CoSN

Leading Education Innovation

Summary of Education Cybersecurity Policy Developments in 2023

January 2024

Contents

CoSN
Leading Education Innovation

This report is based on research funded by the Bill & Melinda Gates Foundation. The findings and conclusions contained within are those of the authors and do not necessarily reflect positions or policies of the Bill & Melinda Gates Foundation.

CoSN's Mission:

CoSN provides current and aspiring K12 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-2023legislation.

Introduction

Cyberattacks are a costly, educationally disruptive, and constantly evolving threat to schools and the confidential personally identifiable information they collect and maintain. According to a recent Government Accountability Office (GAO) report, when a school district is attacked the "…loss of learning following a cyberattack ranged from 3 days to 3 weeks, and recovery time could take anywhere from 2 to 9 months…". The same report said school districts' financial losses from attacks can "…range from $50,000 to $1 million due to expenses caused by a cyber incident."[1] The Consortium for School Networking's 2023 State of Ed Tech Leadership Survey echoes the GAO's troubling findings, noting that "…cybersecurity continues to rank as the number-one concern for EdTech Leaders."[2] Preventing future cyberattacks on schools will require innovative solutions and close collaboration with education leaders and policymakers at all government levels. Given that this challenge spans the nation, CoSN is pleased to publish this annual report highlighting education cybersecurity policy trends for practitioners, legislators, and other government leaders responsible for protecting education networks and data from ransomware attacks and other cybersecurity incidents.

Compared to 2020 when CoSN began monitoring policymakers' response to the growing number of attacks, the number of education cybersecurity bills introduced by state legislators increased by over 250% to 307 and the number of new laws adopted by states increased by 620% to 75. State leaders have not only begun to pay greater attention to the education sector's cybersecurity needs they have also started, incrementally, to adopt a wider range of policy strategies, such as creating cyber risk insurance funds, establishing regional alliances and multistakeholder partnerships, launching scholarship programs and other initiatives to expand the cybersecurity workforce, and, in at least one state, creating a task force to examine the relationship between artificial intelligence and cybersecurity. Congress has been less active than individual states on education specific cybersecurity policy in 2023, but federal agencies, including the Federal Communications Commission and Cybersecurity and Infrastructure Security Administration, have proposed, and taken notable new steps in 2023 to help schools and other education entities better defend themselves.

This year's report inventories the state and federal education cybersecurity bills and laws that emerged in 2023, and highlights notable policy ideas and trends, with the goal of helping education technology leaders, school administrators, and policymakers identify promising models and strategies. Drawing on these developments—and CoSN's other cybersecurity technical assistance initiatives—the report also suggests policy and practice ideas for leaders to evaluate and potentially adopt in their own states and communities.

---

[1] U.S. GAO Watch Blog, *As Cyberattacks Increase on K-12 Schools, Here Is What's Being Done* (Dec. 2022).

[2] CoSN, *2023 State of EdTech Leadership Tenth Annual National Survey,* p.6, available online at www.CoSN.org.

Executive Summary

Compared to 2020, when CoSN initiated the monitoring of policymakers' responses to the escalating number of cyberattacks in the education sector, the year 2023 witnessed a remarkable surge in legislative activity. State legislators introduced an astounding 250% increase in education cybersecurity bills, totaling 307, while the number of new laws enacted by states experienced an unprecedented growth of 620%, reaching a total of 75 laws. This surge is indicative of state leaders' heightened focus on the cybersecurity needs of the education sector, coupled with their gradual exploration and adoption of a broader spectrum of policy strategies.

Noteworthy policy developments in 2023 include:

- Cyber Risk Insurance Funds: States have undertaken the creation of cyber risk insurance funds aimed at mitigating the escalating insurance costs faced by school districts.
- Regional Alliances and Partnerships: Efforts to establish and reinforce regional alliances and multistakeholder partnerships to foster information sharing and collaborative responses to cyberattacks are gaining momentum.
- Cybersecurity Workforce Expansion: Initiatives such as scholarship programs have been launched to address the shortage of adequately trained cybersecurity experts.
- Governance Enhancement: Governance structures are being improved to consolidate responsibility and establish robust prevention and response mechanisms across agencies.
- Cybersecurity Task Forces: The establishment of task forces and similar structures is being pursued to comprehensively study the cybersecurity landscape, including exploring the intersection of artificial intelligence and cybersecurity.

While state legislatures demonstrated remarkable activity, Congress also considered noteworthy ideas in 2023:

- Enhanced Information Exchange: Legislators introduced bills directing the Cybersecurity and Infrastructure Security Agency (CISA) to enhance information exchange efforts, with a specific focus on addressing the needs of K-12 organizations.
- Expanded Apprenticeship System: Congress is considering an idea to expand the national apprenticeship system to encompass nontraditional areas, including cybersecurity.
- Critical Infrastructure Workforce Competencies: Legislation proposes to direct the U.S. Secretary of Education to take measures aimed at enhancing the cybersecurity competencies of the critical infrastructure workforce.
- Cybersecurity Literacy Campaign: Bills also proposed to require the National Telecommunications and Information Administration (NTIA) to develop and execute a cybersecurity literacy campaign, designed to enhance the cybersecurity knowledge and awareness of Americans.

In addition to legislative actions, federal agencies, such as the Federal Communications Commission (FCC) and the Cybersecurity and Infrastructure Security Administration (CISA), have taken notable strides in 2023 to assist schools and educational entities in bolstering their cyber defenses. For example, the FCC proposed a K-12 School and Public Library Cybersecurity Pilot program, offering up to $200 million in grants, and CISA published technical assistance resources and other tools for school districts.

Drawing upon CoSN's extensive collection of cybersecurity technical assistance materials and the policy trends identified in the 2023 report, we formulated policy recommendations aligned with our cybersecurity pillars:

- Planning: We advocate for a comprehensive examination of emerging cybersecurity challenges.
- Prevention & Preparation: Strengthening governance structures and providing adequate training to employees and end users are essential components of a robust cybersecurity strategy.
- Implementation: The allocation of dedicated funding, expansion of the cyber workforce, and the timely replacement of outdated technology are pivotal for effective implementation.
- Response: To enhance response capabilities, we stress the importance of improving information sharing among stakeholders.

In conclusion, the policy landscape in 2023 reflects a significant and dynamic response to the evolving challenges in education cybersecurity. CoSN remains committed to guiding stakeholders through these complex issues and facilitating the development of effective policies and strategies to safeguard our educational institutions.

FIGURE 1: EDUCATION CYBERSECURITY POLICY 2023 LANDSCAPE

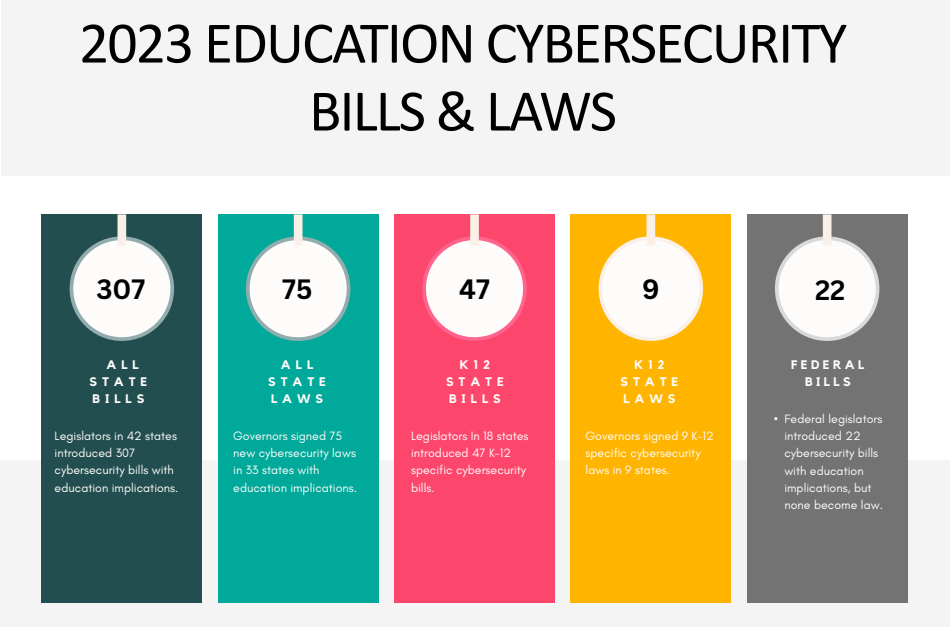
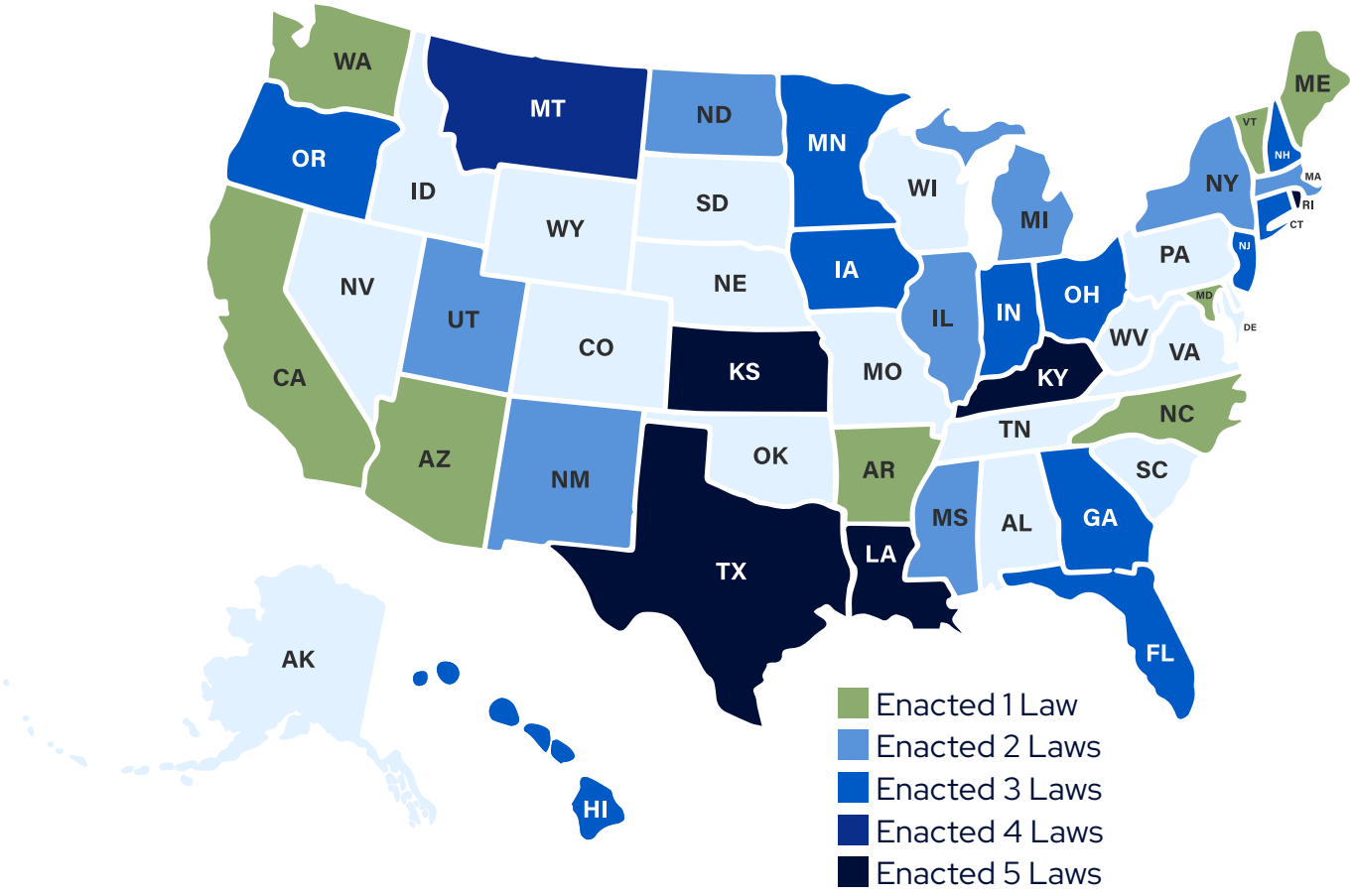


FIGURE 2: COSN CYBERSECURITY POLICY IDEAS

CoSN encourages local, state, and federal leaders to consider the following ideas drawn from our analysis of the 2023 education cybersecurity legislative landscape.

Policy Issue Areas	Cybersecurity Policy Ideas	New State Law Examples
Train Employees and Users	• Encourage school districts to train all employees and users about the district's cyber security policy.	Arkansas (H.B.1369), Florida (S.B.2500), Maryland (S.B.610), Oregon (H.B.2049)
Provide Insurance Funding and Encourage Risk Sharing	• Provide funding to help school districts acquire cyber security insurance; Create statewide mechanisms to pool school districts' risk.	Arkansas (H.B.1780), Arizona (S.B.1720), Minnesota (H.B.2497), Oregon (H.B.2490)
Expand Information Sharing	• Ensure that school districts are included in statewide efforts to coordinate information sharing among government agencies.	California (A.B.1023), Florida (S.B.2500), Hawaii (H.B.1036), Michigan (S.B.173), North Carolina (H.B.259)
Improve Governance	• Adopt a statewide governance structure for oversight and coordination of cybersecurity among state agencies, boards, commissions, and other entities, including school districts.	Connecticut (S.B.933), Kansas (H.B.2019), New Hampshire (H.B.519), New Mexico (S.B.280)
Replace Outdated Technology	• Provide funding for cybersecurity enhancements to help school districts procure, implement, and maintain advanced cybersecurity tools.	Hawaii (S.R.75), Minnesota (H.F.1830), New Hampshire (H.B.25)
Expand the Workforce	• Invest in cybersecurity workforce development programs that leverage public colleges and universities, community colleges, and STEM and CTE programs.	Illinois (H.B.1378), Iowa (S.F.560), Louisiana (H.B.1), Oregon (H.B.2049)
Provide Dedicated Funding for Schools	• Provide funding dedicated to bolstering school districts' cybersecurity readiness.	Texas (H.B.1), Michigan (S.B.173)
Study Artificial Intelligence and Cybersecurity	• Develop a task force or other mechanism for exploring the challenges artificial intelligence may pose school districts' cybersecurity.	Illinois (H.B.3563)

