CoSN

Leading Education Innovation

State and Federal Cybersecurity Policy and Education in 2024

January 2025

Contents

CoSN
Leading Education Innovation

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

CoSN's Mission:

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

www.cosn.org

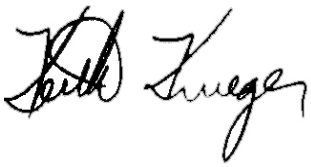
For access to this report, please visit
www.cosn.org/advocacy-policy

In 2024, state and federal leaders intensified their focus on cybersecurity policies for the education sector, driven by the alarming frequency and impact of cyberattacks targeting schools and postsecondary institutions. Between 2018-2023, 491 ransomware attacks affected 8,054 separate schools and colleges, breaching over 6.7 million individual records (Comparitech, 2024).[1] The fallout from these attacks has been devastating, with ransom demands ranging from $5,000 to $40 million, averaging just under $1.4 million per incident (Comparitech, 2024). Beyond financial strain, the disruptions have been profound, as affected schools grapple with an average downtime of 12.6 days, the longest on record, causing months-long recovery in some cases (Comparitech, 2024). This mounting crisis underscores the urgent need for robust cybersecurity measures to protect elementary, secondary, and postsecondary institutions and their sensitive data.

I hope you find this 2024 State and Federal Cybersecurity Policy Report helpful in understanding key trends at the state and national level around cybersecurity in education. This is the third year of this effort, and we continue to see increased policy focus on this key topic.

I also hope you will explore the many public resources that CoSN, the professional association of school system technology leaders/CIO/CTOs, makes available on cybersecurity at www.cosn.org/cybersecurity.

Sincerely,



Keith Krueger

CEO, CoSN

---

[1] Paul Bischoff, On average, US schools & colleges lose $500K per day to downtime from ransomware attacks (updated August 27, 2024) (available at https://www.comparitech.com/blog/information-security/school-ransomware-attacks/)

Introduction

The state and federal education cybersecurity policy landscape continued to evolve rapidly this year as policymakers, especially state leaders, worked to better protect the education sector from serious digital threats. In 2024, state legislators introduced 258 bills addressing various aspects of cybersecurity across 42 states with 29 measures becoming law. While this volume represents a modest decline from 2023's 307 bills and 75 enacted laws, the decrease likely reflects the substantial policy foundation established in previous legislative sessions rather than diminished policymaker interest. Despite fewer total bills, states continued to advance new solutions worthy of consideration across the broader education sector.

K-12 schools and postsecondary institutions received particular attention in state legislatures, with 28 bills in 16 states focusing directly on K-12 cybersecurity and 19 bills in 10 states addressing postsecondary cybersecurity. This attention is not surprising, given that on average, elementary and secondary schools and postsecondary institutions lose $500 thousand per day to downtime from ransomware attacks.[2] The education-specific bills considered in 2024 focused on several key areas: professional development for technology leaders, cybersecurity curriculum requirements, infrastructure standards, incident reporting protocols, and funding mechanisms for security improvements.

Beyond education-specific legislation, many of 2024's general government cybersecurity bills have significant implications for schools and postsecondary institutions as units of state and local government. Notable trends in this broader legislation include:

- Creation of new cybersecurity task forces and offices with education representation
- Development of comprehensive incident reporting frameworks
- Establishment of grant programs accessible to educational institutions
- Specific measures to combat ransomware threats
- Integration of artificial intelligence and cybersecurity considerations

Several states emerged as particularly active in considering a wide range of cybersecurity proposals, with Massachusetts (27 bills), Minnesota (25 bills), New York (23 bills), New Jersey (20 bills), California (14 bills), and Iowa (14 bills) leading in the number of introduced bills. These bills, and the many others considered across the nation, may provide cybersecurity policy models for other states and communities to consider in 2025.

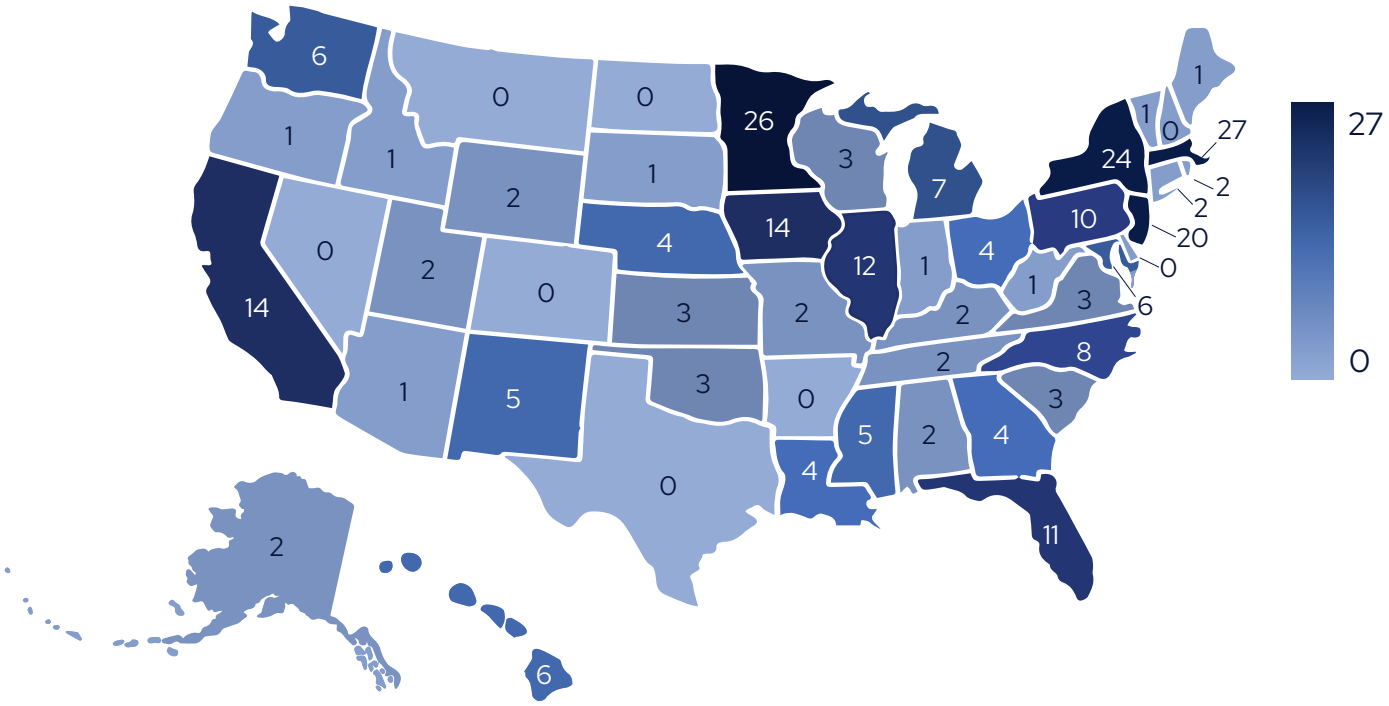
The most significant enacted laws of 2024 demonstrate diverse approaches to strengthening cybersecurity in educational settings, from Alabama's K-12 Technology and Cybersecurity Leadership Act to Maryland's enhanced Cyber Maryland Fund supporting both K-12 and higher education initiatives. These laws reflect strong recognition that effective cybersecurity requires coordinated efforts across all levels of education, supported by robust state frameworks and funding mechanisms.

---

[2] "Map of U.S. Ransomware Attacks", Comparitech.com (2024), https://www.comparitech.com/ransomware-attack-map/

This paper examines the key trends, strategic approaches, and practical implications of 2024's cybersecurity legislation for educational institutions. By highlighting both enacted laws and notable proposed legislation, it provides education leaders and policymakers with actionable insights for strengthening cybersecurity governance, protection, and education in their own communities and schools.

