liaison program to assist local govt units and school districts; also provides training for employees and school districts)
- Illinois H.B.5679 (appropriations for cybersecurity training and preparedness)
- Illinois S.B.3939 (enacted, establishes cybersecurity liaison program to assist local govt units and school districts; also provides training for employees and school districts)
- Illinois S.B.4074 (appropriations for cybersecurity training and preparedness)
- Kansas H.B.2548 (cybersecurity awareness training program for all state agencies)
- Kansas S.B.250 (cybersecurity awareness training for all state agencies)
- Maryland H.B.5 (creation of training program, will be required of certain employees in govt, higher education, and education) [cross-filed with S.B.107]
- Maryland H.B.1202 (vetoed, develop cyber assessments and develop online database of cybersecurity training resources for local govt. personnel – defined to include local school systems and local school boards) [cross-filed with S.B.754]
- Maryland H.B.1410 (publish cyber safety guide and training course to be implemented in public schools)
- Maryland S.B.107 (creation of training program, will be required of certain employees in govt, higher education, and education) [cross-filed with H.B.5]
- Maryland S.B.162 (publish cyber safety guide and training course to be implemented in public schools) [cross-filed with H.B.1410]
- Maryland S.B.754 (enacted, develop cyber assessment and develop an online database of cybersecurity training resources for local govt. personnel – defined to include local school systems and local school boards) [cross-filed with H.B.1202]
- Massachusetts H.112 (plan to hard-wire public education facilities; facilitate statewide PD plan and education materials to support cybersecurity)
- Massachusetts H.5040 (study order of H.112)
- Massachusetts H.4219 (COVID19 funding – may use funds for high demand workforce training program for in-demand fields, including cybersecurity) [published as H.4234]
- Massachusetts H.4234 (COVID19 funding – may use funds for high demand workforce training program for in-demand fields, including cybersecurity) [reported by H.4269]
- Massachusetts H.4269 (enacted, COVID19 funding – may use funds for high demand workforce training program for in-demand fields, including cybersecurity) [signed bill of H.4219 and H.4234]

- New Jersey A.1671 (state, county, and other employees to complete cybersecurity awareness training)
- New Jersey A.1848 (employees with access to state agency computers must receive training in cybersecurity best practices)
- New Mexico H.B.122 (funding to develop cybersecurity program for all schools/districts)
- Oregon H.B.4155 (provides Oregon Cybersecurity Center of Excellence oversees providing education, awareness, and training for public and private sectors, cybersecurity workforce development)

Additional Notable 2022 State Cybersecurity Legislation Themes:

Other notable topics covered in 2022 include cybersecurity insurance requirements (5 bills in 2 states); affirmative defenses where a cybersecurity plan is in place (6 bills in 3 states); defining student information for cybersecurity programs (1 bill in 1 state); and other miscellaneous bills relating to cybersecurity (4 bills in 2 states).

Cybersecurity Insurance Requirements (5 bills in 2 states)

- Arizona H.B.2690 (requires insurance for security system and data breaches)
- Arizona H.B.2857 (enacted, requires insurance for security system and data breaches)
- Arizona S.B.1724 (requires insurance for security system and data breaches)
- Massachusetts H.122 (state agencies that procure IT goods or services must give preference to vendors with cybersecurity insurance)
- Massachusetts H.5040 (study order of H122)

Affirmative Defenses re: Cybersecurity Plan (6 bills in 3 states)

- Illinois H.B.3030 (creates Cybersecurity Compliance Act – affirmative defense for covered entity where maintains written cybersecurity program)
- Illinois H.B.5243 (creates Cybersecurity Compliance Act – affirmative defense for covered entity where maintains written cybersecurity program)
- Iowa H.F.2302 (affirmative defense for entity using cybersecurity programs with certain safeguards)
- Iowa H.S.B.555 (affirmative defense for entities using cybersecurity programs)
- Iowa S.F.2049 (affirmative defense for entities using cybersecurity programs)
- Michigan S.B.672 (affirmative defense for entities with written cybersecurity program)

Student Information (1 bill in 1 state)

- Georgia H.B.260 (standards for cybersecurity programs to protect businesses from liability – personal information defined to include student information, such as grades)

Misc. (4 bills in 2 states)

- Florida H.B.7035 (amendments to conform for correct interpretation of law)
- Florida S.B.848 (enacted, amendments to conform for correct interpretation of law)
- New York A.8561 (crime of larceny by cyber extortion) [same as S.8296]
- New York S.8296 (crime of larceny by cyber extortion) [same as A.8561]

Federal Education Cybersecurity Bills Introduced in 2022

Education cybersecurity was also a popular topic at the federal level in 2022. Members of Congress introduced 22 cybersecurity bills with implications for the education sector, compared to 19 such bills in 2021 and 10 in 2020. Notable strategies featured in the bills include seeking more information and advice about the policy area through the creation of cybersecurity focused task forces or commissions, building the cybersecurity workforce through investments in postsecondary institutions and programs and apprenticeships, and making direct investments through competitive grants.