FIGURE 3: STATE EDUCATION CYBERSECURITY LAWS ENACTED IN 2023

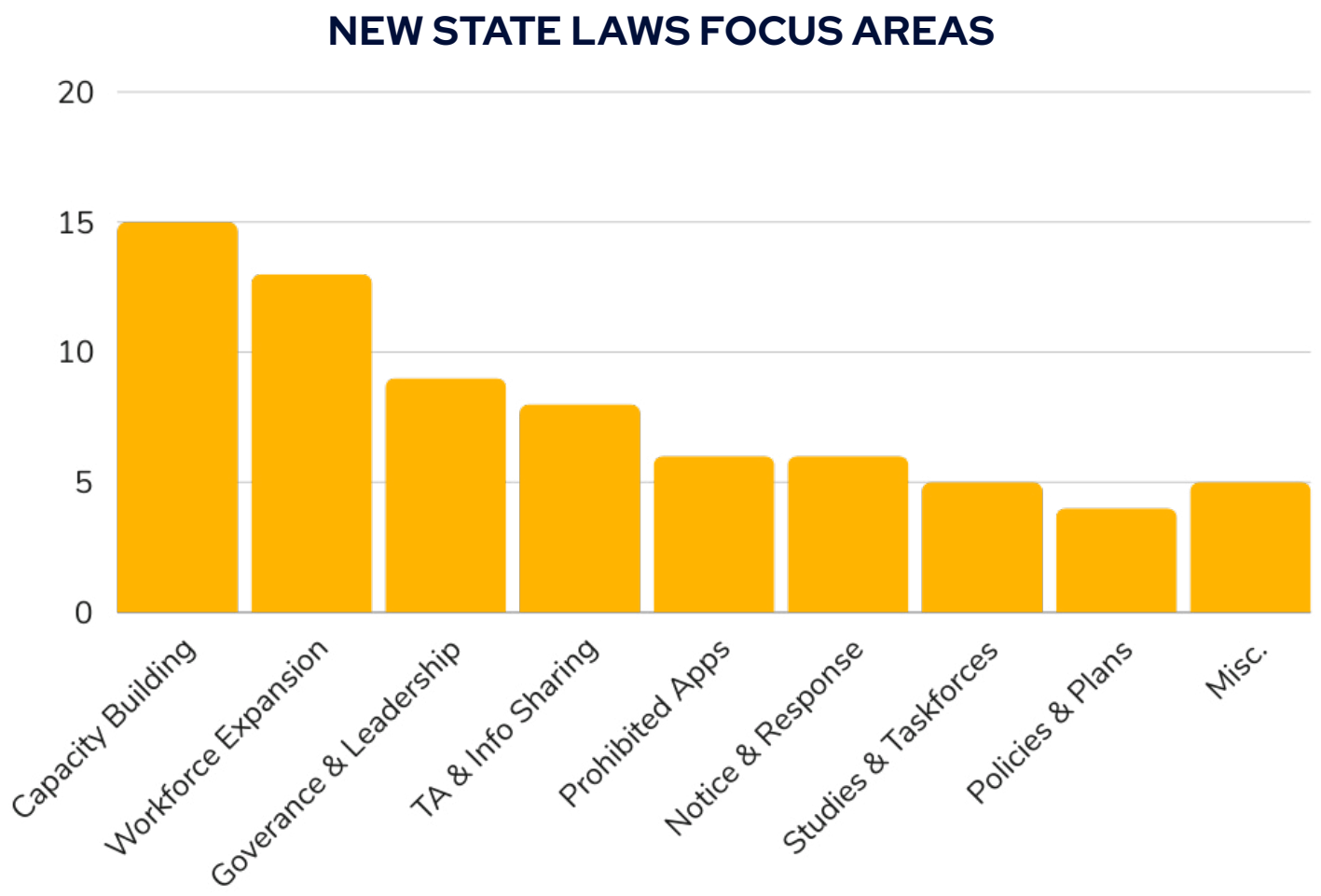


State Education Cybersecurity Laws Overview

In 2023, thirty-three states adopted seventy-five new cybersecurity statutes, including spending measures, affecting the education sector either directly or indirectly. This activity represents a significant increase from previous years, when governors signed thirty-seven bills in 2022, forty-nine in 2021, and ten in 2020. Legislation introduced in 2023 largely sought policy revisions that applied to all state and local government units rather than specifically focusing on school districts. New laws adopted in 2023 cover a variety of cybersecurity policies and strategies, such as providing funding for infrastructure and other capacity building, actions to be taken following cyber-attacks, establishing policies and plans, forming task forces, boards, or commissions, expanding the cybersecurity workforce through recruitment and training, mandating cybersecurity incident reporting, strengthening governance, and studying artificial intelligence's role in cybersecurity.

Nine of the new state laws focus on enhancing cybersecurity in elementary and secondary education. For example, Arkansas mandated annual reviews and updates of schools' cybersecurity policies. California required the California Cybersecurity Integration Center to coordinate and provide information to school districts. Illinois created a task force to develop model policies for schools for addressing artificial intelligence use and its cybersecurity implications. Maryland required virtual schools to provide cybersecurity policy information to parents. Michigan and Minnesota allocated funds to strengthen school cybersecurity measures and infrastructure, including cyber insurance coverage. New Mexico required educational technology plans that describe cybersecurity protections to be submitted to the Department of Education. North Dakota required cybersecurity-inclusive computer science instruction in schools. Lastly, Texas provided significant new funding for K-12 cybersecurity and required the Texas Education Agency to establish standards for electronic devices and software in school districts, ensuring that parents are informed about cybersecurity risks and online safety.

FIGURE 4: FOCUS AREAS OF STATE CYBERSECURITY LAWS ENACTED IN 2023



High Level Summaries of the State Cybersecurity Laws Enacted in 2023

Capacity Building Funding

- **Arizona S.B.1720**—Provides funding to the Arizona Department of Homeland Security for statewide cybersecurity grants. The law also provides an appropriation for the cyber risk insurance fund which was established in 2022 and requires the Arizona Department of Administration to submit a report to the legislature on expenditures made from the cyber risk insurance fund.
- **Arkansas H.B.1780**—Creates the Arkansas Self-Funded Cyber Response Program Act for participating governmental entities to provide coverage for cybersecurity incidents and risks, damages, or losses caused by a cyberattack that are committed against a participating governmental entity. School districts may participate in the program.
- **California S.B.101**—Makes appropriations for the state government for the 2023-24 fiscal year and would provide funding for various cybersecurity programs, including funding for the California Cybersecurity Integration Center. The law requires a report to the legislature on state implementation of cybersecurity initiatives and technical capability investments in Cal-Secure and Cal-CSIC's use of additional resources to address specific capability gaps and goals within Cal-CSIC. A report also must be submitted to the Legislature on the State and Local Cybersecurity Grant program. Funding is provided for community college districts to implement local and systemwide technology and data security measures that support improved oversight of cybersecurity efforts. These funds may be used to hire local cybersecurity staff and for systemwide measures, including security upgrades for CCCApply and education technology platforms and the establishment of systemwide cybersecurity teams.
- **Louisiana H.B.560**—Provides funding to the Board of Regents for cybersecurity software for all institutions of higher education.
- **Maine L.D.206**—Provides appropriations for fiscal year 2022-23 only and authorizes the Department of Administrative and Financial Services to transfer available balances of Personal Services appropriations in the Information Services program, General Fund account after all salary, benefit, and other obligations are met to the "All Other" line category of the Information Services program, General Fund account for the purposes of funding statewide cybersecurity costs.
- **Maryland H.B.552**/**S.B.549** (Companion bills)—Establishes the Build Our Future Grant Pilot Program, which provides grant funding for infrastructure projects intended to support innovation in an eligible technology sector. Grants may be awarded to private companies, nonprofit entities, local governments, or colleges and universities in the state. Eligible technology sectors include cybersecurity.

- **Massachusetts H.58**—Provides funding for the Massachusetts Technology Park Corporation for a matching grant program that enables academic institutions, nonprofits, industry consortiums, federally funded research and development centers, and other technology-based economic development organizations to compete for federal grants in technology and innovation fields, which includes cybersecurity.
- **Massachusetts H.4040**—Provides funds for the Massachusetts Bay Community College, of which not less than $85,000 should be expended for the MassBay Center for Cybersecurity Education. Further funds would be used for the operation of an information technology audit unit within the office of the state auditor to conduct audits of high-risk information technology related activities, including cybersecurity, data access, systems operations, data integrity, and regulatory compliance. Appropriations are also made for the Massachusetts Cybersecurity Innovation Fund to be used for community colleges and state universities, to provide regional security operations center services for the monitoring and detection of cyber threat activity, and include opportunities for cybersecurity workforce training.
- **Michigan S.B.173**—Amends the State School Aid Act—existing law provides for a school consolidation and infrastructure fund. Districts or intermediate districts may apply for these grants, so long as they conduct a feasibility study or analysis. The study or analysis may include consolidation opportunities in a variety of areas, including information technology—this may include cybersecurity. Further, this provides funding for an intermediate district with K to 12 student membership to establish and operate a statewide Security Operations Center in partnership with a statewide educational organization. The law also requires reporting related to this Center that includes measurable outcomes including the response to cybersecurity incidents in order to evaluate the effectiveness of the project. Finally, funds are allocated to the Dearborn City School District to support a cybersecurity certificate program.
- **Minnesota H.F.1830**—Provides funding for the cybersecurity grant program which provides support for state and local cybersecurity improvement projects for political subdivisions and Minnesota Tribal governments. Further, funding is provided for statewide cybersecurity enhancements to procure, implement, and support advanced cybersecurity tools that combat persistent and evolving cybersecurity threats.
- **Minnesota H.F.2497**—Provides funding for grants to school districts and charter schools to improve building security and cybersecurity. Funds may be used for security-related facility improvements, cybersecurity insurance premiums, and associated costs. This is a one-time appropriation. Further this bill amends language relating to the use of safe schools revenue—funds may be used to pay for the cost of cybersecurity measures, including updating computer hardware and software, other systems upgrades, and cybersecurity insurance costs.
- **New Hampshire H.B.2**—Makes an appropriation to the commissioner of the department of safety for the state and local cybersecurity grant program.

- **New Hampshire H.B.25**—Makes appropriations for capital improvements. Funding is provided for the Department of Information Technology for cybersecurity program enhancements.
- **New York S.4000**—Provides funding for the cyber incident response program for the Division of Homeland Security and Emergency Services State Operations.
- **Texas H.B.1**—Provides funds for cybersecurity for state agencies and institutions of higher education. Further, this bill establishes the Interagency Cybersecurity Initiative for Public Schools. Funds may be used to provide cybersecurity services to public school districts and placement and oversight of cybersecurity practitioners to assist local education agencies.
- **Texas S.B.30**—Provides supplemental appropriations and reductions in appropriations. Specifies that the unencumbered appropriations from the ARPA fund and related increase in capital budget authority made to the Department of Information Resources by the Supplemental Appropriations Act (2021) for cybersecurity projects are reduced by $200,000,000. This law also appropriates funds to the Higher Education Coordinating Board for a two-year period for the purposes of data modernization, technology infrastructure, cybersecurity, and application modernization.

Workforce Expansion

- **Florida S.B.2500**—Makes appropriations to several institutions of higher education for cybersecurity-related programs. Funding is also provided for Enterprise Cybersecurity Resiliency at the Florida Center for Cybersecurity at the University of South Florida in order to position Florida as the national leader in cybersecurity and its related workforce through education, research, and community engagement; assist in the creation of jobs in the state's cybersecurity industry and enhance the existing cybersecurity workforce; act as a cooperative facilitator for state business and higher education communities to share cybersecurity knowledge, resources, and training; among other initiatives.
- **Hawaii H.R.88** (Resolution)—Urges Microsoft to consider building a data center in Hawaii. The resolution notes that Microsoft has demonstrated its commitment to workforce development and cybersecurity in the state through a grant to the Hawaii Community College and American Association of Community Colleges' Cyber Skills for All Initiative, which helps fund and provide technical assistance to community colleges to accelerate their cybersecurity programs. Further, this initiative is part of Microsoft's national campaign to help community colleges work to train and recruit people for jobs in the cybersecurity workforce.
- **Illinois H.B.1378**—Creates the Illinois Graduate and Retain Our Workforce (iGROW) Tech Scholarship Fund to recruit and train individuals to work in technology jobs that have a high demand for new employees and offer high wages by awarding scholarships. Eligible applicants include those students who maintain a specific grade point average and who are pursuing or intend to pursue a qualifying degree in a qualified institution. A "qualifying degree", as defined in this bill, includes an associate or bachelor's degree granted by a qualified institution in a variety of fields, including information systems security or information assurance, including cybersecurity, among other fields.

- **Indiana H.B.1266**—Establishes the Indiana cyber civilian corps program advisory board. This board is tasked with providing findings and recommendations concerning the establishment of an Indiana cyber civilian corps program to the legislative council.
- **Iowa S.F.560**—Provides funding to prepare Iowa's future ready workforce and fostering innovation, including addressing the state's workforce needs in certain areas, including cybersecurity.
- **Louisiana H.B.1**—Provides funding for the Louisiana Cybersecurity Talent Initiative Fund. This fund, established in statute, provides money for degree and certificate programs in cybersecurity fields offered by public postsecondary education institutions to meet the state's workforce needs.
- **Maryland S.B.801**—Establishes the Cyber Maryland Program to increase the cybersecurity workforce in the state, build an advanced cybersecurity workforce, and inform cybersecurity training and education programs operated by public or private entities with industry-driven needs. This program would also work to coordinate and accelerate cybersecurity research and innovation in the state. The law also requires the Maryland Higher Education Commission to expand the Cyber Warrior Diversity Program. The law creates a Cyber Maryland Fund—these funds may be used to provide grants to elementary and secondary schools, institutions of higher education, including community colleges, for-profit corporations, and nonprofit organizations to operate cybersecurity programs.
- **Michigan H.B.4437**—Provides funding for cybersecurity programs, including Homeland Security initiative cybersecurity and vendor cybersecurity monitoring. This includes funding to the Michigan Department of Technology, Management, & Budget for agreements to provide spatial information and technical services to other principal executive departments, state agencies, local units of government, and other organizations for information technology services, including cybersecurity. The law further notes that funds appropriated for the information technology investment fund must be used for the modernization of state information technology systems and for the improvement of the state's cybersecurity framework. Funds for vendor cybersecurity monitoring must be used to improve the cybersecurity posture and expand the vulnerability monitoring of the executive departments and agencies and their vendor ecosystems to reduce the risk of cybersecurity breaches. This law provides funds for workforce development grants—from these funds, an allocation is provided to an arts and technology nonprofit organization in a county with a population between 600,000 and 700,000 for a cybersecurity program for students.
- **Minnesota H.F.669**—Provides funding specific to Metropolitan State University to design, renovate, and equip space for a cybersecurity program.

- **Montana H.B.10**—Provides an appropriation to the Department of Administration, State Information Technology Services for the Montana Cybersecurity Enhancement Project. The law also appropriates $6,164,320 to the Montana university system/University of Montana for the cyberMontana cybersecurity initiative.
- **North Dakota H.B.1398**—Amends existing law and specifies that each public and nonpublic elementary and middle school must provide instruction in computer science, including cybersecurity. Further, the law requires each public and nonpublic high school to provide instruction in, or make available to each student, one unit of computer science or cybersecurity. Schools, including elementary, middle, and high school, would be required to develop a computer science and cybersecurity integration plan. Finally, the law amends the minimum requirements for high school graduation, which would now specify, after 2025, that the one unit or two one-half units of any other science may include one unit of computer science or cybersecurity; but one unit of computer science would be required for graduation.
- **Rhode Island H.5200**—Establishes the Rhode Island Longitudinal Data System (RILDS) and specifies the function of the RILDS, which includes transmitting, storing, and enabling access to, permit the use, and dispose of linked data and information, which must be done in accordance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The law also provides funds to support the establishment of the Institute for Cybersecurity and Emerging Technologies at Rhode Island College, which will provide certificate, baccalaureate, and master's level courses with focuses on research and developing highly skilled cybersecurity professionals.
- **Utah H.B.215**—Establishes the Utah Fits All Scholarship Program. The program manager would be tasked with contracting with an entity to develop a system to establish the scholarship accounts. The law also requires the program manager to ensure that the system complies with industry standards for data privacy and cybersecurity.

Governance and Leadership

- **New Hampshire H.B.519**—Establishes a chief information security officer for the department of information technology. This position would have the authority and power to direct the formulation and implementation of cybersecurity and information security strategy, direction, policy, procedures, and standards across the executive branch of the state government. The chief information security officer has many duties, including establishing and maintaining within the department a cybersecurity integration center to serve as the unified state center for coordinating cybersecurity monitoring, sharing information, distributing cybersecurity threat analysis, and enabling situational awareness between and among executive branch agencies and departments.