FIGURE 1: CYBERSECURITY BILLS INTRODUCED IN STATE LEGISLATURES - 2024



Cybersecurity Policy Recommendations for State and Local Education Leaders

FIGURE 2: STRENGTHENING EDUCATION'S DIGITAL DEFENSE: CRITICAL CYBERSECURITY POLICIES

Based on our comprehensive review of the 2024 cybersecurity legislation and new laws, we recommend that state and local leaders carefully evaluate the following five policy areas and related state exemplars to help better protect school networks and the confidential student and personnel data they contain. States that lack any cybersecurity policies focused on protecting the education sector should consider adopting comprehensive polices in 2025 that draw from across these areas, while other states should evaluate whether these ideas might help fill gaps in their defenses.[3]

COMPREHENSIVE CYBERSECURITY EDUCATION PROGRAMS

Recommendation: Develop comprehensive K-12 through higher education cybersecurity programs that include:

- Grade-appropriate cybersecurity curriculum standards
- Professional qualifications for technology leadership positions
- Mandatory professional development in cybersecurity
- Integration with career pathway programs
- Collaboration between K-12 and higher education institutions

Enacted Example: Alabama's K-12 Technology and Cybersecurity Leadership Act

Other Un-Enacted Examples:

- Arizona HB2699 (requiring internet safety instruction for grades 5-12)
- Florida SB1344 (mandating K-12 computer science instruction, including cybersecurity)
- New Jersey S3222 (requiring cybersecurity instruction in grades 9-12 and the development of a cybersecurity model curriculum for use by four-year institutions of higher education)

CYBERSECURITY GRANT PROGRAMS

Recommendation: Establish flexible grant programs that:

- Support both infrastructure and training needs
- Include K-12 schools and higher education institutions as eligible recipients
- Provide funding for cybersecurity assessments
- Support regional collaboration
- Include provisions for ongoing program evaluation

Enacted Example: Maryland's Enhanced Cyber Maryland Fund (update to existing law)

Other Un-Enacted Examples:

- Pennsylvania SB1247 (establishing cybersecurity improvement grants)
- Wisconsin AB43 (establishing security operations centers)

[3] Further details on each enacted example discussed in these recommendations are provided later in this report.

INCIDENT REPORTING AND RESPONSE

Recommendation: Create comprehensive incident reporting frameworks that:

- Establish clear reporting requirements and timeframes
- Protect sensitive information about incidents
- Require post-incident assessments
- Create mechanisms for sharing threat information
- Provide support for incident response

Enacted Example: Tennessee's System Hacker Prevention Act

Other Un-Enacted Examples:

- Illinois HB2353 (requiring school districts to report cyber-attacks)
- Minnesota SF4874 (mandating reporting of cybersecurity incidents)
- New Jersey A3897 (requiring cybersecurity incident audits)

PUBLIC-PRIVATE PARTNERSHIPS

Recommendation: Foster greater collaboration between government, K-12 and postsecondary education, and private sector through:

- Regional cybersecurity centers
- Shared security operations centers
- Industry-education partnerships
- Collaborative training programs
- Joint threat assessment and response

Enacted examples: Louisiana's Cyber Assurance Program; Massachusetts Cybersecurity Innovation Fund

Other Un-Enacted Examples:

- Kentucky HB139 (creating network of cyber centers)

AI AND CYBERSECURITY INTEGRATION

Recommendation: Create frameworks to address emerging technology risks through:

- Regular assessment of AI cybersecurity implications
- Integration of AI in cybersecurity monitoring
- Development of AI security standards
- Cross-sector collaboration on emerging threats
- Regular policy updates to address new technologies

Enacted Example: Indiana's AI Task Force

Other Un-Enacted Examples:

- California AB1667 (establishing Cybersecurity Awareness and Education Council)
- New Mexico SB130 (creating AI Work Group)

These recommendations reflect valuable approaches from both enacted and proposed legislation and provide a starting point for states and communities seeking to strengthen their cybersecurity frameworks to better protect schools and other educational institutions.

Spotlight on Selected New Education Cybersecurity Laws

Our 2024 "spotlight" states enacted comprehensive cybersecurity legislation with a strong focus on educational institutions, reflecting a growing recognition of cyber threats in the education sector. From Alabama's redefinition of technology leadership roles to Florida's enhancement of statewide cybersecurity infrastructure through Cyber Florida, these laws demonstrate an evolving approach to cybersecurity governance in education.

FIGURE 3: 2024 SPOTLIGHT STATES

The new laws across these eight states shares common themes: strengthening institutional leadership, protecting sensitive information, expanding professional development requirements, and creating sustainable funding mechanisms for cybersecurity initiatives.

Notable trends include the integration of cybersecurity into existing educational frameworks, as seen in Indiana's comprehensive framework linking AI and cybersecurity, and the establishment of dedicated oversight bodies, exemplified by Mississippi's Cyber Security Review Board. These laws collectively represent a shift toward more structured, professional approaches to managing cybersecurity risks in educational settings while balancing transparency with security needs.

Alabama's K-12 Technology and Cybersecurity Leadership Act (HB439)

Alabama new cybersecurity law focuses directly on K-12 cybersecurity leadership:

- Renames "technology coordinator" position to "technology director" with expanded cybersecurity responsibilities
- Establishes minimum qualifications including:
  - A technology-related degree from an accredited institution, or
  - A degree in another field plus full-time technology management experience, or
  - A high school diploma with industry-recognized certifications in networking, cybersecurity, or data management plus work experience
- Requires completion of mandatory professional development including:
  - Information technology management and cybersecurity training
  - Annual continuing education units
- Mandates completion of Chief Technology Officer Academy training within 24 months for new directors

California's Critical Infrastructure Protection (AB2715)

California enacted legislation addressing how public entities, including educational institutions, can discuss cybersecurity matters. The law:

- Authorizes closed sessions for discussions about threats to critical infrastructure controls relating to cybersecurity
- Enables local educational agencies to have confidential discussions about sensitive cybersecurity matters
- Balances public transparency with the need to protect sensitive cybersecurity information
- Provides a mechanism for educational institutions to address cybersecurity threats while maintaining appropriate confidentiality

Florida's Enhancement of Cyber Florida (HB1555)

Florida strengthened its cybersecurity infrastructure through amendments to the Florida Center for Cybersecurity (Cyber Florida). The law:

- Refocuses Cyber Florida's mission to prioritize:
  - Advancing and funding education and research initiatives in cybersecurity
  - Supporting workforce development through education
  - Engaging with communities on cybersecurity awareness
- Authorizes Cyber Florida to:
  - Conduct cybersecurity training and professional development for state and local government employees, including school districts
  - Assist in improving cybersecurity effectiveness of school districts' technology platforms and infrastructure
- Creates a systematic approach to developing cybersecurity expertise through education and training programs

Indiana's Comprehensive Cybersecurity Framework (SB150)
Indiana created an integrated approach linking AI and cybersecurity with direct implications for education:

- Allows school corporations and state educational institutions to:
  - Adopt cybersecurity policies based on state guidelines
  - Implement mandatory cybersecurity training programs
  - Develop technology resource usage policies
- Requires educational institutions connecting to state technology infrastructure after July 2027 to:
  - Complete cybersecurity assessments every three years
  - Implement secondary end-user authentication
  - Maintain compliance with state cybersecurity standards

Maryland's Enhanced Cyber Maryland Fund (SB816)
Maryland strengthened its existing cybersecurity program with significant educational components:

- Continues to authorize grants to elementary/secondary schools, higher education institutions, and community colleges
- Affirms the focus on developing cybersecurity programs and workforce initiatives
- Requires the Maryland Technology Development Corporation to:
  - Adopt standards for awarding grants
  - Continue to serve as a hub for employers seeking cybersecurity workforce development programs
  - Continue to inform cybersecurity training and education programs based on industry needs
- Provides dedicated funding for talent pipeline management

Mississippi's Cyber Security Review Board (SB2698)
Mississippi established a comprehensive approach to statewide cybersecurity governance with direct implications for education. The law creates the Cyber Security Review Board with the State Superintendent of Education serving as a voting member. This structure ensures that K-12 education has a voice in:

- Creating systems for reporting cybersecurity attacks
- Researching and implementing best practices to mitigate cybersecurity risks
- Connecting educational institutions with federal and industry partners
- Developing and distributing best practices in cybersecurity throughout the state