None of the education focused federal cybersecurity measures became law, but that outcome is not a complete surprise given the general cybersecurity investments that Congress approved as part of the Infrastructure Investment and Jobs Act in late 2021, which included the Digital Equity Act (H.R.1841 & S.2018). Given that a new congress will begin in January 2023, legislators must reintroduce any bills that contain strategies that they want to continue championing during the 118th Congress.

School Security Coordinating Council (1 bill)

One bill introduced by Congress in 2022 focuses on ensuring protection against threats in daycares and schools.

- **School and Daycare Protection Act** (H.R.6387) – Proposes to establish a school security coordinating council, which works to enhance the security of early childhood education programs and schools against acts of terrorism and other homeland security threats. The Director of the Cybersecurity and Infrastructure Security must be on this council.

Cybersecurity Policies (1 bill)

One bill introduced by Congress focuses on improving the cybersecurity of small entities, including governments with less than 50,000, as well as nonprofits and small businesses.

- **Improving Cybersecurity of Small Businesses, Nonprofits, and Local Governments Act** (H.R.6541) – Proposes to require the Director of the Cybersecurity and Infrastructure Security Agency to establish cybersecurity guidance for small organizations.

Funding and Appropriations (1 bill)

One bill introduced by Congress this session addressed funding and appropriations for cybersecurity-related measures, including by providing grants for schools.

- **Cybersecurity Grants for Schools Act of 2022** (H.R.6868) – Proposes grants for cybersecurity and infrastructure security education and training programs in elementary and secondary schools.

Task Forces or Commissions (3 bills)

Three bills would create task forces or foundations to improve responses to cybersecurity attacks.

- **Digital Equity Foundation Act of 2022** (H.R.8858 and S.4865) – Proposes to establish a Foundation for Digital Equity, which would, among many actions, work to strengthen and share best practices relating to projects promoting digital inclusion, digital literacy, and digital equity, including working to obtain basic awareness of measures to ensure online privacy and cybersecurity.
- **Improving Digital Identity Act of 2022** (S.4528) – Proposes to establish the Improving Digital Identity Task Force to initiate a government-wide effort related to securing methods for governmental agencies to protect the privacy and security of individuals.

Postsecondary Education (4 bills)

Four bills filed in 2022 relate to cybersecurity programs and funding at postsecondary institutions.

- **National Community College Cybersecurity Challenge Act** (H.R.8970) – Proposes funding to strengthen cybersecurity defenses and capabilities by expanding community colleges programs leading to the award of cybersecurity credentials.
- **Cybersecurity Clinics Grant Program Act** (H.R.9085) – Proposes a grant program to be carried out by the Department of Homeland Security to fund university-based cybersecurity clinics at junior or community colleges, historically Black colleges and universities (HBCUs), Hispanic-serving institutions (HSIs), and other minority-serving institutions.
- **Student Right to Know Before You Go Act of 2022** (S.3952) – Proposes a higher education data system to allow for more accurate, complete, and secure data relating to student retention, graduation, and earning outcomes – when designing, establishing, and maintaining the data system, the Secretary is required to use the best available cybersecurity and privacy-enhancing technologies to protect data.

- **National Innovation and Modern Skills Training Act of 2022** (S.4730) – Proposes a pilot program to provide competitive grants to land-grant colleges and universities relating to research and rapid workforce development and promote entrepreneurship – research programs must immerse participants in emerging science, technology, engineering, and mathematics fields and technologies, such as cybersecurity, among others.

Registered Apprenticeships (2 bills)

Two bills established registered apprenticeship programs focused on cybersecurity.

- **Cyber Ready Workforce Act** (H.R.6588 and S.3570) – Proposes a grant program to support the creation, implementation, and expansion of registered apprenticeship programs in cybersecurity.

Expanding Awareness (2 Resolutions)

Two resolutions filed in the House and Senate would expand awareness of cybersecurity issues.

- H.Res. 1154 - This resolution would express support for the designation of June 2022 as National Cybersecurity Education Month.
- S.Res. 680 – This resolution would designate June 2022 as National Cybersecurity Education Month.

Federal Cybersecurity Bills (8 bills)

Eight bills in 2022 focus on cybersecurity at the federal level.

- **Federal Information Security Modernization Act of 2022** (H.R.6497) – Proposes to modernize federal information security management and improves federal cybersecurity to combat persisting and emerging threats.
- **Quantum Computing Cybersecurity Preparedness Act** (H.R. 7535 and S.4592) – Proposes to encourage the migration of federal government information technology systems to quantum-resistant cryptography.
- **FedRAMP Authorization Act** (H.R.8956) – Proposes general improvements to the cybersecurity of the federal government.
- **Proactive Cyber Initiatives Act of 2022** (H.R.8403) – Proposes to encourage and enhance federal cybersecurity initiatives.
- **Strengthening American Cybersecurity Act of 2022** (S.3600) – Proposes to address cybersecurity threats against critical infrastructure and the federal government.
- **Advancing Cybersecurity Through Continuous Diagnostics and Mitigation Act** (S.3894) – Proposes to authorize the Secretary of Homeland Security to establish a continuous diagnostics and mitigation program in the Cybersecurity and Infrastructure Security Agency.