- **New Jersey A.4184**—Prohibits the Department of Community Affairs from excluding the hiring of information technology or cybersecurity professionals pursuant to a shared services agreement from any program, activity, assistance, or offering, administered by the Department of Community Affairs to incentivize local units into shared services agreements when information technology or cybersecurity shared services are potential eligible uses of program funds.
- **New Jersey A.4836**—Requires the Office of Information Technology to develop a coordinated statewide response plan to address internet outages caused by a cyberattack—the plan must incorporate a framework to address cybersecurity incidents that shall, at a minimum, serve as a mechanism to facilitate and coordinate preparation for detection, analysis, containment, and eradication of, and recovery from, a cybersecurity incident, and to prescribe post-incident activity.
- **New Mexico S.B.280**—Creates the Cybersecurity Act, which establishes the cybersecurity office—this office would be responsible for all cybersecurity and information security related functions for agencies, as well as other tasks. The law also establishes the cybersecurity advisory committee which is created to assist in developing a statewide cybersecurity plan and guidelines for best cybersecurity practices for agencies, as well as recommendations on how to respond to a specific cybersecurity threat or attack.
- **New York A.3005**—Amends existing law regarding reporting requirements that fall under New York law relating to the division of homeland security and emergency services. Amendments specify that the chief information security officer of the state office of information technology services would also participate in the meetings to supplement the report delivered by the director to the legislature. The chief information security officer would supplement the report with information on the state's cybersecurity infrastructure and cybersecurity resiliency efforts.
- **North Dakota S.B.2073**—Existing law specifies that the information technology department performs certain services for state agencies including overseeing cybersecurity strategy for all executive branch state agencies, including institutions under the control of the state board of higher education, counties, cities, school districts, or other political subdivisions. This law amends existing law to specify that the department may provide information technology and cybersecurity services to any administrative, elementary education, secondary education, and higher education institution under the control of a tribal government of this state. The services provided and the cost of services must be equal to those provided to state agencies.
- **Oregon H.B.2806**—Authorizes governing bodies of public bodies to meet in executive session to consider matters relating to safety of governing bodies, public body staff, and public body volunteers and to security of public body facilities and meeting spaces, and relating to cybersecurity infrastructure and responses to cybersecurity threats.

- **Oregon H.B.2049**—Transfers the Oregon Cybersecurity Advisory Council from the Office of Enterprise Information Services to Oregon Cybersecurity Center of Excellence. The Oregon Cybersecurity Center of Excellence is established at Portland State University. This center seeks to supplement the activities of the State Chief Information Officer regarding cybersecurity in the state. This includes coordinating, funding, or providing: awareness, education, and training about cybersecurity for public, private, and nonprofit sectors; cybersecurity workforce development programs in coordination with public universities, community colleges, STEM, and CTE programs; research about cybersecurity education and training methodologies; cybersecurity-related goods and services to Oregon public bodies, with priority given to education service districts, school districts, and libraries; among others. This law also provides appropriations for the Oregon Cybersecurity Center of Excellence Operating Fund, the Oregon Cybersecurity Workforce Development Fund, and the Oregon Cybersecurity Grant Program Fund.
- **Texas H.B.18**—Amends existing statutes relating to the transfer of data processing equipment and electronic devices to students. The law specifies that the Texas Education Agency must adopt standards for permissible electronic devices and software applications used by school districts. In adopting these standards, the Agency must ensure that parents are provided the resources necessary to understand cybersecurity risks and online safety regarding their child's use of electronic devices before the child uses an electronic device at school. The standards must also ensure that the appropriate officer of a district or school is assigned the duty to receive complaints or concerns regarding student use of electronic devices, including cybersecurity and online safety concerns, from district or school staff, other students, or parents. Further, the law amends existing statutes to specify that prior to transferring data processing equipment or an electronic device to a student, the school district must adopt rules establishing programs promoting parents as partners in cybersecurity and online safety that involve parents in students' use of transferred equipment or electronic devices.

Technical Assistance and Information Sharing

- **California A.B.569**—Establishes the Cybersecurity Regional Alliances and Multistakeholder Partnerships Pilot Program to address the cybersecurity workforce gap, in several ways, including by stimulating cybersecurity education and workforce development, aligning the cybersecurity workforce needs of employers with education and training, increasing the pipeline of students pursuing cybersecurity careers, and developing the cybersecurity workforce to meet industry needs. Requires the Office of the Chancellor of the California State University to submit a comprehensive report on the pilot program to the legislature by July 1, 2028.
- **California A.B.1023**—Requires the California Cybersecurity Integration Center to include representatives from the State Department of Education. Expressly includes school districts, county offices of education, and charter schools among the specified entities with which Cal-CSIC coordinates information sharing, including cyber threat information.

- **California A.B.1637**—Requires local agencies that maintain internet websites for use by the public to ensure that the website utilizes a ".gov" top-level domain or a ".ca.gov" second-level domain, which increases security. Further, any local agency that maintains public email addresses must ensure that each email address provided to its employees utilizes a ".gov" domain name or a ".ca.gov" domain name. Both must occur by January 1, 2029. The law specifies that if the Commission on State Mandates determines that the act contains costs mandated by the state, reimbursement to local agencies and school districts for those costs shall be made pursuant to the Government Code. Defines "local agency" to mean a county, city, or city and county.
- **Hawaii H.B.1036**—Establishes the Hawaii state fusion center within the office of homeland security. This center would monitor all crimes and hazards and would coordinate with local, state, and federal agencies for homeland security response activities, which would include furnishing technical assistance to affected agencies to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents.
- **Iowa S.F.557**—Provides funding through the Department of Management for cybersecurity services to local governments.
- **Louisiana H.B.388**—Provides funding for the Cyber Assurance Program to properly align and invest in proven cyber capabilities to provide sustainable cyber assurance services to state and local entities which operationally increase visibility/awareness to threats and reduce cyber risk to an acceptable level.
- **Louisiana S.B.152**—Creates the Louisiana Cybersecurity Commission to ensure continuation of its current mission, to solidify the collaboration between governments and the private sector, and as a result of the increasing threats of cyber-attacks. This Commission is created within the division of administration to coordinate cybersecurity efforts among state governmental entities, local governments, tribal governments, private companies, academic institutions, and other entities in both the public and private sectors. The commission has many purposes, including developing a cybersecurity strategy for the state, promoting cybersecurity awareness, growing Louisiana's cybersecurity workforce, and educating the public and private sectors about cybersecurity, in addition to many other purposes.
- **North Carolina H.B.259**—Amends existing law relating to cybersecurity reporting and specifies that requests from local jurisdictions, state agencies, or critical infrastructure partners for operational support from or access to operational cyber resources must be sent to the North Carolina Emergency Management 24-hour Watch for intake and activation. The law also reopens the proposal period for the cybersecurity pilot program to allow for additional offerings not awarded in the original pilot program and to select additional vendors to enhance the program.

Prohibited Apps

- **Florida S.B.258**—Prohibits certain applications on government-issued devices. A prohibited application is defined to mean any internet application that is created, maintained, or owned by a foreign principal and that participates in various activities that include, but are not limited to, compromising e-mail, and acting as a vector for ransomware deployment and conducting cyber-espionage against a public employer, among others. Public employer is defined to include any county, district school board, charter school governing board, or municipality, university, or institution of higher education.
- **Georgia S.B.93**—Restricts the use of certain social media platforms on state equipment with certain exceptions, including for cybersecurity research and development. "State agency" is defined to mean any agency, authority, department, institution, board, bureau, commission, committee, office, or instrumentality of the executive, legislative, or judicial branch of government of the state.
- **Kentucky S.B.20**—Bans social media applications, specifically TikTok, from state government technology. The law specifies that this ban does not apply to public postsecondary education institutions in certain circumstances and executive branch agencies that determine that the use of TikTok is necessary for law enforcement activities or research on security practices or security threats, as well as other exceptions.
- **Louisiana H.B.361**—Prohibits the use of TikTok and related applications on computers and networks owned or leased by the state. Specifically, this bill would require the office of technology services to develop a policy, subject to the approval of the Joint Legislative Committee on Technology and Cybersecurity, to prohibit the use of any covered application on any computer, device, or network owned or leased by the state. The law provides an exception to this policy—the policy shall not prohibit a public servant from unrestricted access to a covered application for a legitimate scientific, educational, or law enforcement purpose, provided the use is approved by the agency prior to access to the covered application.
- **Mississippi S.B.2140**—Prohibits state employees from downloading or using the TikTok application or accessing the TikTok website on a state-issued device, as well as prohibiting state employees from the downloading the application or accessing the website via a state-operated network. "State agency" is defined to mean any agency, department, commission, board, bureau, institution, or other instrumentality of the state. This bill does provide exceptions for law enforcement agencies in certain situations.

- **Ohio H.B.33**—Prohibits the downloading, installation, or use of a covered application, including TikTok, on equipment owned or leased by a state agency. State agency is defined to include every organized body, office, or agency established by the laws of this state for the exercise of any function of state government, other than any state-supported institution of higher education. This law also amends statutes relating to the state's civilian cyber security reserve forces that work to educate and protect state, county, and local government entities, critical infrastructure, and businesses and citizens from cyber-attacks. The amendments specify the adjutant general may provide appropriate training to current and potential members of the Ohio cyber reserve.

Notice and Response

- **Arkansas H.B.1555**—Amends the requirements for meetings to address a cybersecurity incident involving, or a cyberattack on, a public entity. Specifies that the meetings of the Joint Committee on Advanced Communications and Information Technology to review a cybersecurity incident involving, or a cyberattack on, a public entity are closed and exempt from public observance under the Freedom of Information Act. "Public entity" is defined to include a school district.
- **Kansas H.B.2019**—Requires any public entity that has a significant cybersecurity incident to notify the Kansas information security office within 12 hours after discovery of the event. Further amends laws relating to the Kansas information security office relating to cybersecurity training for all branches of government.
- **Mississippi S.B.2717**—Amends existing law to require the Mississippi Department of Information Technology Services to evaluate the Enterprise Security Program, which would include evaluating whether opportunities exist to centralize and coordinate oversight of cybersecurity efforts across all state agencies. The law also requires, after July 1, 2023, all state agencies to notify the Mississippi Department of Information Technology Services of any cyberattack or demand for payment because of ransomware no later than the close of the next business day following the discovery of such cyberattack or demand. The Department of Information Technology Services must then analyze all reports and attempt to identify any patterns or weaknesses in the state's cybersecurity efforts.
- **Montana S.B.50**—Requires state agencies to provide immediate notification without reasonable delay to the chief information security officer when a security incident is discovered. Security incident is defined to mean an occurrence that "actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." "State agency" is defined to mean an agency, board, bureau, college, commission, committee, council, department, hospital, institution, office, university, or other instrumentality of the legislative or executive branch of state government.

- **New Jersey S.297**—Requires public agencies and government contractors to report cybersecurity incidents to the New Jersey Office of Homeland Security and Preparedness.
- **Texas S.B.271**—Amends existing law relating to security breaches or incidents with notification by a state agency or local government. Amends the definition of "security incident" to include the introduction of ransomware into a computer, computer network, or computer system.
- **Utah S.B.127**—Makes amendments to existing statutes relating to cybersecurity, including amending the disclosure requirement for system security breaches. Further, this bill creates the Utah Cyber Center and requires governmental entities in the state to report a breach of system security to the Utah Cyber Center. The Utah Cyber Center is required to partner with institutions of higher education and other public and private sector organizations to increase the state's cyber resilience.

Studies/Task Forces

- **Connecticut S.B.933**—Establishes a task force to study cybersecurity—this includes developing a strategic plan that includes findings and recommendations on establishing a structure for oversight and coordination of cybersecurity among state agencies, boards, commissions, and other entities, including the constituent units of the state system of higher education; and critical information technology infrastructure needs related to cybersecurity in the state; and others.
- **Hawaii S.R.75** (Resolution)—Requests the Chief Information Officer to review whether all departments, agencies, and offices of the state have up-to-date technology to reduce cyber threats and help protect the state against cyberattacks. Further all departments, agencies, and offices of the state are requested to cooperate with the Chief Information Officer to determine whether any and what upgrades are needed to current technology to reduce the chances of falling victim to cyber threats, including but not limited to disruptive hacks, ransomware attacks, data breaches, and digital scams.
- **Illinois H.B.3563**—Establishes the Generative AI and Natural Language Processing Task Force. The task force has several responsibilities, including creating model policies for schools to address AI use by students and model policies for schools to address use of AI in the classroom, as well as the challenges of AI for cybersecurity.
- **Washington S.B.5518**—Creates the cybersecurity advisory committee to provide advice and recommendations that strengthen cybersecurity in both industry and public sectors across all critical infrastructure sectors. The committee will bring together certain organizations, including local government and state agencies, as well as institutions of higher education with a goal of providing recommendations on building and sustaining the state's capability to identify and mitigate cybersecurity risk and to respond to and recover from cybersecurity-related incidents, including ransomware incidents.

- **Vermont H.291**—Creates the Cybersecurity Advisory Council to advise on the State's cybersecurity infrastructure, best practices, communications protocols, standards, training, and safeguards. One of the duties of this Council is to build strong partnerships with local universities and colleges to leverage cybersecurity resources.

Policies and Plans

- **Arkansas H.B.1369**—Requires public entities to develop a technology resources policy, as well as a cybersecurity policy for all technology resources of the public entity based on the standards and guidelines set by the State Cyber Security Office. Further, public entities must develop a training program for all employees of the public entity concerning the technology resources policy and cyber security policy. "Public entity" is defined to include The Department of Education, public school districts, charter schools, and institutions of higher education. The law further requires the Department of Education to develop technology resources policies and a cyber security policy to be used by each type of state educational institution.
- **Arkansas S.B.294**—Requires each public school and open-enrollment charter school to promote school safety and security in several ways, including reviewing and updating cybersecurity policies and procedures annually.
- **Montana H.B.47**—Revises the Montana Information Technology Act to require third-party providers of information technology resources to comply with state security and information technology policies, risk management framework, controls, standards, procedures, and guidelines when providing information technology resources to government entities. The law also eliminates references to "cyber risks" and instead just use the phrase "risk to information technology."
- **New Mexico H.B.401**—Amends existing law related to the Technology for Education Act—renamed the Digital Equity in Education Act. Requires school districts and charter schools to develop, implement, and submit to the department educational technology plans for utilizing educational technology in the school system. The plans must include a description of cybersecurity protection provided for the devices and applications issued to teachers and students.