Virginia's Cybersecurity Information Protection (SB222)
Virginia enacted legislation to protect sensitive cybersecurity information while maintaining institutional security. The law:

- Exempts cybersecurity information received by the Virginia Information Technologies Agency from Freedom of Information Act or the Government Data Collection and

Dissemination Practices Act requirements
- Applies specifically to both school boards and institutions of higher education
- Requires all individuals having access to cybersecurity information maintained by the Virginia Information Technologies Agency to be kept confidential
- Creates a framework for educational institutions to manage sensitive cybersecurity information without compromising security through public disclosure

West Virginia's Adult Cybersecurity Education Initiative (HB4986)
West Virginia enacted a law focused on expanding cybersecurity education for adult learners. Key provisions include:
- Authorizing the State Superintendent to seek and administer federal and private grants for computer science and cybersecurity instruction
- Distributing up to $300,000 per recipient to eligible entities including school districts, career centers, and adult education providers
- Supporting instructional costs and teacher compensation
- Placing programs under State Department of Education oversight

These new state laws showcase different approaches to strengthening cybersecurity through governance structures, professional development requirements, adult education initiatives, workforce development programs, and integration with emerging technologies. Together, they provide a range of options for other states considering similar legislation.

All Other Enacted Education Cybersecurity Laws

Other 2024 state cybersecurity laws reveal several distinct trends in how states are approaching cyber threats and preparedness. Education emerged as a major focus area, with legislation addressing both K-12 and higher education cybersecurity needs through various approaches: direct funding, workforce development programs, infrastructure improvements, and training requirements.

Many states recognized schools as critical infrastructure requiring specific protections, while others focused on developing cybersecurity talent pipelines through educational programs. Workforce development emerged as another key priority, with several states creating dedicated funding streams and programs for cybersecurity education and training.

Local government support was also prominent, with multiple states creating programs to help municipalities improve their cybersecurity posture. Funding mechanisms were a common feature, whether through direct appropriations or grant programs. Another notable trend was the integration of cybersecurity considerations into emerging technology initiatives, particularly evident in artificial intelligence deployment.

Florida - HB5001: Appropriations Act

- Funds EASE Plus incentive program supporting students in cybersecurity programs
- Supports University of South Florida's cybersecurity center
- Aims to enhance existing cybersecurity workforce through education
- Provides cyber-attack simulation range for training

Florida - SB1680: Government Technology Modernization Council

- Focuses on digital literacy skills for school-age audiences
- Requires quarterly meetings with Cybersecurity Advisory Council
- Emphasizes preparing students for digital information landscape

Iowa - HF2708: Cybersecurity Operations

- Creates "whole of state" collaborative approach including educational institutions
- Establishes reporting functions affecting schools
- Provides grant opportunities for educational entities

Iowa - SF2433: Department of Management Appropriation

- Provides a small appropriation for local government cybersecurity services potentially benefiting educational institutions

Louisiana - HB1: Appropriations

- Provides funding for the Louisiana Cybersecurity Talent Initiative Fund to support degree and certificate programs
- Focuses on developing cybersecurity workforce through education

Louisiana - HB314: Cyber Assurance Program

- Includes funding for Cyber Assurance Program supporting local government entities
- Provides sustainable cyber protection for education sector

Louisiana - HB700: Provides Relative to Broadband

- Provides that remaining GUMBO 2.0 funds for deployment of broadband service may be used to address certain challenges, including cybersecurity

Louisiana - HB845: Joint Legislative Committee

- Update the JLC's authority to review cybersecurity budgets to include technology and cybersecurity procurement

Maine - LD877: Critical Infrastructure Protection

- Includes school districts in restrictions on technology procurement in critical infrastructure
- Protects educational institutions' information systems

Massachusetts - H4204: Cybersecurity Contracting

- Allows educational institutions and other units of government to participate in cybersecurity services, including cybersecurity training and workforce development, through a grant from the Massachusetts Cybersecurity Innovation Fund

Massachusetts - H4800: Comprehensive Cybersecurity Appropriations

- State Auditor's Office:
  - Funds to conduct audits of high risk information technology related activities including cybersecurity
- Massachusetts Innovation Fund:
  - Partners with community colleges and state universities
  - Creates regional security operations centers
  - Provides cyber threat monitoring and detection services for:
    - Municipalities
    - Nonprofit organizations
    - Small businesses
- Massachusetts Bay Community College:
  - Funds MassBay Center for Cybersecurity Education
  - Supports cybersecurity workforce development
  - Enhances educational capacity in cybersecurity field

Massachusetts - H4889: Capital Investment

- Provides information technology capital investments, includes funding for certain public school cybersecurity improvements
- Supports educational infrastructure protection

New Mexico - HB303: Workforce Training Support

- Creates the New Mexico Workforce Training Economic Support Pilot Program for certain priority industries or fields, including cybersecurity

Ohio - HB2: Appropriations

- Provides funds for the Ohio Cyber Range Institute (state agencies collaboration) and Tolles Cybersecurity Lab Renovation (CTE lab)

Rhode Island - H7225: Higher Education Cybersecurity

- Provides funding for the Rhode Island College, Cybersecurity Building renovation fund for the college's Institute for Cybersecurity & Emerging Technologies
- Focuses on postsecondary cybersecurity education

South Dakota - SB187: Local Government Cybersecurity

- Provides funds to create a local government cybersecurity services initiative to be used to expand and improve cybersecurity for local governments in the state

Tennessee - HB1733: System Hacker Prohibition

- Prohibits state entities from contracting with, negotiating with, or paying an individual or entity if the state entity has proof that the individual or entity is a system hacker

Utah - SB98: Cybersecurity Amendments

- Includes educational institutions in breach notification requirements
- Protects information provided to the Utah Cyber Center, including information relating to data breaches

Utah - SB149: AI Policy Act

- Establishes the Artificial Intelligence Policy Act and the Office of Artificial Intelligence Policy
- Requires creation of rules that would establish data usage limitations and cybersecurity criteria for participants, and the office may establish additional cybersecurity auditing procedures applicable to participants demonstrating artificial intelligence technologies that the office considers high risk

Washington - HB1947: Technology Solutions Reorganization

- Renames the Consolidated Technology Services Agency to the Washington Technology Solutions
- This office is tasked with establishing clear policies and standards for efficient and acceptable use of technology in state government

Wyoming - HB1: Enterprise Technology Funding

- Provides funding for Enterprise Technology Services, including funds for investment in information technology and cybersecurity initiatives, as well as funding for authorized employees for these initiatives

Key Trends in K-12 Cybersecurity Legislation for 2024

Analysis of 2024 state legislation – including bills that did not become law – also reveals significant attention to K-12 cybersecurity, with 28 bills introduced across 16 states specifically addressing K-12 needs. This legislation reflects growing recognition of schools' unique cybersecurity challenges, from protecting sensitive student data to securing increasingly technology-dependent learning environments. While some bills focus on traditional concerns like infrastructure security and incident reporting, others address emerging needs such as professional development for technology leaders and cybersecurity curriculum for students. The most comprehensive legislation, such as Alabama's

K-12 Technology and Cybersecurity Leadership Act, demonstrates how states are moving beyond piecemeal approaches to create integrated frameworks for school cybersecurity. This shift toward comprehensive solutions is particularly evident in five key trends emerging from 2024's legislative activity.[4]

Cybersecurity Training and Professional Development

Bills focusing on providing cybersecurity guidance, training, and technical assistance to school personnel:

- Alabama (HB439*): Requires technology directors to complete cybersecurity training and continuing education
- Georgia (HB338): Requires department to provide guidance and training on basic cybersecurity issues for schools
- Georgia (HR68): Encourages Department of Education to promote cybersecurity education and training
- Indiana (SB150*): Allows school corporations to implement mandatory cybersecurity training programs

Curriculum and Student Instruction

Legislation requiring or promoting cybersecurity education for students:

- Arizona (HB2699): Requires internet safety instruction for grades 5-12 including cybersecurity
- Florida (SB1344): Requires the Department to adopt a strategic plan for a statewide computer science education program, which would include cybersecurity standards
- Illinois (HB4625): Requires developmentally appropriate digital literacy skills including cybersecurity
- New Jersey (A2999): Requires cybersecurity instruction in grades 9-12

Infrastructure and Security Requirements

Bills establishing cybersecurity infrastructure standards and requirements for schools:

- Indiana (SB150*): Requires schools connecting to state infrastructure to complete regular cybersecurity assessments
- Nebraska (LB638): Proposes K-12 Cybersecurity and Data Protection Act with specific security measures
- South Carolina (H4596): Requires schools to prohibit access to applications threatening cybersecurity
- Virginia (SB222*): Establishes protections for school cybersecurity information

[4] All bills in the remainder of the document are noted by an asterisk if they were signed into law in 2024.