- **Intragovernmental Cybersecurity Information Sharing Act** (S.4000) – Proposes to require the establishment of cybersecurity information sharing agreements between the Department of Homeland Security and Congress.

Federal bills that carried over from 2021 but did not yet become law

- **National Apprenticeship Act of 2021** (H.R.447) – Proposes to amend the National Apprenticeship Act and would allow for the awarding of grants to expand the offerings of programs under the national apprenticeship system, including creating new apprenticeship programs in nontraditional apprenticeship industry or occupation, such as cybersecurity.
- **Connect America Act of 2021** (H.R.1672) - Proposes to establish a program to expand access to broadband service for "unserved anchor institutions," which may include schools. Any project must incorporate "prudent cybersecurity and supply chain risk management practices."
- **Accessible, Affordable Internet for All Act** (H.R.1783) - Proposes to establish the State Digital Equity Capacity Grant Program – This step would ensure that states have the capacity to "promote the achievement of digital equity and support digital inclusion activities." "Digital inclusion" is defined to include "obtaining basic awareness of measures to ensure online privacy and cybersecurity."
- **Digital Equity Act of 2021** (H.R.1841 & S.2018) – Proposes to establish the State Digital Equity Capacity Grant Program – this would ensure that states have the capacity to "promote the achievement of digital equity and support digital inclusion activities." "Digital inclusion" is defined to include "obtaining basic awareness of measures to ensure online privacy and cybersecurity."

- **College Transparency Act** (H.R.2030 & S.839) – Proposes to create a postsecondary student data system. The Commissioner is tasked with ensuring data privacy and security is consistent with federal law, including security requirements, guidelines and controls are consistent with cybersecurity standards and best practices developed by the National Institute of Standards and Technology.
- **Securing American Leadership in Science and Technology Act of 2021** (H.R.2153) – Proposes to protect research from cyber theft by improving cybersecurity of institutions of higher education, among other actions.
- **State and Local Cybersecurity Improvement Act** (H.R.3138 & S.2585) – Proposes to authorize a grant program relating to the cybersecurity of State, local, Tribal, and territorial governments. Eligible entities that receive grants must establish a cybersecurity planning committee which must include representatives from institutions of public education within the entity's jurisdiction.
- **Jobs, On-the-Job 'Earn-While-You-Learn' Training, and Apprenticeships for Young African Americans Act** (H.R.3445) – Proposes to amend the National Apprenticeship Act and would allow for the awarding of grants to registered entities to expand or create diversity in registered apprenticeship programs. The registered apprenticeship target programs include programs demonstrating demand in cybersecurity.
- **Enhancing K-12 Cybersecurity Act** (H.R.4005) – Proposes to require the Director of the Cybersecurity and Infrastructure Security Agency to establish a School Cybersecurity Improvement Program. Further, this bill would create a new publicly accessible website – School Cybersecurity Information Exchange – to disseminate information, cybersecurity best practices, and lessons learned that are tailored to the specific needs for K-12 organizations.
- **21st Century Jobs Act** (H.R.4461) – Proposes to provide, among many things, funds to federal, state, and local agencies for programs and research in certain technology sectors, which includes cybersecurity.
- **State Cyber Resiliency Act** (H.R.4910) – Proposes to establish the State Cyber Resiliency Grant Program to assist state, local, and tribal governments in preventing, preparing for, protecting against, and responding to cyber threats.
- **Cybersecurity Opportunity Act** (H.R.5593 & S.2305) – Proposes to establish grants to assist institutions of higher education to establish or expand cybersecurity programs, with a particular focus on needy students, historically Black colleges and universities, and minority-serving institutions.
- **Accessible, Affordable Internet for All Act** (S.745) – Proposes to establish the State Digital Equity Capacity Grant Program – this would ensure that states have the capacity to "promote the achievement of digital equity and support digital inclusion activities." "Digital inclusion" is defined to include, "obtaining basic awareness of measures to ensure online privacy and cybersecurity."

- **Children and Teens' Online Privacy Protection Act** (S.1628) – Proposes to prohibit the sale of internet-connected devices targeted to children and minors unless they meet certain cybersecurity and data security standards.
- **Department of Homeland Security Appropriations Act 2022** (S.3058) - Proposes to provide an appropriation for the Cybersecurity and Infrastructure Security Agency for cyber response and recovery. This funding must be used to, "provide support to critical infrastructure, including through the provision of services, technology, or capabilities." This support may include assistance to private entities and government agencies in responding to or recovering from a significant cyber incident.
- **BRIDGE Act** (S.2071) – Proposes to provide for certain grants, which eligible entities may use for digital inclusion, such as digital literacy and digital equity programs. "Digital inclusion" is defined to include, "obtaining basic awareness of measures to ensure online privacy and cybersecurity."
- **University Cybersecurity Consortia Improvement Act of 2021** (S.2905) – Proposes to establish requirements relating to establishment of a consortium of universities to advise the Secretary of Defense on cybersecurity matters.

LEADING EDUCATION INNOVATION

www.cosn.org/cybersecurity/2022legislation