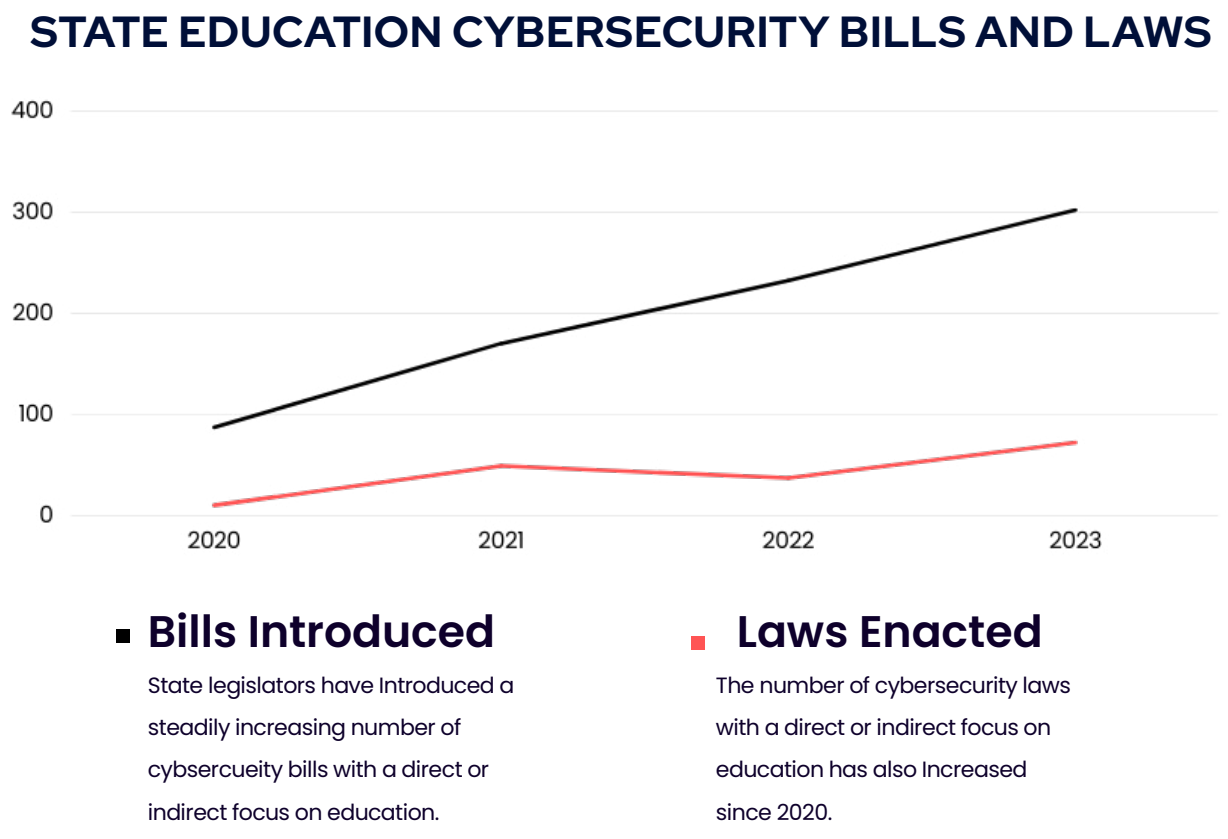
Criminalization and Miscellaneous

- **Florida S.B.32**—Amends existing statutes relating to the Florida Cybersecurity Advisory Council to delete obsolete language.
- **Iowa H.F.143**—Prohibits the use of ransomware. Provides that a person shall not commit a prohibited act with the intent to interrupt or impair the function of the state government, or a public elementary or secondary school, community college, or area education agency under the supervision of the department of education, among other prohibitions. Provides an exception for the use of ransomware for research purposes by a person who has a bona fide scientific, educational, governmental, testing, news, or other similar justification for possessing ransomware.

- **Maryland S.B.610**—Amends existing law to require virtual schools to provide parents with informational materials on certain topics, including cybersecurity policy and best practices.
- **Montana H.B.161**—Amends existing law relating to the crime of unlawful use of a computer—makes clear that this crime includes destroying or rendering inoperable a computer, computer system, or computer network in order to make that device or system physically inaccessible or rendering data, programs, or supporting documentation inaccessible or unusable; as well as introducing a computer contaminant that deletes, modifies, or renders unavailable data, programs, or supporting documentation.
- **Oregon H.B.2490**—Exempts from required disclosure records, documents, or plans concerning protection relating to the existence, nature, location or function of cybersecurity devices, programs, or systems. This includes both records pertaining to devices, programs or systems that depend for their effectiveness in whole or part upon a lack of public knowledge and contractual and insurance records that set forth cybersecurity specifications, insurance application and coverage details.

FIGURE 5: STATE EDUCATION CYBERSECURITY POLICY ACTIVITY 2020-23

2023 Education Cybersecurity Legislation (All bills Passed/Unpassed)

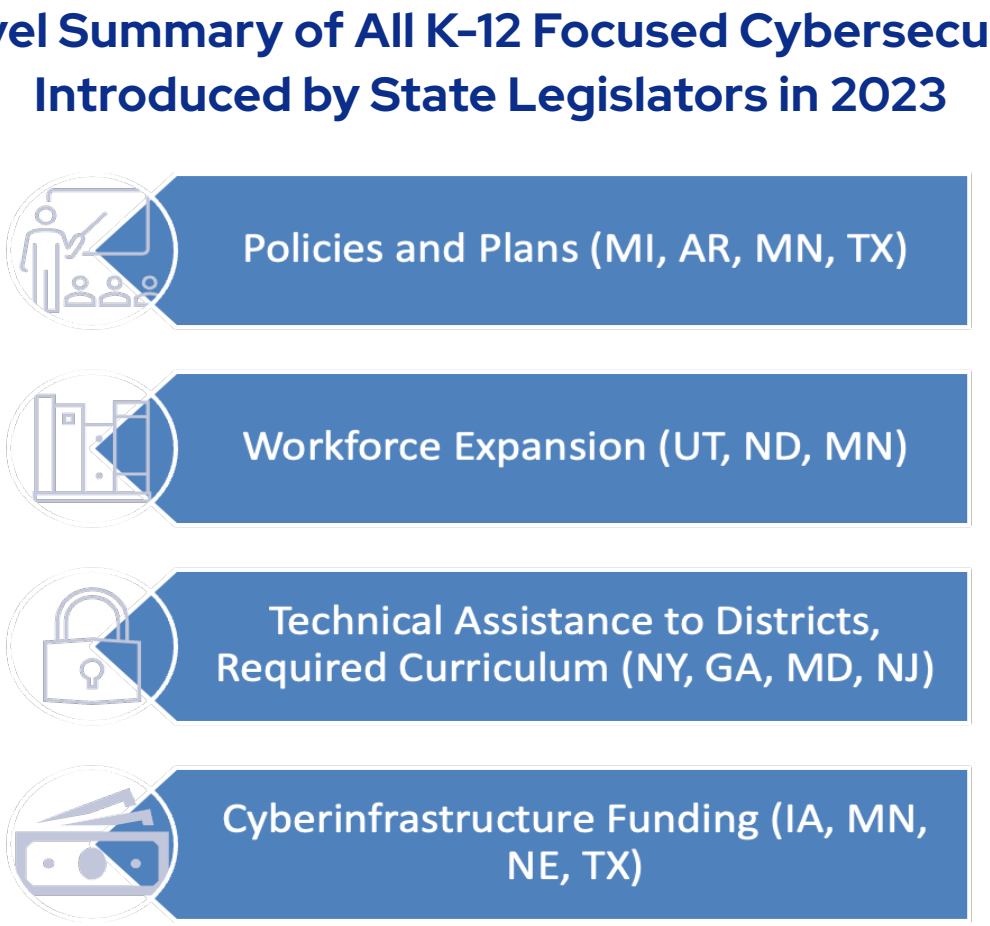


In 2023, legislators in forty-two states introduced cybersecurity bills that have direct or indirect application to the education sector. This section briefly summarizes these bills, organized into K-12 and postsecondary categories, and highlights common policy strategies suggested across states. The following jurisdictions did not have any education cybersecurity legislation in 2023: Alabama, Alaska, Colorado, Delaware, Idaho, Nevada, Tennessee, Virginia, and Washington, D.C.

Elementary and Secondary Schools Focused Legislation (47 bills in 18 states)

In 2023, legislators in 18 states introduced forty-seven elementary and secondary school focused cybersecurity bills.[3] This total is 13 more bills than legislators introduced in 2022 (34 bills in 18 states), compared with 38 bills in 16 states in 2021; and 19 bills in 13 in 2020.

FIGURE 6: MAJOR THEMES FEATURED IN 2023 K-12 FOCUSED CYBERSECURITY LEGISLATION



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

Midwest:

- **Illinois H.B.2353** Proposes to require a report by school districts of cyber security attack to State Board immediately upon breach of computer system or network.
- **Indiana S.B.142** Proposes internet safety curricula for schools, including curriculum relating to practicing cybersecurity.
- **Iowa H.F.452** Proposes to amend existing law relating to school district expenditure of funds from the secure an advanced vision for education fund—defines school infrastructure and cybersecurity event.
- **Iowa H.F.632** Proposes to amend the definition of "school infrastructure" to include the acquisition, development, and improvement of school information systems to protect against cybersecurity events.
- **Michigan H.B.4286** Proposes to amend State School Aid act relating to school consolidation and infrastructure fund. Schools may apply for grants so long as they conduct a feasibility study or analysis, which may include cybersecurity issues.
- **Michigan S.B.173** (enacted) Amends the State School Aid Act relating to school consolidation and infrastructure fund—schools may apply for grants so long as they conduct a feasibility study or analysis, which may include cybersecurity issues; establishes Security Operations Center, with reporting requirements that include reporting on measurable outcomes including the response to cybersecurity incidents.
- **Michigan S.B.380** Proposes amendments to state aid and pupil membership counts that would require department of education to count as hours and days of student instruction any day in which student instruction is not provided due to a ransomware attack.
- **Minnesota H.F.1360/S.F.1884** Proposes to permit safe schools revenue to be used to pay for the cost of cybersecurity measures, including updating computer hardware and software, other systems upgrades, and cybersecurity insurance costs.
  - > These two bills are labeled by the legislature as companion bills.
- **Minnesota H.F.2497** (enacted) Provides funding to improve building security and cybersecurity; funds may be used for cybersecurity insurance premiums; amends language relating to safe schools' revenue.
- **Missouri H.B.492** Proposes to establish pilot program for media literacy and critical thinking and studies would include information on social media behavior that ensure cyber safety, cybersecurity, and cyber ethics.

- **Missouri S.B.678** Proposes to establish pilot program for media literacy and critical thinking and studies would include information on social media behavior that ensure cyber safety, cybersecurity, and cyber ethics.
- **Missouri S.B.683** Proposes to amend law relating to data privacy in elementary and secondary education and would require model policy that establishes procedures for identifying and mitigating cybersecurity risks to protect the personally identifiable information of students and staff.
- **Nebraska L.B.638** Proposes to establish the K-12 Cybersecurity and Data Protection Act to institute protective cybersecurity measures within the Nebraska school system.
- **North Dakota H.B.1398** (enacted) Requires public and nonpublic elementary, middle school, and high schools to provide instruction in computer science, including cybersecurity; amends graduation requirements relating to cybersecurity courses.

Northeast and Mid-Atlantic

- **Maryland H.B.1110** Proposes to require the department to develop curriculum content standards for a course on peace and conflict for high school students, which includes instruction on cybersecurity.
- **Maryland H.B.1297/S.B.820** Proposes to require virtual schools to provide parents with informational materials on certain topics, including cybersecurity policy and best practices.
  - > These two bills are labeled by the legislature as companion bills.
- **Maryland S.B.610** (enacted) Virtual schools must provide parents with informational materials on certain topics, including cybersecurity policy and best practices.
- **Maryland S.B.799** Proposes to require the development of a cyber safety guide to be made available to all public schools.
- **Maryland S.B.829** Proposes to require virtual schools to provide parents with informational materials on certain topics, including cybersecurity policy and best practices.
- **Massachusetts H.532** Proposes to establish a new student and educator data privacy law; in promulgating regulations, the Board must consult with cybersecurity experts.
- **Massachusetts S.280** Proposes to establish a new student and educator data privacy law; in promulgating regulations, the Board must consult with cybersecurity experts.
- **New Jersey A.1982** Proposes to require cybersecurity instruction in grades 9-12; requires Office of Secretary of Higher Education to develop cybersecurity model curricula and loan redemption programs for individuals in certain cybersecurity occupations.

- **New York A.1646** Proposes to establish a school district cybercrime prevention services program to provide districts with information on strategies, best practices, and programs offering training and assistance in prevention of cybercrimes in school districts.
- **New York S.2564** Proposes to require annual notification relating to combatting cybercrimes to certain individuals in each school district in the state.

South:

- **Arkansas S.B.294** (enacted) Requires schools to promote safety and security including by reviewing and updating cybersecurity policies and procedures.
- **Georgia H.B.338** Proposes to require the Department to provide guidance and technical assistance to schools and school systems that focus on basic cybersecurity issues.

Southwest

- **New Mexico H.B.256** Proposes to establish a cybersecurity hybrid dual credit pilot project—students graduate with a high school diploma and associate degree or certificate in cybersecurity.
- **New Mexico H.B.401** (enacted) Amends the Technology for Education Act (renamed Digital Equity in Education Act), requiring education technology plans to include a description of cybersecurity protection for devices and applications used by teachers and students.
- **Texas H.B.18** (enacted) Amends existing law relating to transfer of data processing equipment and electronic devices to students; TEA must ensure when adopting standards for using electronic devices and applications that parents are provided with information on cybersecurity risks and online safety; provides for an officer assigned to receive complaints or concerns regarding student use of devices, including cybersecurity concerns.
- **Texas H.B.100** Proposes to require allotment to districts if they offer program of study in certain subjects, including cybersecurity.
- **Texas H.B.681** Proposes to require the commissioner to adopt rules relating to full-time virtual campuses or full-time hybrid campuses; district must develop operations plan that addresses cybersecurity.
- **Texas H.B.1569** Proposes to require the commissioner to establish professional development grant program for courses in coding, computational thinking, cybersecurity, and others.
- **Texas H.B.2615** Proposes to establish a foundation and trade diploma program, which would require certain courses for a diploma to be issued—career and technical education courses are limited but may include cybersecurity courses.

- **Texas H.B.2673** Proposes to require adoption of standards for permissible electronic devices and software applications used by a district or charter school; parents must receive resources to be partner in cybersecurity.
- **Texas H.B.2710** Proposes to permit, after emergency, school districts to enter contracts to respond to emergencies, which include responding to cybersecurity threats.
- **Texas H.B.3141** Proposes to require the Commissioner to adopt rules relating to full-time virtual campuses or full-time hybrid campuses and districts would be required to develop operations plan that address cybersecurity.
- **Texas H.B.4322** Proposes to establish STEM and computer science strategic advisory committee and the reporting requirement includes recommendations regarding cybersecurity in public schools.
- **Texas H.B.4407** Proposes to create law relating to certification examinations of educators focused on cybersecurity.
- **Texas H.B.4944** Proposes to require adoption of cybersecurity controls and requirements for school districts, charter schools, and vendors.
- **Texas S.B.717** Proposes to require adoption of cybersecurity controls and requirements for school districts, charter schools, and vendors.
- **Texas S.B.1087** Proposes to create law relating to certification examinations of educators focused on cybersecurity.

- **Texas S.B.1315** Proposes to require the commissioner to establish professional development grant program for courses in coding, computational thinking, cybersecurity, and others.
- **Texas S.B.1861** Proposes to establish STEM and computer science strategic advisory committee and the reporting requirement includes recommendations regarding cybersecurity in public schools.

West:

- **California A.B.1023** (enacted) Requires the state's Cybersecurity Integration Center to include

representatives from the state Department of Education and includes school districts among entities which Cal-CSIC coordinates information sharing, including cyber threat information.