Funding and Grant Programs

Legislation creating funding mechanisms for school cybersecurity:

- Iowa (HF2032): Allows district management levy funds to be used for cybersecurity
- Minnesota (HF2497/SF2684* (2023)): Provides grants for school cybersecurity improvements
- New York (A1646/S2563): Authorizes loans and grants for preventing cybercrimes against school districts
- West Virginia (HB4986*): Provides grants for cybersecurity instruction for adult learners

Incident Response and Reporting

Bills establishing requirements for cybersecurity incident reporting and response:

- Florida (HB473): Addresses liability related to cybersecurity incidents
- Illinois (HB2353): Requires school districts to report cyber security attacks
- Minnesota (HF4749/SF4874): Requires schools to report cybersecurity incidents
- New Jersey (A3897): Requires schools to report incidents and undergo cybersecurity audits

These trends demonstrate states' growing recognition of the need to address school cybersecurity through multiple approaches, including professional development, student education, infrastructure improvements, funding support, and incident management protocols. The variety of approaches provides models for other states considering similar legislation.

Key Trends in Postsecondary Cybersecurity Legislation for 2024

State legislatures in 2024 also recognized higher education's needs and dual role in cybersecurity: both as institutions requiring protection and as key partners in developing cybersecurity workforce solutions. Analysis reveals 21 bills across 10 states specifically addressing postsecondary cybersecurity needs, with approaches ranging from infrastructure protection to program development. Notable in this year's legislation is an emphasis on creating physical spaces for cybersecurity education, such as Rhode Island's Institute for Cybersecurity and Minnesota's cybersecurity program facilities, alongside traditional security requirements. Many bills also reflect higher education's crucial role in workforce development, with several states creating mechanisms to align cybersecurity education with industry needs. The most significant trends in postsecondary cybersecurity legislation cluster around five key areas.

Program Development and Facilities

Bills focusing on establishing or enhancing cybersecurity programs and facilities:

- Hawaii (SB1249): Appropriates funding for cybersecurity programs at the University of Hawaii Maui College

- Illinois (HB2538): Funds Illinois Institute of Technology Cybersecurity Bootcamp program
- Minnesota (HF2071/SF1547, HF2880/SF2892, SF676): Multiple bills providing funding to design, renovate, and equip space for cybersecurity programs at Metropolitan State University
- Rhode Island (H7224, H7225*): Supports establishment of Institute for Cybersecurity and Emerging Technologies at Rhode Island College

Workforce Development and Training

Legislation addressing cybersecurity workforce needs through higher education:

- California (AB101, AB221): Implements technology and data security measures for community college districts and cybersecurity oversight
- New Jersey (A2999): Requires Office of Secretary of Higher Education to develop cybersecurity model curricula
- New Mexico (HB303*): Creates workforce training economic support pilot program identifying cybersecurity as priority field
- North Carolina (HB842): Creates cybersecurity apprenticeship program through Community Colleges System Office

Security Requirements and Infrastructure

Bills establishing cybersecurity standards for higher education institutions:

- Indiana (SB150*): Provides that state educational institutions may implement cybersecurity policies and assessments
- Maryland (HB1486/SB816*): Provides for cybersecurity programs operated by public or private entities
- Minnesota (HF4749/SF4874): Requires postsecondary institutions to report cybersecurity incidents
- Virginia (SB222*): Protects confidentiality of higher education institutions' cybersecurity information

Grant Programs and Funding Mechanisms

Legislation creating funding streams for postsecondary cybersecurity initiatives:

- Florida (HB5001*): Provides funding for cybersecurity projects at the University of South Florida
- Kentucky (HB139): Creates network of cyber centers across public and private universities
- Massachusetts (H51): Enables academic institutions to compete for federal grants in cybersecurity
- New York (S924): Requires higher education capital matching grants for cybersecurity infrastructure

Research and Innovation Centers

Bills establishing cybersecurity research and innovation capabilities:

- Florida (HB5001*): Funds Cyber Attack and Simulation Range for training
- Kentucky (HB319): Creates network of cyber centers for research and infrastructure
- Michigan (SB737): Creates coordinated cybersecurity defense organization for public universities
- Minnesota (HF5344/SF5416): Provides for cyber range services at Metropolitan State University

These trends reflect states' recognition of higher education's crucial role in cybersecurity through program development, workforce training, infrastructure improvement, research advancement, and innovation. The variety of approaches provides models for other states considering similar legislation to strengthen postsecondary cybersecurity education and research capabilities.

Key Trends in General Government Cybersecurity Legislation for 2024

While not specifically targeted at educational institutions, general government cybersecurity legislation often has significant implications for schools and postsecondary institutions, which typically must comply with state and local government requirements. In 2024, state legislatures introduced over 200 bills addressing general government cybersecurity, with educational institutions often included as units of government. This legislation reflects an increasingly sophisticated approach to cybersecurity governance, from creating specialized offices and task forces to establishing comprehensive incident reporting frameworks. Particularly notable is the emergence of legislation addressing persistent threats like ransomware and new challenges like artificial intelligence, alongside traditional concerns about infrastructure security and training. The intersection of these government-wide initiatives with educational institutions is evident in seven key trends emerging from 2024's legislative activity.

Creation of Task Forces, Commissions, and Offices

Bills establishing new governance structures for cybersecurity:

- Connecticut (SB2): Establishes Artificial Intelligence Advisory Council
- Mississippi (SB2698*): Establishes Cyber Security Review Board
- New Jersey (SJR105): Creates Cybersecurity Task Force
- New Mexico (SB130): Creates Artificial Intelligence Work Group for cybersecurity
- Utah (SB149*): Establishes Office of Artificial Intelligence Policy with cybersecurity responsibilities
- Wisconsin (AB43): Establishes security operations centers

Incident Reporting and Response Requirements

Legislation mandating reporting and response protocols:

- Iowa (HF2708*): Requires collaborative approach to protect against cybersecurity risks

- Massachusetts (S2571): Requires cities and towns to report cybersecurity incidents
- Minnesota (HF4749/SF4874): Mandates reporting of cybersecurity incidents
- Mississippi (SB2703): Requires ransomware incident reporting
- Washington (HB1464): Requires design of ransomware protection standards

Training and Professional Development

Bills focusing on cybersecurity awareness and training:

- Kansas (HB2077): Requires cybersecurity awareness training program
- Maryland (HB1486/SB816*): Creates training programs through Cyber Maryland Fund
- Massachusetts (S2539): Mandates online training programs for state employees
- New Jersey (A1912/S3665, A2424): Requires state employees to complete cybersecurity training
- Washington (HB1464): Mandates prevention education for state employees

Infrastructure and Security Standards

Legislation establishing cybersecurity standards and requirements:

- Alabama (HB68): Requires adoption of NIST Cybersecurity Framework
- California (AB749): Requires implementation of Zero Trust architecture
- Indiana (SB150*): Establishes technology resources and infrastructure standards
- New York (A9312/S9364): Prohibits procurement of technology posing security threats
- Washington (HB1947*): Establishes policies for efficient technology use

Funding and Grant Programs

Bills creating funding mechanisms for cybersecurity:

- Hawaii (SB1249): Appropriates funding for cybersecurity programs
- Iowa (HF2708*): Authorizes grant program for cybersecurity
- Louisiana (HB314*): Funds Cyber Assurance Program
- Maryland (HB1486/SB816*): Establishes Cyber Maryland Fund
- Wyoming (HB1*/SF1): Provides funding for cybersecurity initiatives

Ransomware-Specific Measures

Legislation specifically addressing ransomware threats:

- California (AB1812): Requires reporting of ransomware incidents
- Illinois (SB1740): Prohibits payment of ransomware demands
- Massachusetts (S35): Prohibits ransom payments
- Mississippi (SB2703): Addresses ransomware incident reporting
- Pennsylvania (SB563): Creates criminal acts relating to ransomware

Technology Procurement and Restrictions

Bills governing technology acquisition and use:

- California (SB74): Restricts social media applications on state devices
- Kansas (HB2314): Prohibits certain social media platform access
- Louisiana (HB845): Gives Joint Legislative Committee on Technology and Cybersecurity authority to review and approve procurement requests related to technology or cybersecurity

- Massachusetts (H3062): Requires preference for vendors with cybersecurity insurance for procurement of information technology goods or services
- New York (A2833): Provides that when commissioner and state agencies procure end point devices, the devices must meet the NIST Cybersecurity Framework
- Virginia (HB651): Creates Cyber Civilian Corps for response assistance
- Washington (HB1947*): Renames and expands technology solutions agency

These trends demonstrate states' comprehensive approach to cybersecurity governance, with particular attention to organizational structures, incident management, professional development, infrastructure standards, funding mechanisms, and specific threat responses. While many of these bills do not specifically target educational institutions, they often affect schools as units of state and local government.

Federal Education Sector Cybersecurity Developments

Congress

During the 118th Congress (2023-2024), a significant number of cybersecurity education and workforce development bills were introduced, reflecting not only growing concerns about the cybersecurity talent pipeline but also a strong focus on increasing accessibility and diversity in the field.[5] Key trends include expanding educational pathways through apprenticeships and internships, reducing barriers to entry, supporting institutions from K-12 through higher education, emphasizing public-private partnerships, and promoting cybersecurity literacy among the public. The legislation demonstrates a comprehensive approach to addressing the cybersecurity workforce challenge, with particular attention to creating opportunities for underserved communities, standardizing training frameworks, and developing alternative paths to cybersecurity careers.

Key Education-Related Cybersecurity Legislation

2024 Bills:

Workforce Development and Training

- Cyber PIVOTT Act (H.R. 9770): Establishes partnerships between CISA and community colleges/technical schools
- DHS Cybersecurity Internship Program Act (H.R. 9689/S. 5321): Creates paid internships aligned with education
- Cyber Ready Workforce Act (H.R. 9270/S. 4813): Supports apprenticeship programs
- Smart Cities and Communities Act (H.R. 9892): Creates TechHire Workforce Training program with industry-recognized certifications

[5] Please see Appendix C for the five-year trend of federal cybersecurity bills.

- NSF AI Education Act (S. 4394): Updates NICE Cybersecurity Workforce Framework

Diversity and Inclusion Initiatives

- Jobs Training for Young African-Americans Act (HR9739): Focuses on apprenticeships for younger students
- Cybersecurity Clinics Grant Program Act (H.R. 8770): Funds clinics at community colleges, HBCUs, HSIs, and minority-serving institutions
- Diverse Cybersecurity Workforce Act (H.R. 8469): Promotes cybersecurity to disadvantaged communities

Public Awareness

- S.Res. 755: Designates June 2024 as National Cybersecurity Education Month

2023 Bills:

K-12 and Higher Education

- Enhancing K-12 Cybersecurity Act (HR2845/S1191): Establishes School Cybersecurity Improvement Program
- Cybersecurity Skills Integration Act (HR6124): Creates grants for cybersecurity education programs
- Energy Cybersecurity University Leadership Act (HR302): Supports graduate students in cybersecurity
- National Apprenticeship Act of 2023 (HR2851/S2122)

Workforce Development and Access

- Federal Cybersecurity Workforce Expansion Act (S2256): Creates apprenticeships and veteran training programs
- Modernizing the Acquisition of Cybersecurity Experts Act (HR4502): Limits educational requirements for certain federal cybersecurity positions

Public Education and Awareness

- American Cybersecurity Literacy Act (HR1360/S2201): Establishes a cybersecurity literacy campaign
- National Cybersecurity Awareness Act (S1835): Requires CISA to develop cybersecurity awareness campaign

The federal legislation showcases a multi-faceted approach to building the cybersecurity workforce, combining traditional educational pathways with alternative training options while emphasizing inclusion and public awareness.

Executive Branch

The federal executive branch took significant steps in 2024 to address growing cybersecurity threats to educational institutions. Three major agencies - the Federal Communications Commission, the U.S. Department of Education, and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency - advanced initiatives that will shape how schools protect their digital infrastructure and respond to cyber incidents. These efforts reflect increasing recognition of schools as critical infrastructure and the need for coordinated federal support to help educational institutions build cyber resilience.

Federal Communications Commission

One of the most important K-12 cybersecurity developments at the federal level was the Federal Communications Commission's approval of a new Schools and Libraries Cybersecurity Pilot Program. The program is a three-year initiative providing up to $200 million to assist eligible schools, libraries, and consortia in acquiring cybersecurity services and equipment. The FCC received, by the program's November 1, 2024 deadline, 2,734 applications totaling $3.7 billion in requests from schools, libraries, and consortia of schools and libraries. The program aims to protect broadband networks and data, while assessing the viability of long-term funding for cybersecurity through Universal Service funding. Inspired by the FCC's Connected Care Pilot, this program highlights the critical need for secure digital infrastructure in education and library systems. The pilot represents a significant step toward enhancing cybersecurity resilience across the nation's schools and libraries, safeguarding vital educational and informational resources.

U.S. Department of Education

The U.S. Department of Education also worked in 2024 to address the threats faced by K-12 schools. In its federal coordination role, the Department worked with other stakeholders across all levels of government and Tribal communities to bolster cybersecurity resilience in schools. Its efforts include providing training tools and resources through emergency management and student privacy technical assistance centers, sharing cybersecurity best practices, and establishing a K-12 council to coordinate cross-government mitigation strategies. Collaborating with federal agencies like the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the National Security Council, the Department aimed to raise awareness and develop resources to assist school districts, especially those with limited capacity to counter threats.

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) established new cybersecurity incident reporting requirements that will affect educational institutions. The Cybersecurity and Infrastructure Security Agency published a notice of proposed rulemaking in April 2024 to implement CIRCIA. Covered entities, including certain larger school systems, will be required to report cyber incidents within 72 hours and ransomware payments within 24 hours.

Once CISA reviews public comments and issues the Final Rule, educational institutions will need to prepare for implementation by establishing processes to identify, assess, and report covered cyber incidents and ransom payments within the required timeframes. The regulations aim to help CISA rapidly deploy resources to victims, analyze cross-sector trends, and share threat information to prevent future attacks.

The Department of Homeland Security also launched a Federal School Safety Clearinghouse External Advisory Board, a panel of school safety experts and education leaders tasked with enhancing K-12 school security. Established under the Bipartisan Safer Communities Act, the Board advises the Secretary of Homeland Security through CISA's Director on implementing evidence-based practices and recommending additional strategies for publication on SchoolSafety.gov, a federal resource hub for school safety.

Conclusion

As the education sector continues to rely heavily on technology, the need for robust cybersecurity measures is paramount. The legislative efforts and trends of 2024 demonstrate that many policymakers recognizing the unique vulnerabilities of schools and higher education institutions, are taking proactive steps to address them through comprehensive policies. By investing in professional development, establishing grant programs, creating robust incident response frameworks, integrating cybersecurity into curricula, and fostering public-private partnerships, state and local leaders can fortify the digital infrastructure that underpins modern education.

However, these steps should only be the beginning. Cybersecurity threats will continue to evolve, requiring a dynamic and adaptive approach. Collaboration among policymakers, educators, technology experts, and private sector stakeholders is critical to staying ahead of these challenges. By drawing on the successful initiatives and recommendations outlined in this report, education leaders can set a new standard for cybersecurity in education—one that protects students, educators, and institutions while enabling innovation and digital learning.

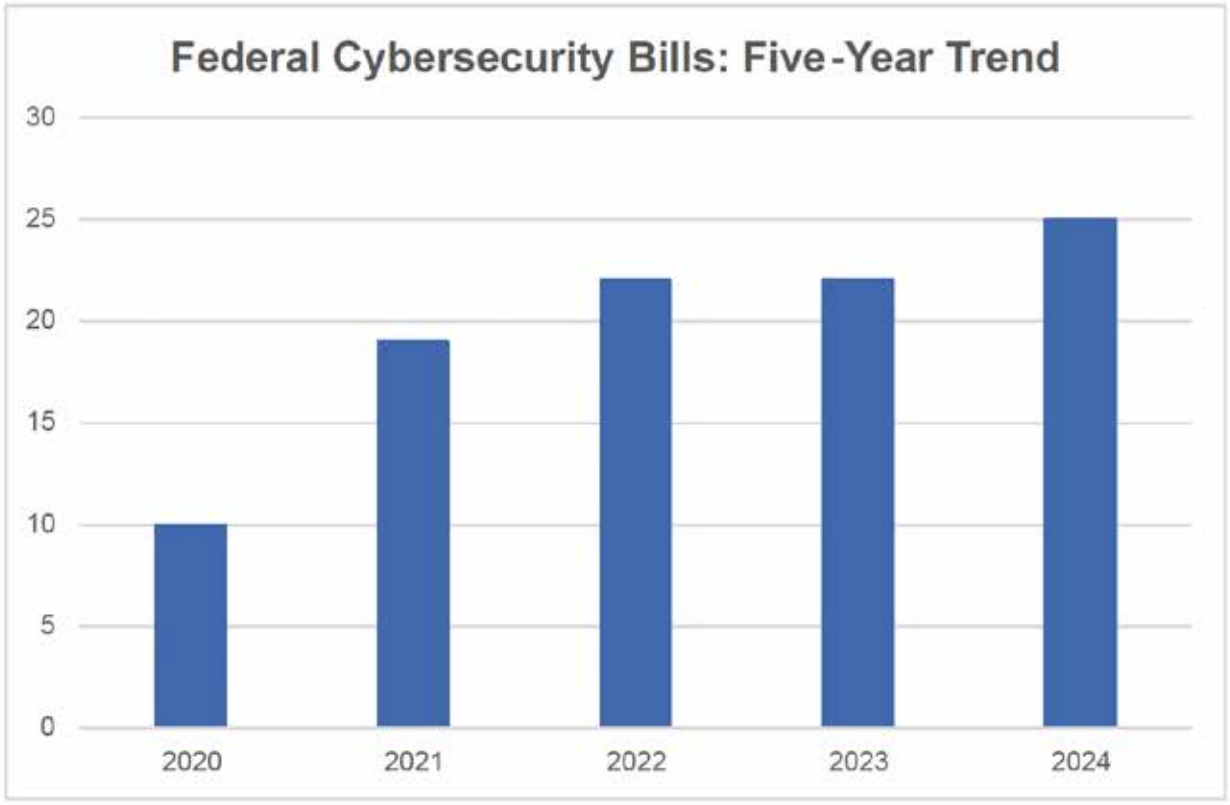
Appendix A: Chart of K-12, Postsecondary, and General Government Policy Trends

K-12 Education Cybersecurity Policy Trends
1. **Cybersecurity Training and Professional Development**
• AL, GA, IN
2. **Curriculum and Student Instruction**
• AZ, FL, IL, NJ
3. **Infrastructure and Security Requirements**
• IN, NE, SC, VA
4. **Funding and Grant Programs**
• IA, MN, NY, WV
5. **Incident Response and Reporting**
• FL, IL, MN, NJ
Postsecondary Education Cybersecurity Policy Trends
1. **Program Development and Facilities**
• HI, IL, MN, RI
2. **Workforce Development and Training**
• CA, NJ, NM, WI
3. **Security Requirements and Infrastructure**
• IN, KY, MN, VA
4. **Grant Programs and Funding Mechanisms**
• FL, KY, MA, NY
5. **Research and Innovation Centers**
• FL, KY, MI, MN
General Government Cybersecurity Trends
1. **Creation of Task Forces, Commissions, and Offices**
• CT, MS, NJ, NM, UT, WI
2. **Incident Reporting and Response Requirements**
• IA, MA, MN, MS, WA
3. **Training and Professional Development**
• KS, MD, MA, NJ, WA
4. **Infrastructure and Security Standards**
• AL, CA, IN, NY, WA
5. **Funding and Grant Programs**
• HI, IA, LA, MD, WY
6. **Ransomware-Specific Measures**
• CA, IL, MA, MS, PA
7. **Technology Procurement and Restrictions**
• CA, KS, LA, MA, NY, VA, WA

Appendix B: Chart of States with Cybersecurity Workforce Development Bills

Comprehensive Workforce Development Programs
• Florida (HB5001*): Created the EASE Plus incentive program to support students in high-demand programs including cybersecurity
• Kentucky (HB139): Created Kentucky Cybersecurity Program to: Develop nonacademic credentialing programs; Provide reskilling and upskilling opportunities; Facilitate cooperation between universities and businesses
• New Mexico (HB303*): Created Workforce Training Economic Support Pilot Program; Identified cybersecurity as priority industry; Provided stipends up to $1,000/month for participants; Created pathways through state institutions
Higher Education Focused Initiatives
• Hawaii (SB1249): Funded cybersecurity and data science programs at the University of Hawaii Maui College
• Minnesota (HF2071/SF1547, HF2880/SF2892, SF676): Funding cybersecurity program space at Metropolitan State University
• Minnesota (HF5344/SF5416): Funded cyber range services for enrolled students and government agencies
• Rhode Island (H7224, H7225*): Supported establishment of Institute for Cybersecurity and Emerging Technologies
Industry-Education Partnership Programs
• Maryland (HB1486/SB816*): Enhanced Cyber Maryland Fund to: Develop cybersecurity programs based on industry needs; Create talent pipeline management; Coordinate between employers and educational institutions
• New Jersey (A2999): Required: Development of cybersecurity model curricula; Creation of loan redemption programs for cybersecurity occupations; Alignment of education with career pathways
Community College and Technical Training
• California (AB101, AB221): Provided funding for community college cybersecurity staff and programs
• North Carolina (HB842): Created cybersecurity apprenticeship program through community colleges

Appendix C: Federal Education Sector Cybersecurity Activity Since 2020



Appendix D: 2024 State Cybersecurity Legislation

Alabama

- HB68: Requires Secretary of Office of Information Technology to adopt rules governing cybersecurity.
- HB439*: Creates K-12 Technology and Cybersecurity Leadership Act, renaming technology coordinator positions.

Alaska

- HB306: Adds sections relating to state agencies' use of artificial intelligence and cybersecurity.
- SB177: Adds sections relating to state agencies' use of artificial intelligence and cybersecurity.

Arizona

- HB2699: Requires State Board to include minimum cybersecurity standards in course instruction starting 2024-2025.

California

- AB101: Makes appropriations for 2023-24 fiscal year including cybersecurity funding.
- AB221: Provides funding for community college cybersecurity implementation.
- AB227: Prohibits social media platform installation on state devices, except for cybersecurity research.
- AB749: Requires state agencies to implement specified data and hardware security actions.
- AB1667: Establishes California Cybersecurity Awareness and Education Council.
- AB1812: Provides 2024 budget funding for community college cybersecurity programs.
- AB2715*: Amends law regarding open meetings of legislative bodies and cybersecurity measures.
- AB2777: Addresses security status reporting requirements for state agencies.
- SB72: Appropriates funds for community college cybersecurity implementation.
- SB74: Amends law relating to California Cybersecurity Integration Center.
- SB102: Amends Budget Act 2023 provisions relating to cybersecurity reporting.
- SB265: Requires Cal OES to prepare strategic multiyear outreach plan for cybersecurity.
- SB917: Provides 2024 budget funding for community college cybersecurity programs.
- SB1070: Authorizes State Personnel Board to prescribe cybersecurity rules.