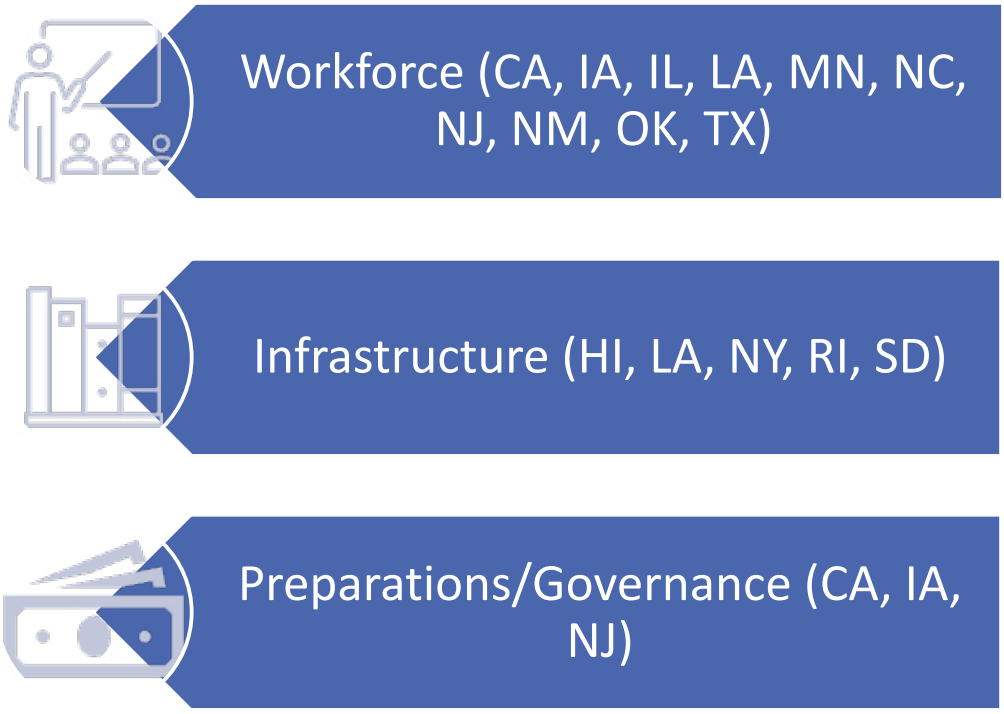
- **Utah H.B.215** (enacted) Creates a new scholarship program and requires the program manager to ensure the scholarship program accounts comply with industry standards for cybersecurity.

Postsecondary Focused State Cybersecurity Legislation (28 bills in 14 states)

Legislators' interest in postsecondary focused cybersecurity policymaking decreased slightly in 2023. Policymakers in 14 states introduced 28 bills in 2023, which is less than the 34 bills filed in 12 states in 2022, and 6 bills in 4 states in both 2020 and 2021. Many of 2023's postsecondary focused bills provided funding for cybersecurity programs and pilot programs to work to build the cyber workforce and to strengthen cybersecurity programs in institutions of higher education, including for cybersecurity workforce training programs, internships, and apprenticeships.

FIGURE 7: MAJOR THEMES FEATURED IN 2023 POSTSECONDARY FOCUSED LEGISLATION

High Level Summary of All Postsecondary Focused Cybersecurity Bills Introduced in 2023



Midwest:

- **Illinois H.B.1378** (enacted) Creates Graduate and Retain Our Workforce (iGrow) Tech Scholarship Fund to recruit for technology demands; qualifying degree is defined to include a degree in information systems security or information assurance, including cybersecurity.
- **Illinois H.B.2538** Proposes an appropriation of funds for the Illinois Institute of Technology Cybersecurity Bootcamp Program at the Illinois Institute of Technology.
- **Iowa H.F.139** Proposes to establish Cybersecurity Simulation Training Center at Iowa State University of Science and Technology.
- **Iowa H.F.698** Proposes to establish Cybersecurity Simulation Training Center at Iowa State University of Science and Technology.
- **Iowa H.F.731** Proposes an appropriation of funds to prepare future ready workforce and fostering innovation, including for addressing workforce needs in cybersecurity.
  - The original study bill was H.S.B.254, but was renumbered as H.F.731.
- **Iowa S.F.560** (enacted) Appropriates funds to prepare future ready workforce and fostering innovation, including for addressing workforce needs in cybersecurity.
- **Minnesota H.F.669/S.F.676** Proposes an appropriation of funds to Metropolitan State University to design, renovate, and equip space for the cybersecurity program.
  - These two bills are labeled by the legislature as companion bills.
- **Minnesota H.F.2071/S.F.1547** Proposes an appropriation of funds to Metropolitan State University to design, renovate, and equip space for the cybersecurity program.
  - These two bills are labeled by the legislature as companion bills.
- **Minnesota H.F.2880/S.F.2892** Proposes an appropriation of funds to Metropolitan State University to design, renovate, and equip space for the cybersecurity program.
  - These two bills are labeled by the legislature as companion bills.
- **South Dakota S.B.32** Proposes an appropriation of funds to the Board of Regents to purchase cybersecurity upgrades to enhance and protect network security.

Northeast and Mid-Atlantic:

- **New Jersey A.1982** Proposes requiring cybersecurity instruction in grades 9-12; requires Office

of Secretary of Higher Education to develop cybersecurity model curricula and loan redemption programs for individuals in certain cybersecurity occupations.

- **New Jersey A.3379** Proposes requiring public institutions of higher education to establish plans concerning cyber security and prevention of cyber attacks.
- **New York S.924** Proposes requiring state higher education capital matching grant board to award matching capital grants for projects to implement, modify, or otherwise enhance cybersecurity infrastructure.
- **Rhode Island H.5200** (enacted) Establishes Rhode Island Longitudinal Data system and provides funds to establish Institute for Cybersecurity and Emerging Technologies at Rhode Island College.

South:

- **North Carolina H.B.842** Proposes funds to community colleges to create cybersecurity apprenticeship program.
- **Louisiana H.B.560** (enacted) Provides funding to Board of Regents for cybersecurity software for all institutions of higher education.
- **Louisiana H.B.1** (enacted) Provides funding for the Louisiana Cybersecurity Talent Initiative Fund to provide money for degree and certificate programs in cybersecurity fields.

Southwest:

- **New Mexico H.B.256** Proposes to establish cybersecurity hybrid dual credit pilot project to allow students to graduate with high school diploma and associate's degree or certificate in cybersecurity.
- **Oklahoma H.B.2555** Proposes creation of the Oklahoma Critical Industries Scholarship Program, a pilot program to encourage high school graduates to pursue degree or certificate in industries that are critical to economic growth of state, including cybersecurity.
- **Texas H.B.1755** Proposes to establish Lone Star Workforce of the Future Fund relating to workforce training programs, work-based experiences internships, or apprenticeships in certain high growth fields, including cybersecurity.
  - Note: When the bill was signed by the Governor, mention of cybersecurity was removed.
- **Texas S.B.592** Proposes to establish Lone Star Workforce of the Future Fund relating to workforce training programs, work-based experiences internships, or apprenticeships in certain high growth fields, including cybersecurity.

West

- **California A.B.569** (enacted) Creates a pilot program to address cybersecurity workforce gap, including aligning cybersecurity workforce needs of employers with education and training and increasing the pipeline of students pursuing cybersecurity careers.
- **California S.B.72** Proposes funds for community college districts to implement local and systemwide technology and data security measures that support improved oversight of cybersecurity efforts.
- **Hawaii H.R.88** (Resolution) (enacted) Urges Microsoft to consider building data center in state, part of national campaign to help community colleges work to train and recruit people for jobs in the cybersecurity workforce.
- **Hawaii S.B.1249** Proposes funding for cybersecurity and data science programs at the University of Hawaii Maui College.

2023 General Government State Cybersecurity Bills that Reference K-12 (29 bills in 17 states)

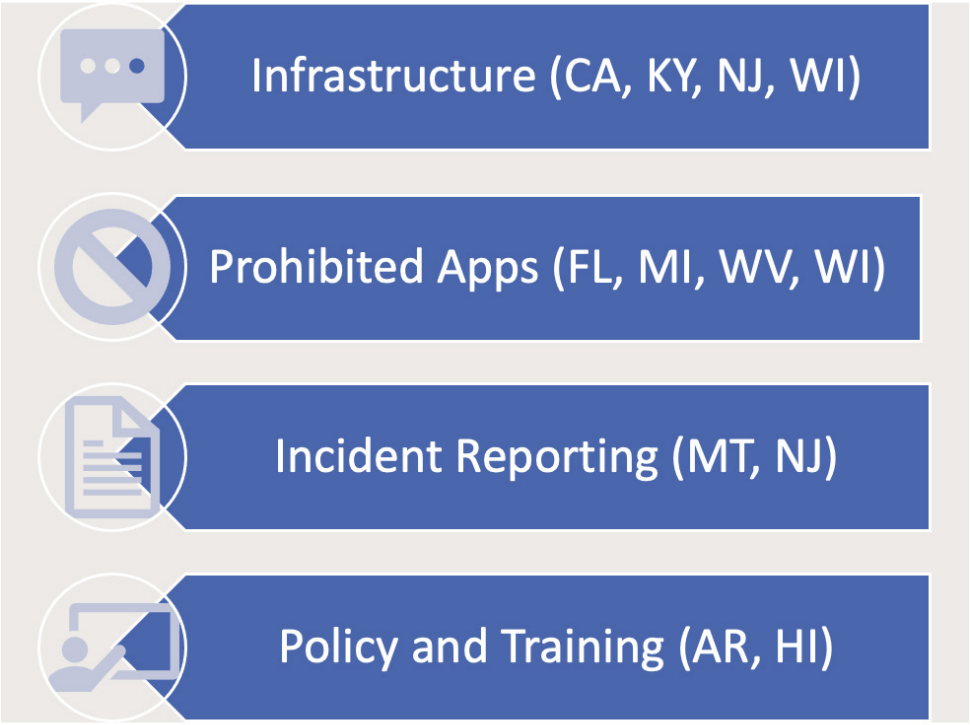
Legislators in 17 states introduced 29 cybersecurity bills that focus on government agencies generally but include references to K-12 schools. This compares to 27 bills in 12 states in 2022, 16 bills in 11 states in 2021, and 9 bills in 4 states in 2020.

Common topics in 2023 included establishing cybersecurity policies; closing confidential meetings relating to cybersecurity incidents; expanding education and training on cybersecurity threats; requiring reporting cyberattacks; reviewing institutions' cybersecurity infrastructure; and providing appropriations targeting the problem. Six bills, measures introduced in Florida, Michigan, West Virginia, and Wisconsin, prohibited certain software applications from being installed on state-owned devices or computers.

FIGURE 8: MAJOR THEMES FEATURED IN 2023 GENERAL GOVERNMENT STATE CYBERSECURITY BILLS THAT REFERENCE K-12

High Level Summaries of All General

Government Cybersecurity Bills with a K-12 Focus Introduced in 2023



Midwest:

- **Iowa H.F.554** Proposes to prohibit revenue received from taxpayers to be used to pay for ransomware; political subdivision is defined to include school district.
  - Original study bill H.S.B.153 (renumbered as H.F.554)
- **Michigan H.B.5065** Proposes to prohibit use of certain applications on government-issued devices; public employer is defined to include school districts.
- **North Dakota S.B.2073** (enacted) Requires information technology department to oversee cybersecurity strategy for all executive branch state agencies, including state board of higher education, school, districts, and others.
- **Wisconsin A.B.43** Proposes to make appropriations for security operations centers to provide cybersecurity of information technology systems maintained by eligible entities, which is defined to include educational agencies.
- **Wisconsin S.B.70** Proposes to make appropriations for security operations centers to provide cybersecurity of information technology systems maintained by eligible entities, which is defined to include educational agencies.

> Note: S.B.70 was signed by the Governor but did not mention cybersecurity in final bill.

- **Wisconsin A.B.263** Proposes to prohibit employees of state agencies or local governmental units to access or use certain mobile or online software applications that are deemed cybersecurity threats; local government unit is defined to include school districts.
- **Wisconsin S.B.250** Proposes to prohibit employees of state agencies or local governmental units to access or use certain mobile or online software applications that are deemed cybersecurity threats; local government unit is defined to include school districts.

Northeast and Mid-Atlantic:

- **New Jersey A.1983** Proposes to require municipalities, countries, and school districts to report cybersecurity incidents.
- **New Jersey A.4013/S.484** Proposes to require each principal department in Executive Branch and each state college to conduct review of each department's or college's cybersecurity infrastructure.

> These two bills are labeled by the legislature as identical bills.

- **Pennsylvania H.B.1139** Proposes to establish a Cybersecurity Coordination Board to collect, study, and share information relating to cybersecurity issues and initiatives; Secretary of Education would serve on Board.
- **Pennsylvania S.B.563** Proposes to provide for criminal acts relating to ransomware; defines ransomware attacks on Commonwealth agencies to include school districts, career and technical schools, charter schools, and community colleges.

South:

- **Arkansas H.B.1369** (enacted) Requires public entities to develop technology resources policy and cybersecurity policy; training program would be required for all employees of the public entity; public entity is defined to include the Department of Education, public school districts, charter schools, and institutions of higher education.
- **Arkansas H.B.1555** (enacted) Requires meetings to review cybersecurity incidents on public entities to be closed; public entity is defined to include a school district.
- **Arkansas H.B.1704** Proposes to prohibit public entities from paying ransom for a cyberattack and requires creation of policy to prohibit payment of a ransom for a cyberattack. Public entity is defined to include the Department of Education, public school districts, and institutions of higher education.

- **Arkansas H.B.1780** (enacted) Creates the Arkansas Self-Funded Cyber Response Program Act for participating governmental entities to provide coverage for cybersecurity incidents and risks, damages, or losses caused by a cyberattack that are committed against a participating governmental entity. School districts may participate in the program.
- **North Carolina S.B.194/S.B.196** Proposes a Student Borrowers' Bill of Rights, including providing discretion to require applicant to obtain insurance coverage to address cybersecurity risks as it relates to student loan servicing.
  - > These two bills are labeled by the legislature as identical bills.
- **Kentucky S.B.33** Proposes to create a Kentucky Cybersecurity Center at University of Louisville, tasked with educating agencies and private sector participants about how to maintain secure cyberinfrastructure and accelerate adoption of cybersecurity systems.
- **Florida H.B.563** Proposes to prohibit certain applications on government-issued devices; public employer is defined to include school districts, charter school governing boards, universities and institutions of higher education.
- **Florida S.B.258** (enacted) Prohibits applications on government-issued devices; public employer is defined to include school districts, charter school governing boards, universities and institutions of higher education.
- **West Virginia S.B.426** Proposes to require all state agencies to enforce statewide standards regarding high-risk platforms, including TikTok, and which include those designated as such in the statewide cybersecurity standard.

Southwest:

- **New Mexico H.B.388** Proposes a cybersecurity fund established for cyber-attack response and recovery; applies to all branches of state government, political subdivisions, public schools, or tribal entities.
- **Texas H.B.1** (enacted) Provides funds for cybersecurity for state agencies and institutions of higher education; establishes Interagency Cybersecurity Initiative for Public Schools; may use funds to provide cybersecurity services to public school districts and placement and oversight of cybersecurity practitioners to assist LEAs.

West:

- **California A.B.1023** (enacted) Requires the Cybersecurity Integration Center to include representatives from the state Department of Education and includes school districts among entities which Cal-CSIC coordinates information sharing, including cyber threat information.

- **California A.B.1637** (enacted) Requires local agencies with internet websites to utilize a .gov top-level domain or .ca.gov second-level domain.
- **Hawaii H.B.1038** Proposes outreach, education, and training on targeted violence, and reporting of threats which includes unauthorized access to state information systems.
- **Hawaii S.B.1336** Proposes outreach, education, and training on targeted violence, and reporting of threats which includes unauthorized access to state information systems.
- **Montana S.B.50** (enacted) Requires state agencies to provide immediate notification when security incident is discovered; state agency is defined to mean agency, board, bureau, college, commission, committee, council, department, university, and others.