Connecticut

- SB2: Requires AI system developers to meet cybersecurity standards.
- SB227: Requires municipalities to register .gov domains with DHS CISA by 2026 for cybersecurity purposes.

Florida

- HB473: Provides limited liability for entities that satisfies certain cybersecurity compliance standards.
- HB483: Establishes AI in Education Task Force including cybersecurity components.
- HB1459: Requires report on artificial intelligence and cybersecurity impacts.
- HB1555*: Amends Florida Center for Cybersecurity provisions.
- HB5001*: Provides funding for EASE Plus program including cybersecurity education.
- SB658: Provides limited liability for entities that satisfies certain cybersecurity compliance standards.
- SB1344: Requires K-12 public schools to provide computer science instruction including cybersecurity.
- SB1626: Requires cybersecurity protocols for entities treating minors for mental illness.
- SB1662: Amends laws relating to cybersecurity incident reporting timelines.
- SB1680*: Creates Government Technology Modernization Council for cybersecurity monitoring.
- SB2500: Allocates funds for 2024-2025 cybersecurity projects.

Georgia

- HR68: Encourages Department of Education to fund cybersecurity initiatives.
- HB338: Requires department guidance for school cybersecurity.
- HR1083: Creates House Study Committee on STEM Education including cybersecurity.
- SB97: Creates Georgia Cyber Command division for strategic planning.

Hawaii

- HB460: Prohibits state employees from accessing certain websites for cybersecurity.
- HB1038: Provides targeted violence prevention through cybersecurity training.
- SB1249: Appropriates funding for University of Hawaii cybersecurity programs.
- SB1334: Establishes Hawaii state fusion center for cybersecurity coordination.
- SB1336: Creates targeted violence prevention program including cybersecurity training.
- SB1478: Establishes offensive cybersecurity program within Office of Enterprise Technology.

Idaho

- HB663: Amends law relating to school board internet use policies and cybersecurity.

Illinois

- HB1381: Creates Right to Know Act for commercial website operators' cybersecurity.
- HB2353: Requires school districts to report cyber attacks to the state board of education.
- HB2538: Funds Illinois Institute of Technology cybersecurity initiatives.
- HB2703: Provides Department of Innovation and Technology cybersecurity funding.
- HB4081: Establishes Cybersecurity Compliance Act for affirmative defense.
- HB4625: Mandates age-appropriate cybersecurity instruction for students.
- HB5365: Requires Government Finance Research Center cybersecurity report.

- HB5686: Appropriates funds for Department of Innovation and Technology cybersecurity.
- SB1740: Creates Ransomware Attack Act prohibiting government payments.
- SB2497: Provides cybersecurity funding for Department of Innovation and Technology.
- SB3240: Creates Illinois Cyber Auxiliary program.
- SB3844: Allocates funds for Department of Innovation and Technology cybersecurity.

Indiana

- SB150*: Creates Artificial Intelligence Task Force to assess state agency cybersecurity.

Iowa

- HF554: Prohibits ransomware payment using taxpayer funds.
- HF632: Expands school infrastructure definition to include cybersecurity.
- HF698: Establishes cybersecurity simulation training center at Iowa State University.
- HF2032: Allows district management levy use for cybersecurity.
- HF2622: Adds cybersecurity duties to Department of Management director.
- HF2708*: Requires state and local government cybersecurity collaboration.
- HSB15: Creates cybersecurity unit within chief information officer's office.
- HSB16: Modifies essential county purpose definition to include cybersecurity purposes for funding.
- SF195: Modifies essential county purpose definition to include cybersecurity purposes for funding.
- SF203: Amends Computer Spyware Protection Act for ransomware.
- SF402: Creates cybersecurity simulation center at Iowa State University.
- SF2375: Adds cybersecurity responsibilities to Department of Management.
- SF2409: Authorizes adoption of cybersecurity policies and monitoring.
- SF2433*: Allocates funds for local government cybersecurity services.

Kansas

- HB2077: Requires cybersecurity awareness training program.
- HB2314: Prohibits state employees from accessing certain social media on state devices.
- HB2842: Places cybersecurity under chief information technology officer.

Kentucky

- HB139: Creates Kentucky Cybersecurity Program for education and infrastructure.
- HB319: Creates Kentucky Cybersecurity Program for education and infrastructure.

Louisiana

- HB1*: Funds Louisiana Cybersecurity Talent Initiative.
- HB314*: Provides funding for Cyber Assurance Program.
- HB700*: Allows GUMBO 2.0 funds for broadband and cybersecurity challenges.
- HB845*: Expands Joint Legislative Committee on Technology and Cybersecurity authority.

Maine

- LD877*: Prohibits certain school district and other government technology contracts for cybersecurity risks.

Maryland

- HB617: Prohibits certain applications on state devices for cybersecurity.
- HB1486: Administers Cyber Maryland Fund for workforce development.
- SB692: Establishes workgroup to study data security.
- SB757: Restricts certain applications on state devices.
- SB816*: Administers Cyber Maryland Fund for workforce development.
- SB981: Creates Local Cybersecurity Support Fund.

Massachusetts

- H51: Supports technology innovation including cybersecurity.
- H60: Establishes Massachusetts Information Privacy and Security Act.
- H66: Amends civil defense definition to include cybersecurity attacks.
- H82: Restricts social media applications on state devices.
- H83: Establishes data privacy protection requirements.
- H532: Creates student data privacy requirements.
- H2821: Creates digital advertising revenue commission including cybersecurity.
- H3062: State agency procurement must preference vendors with cyber insurance.
- H4204*: Allows contracting for cybersecurity services.
- H4601: Funds IT audit unit and cybersecurity operations.
- H4632: Creates data privacy protection requirements.
- H4648: Funds IT and cybersecurity improvements.
- H4725: Studies digital advertising revenue for cybersecurity.
- H4800*: Modernize state IT and provide cybersecurity funding.
- H4889*: Funds government IT and cybersecurity improvements.
- S25: Establishes data privacy protection standards.
- S26: Modernizes state agency IT systems and cybersecurity.
- S32: Establishes Cyber Incident Response Team.
- S35: Prohibits ransomware payments by state and local agencies.
- S36: Establishes cybersecurity control and review commission.
- S37: Prohibits certain applications on state devices.
- S227: Creates Information Privacy and Security Act.
- S280: Establishes student and educator data privacy standards.
- S2539: Creates comprehensive cybersecurity training program.
- S2571: Requires reporting of cybersecurity incidents.
- S2770: Creates data privacy protection requirements.
- S2827: Mandates cybersecurity incident reporting.

Michigan

- HB4286: Allows use of school infrastructure funds for cybersecurity.
- HB5065: Prohibits certain applications on government devices.
- HB5459: Funds local government cybersecurity programs.
- HB5516: Funds state information technology modernization.
- SB189: Provides homeland security and cybersecurity funding.
- SB380: Amends state aid formulas to permit counting hours and days when instruction does not occur because of ransomware attack.
- SB737: Establish coordinated cybersecurity defense organization and center.

Minnesota

- HF1360: Allows safe schools revenue to be used for cybersecurity.
- HF1409: Funds public radio stations cybersecurity technology.
- HF1693: Amends legislative cybersecurity commission procedures.
- HF1710: Updates cybersecurity commission procedures.
- HF1826: Modifies cybersecurity commission operations.
- HF1960: Enables governor to declare peacetime emergency for cyber-attacks.
- HF2071: Supports Metropolitan State University cybersecurity program.
- HF2497: Provides school security and cybersecurity grants.
- HF2880: Funds Metropolitan State University cybersecurity facilities.
- HF2940: Funds IT and cybersecurity grant program.
- HF4749: Requires cybersecurity incident reporting.
- HF5324: Establishes cybersecurity grant account for cities and counties.
- HF5344: Provides cyber range services funding for Metropolitan State University.
- S8305: Creates Secure Our Data Act.
- SF676: Supports Metropolitan State cybersecurity program.
- SF1424: Modifies cybersecurity records requirements for legislative commission.
- SF1426: Supports cybersecurity improvements for state and local government.
- SF1514: Supports public radio station cybersecurity technology.
- SF1547: Funds Metropolitan State University cybersecurity facilities.
- SF1703: Modifies cybersecurity commission meetings procedures.
- SF1746: Updates cybersecurity commission procedures.
- SF2001: Allows governor to declare peacetime emergency for cyber-attacks.
- SF2684: Funds school security and cybersecurity improvements.
- SF2892: Supports Metropolitan State University cybersecurity program.
- SF2979: Funds IT and cybersecurity enhancement program.
- SF4874: Mandates cybersecurity incident reporting.
- SF5416: Provides cyber range services funding for Metropolitan State Univesity.

Mississippi

- HB1575: Limits liability for agencies that meet cybersecurity standards.
- SB2698*: Creates Cyber Security Review Board to promote collaboration.
- SB2703: Requires ransomware incident reporting.
- SB2777: Limits liability for agencies that meet cybersecurity standards.
- SB2846: Funds Mississippi Cybersecurity Center.

Missouri

- HB1513: Creates Media Literacy pilot program including cybersecurity.
- SB1311: Creates Media Literacy pilot program including cybersecurity.

Nebraska

- LB638: Creates K-12 Cybersecurity and Data Protection Act.
- LB650: Protects cybersecurity records from public disclosure.
- LB651: Appropriates funds for cybersecurity activities.
- LB1302: Adopts Cybersecurity Preparedness Act.

New Jersey

- A817: Requires higher education institution cybersecurity plans.
- 1204: Mandates cybersecurity infrastructure study.
- A1410: Requires postsecondary institution cybersecurity infrastructure review.
- A1912: Requires cybersecurity training for state employees.
- A2424: Mandates government employee cybersecurity awareness training.
- A2999: Requires cybersecurity instruction in schools.
- A3897: Requires cybersecurity incident reporting.
- A3949: Requires cybersecurity incident procedures.
- A4768: Creates Cyber Security Reserve Corps.
- A5036: Establishes Office of Cybersecurity Infrastructure.
- S205: Develops advanced cyberinfrastructure plan.
- S1053: Requires study of postsecondary institution cybersecurity infrastructure.
- S2271: Mandates cybersecurity infrastructure assessment.
- S3220: Establishes cybersecurity employment grant program.
- S3222: Mandates cybersecurity education requirements.
- S3313: Mandates cybersecurity incident procedures.
- S3569: Creates New Jersey Cybersecurity Grant Program.
- S3665: Requires state employee cybersecurity training.
- S3835: Creates Office of Cybersecurity Infrastructure.
- SJR105: Establishes Cybersecurity Task Force.

New Mexico

- HB72: Establishes cybersecurity fund for government response and recovery.
- HB303*: Creates workforce training program including cybersecurity.
- SB129: Amends Cybersecurity Act requirements.
- SB130: Creates Artificial Intelligence Work Group.
- SB211: Establishes Science Education Promotion Fund.

New York

- A1646: Creates school cybercrime prevention program.
- A2529: Studies EU data protection and state cybersecurity.
- A2833: Requires NIST standards for endpoint devices.
- A3094: Creates Critical Infrastructure Standards and Procedures Act.
- A4640: Creates cybersecurity enhancement fund.
- A5736: Establishes ransomware protection standards.
- A7331: Requires multifactor authentication implementation, including for schools.
- A7504: Develops digital equity plan including cybersecurity.
- A8195: Requires AI system cybersecurity compliance.
- A9312: Prohibits procurement from cybersecurity risks.
- A9642: Establishes data sharing agreement requirements.
- A10455: Creates community college workforce program including for high demand sectors such as cybersecurity.
- S924: Funds higher education cybersecurity grants.
- S1693: Creates digital equity plan with cybersecurity.
- S2563: Establishes school cybercrime prevention services.
- S2564: Requires annual cybercrime notifications.
- S4512: Creates local government cybersecurity fund.
- S5007: Develops ransomware protection standards.
- S5615: Mandates NIST standards compliance.
- S5646: Creates Critical Infrastructure Standards and Procedures Act.
- S6474: Mandates cybersecurity authentication standards.
- S8305: Creates Secure Our Data Act to require rules to design and develop standards for malware and ransomware protection and requires annual workforce training
- S9124: Creates secure data sharing requirements.
- S9364: Restricts procurement from security risks.

North Carolina

- HB196: Requires annual cybersecurity reporting.
- HB263: Provides comprehensive cybersecurity funding.
- HB671: Establishes cybersecurity fund for state and local government.
- HB842: Creates community college cybersecurity apprenticeship program.

- HB1036: Creates AI Task Force with cybersecurity components.
- SB83: Restricts high-risk platform access.
- SB194: Establishes student loan servicer requirements.
- SB196: Creates student borrower protection standards.

Ohio

- HB2*: Funds Ohio Cyber Range improvements and Tolles Cybersecurity Lab renovation
- HB74: Establishes cybersecurity advisory board.
- HB629: Funds Ohio Cyber Range improvements and Tolles Cybersecurity Lab
- SB292: Funds Ohio Cyber Range improvements and Tolles Cybersecurity Lab

Oklahoma

- HB2555: Creates Critical Industries Scholarship Program.
- SB107: Restricts critical infrastructure contracts.
- SB320: Requires cybersecurity incident tracking.

Oregon

- HB4152: Requires cybersecurity study by Office of Enterprise Information Services.

Pennsylvania

- HB883: Establishes information technology reform, including security governance.
- HB1139: Establishes Cybersecurity Coordination Board.
- HB1552: Provides cybersecurity funding for the Department of Community and Economic Development.
- HR170: Studies artificial intelligence impacts including on cybersecurity.
- SB284: Creates Office of Information Technology with cybersecurity responsibilities.
- SB301: Appropriates cybersecurity funding.
- SB480: Provides information technology funding.
- SB563: Prohibits ransomware attacks on Commonwealth agencies.
- SB1247: Creates Local Cybersecurity Improvement Act.
- SR143: Conduct a study to examine AI including cybersecurity implications.

Rhode Island

- H7224: Support the RI College Institute for Cybersecurity & Emerging Technologies.
- H7225*: Support the RI College Institute for Cybersecurity & Emerging Technologies.

South Carolina

- H3448: Prohibits access to cybersecurity threat websites on state devices.
- H4596: Prohibits access to cybersecurity threat websites on state devices.
- H4702: Enacts Computer Science Education Initiative including cybersecurity pathways.

South Dakota

- SB187*: Creates local government cybersecurity services initiative.

Tennessee

- HB1733*: Prohibits state contracts with system hackers.
- SB1825: Prohibits state contracts with system hackers.

Utah

- SB98*: Amends online data security and privacy requirements, including requiring breach notification.
- SB149*: Creates Artificial Intelligence Policy Act with cybersecurity criteria.

Vermont

- H136: Prohibits certain social media platforms on state networks.

Virginia

- HB651: Creates Cyber Civilian Corps for incident response.
- HB1095: Protects cybersecurity information from public disclosure.
- SB222*: Protects cybersecurity information from public disclosure.

Washington

- HB1140: Funds Office of Cybersecurity and cloud computing.
- HB1464: Requires enterprise malware protection standards.
- HB1947*: Renames and updates the state's technology services agency.
- HB2104: Provides supplemental funding for state cybersecurity office.
- SB5619: Establishes cybersecurity advisory committee.
- SB5950: Provides Office of Cybersecurity funding.

West Virginia

- HB4986*: Provides grants for schools, career centers, and more for computer operations and cybersecurity courses for adults.

Wisconsin

- AB43: Establishes cybersecurity operations centers, including for schools.
- AB263: Prohibits state and local agencies form using applications that pose cybersecurity threats.
- SB250: Bans applications deemed cybersecurity risks.

Wyoming

- HB1*: Funds Enterprise Technology Services cybersecurity initiatives.
- SF1: Funds Enterprise Technology Services cybersecurity initiatives.