General Government State Cybersecurity Bills that Reference Postsecondary Institutions (46 bills in 19 states)

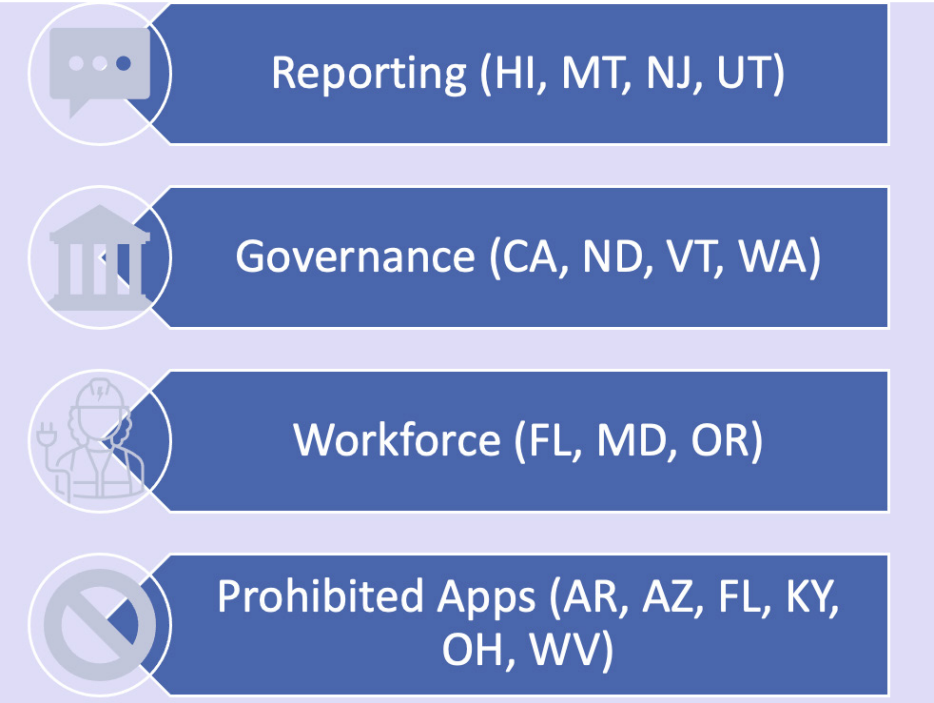
State leaders' interest in general state government cybersecurity bills with a reference on postsecondary institutions, increased significantly. Legislators introduced 46 bills in 19 states in 2023, compared to 21 bills in 11 states in 2022, and 4 bills in 2 states in 2021.

Four of the bills proposed to prohibit certain applications on government-owned devices. The measures in this category also focused on expanding the cybersecurity workforce, mandatory incident reporting, making governance improvements, and more.

FIGURE 9: MAJOR THEMES FEATURED IN GEN GOV BILLS WITH A POSTSECONDARY REFERENCE

Complete List of 2023 General Government Cybersecurity Bills that Reference Postsecondary Education

Midwest:



- **North Dakota S.B.2073** (enacted) Requires information technology department to oversee cybersecurity strategy for all executive branch state agencies, including state board of higher education, school, districts, and others.
- **Ohio H.B.33** (enacted) Prohibits downloading, installation, or use of covered application, including TikTok, on equipment owned or leased by state agency; does not apply to state-supported institutions of higher education.

Northeast and Mid-Atlantic:

- **Maryland H.B.552/S.B.549** (enacted) Establishes Build Our Future Grant Pilot Program for infrastructure projects intended to support innovation in eligible technology sector, which includes cybersecurity; grants may be awarded to private companies, nonprofits, local governments, or colleges and universities.
  - > These two bills are labeled by the legislature as cross-filed bills.
- **Maryland H.B.1189** Proposes to establish a Cyber Maryland Program to increase cybersecurity workforce and inform cybersecurity training and education programs; requires Higher Education Commission to expand the Cyber Warrior Diversity Program.

> Note: This bill was cross-filed with S.B.801, but only S.B. 801 was signed.

- **Maryland S.B.801** (enacted) Establishes a Cyber Maryland Program to increase cybersecurity workforce and inform cybersecurity training and education programs; requires Higher Education Commission to expand the Cyber Warrior Diversity Program.
- **Massachusetts H.51** Proposes appropriations for academic institutions, nonprofits, and others to compete for federal grants in technology and innovation fields, including cybersecurity.
- **Massachusetts H.58** (enacted) Provides appropriations for academic institutions, nonprofits, and others to compete for federal grants in technology and innovation fields, including cybersecurity.
- **Massachusetts H.3548** Proposes to provide appropriations for academic institutions, nonprofits, and others to compete for federal grants in technology and innovation fields, including cybersecurity.
- **Massachusetts H.3901** Proposes to provide appropriations to community colleges for cybersecurity education; funds also for state auditor to conduct audits of high-risk information technology related activities.
- **Massachusetts H.4040** Proposes to provide appropriations to community colleges for cybersecurity education and funds for the Cybersecurity Innovation Fund for community colleges and state universities to provide services for the monitoring and detection of cyber threat activity; funds also for state auditor to conduct audits of high-risk information technology related activities.
- **Massachusetts S.23** Proposes to provide appropriations for academic institutions, nonprofits, and others to compete for federal grants in technology and innovation fields, including cybersecurity.
- **Massachusetts S.24** Proposes to provide appropriations for academic institutions, nonprofits, and others to compete for federal grants in technology and innovation fields, including cybersecurity.
- **Massachusetts S.2400** Proposes to provide appropriations to community college for cybersecurity education; funds also for state auditor to conduct audits of high-risk information technology related activities.
- **New Jersey A.1983** Proposes to require municipalities, countries, and school districts to report cybersecurity incidents.
- **New Jersey A.4013/S.484** Proposes to require each principal department in Executive

Branch and each state college to conduct review of a department's or college's cybersecurity infrastructure.

  > These two bills are labeled by the legislature as identical bills.

- **Pennsylvania S.B.563** Proposes to amend existing law providing for criminal acts relating to ransomware; defines ransomware attacks on Commonwealth agencies to include school districts, career and technical schools, charter schools, and community colleges.
- **Vermont H.291** (enacted) Creates Cybersecurity Advisory Council; duties would include building strong partnerships with local universities and colleges to leverage cybersecurity resources.
- **West Virginia S.B.426** Proposes to require all state agencies to enforce statewide standards regarding high-risk platforms, including Tiktok, and which include those designated as such in the statewide cybersecurity standard.

South:

- **Arkansas H.B.1369** (enacted) Requires public entities to develop technology resources policy and cybersecurity policy; training program required for all employees of the public entity; public entity is defined to include the Department of Education, public school districts, charter schools, and institutions of higher education.
- **Arkansas H.B.1704** Proposes to prohibit public entities from paying ransom for a cyberattack and requires creation of policy to prohibit payment of a ransom for a cyberattack; public entity is defined to include the Department of Education, public school districts, and institutions of higher education.
- **Arkansas S.B.4** Proposes new cybersecurity protections and to prohibit state entities or state employees from downloading or using TikTok.
- **Florida H.B.563** Proposes to prohibit applications on government-issued devices; public employer is defined to include school districts, charter school governing boards, universities and institutions of higher education.
- **Florida H.B.5001** Proposes to provide appropriations for cybersecurity programs at institutes of higher education and assist in creation of jobs in cybersecurity industry and enhance existing workforce.
- **Florida S.B.258** (enacted) Prohibits applications on government-issued devices; public employer is defined to include school districts, charter school governing boards, universities, and institutions of higher education.
- **Florida S.B.2500** (enacted) Provides appropriations for cybersecurity programs at institutes of higher education and assist in creation of jobs in cybersecurity industry and enhance existing workforce.

- **Kentucky S.B.20** (enacted) Bans social media applications from state government technology; ban does not apply to public postsecondary education institutions in certain circumstances.
- **Kentucky S.B.33** Proposes to create a Kentucky Cybersecurity Center at University of Louisville; Center is tasked with educating agencies and private sector participants about how to maintain secure cyberinfrastructure and accelerate adoption of cybersecurity systems.

Southwest:

- **Arizona H.B.2416** (vetoed) Would have required the development of standards, guidelines, and practices for state agencies, contractors, and public institutions of higher education regarding removal of any covered application from state information technology.
- **Texas H.B.1** (enacted) Provides funds for cybersecurity for state agencies and institutions of higher education; establishes Interagency Cybersecurity Initiative for Public Schools; may use funds to provide cybersecurity services to public school districts and placement and oversight of cybersecurity practitioners to assist LEAs.
- **Texas H.B.1412** Proposes to strengthen the resilience of the electric grid; training Texas National Guard as first responders to cybersecurity threats; identify universities with expertise in cybersecurity that can contribute to goal of mitigating all hazards to grid.
- **Texas H.B.1508** Proposes to require guidelines for state agencies regarding continuing education requirements for cybersecurity training; notification required as to how the guidelines apply to institutions of higher education.
- **Texas S.B.30** (enacted) Provides supplemental appropriations and reductions for cybersecurity projects; appropriates funds to Higher Education Coordinating Board for cybersecurity purposes, and others.
- **Texas S.B.1205** Proposes funding to be used to share information resources technology services offered by department, including cybersecurity services; requires state agencies to use .gov or .texas.gov for official website, but would not apply to university system or institutions of higher education.

West:

- **California A.B.101** Proposes appropriations for cybersecurity programs and funding for community college districts to support improved oversight of cybersecurity efforts.

- **California A.B.221** Proposes appropriations to fund community college districts to support improved oversight of cybersecurity efforts.
- **California S.B.101** (enacted) Provides appropriations for cybersecurity programs and funding for community college districts to support improved oversight of cybersecurity efforts.
- **Hawaii H.B.1038** Proposes to provide outreach, education, and training on targeted violence, and reporting of threats which includes unauthorized access to state information systems.
- **Hawaii S.B.1336** Proposes to provide outreach, education, and training on targeted violence, and reporting of threats which includes unauthorized access to state information systems.
- **Montana H.B.10** (enacted) Provides appropriations for Montana Cybersecurity Enhancement Project and to university system for cyberMontana cybersecurity initiative.
- **Montana S.B.50** (enacted) Requires state agencies to provide immediate notification when security incident is discovered; state agency is defined to mean agency, board, bureau, college, commission, committee, council, department, university, and others.
- **Oregon H.B.2049** (enacted) Establishes a Cybersecurity Center of Excellence; supplements activities of State Chief Information Officer regarding cybersecurity; includes focus on education, training, awareness, workforce development, and others.
- **Utah S.B.127** (enacted) Provides disclosure requirements for system security breaches; Utah Cyber Center are required to partner with institutions of higher education to increase state's cyber resilience.
- **Washington S.B.5518** (enacted) Establishes a cybersecurity advisory committee to strengthen cybersecurity in industry and public sectors; bring together government and institutions of higher education to provide recommendations relating to cybersecurity risks and recovering from cybersecurity-related incidents.
- **Washington S.B.5619** Proposes to establish a cybersecurity advisory committee to strengthen cybersecurity in industry and public sectors; brings together government and institutions of higher education to provide recommendations relating to cybersecurity risks and recovering from cybersecurity-related incidents.

General State Government Cybersecurity Bills (126 bills in 33 states)

In 2023, state legislators introduced a slightly greater number of general government cybersecurity bills compared to 2022. Policymakers introduced 126 bills in 33 states, compared to 120 bills in 31 states in 2022, 96 bills in 33 states in 2021, and 55 bills introduced in 21 states in 2020. The

most frequent strategies embedded in bills focused on general state government cybersecurity readiness included:

1. **Prohibitions on Specific Applications:** Many bills focus on prohibiting the use of specific applications on state-issued devices, particularly social media platforms like TikTok, due to cybersecurity concerns.
2. **Providing Direct Appropriations for Cybersecurity:** A significant number of bills involve providing appropriations or funding for various cybersecurity initiatives. These proposals include establishing funds for cyber risk insurance, grants for cybersecurity projects, and investments in cybersecurity infrastructure and training.
3. **Cybersecurity Governance and Workforce Development:** Several bills aim to enhance cybersecurity governance frameworks, establish committees or positions such as Chief Information Security Officers, and create programs for cybersecurity education and workforce development to address the skills gap in the cybersecurity field.

High Level Summaries of All General Government Cybersecurity Bills Introduced in 2023

Midwest:

- **Illinois H.B.2703** Proposes appropriations for the Cybersecurity Liaison program and for expenses related to addressing cybersecurity risks and threats.
- **Illinois S.B.2497** Proposes appropriations for the Cybersecurity Liaison program and for expenses related to addressing cybersecurity risks and threats.
- **Iowa H.S.B.15** Proposes to create cybersecurity unit within the office of the chief information officer.
- **Iowa H.S.B.16** Proposes modifications to essential county purpose and essential corporate purpose to include cybersecurity purposes.
- **Iowa S.F.195** Proposes modifications to essential county purpose and essential corporate purpose to include cybersecurity purposes.
  - > Note: The original study bill was S.F.46, but the measure was renumbered as S.F.195.
- **Iowa S.F.557** (enacted) Provides funding for cybersecurity services to local governments.
- **Kansas H.B.2019** (enacted) Requires any public entity that has a significant cybersecurity incident to notify the Kansas information security office within 12 hours after discovery of the event. Further amends laws relating to the Kansas information security office relating to cybersecurity training for all branches of government.

- **Kansas H.B.2077** Proposes cybersecurity awareness training program must be made available to all branches of state government.
- **Kansas H.B.2314** Proposes prohibition on use of electronic devices that are owned or issued to employee by a state agency to be used to access a social media platform of concern.
- **Michigan H.B.4292** Proposes funding for Homeland security initiative/cybersecurity and a cybersecurity federal match.
- **Michigan H.B.4437** (enacted) Provides appropriations for cybersecurity programs, including homeland security initiative cybersecurity and vendor cybersecurity monitoring, among others.
- **Michigan S.B.189** Proposes appropriations for Homeland security initiative/cybersecurity and a cybersecurity federal match.
- **Minnesota H.F.1409/S.F.1514** Proposes appropriations, including administration of grants to the Association of Minnesota Public Educational Radio Stations to purchase cybersecurity and broadcast technology.
  - > These two bills are labeled by the legislature as companion bills.
- **Minnesota H.F.1830/S.F.1426** (enacted) Provides appropriations for cybersecurity grant program to provide support for state and local cybersecurity improvement projects for political subdivisions and Minnesota tribal governments.
  - > These two bills are labeled by the legislature as companion bills.
- **Minnesota H.F.1960/S.F.2001** Proposes amendments to existing law relating to peacetime emergencies; governor may declare peacetime emergency for cyber attack.
  - > These two bills are labeled by the legislature as companion bills.
- **Minnesota H.F.2940/S.F.2979** Proposes appropriations for information technology services, specifically for a cybersecurity grant program and for statewide cybersecurity enhancements.
  - > These two bills are labeled by the legislature as companion bills.
- **Missouri S.B.7** Proposes to establish a chief data officer position and may require agencies to develop and adopt policies and procedures relating to management and security of electronic data.
- **Missouri S.B.319** Proposes to study issues relating to cybersecurity and relating to the Joint Committee on Disaster Preparedness and Awareness.
- **Nebraska L.B.650** Proposes to withhold from the public records relating to cybersecurity by state or political subdivisions.

- **Nebraska L.B.651** Proposes appropriations, including funds for cybersecurity activities including preparedness activities, procuring tools, promote training and awareness, and support workforce development.

Northeast and Mid-Atlantic:

- **Connecticut S.B.635** Proposes to authorize the National Guard to provide the state and municipalities with cybersecurity functional support.
- **Connecticut S.B.1191** Proposes to prohibit use of certain applications on state government devices.
- **Maine L.D.206** (enacted) Provides appropriations, including funds for statewide cybersecurity costs.
- **Maryland H.B.1065** Proposes to establish a Head of Cyber Preparedness Unit to work to improve cybersecurity preparedness for units of local government.
- **Maryland H.B.1131/S.B.891** Proposes to require assignment of National Guard members to support certain state cybersecurity programs.
  - > These two bills are labeled by the legislature as cross-filed bills.
- **Maryland S.B.868** Proposes to establish a Head of Cyber Preparedness Unit to work to improve cybersecurity preparedness for units of local government.
- **Massachusetts H.60** Proposes to establish the Massachusetts Information Privacy and Security Act and the attorney general would be required to adopt regulations including supplementing or revising the list of industry recognized cybersecurity frameworks.
- **Massachusetts H.66** Proposes to establish definition of civil defense to include a cybersecurity attack or threat.
- **Massachusetts H.82** Proposes to prohibit employees of commonwealth, country, or municipality from downloading applications or software from social media company on commonwealth owned devices.
- **Massachusetts H.3062** Proposes to require state agency procurements to give preference to vendors which carry cybersecurity insurance.
- **Massachusetts S.26** Proposes law relating to modernization of state agency information technology systems.
- **Massachusetts S.32** Proposes to establish cyber incident response team to respond to, mitigate against, and recover from significant cybersecurity incidents.

- **Massachusetts S.37** Proposes to prohibit employees of commonwealth, country, or municipality from downloading applications or software from social media company on commonwealth owned devices.
- **Massachusetts S.227** Proposes to establish Massachusetts Information Privacy and Security Act and the attorney general to adopt regulations including supplementing or revising the list of industry recognized cybersecurity frameworks.
- **New Hampshire H.B.2** (enacted) Provides for appropriations, including funding for state and local cybersecurity grant program.
- **New Hampshire H.B.25** (enacted) Provides for appropriations, including funding for cybersecurity program enhancements.
- **New Hampshire H.B.519** (enacted) Establishes chief information security officer which has the authority and power to direct the formulation and implementation of cybersecurity and information security strategy, direction, policy, procedures and standards across the executive branch.
- **New Jersey A.493** Proposes to require reporting of cybersecurity incidents to Office of Homeland Security and Preparedness.
- **New Jersey A.1450** Proposes that the Office of Information Technology must provide minimum information security standards and guidelines to be followed by state agencies.
- **New Jersey A.1671** Proposes to require state, county, and municipal employees and state contracts to complete cybersecurity awareness training.
- **New Jersey A.1848** Proposes to require state employees who have access to state agency computers to receive training in cybersecurity best practices.
- **New Jersey A.1962/S.423** Proposes a law that relates to development of advanced cyberinfrastructure strategic plan.
  - > These two bills are labeled by the legislature as identical bills.
- **New Jersey A.4184/S.2827** (enacted) Creates a law relating to hiring of information technology or cybersecurity professionals.
  - > These two bills are labeled by the legislature as identical bills.
- **New Jersey A.4836/S.3417** (enacted) Creates a law relating to developing a coordinated statewide response plan to address internet outages caused by a cyberattack.
  - > These two bills are labeled by the legislature as identical bills.
- **New Jersey A.5065/S.3645** Proposes to require the NJ Cybersecurity and Communications

Integration Cell to conduct study of cybersecurity infrastructure of public entities and private businesses to identify cybersecurity threats and vulnerabilities.

  > These two bills are labeled by the legislature as identical bills.

- **New Jersey A.5530/S.3826** Proposes to establish state and local government purchasing and use requirements for cybersecurity systems.

  > These two bills are labeled by the legislature as identical bills.

- **New Jersey S.297** (enacted) Requires public agencies and others to report cybersecurity incidents to Office of Homeland Security and Preparedness.

- **New York A.2833/S.5615** Proposes to require the commissioner and state agencies, when procuring end point devices, to require devices, services, and solutions to meet NIST Cybersecurity Framework.

  > These two bills are labeled by the legislature as identical bills.

- **New York A.3000** Proposes to provide funding in this budget bill for a cyber incident response program.

- **New York A.3005/S.4005** (enacted) Creates a law relating to reporting on the state's cybersecurity infrastructure and cybersecurity resiliency efforts.

  > These two bills are labeled by the legislature as identical bills.

- **New York A.3094/S.5646** Proposes to require determination of critical infrastructure which would be considered vital and vulnerable to cybersecurity acts.

  > These two bills are labeled by the legislature as identical bills.

- **New York A.4640/S.4512** Proposes to create the cybersecurity enhancement fund and restricts use of taxpayer dollars to pay ransoms in ransomware attacks.

  > These two bills are labeled by the legislature as identical bills.

- **New York A.7331/S.6474** Proposes to require governmental entities to implement multifactor authentication for local and remote network access, and other requirements.

  > These two bills are labeled by the legislature as identical bills.

- **New York A.7504/S.1693** Proposes to require development of state digital equity plan to increase broadband access to underserved populations; plan must identify barriers including awareness and use of measures to secure online privacy and cybersecurity of individual.

  > These two bills are labeled by the legislature as identical bills.

- **New York S.4000** (enacted) Provides funding in the budget bill for cyber incident response program.
- **Pennsylvania H.B.611** Proposes appropriations and requires supplement funds be used for general government operations, including funds for IIJA State and Local Cybersecurity.
  - > Note: H.B.611 was signed by the Governor, but cybersecurity was not addressed in the final bill.
- **Pennsylvania H.B.883** Proposes to create new law relating to information technology and addresses cybersecurity throughout.
- **Pennsylvania H.B.1552** Proposes appropriations for general government operations, including funds for IIJA State and Local Cybersecurity.
- **Pennsylvania S.B.284** Proposes a new law relating to information technology and requiring the Office of Information Technology to be responsible for maintaining and strengthening the state's cybersecurity posture.
- **Pennsylvania S.B.301** Proposes appropriations for information technology cybersecurity.
- **Pennsylvania S.B.480** Proposes appropriations for information technology cybersecurity.
- **Vermont H.136** Proposes to prohibit applications for social media platforms from being used in or connected to any state network or from being downloaded or installed on state-owned or state-issued device; prohibits use of certain vendors, products, and entities that introduce unacceptable level of cybersecurity risk to the state.

Southwest:

- **Arizona H.B.2570** Proposes appropriations for state cyber risk insurance fund.
- **Arizona H.B.2810** Proposes appropriations for statewide cybersecurity grants.
- **Arizona S.B.1041** Proposes to secure enterprise license for state agencies for security software.
- **Arizona S.B.1523** Proposes appropriations for state cyber risk insurance fund.
- **Arizona S.B.1720** (enacted) Provides appropriations for statewide cybersecurity grants and cyber risk insurance fund.
- **New Mexico H.B.214** Proposes appropriations to provide enterprise cybersecurity services to state agencies.
- **New Mexico S.B.269** (enacted) Creates a law that relates to the chief information officer and coordinating, deploying, offering, or providing cybersecurity risk prevention and information technology and mitigation.

- **New Mexico S.B.280** (enacted) Creates the Cybersecurity Act; office is responsible for all cybersecurity and information security related functions for agencies; establishes cybersecurity advisory committee to develop statewide cybersecurity plan and guidelines.
- **Oklahoma S.B.107** Proposes to prohibit state agencies from entering into contracts with companies directly influenced or owned by certain countries that are related to critical infrastructure, including cybersecurity systems.
- **Oklahoma S.B.320** Proposes a law that relates to responsibility of assessing and tracking cybersecurity incidents.
- **Texas H.B.2156** Proposes to establish a chief information security officer position, which will oversee cybersecurity matters for the state.
- **Texas S.B.621** (enacted) Establishes chief information security officer position, which will oversee cybersecurity matters for the state.
- **Texas S.B.1204** Proposes a law that relates to interstate information sharing and analysis organization to provide forum for states to share information regarding cybersecurity threats; defines security incident to include introduction of ransomware.

West:

- **California A.B.227** Proposes to prohibit applications installed on state-owned or state-issued devices, exception if installed for cybersecurity research.
- **California A.B.749** Proposes actions related to data, including multifactor authentication for access to systems of state agencies, and implements a zero trust architecture.
- **California S.B.74** Proposes to require state entities to prohibit applications from social media platforms from being downloaded or installed on state-owned or state-issued devices.
- **California S.B.102** Proposes a law that relates to a report on state implementation of cybersecurity initiatives.
- **California S.B.265** Proposes to require strategic multiyear outreach plan to assist critical infrastructure sectors, including information technology sectors, in efforts to improve cybersecurity.
- **Hawaii H.B.460** Proposes to prohibit employees of the state government from downloading or using the TikTok application, in order to protect state's cybersecurity.
- **Hawaii H.B.1036** Proposes to establish a center to monitor crimes and hazards and coordinate on response activities, including furnishing technical assistance to reduce impacts of cyber incidents.
- **Hawaii S.B.1334** Proposes to establish a center to monitor crimes and hazards and coordinate on

response activities, including furnishing technical assistance to reduce impacts of cyber incidents.

- **Hawaii S.B.1478** Proposes to establish offensive cybersecurity program to analyze and evaluate cybersecurity threats and increase cybersecurity awareness and education.
- **Hawaii S.C.R.84** (Resolution) Proposes to request the Chief Information Officer to conduct a review on up-to-date technology in all departments, agencies, and offices, to reduce cyber threats and help protect state against cyberattacks.
- **Hawaii S.R.75** (Resolution enacted) Requests Chief Information Officer to conduct review on up-to-date technology in all departments, agencies, and offices, to reduce cyber threats and help protect state against cyberattacks.
- **Montana H.B.161** (enacted) Amends existing law relating to the unlawful use of a computer.
- **Oregon H.B.2490** (enacted) Exempts from required disclosure records, documents or plans concerning protection relating to cybersecurity devices, programs, or systems.
- **Oregon H.B.2806** (enacted) Requires governing bodies of public bodies to meet in executive session when considering matters relating to safety, including matters relating to cybersecurity infrastructure, and responses to cybersecurity threats.
- **Washington H.B.1464** Proposes a law that relates to malware and ransomware protection; prevention education for state employees who use state technology services.
- **Wyoming H.B.184** Proposes to appoint administrator of cybersecurity division, which ensures other state agencies' compliance with information security policies and regulations.

South:

- **Florida H.B.1511** Proposes to create the Florida Cyber Protection Act and establishes operations committee to ensure collaboration between agencies and governmental entities relating to cybersecurity; requires reporting ransomware.
- **Florida S.B.1708** Proposes to create the Florida Cyber Protection Act and establishes operations committee to ensure collaboration between agencies and governmental entities relating to cybersecurity; requires reporting ransomware.
- **Florida S.B.2508** Proposes a law that relates to moving cybersecurity operations to the Department of Law Enforcement and cybersecurity governance framework guidelines, and mandatory cybersecurity awareness training for state employees.
- **Georgia H.R.68** (Resolution) Proposes to encourage dedication of funds to efforts to promote and improve cybersecurity education, training, and workforce development.

- **Georgia S.B.93** (enacted) Restricts use of certain social media platforms on state equipment, with exceptions for cybersecurity research and development.
- **Georgia S.B.97** Proposes to create the Georgia Cyber Command division.
- **Kentucky H.B.124** Proposes to ban social media applications, including TikTok from state government technology.
- **Kentucky H.B.155** Proposes to ban social media applications, including TikTok from state government technology.
- **Louisiana H.B.361** (enacted) Prohibits use of TikTok and other applications on computers and networks owned or leased by the state.
- **Louisiana H.B.388** (enacted) Provides appropriations for the Cyber Assurance Program to align and invest in proven cyber capabilities.
- **Louisiana H.B.431** Proposes to amend existing law relating to power to review procurement requests related to technology or cybersecurity.
- **Mississippi S.B.2140** (enacted) Prohibits state employees from downloading or using TikTok on a state-issued device.
- **Mississippi S.B.2717** (enacted) Requires department of information technology to evaluate the Enterprise Security Program, including evaluating whether opportunities exist to centralize and coordinate oversight of cybersecurity efforts across all state agencies; also requires state agencies to notify department of a cyberattack or demand for ransom.
- **Mississippi S.B.2870** Proposes to prohibit state employees from downloading or using TikTok on a state-issued device.
- **North Carolina H.B.196** Proposes to address reporting requirements by the state Chief Information Officer relating to cybersecurity.
- **North Carolina H.B.259** (enacted) Relates to cybersecurity reporting and requests for support; reopens proposal period for cybersecurity pilot program.
- **North Carolina H.B.671** Proposes to establish cybersecurity fund and funds will be used to address cybersecurity risks and ensure personnel are properly trained.
- **North Carolina S.B.83** Proposes to prohibit public agencies from allowing employees to install, use, or access a high-risk platform on public agency-owned devices, with some exceptions.
- **South Carolina H.B.3448** Proposes to prohibit electronic devices the Department of Administration manages for executive agencies from using websites and applications that threaten cybersecurity and infrastructure from foreign and domestic threats.

Ransomware Focused Legislation (19 bills in 11 states)

In 2023, legislators in eleven states introduced 19 bills related to payments and reporting of ransomware incidents. This list compares to 18 bills in 10 states in 2022, and 7 ransomware bills that were introduced in 6 states in 2021.

Ransomware legislation introduced in 2023 focused on: establishing new reporting requirements (FL, IL, and TX), prohibiting ransomware payments (AR, IA, MA), and criminalizing ransomware (IA, PA). Several ransomware laws adopted in 2023 include Mississippi's required evaluation of the state's Enterprise Security Program, including evaluating whether opportunities exist to centralize and coordinate oversight of cybersecurity efforts across all state agencies. This new law also requires state agencies to notify the department of a cyberattack or demand for ransom. Iowa prohibited the use of ransomware with the intent to interrupt or impair function of state government, public elementary or secondary school, community college, and others, with an exception for research purposes. Texas passed a law requiring security breach notifications by a state agency or local government, including defining security incident to include ransomware.

South:

- **Arkansas H.B.1704** Proposes to prohibit public entities from paying ransom for a cyberattack and requires creation of policy to prohibit payment of a ransom for a cyberattack. Public entity is defined to include the state Department of Education, public school districts, and institutions of higher education.
- **Florida H.B.1511** Proposes creation of Florida Cyber Protection Act and establishes operations committee to ensure collaboration between agencies and governmental entities relating to cybersecurity, also requires reporting ransomware.
- **Florida S.B.1708** Proposes creation of Florida Cyber Protection Act and establishes operations committee to ensure collaboration between agencies and governmental entities relating to cybersecurity; also requires reporting ransomware.
- **Mississippi S.B.2717** (enacted) Requires the Department of Information Technology to evaluate the Enterprise Security Program, including evaluating whether opportunities exist to centralize and coordinate oversight of cybersecurity efforts across all state agencies; also requires state agencies to notify the department of a cyberattack or demand for ransom.

Midwest:

- **Illinois S.B.1740** Proposes to create the Ransomware Attack Act which would require governmental units to report ransomware attacks to the Department of Innovation and Technology within 24 hours of discovery; the Department of Innovation and Technology is also required to implement reporting requirements.

- **Iowa H.F.143** (enacted) Prohibits the use of ransomware with the intent to interrupt or impair function of state government, public elementary or secondary school, community college, and others, with an exception for research purposes.
  - The original study bill was H.S.B.13 but was renumbered as H.F.143.
- **Iowa H.F.554** Proposes to prohibit revenue received from taxpayers to be used to pay for ransomware; political subdivision is defined to include school district.
  - The original study bill was H.S.B.153 but was renumbered as H.F.554.
- **Iowa S.F.203** Proposes to amend the state's Computer Spyware Protection Act to include malware and ransomware.
  - The original study bill was S.S.B.1072 but was renumbered as S.F.203.
- **Michigan S.B.380** Proposes amendments to state aid and pupil membership counts that would require the state department of education to count as hours and days of student instruction any day in which student instruction is not provided due to a ransomware attack.

Northeast and Mid-Atlantic

- **Massachusetts S.35** Proposes to prohibit state agencies, local government entities, or municipalities from submitting ransomware payments.
- **New York A.4640/S.4512** Proposes to create a cybersecurity enhancement fund and restrict the use of taxpayer dollars to pay ransoms in ransomware attacks.
  - These two bills are labeled by the legislature as identical bills.
- **New York A.5736/S.5007** Proposes the promulgation of regulations that design and develop standards for malware and ransomware protection for mission critical information systems.
  - These two bills are labeled by the legislature as identical bills.
- **Pennsylvania S.B.563** Proposes to amend existing law providing for criminal acts relating to ransomware; defines ransomware attacks on Commonwealth agencies to include school districts, career and technical schools, charter schools, and community colleges.

Southwest:

- **Texas H.B.712** Proposes to amend existing law relating to security breaches with notification by a state agency or local government; security incident defined to include ransomware.
- **Texas S.B.271** (enacted) Amends existing law relating to security breaches with notification by a state agency or local government; security incident defined to include ransomware.

- **Texas S.B.1204** Proposes an interstate information sharing and analysis organization to provide forum for states to share information regarding cybersecurity threats; defines security incident to include introduction of ransomware.

West:

- **Washington H.B.1464** Proposes malware and ransomware protections; proposes prevention education for state employees who use state technology services.

Creation of Task Force, Commission, or Office Related to Cybersecurity (27 bills in 15 states)

In 2023, state legislators in 15 states introduced 27 bills that proposed to create a task force, commission, or office of cybersecurity. This list compares to 30 bills in 15 states in 2022 and 28 such bills introduced in 14 states in 2021. States (CT, IL, IN, LA, NM, VT, WA) adopted 7 new laws that included the creation of a task force, commission, or office related to cybersecurity.

Northeast and Mid-Atlantic:

- **Connecticut S.B.572** Proposes to establish a cybersecurity task force.
- **Connecticut S.B.933** (enacted) Establishes a task force to study cybersecurity.
- **Massachusetts H.2821** Proposes to establish a digital advertising revenue commission to study digital advertising in the state; report must include suggested revenue uses, including creation of municipal cybersecurity grant program.
- **Massachusetts S.36** Proposes to establish a cybersecurity control and review commission to recommend standards relating to interagency cybersecurity data collaboration.
- **New Jersey A.2037** Proposes to establish a New Jersey Information Technology Commission.
- **New Jersey A.J.R.66/S.J.R.12** Proposes to establish a New Jersey Cybersecurity Task Force to address cybersecurity threats.
  - > These two bills are labeled by the legislature as identical bills.
- **New York A.2529** Proposes to establish a commission to study EU's general protection data regulation and current state of cybersecurity in the state.
- **Pennsylvania H.B.1139** Proposes to establish a Cybersecurity Coordination Board to collect, study, and share information relating to cybersecurity issues and initiatives; Secretary of Education would serve on Board.
- **Pennsylvania H.R.170** (Resolution) Proposes to establish an advisory committee to conduct study on AI; includes reference to concerns with quality of cybersecurity provided by AI programs.

- **Pennsylvania S.R.143** (Resolution) Proposes to establish an advisory committee to conduct study on AI; includes reference to concerns with quality of cybersecurity provided by AI programs.

Midwest:

- **Illinois H.B.3563** (enacted) Establishes the Generative AI and Natural Language Processing Task Force, addressing challenges of AI for cybersecurity.
- **Indiana H.B.1266** (enacted) Establishes the Indiana cyber civilian corps program advisory board.
- **Minnesota H.F.1693/S.F.1746** Proposes to amend existing law relating to legislative commission on cybersecurity, which oversees state's cybersecurity measures; defines closed meeting records.
  - > These two bills are labeled by the legislature as companion bills.
- **Minnesota H.F.1710/S.F.1703** Proposes to amend existing law relating to legislative commission on cybersecurity, which oversees state's cybersecurity measures; defines closed meeting records.
  - > These two bills are labeled by the legislature as companion bills.
- **Minnesota H.F.1826/S.F.1424** Proposes to amend existing law relating to legislative commission on cybersecurity; adds definition for security records.
  - > These two bills are labeled by the legislature as companion bills.

South:

- **Louisiana S.B.152** (enacted) Establishes the Louisiana Cybersecurity Commission.

Southwest:

- **New Mexico S.B.280** (enacted) Creates the Cybersecurity Act including a new office responsible for all cybersecurity and information security related functions for agencies; establishes cybersecurity advisory committee to develop statewide cybersecurity plan and guidelines.
- **Ohio H.B.74** Proposes to establish a cybersecurity and fraud advisory board, focused on best practices in, shared experiences regarding, and future efforts to improve cybersecurity and fraud prevention.
- **Texas H.B.4322** Proposes to establish a STEM and computer science strategic advisory committee; reporting requirement includes recommendations regarding cybersecurity in public schools.
- **Vermont H.291** (enacted) Creates a Cybersecurity Advisory Council; duties would include building strong partnerships with local universities and colleges to leverage cybersecurity resources.
- **Washington S.B.5518** (enacted) Establishes cybersecurity advisory committee to strengthen

cybersecurity in industry and public sectors; brings together government and institutions of higher education to provide recommendations relating to cybersecurity risks and recovering from cybersecurity-related incidents.

- **Washington S.B.5619** Proposes to establish cybersecurity advisory committee to strengthen cybersecurity in industry and public sectors; brings together government and institutions of higher education to provide recommendations relating to cybersecurity risks and recovering from cybersecurity-related incidents.

West:

- **California A.B.1667** Proposes to establish a California Cybersecurity Awareness and Education Council.

Cybersecurity Training Requirements (20 bills in 14 states)

In 2023, legislators in 14 states introduced 20 bills focused on cybersecurity training requirements. This list compared to 27 bills in 9 states in 2022 and 15 such bills that were introduced in 7 states in 2021.Three states (AR, CA, and OR) adopted such requirements.

Northeast and Mid-Atlantic:

- **Connecticut S.B.1089** Proposes the creation of apprenticeship program, including training in cybersecurity.
- **Maryland H.B.1189** Proposes establishing the Cyber Maryland Program to increase cybersecurity workforce and inform cybersecurity training and education programs; requires Higher Education Commission to expand the Cyber Warrior Diversity Program.
- **New Jersey A.1671** Proposes requiring state, county, and municipal employees, and state contracts to complete cybersecurity awareness training.
- **New Jersey A.1848** Proposes requiring state employees who have access to state agency computers to receive training in cybersecurity best practices.
- **New York A.1646/S.2563** Proposes establishing school district cybercrime prevention services program to provide districts with information on strategies, best practices, and programs offering training and assistance in prevention of cybercrimes in school districts.
    - > These two bills are labeled by the legislature as identical bills.

South:

- **Arkansas H.B.1369** (enacted) Requires public entities to develop technology resources policy and cybersecurity policy; training program required for all employees of the public entity; public entity is defined to include the Department of Education, public school districts, charter schools,

and institutions of higher education.

- **Florida S.B.2508** Proposes moving cybersecurity operations to the Department of Law Enforcement and cybersecurity governance framework guidelines; includes mandatory cybersecurity awareness training for state employees.
- **Georgia H.R.68** (Resolution) Proposes to encourage dedication of funds to efforts to promote and improve cybersecurity education, training, and workforce development.
- **North Carolina H.B.671** Proposes establishing a cybersecurity fund; funds to be used to address cybersecurity risks and ensure personnel are properly trained.

Midwest:

- **Iowa H.F.139** Proposes establishing a Cybersecurity Simulation Training Center at Iowa State University of Science and Technology.
  - > The original study bill was H.S.B.14 but was renumbered as H.F.139.
- **Iowa H.F.698** Proposes establishing a Cybersecurity Simulation Training Center at Iowa State University of Science and Technology.
- **Iowa S.F.402** Proposes establishing a Cybersecurity Simulation Training Center at Iowa State University of Science and Technology.
  - > The original study bill was S.S.B.1160 but was renumbered as S.F.402.
- **Kansas H.B.2077** Proposes establishing a cybersecurity awareness training program must be made available to all branches of state government.
- **Nebraska L.B.651** Proposes funding for cybersecurity activities including preparedness activities, procuring tools, promote training and awareness, and support workforce development.

Southwest:

- **Texas H.B.1412** Proposes strategies to promote the resilience of the electric grid; training Texas National Guard as first responders to cybersecurity threats; identify universities with expertise in cybersecurity that can contribute to goal of mitigating all hazards to grid.
- **Texas H.B.1508** Proposes guidelines for state agencies regarding continuing education requirements for cybersecurity training; notification required as to how the guidelines apply to institutions of higher education.
- **Texas S.B.330** Proposes strategies to promote the resilience of the electric grid; training Texas National Guard as first responders to cybersecurity threats; identify universities with expertise in cybersecurity that can contribute to goal of mitigating all hazards to grid.

West:

- **California A.B.569** (enacted) Establishes a pilot program to address cybersecurity workforce gap, including aligning cybersecurity workforce needs of employers with education and training and increasing the pipeline of students pursuing cybersecurity careers.
- **Oregon H.B.2049** (enacted) Establishes a Cybersecurity Center of Excellence; supplements activities of State Chief Information Officer regarding cybersecurity; includes focus on education, training, awareness, workforce development, and others.

Federal Education Cybersecurity Bills Introduced in 2023

Federal legislators' attention on education cybersecurity remained steady in 2023. Members of Congress introduced 22 cybersecurity bills with implications for the education sector, compared to 22 cybersecurity bills in 2022, 19 such bills in 2021, and 10 bills in 2020.

Federal leaders proposed a range of strategies for enhancing the nation's cyber defenses across various sectors. The education-focused federal cybersecurity bills, such as H.R.2845, H.R.2851, H.R.6124, S.1191, and S.2122, aim to bolster cybersecurity within K-12 educational institutions and improve the cybersecurity competencies of the workforce, particularly in critical infrastructure roles through specialized postsecondary education programs.

Awareness and preparedness are central themes in bills like H.R.1360 and S.1835, which seek to launch campaigns to increase cybersecurity literacy among Americans and raise awareness about the importance of cyber defenses.

To address the cybersecurity resilience of federal agencies, H.R.5201 proposes directives to the Federal Emergency Management Agency to mitigate cybersecurity risks. In the realm of cyber insurance, S.513 calls for the establishment of a working group to explore cyber insurance policies.

Workforce development was also a focal point of federal cybersecurity legislation in 2023. Bills like H.R.302, H.R.4502, and S.2256, proposed measures ranging from financial support for cybersecurity students to the creation of apprenticeship and training programs for veterans.

Policy development and response to vulnerabilities are addressed in bills such as H.R.1345 and H.R.5255, which would create dedicated offices and require contractors to implement vulnerability disclosure policies. H.R.3286, S.917, and S.2251 proposed updated responsibilities for the Cybersecurity and Infrastructure Security Agency (CISA), particularly concerning open-source software security and federal information security modernization. H.R.2866 would establish cybersecurity-focused Critical Technology Security Centers to evaluate and test the security of critical technology, with one goal relating to informing and supporting the future work of CISA. And H.R.3369 would require a study on accountability measures for artificial intelligence systems, including researching how accountability measures may reduce cybersecurity risks

related to AI systems.

H.R.4512 suggests the creation of a Digital Economy and Cybersecurity Board of Advisors, signifying a move towards structured governance and strategic oversight of cybersecurity measures at the national level.

Lastly, H.R.231 would prohibit federal funds from being provided to an institution of higher education unless the institution has banned the use of TikTok on electronic devices. An exception is provided here for research, if it pertains to national security, law enforcement, telecommunications, or cybersecurity.

None of the education focused federal cybersecurity measures became law.

Federal Cybersecurity Bills with an Education Focus

- **H.R.2845**—Proposes to establish a School Cybersecurity Improvement Program. The bill would require the Director of the Cybersecurity and Infrastructure Security Agency to enhance existing information exchange efforts, focusing on the needs of K-12 organizations with regards to cybersecurity. Information would be disseminated through the School Cybersecurity Information Exchange.
- **H.R.2851**—Proposes to amend the National Apprenticeship Act and expand the national apprenticeship system, which would include new apprenticeship programs in nontraditional apprenticeship occupations, including cybersecurity and information technology.
- **H.R.6124**—Proposes to direct the U.S. Secretary of Education to take steps to improve the cybersecurity competencies of the critical infrastructure workforce, particularly operators of critical infrastructure technology, by developing postsecondary career and technical education programs that integrate cybersecurity education.
- **S.1191**—Proposes to establish a School Cybersecurity Improvement Program. The bill would require the Director of the Cybersecurity and Infrastructure Security Agency to enhance existing information exchange efforts, focusing on the needs of K-12 organizations with regards to cybersecurity. Information would be disseminated through the School Cybersecurity Information Exchange.
- **S.2122**—Proposes to amend the National Apprenticeship Act and expand the national apprenticeship system, which would include new apprenticeship programs in nontraditional apprenticeship occupations, including cybersecurity and information technology.

Cybersecurity Awareness

- **H.R.1360**—Proposes to require the National Telecommunications and Information Administration to develop and conduct a cybersecurity literacy campaign to increase American's cybersecurity knowledge and awareness.

  - Related bill: S.2201

- S.1835—Proposes to require the Cybersecurity and Infrastructure Security Agency to develop a campaign to raise awareness regarding the importance of cybersecurity in the United States.

FEMA Cybersecurity Improvement Act

- H.R.5201—Proposes to amend the Homeland Security Act 0f 2022 to provide for the mitigation of cybersecurity risks by FEMA.

Cyber Insurance Policies

- S.513—Proposes to require the National Telecommunications and Information Administration to establish a working group on cyber insurance policies.

Cybersecurity Workforce

- H.R.302—Proposes to direct the U.S. Secretary of Energy to provide financial assistance to graduate students and postdoctoral researchers pursuing certain courses of study relating to cybersecurity and energy infrastructure.
- H.R.4502—Proposes to limit the use of educational requirements or qualifications in evaluating candidates for certain cybersecurity positions in the competitive service.
- S.2256—Proposes to authorize the Director of CISA to establish apprenticeship program and to establish a pilot program on cybersecurity training for veterans and members of the Armed Forces transitioning to civilian life.

Federal Vulnerabilities & Policies

- H.R. 1345—Proposes to establish an Office of Policy Development and Cybersecurity within the National Telecommunications and Information Administration to analyze and develop policies related to internet and communications technologies. Specific activities of the office would include, for example, developing policies that promote (1) innovation, competition, and other elements of the communications, media, and technology markets; (2) security and resilience to cybersecurity incidents while fostering innovation; and (3) commercialization of communications technologies.
- H.R.2866—Proposes to create the Critical Technology Security Centers Act of 2023, which requires establishment of at least two cybersecurity-focused Critical Technology Security Centers to evaluate and test the security of critical technology. One goal includes sharing findings to inform and support the future work of the Cybersecurity and Infrastructure Security Agency.
- H.R 3286—Proposes to establish new duties of CISA as they relate to open-source

software security.

- **H.R.3369**—Proposes a study on accountability measures for artificial intelligence systems, including examining how accountability measures may reduce cybersecurity risks related to AI systems.
- **H.R.5255**—Proposes to require contractors to implement a vulnerability disclosure policy that is consistent with NIST guidelines.
- **S.917**—Proposes to establish new duties of CISA as they relate to open-source software security.
- **S.2251**—Proposes to improve the cybersecurity by modernizing federal information security practices.

Creation of Board

- **H.R.4512**—Proposes to establish a Digital Economy and Cybersecurity Board of Advisors

Banning Applications

- **H.R.4512**—Proposes to prohibit federal funds from being provided to an institution of higher education, unless the institution has banned the use of TikTok on electronic devices; provides exceptions for research purposes, including research as it pertains to national security, law enforcement, telecommunications, or cybersecurity.

Methodology

CoSN gathered the data presented in this report through the legislative information systems of all 50 states, along with federal sourcing information from Congress.gov. Our policy team examined each bill, creating concise summaries for each measure, and closely tracked the progress of these bills from their introduction to committee deliberation and, when relevant, subsequent actions taken by the legislative body or executive branch. Leveraging our comprehensive analysis, we organized and presented the measures in this report according to their respective policy topics, their journey through the legislative process, and their geographical origin.