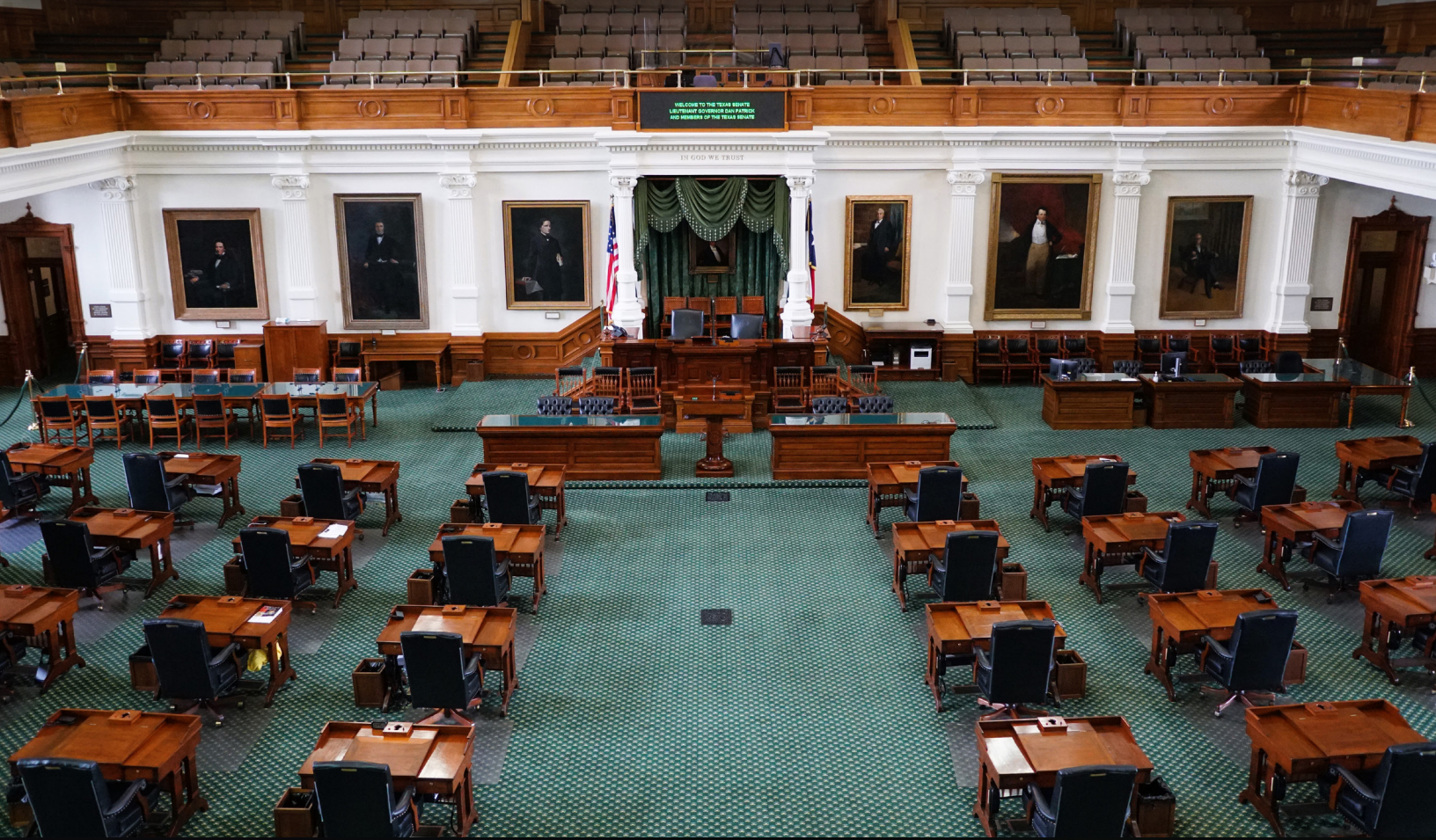


U C B E R K E L E Y
C E N T E R F O R L O N G - T E R M C Y B E R S E C U R I T Y



CLTC WHITE PAPER SERIES

Tracking Cybersecurity Policy Developments Across State Legislatures

2025 ENACTED LEGISLATION

SHANNON PIERSON and SREE VARSHA BHANOOR

CLTC WHITE PAPER SERIES

Tracking Cybersecurity Policy Developments Across State Legislatures

2025 ENACTED LEGISLATION

SHANNON PIERSON and SREE VARSHA BHANOOR

February 2026



Contents

EXECUTIVE SUMMARY	1
INTRODUCTION	3
METHODOLOGY	6
RESULTS	7
Summary Statistics	7
Emerging Themes in 2025 State Cybersecurity Legislation	8
Sectoral Priorities in 2025 State Cybersecurity Legislation	16
TOP STATE CHAMPIONS	23
Case Studies from Key State Legislation: Maryland and Texas	23
Case Study 1: Maryland Protects Local Water and Wastewater Systems	23
Case Study 2: Texas Electric Utilities and Cooperatives	25
ANALYSIS AND RECOMMENDATIONS FOR 2026	26
CONCLUSION	29
APPENDICES	30
Appendix I — Methodology	30
Appendix II — Cybersecurity Policy Action Types in 2025 State Legislation, Ranked by Frequency	32
Appendix III — Definitions of Intended Beneficiary Coding Categories	33
Appendix IV — Description of Cybersecurity Policy Action Coding Categories	34
ABOUT THE AUTHORS	37

Executive Summary

Amid shifting headwinds in U.S. federal leadership on cyber defense and cyber capacity building, states are increasingly taking up the mantle of cybersecurity leadership. State legislatures have become the primary engines of cybersecurity policymaking in the U.S. In 2025, lawmakers across 37 states passed 99 cybersecurity-related bills, establishing 393 new cybersecurity statutory requirements.

This report presents a comprehensive review of every cybersecurity-related bill enacted in all 50 states during the 2025 legislative sessions. This analysis was conducted by researchers with the Center for Long-Term Cybersecurity (CLTC) Public Interest Cybersecurity Program, based at the University of California, Berkeley. It identifies nationwide patterns in the policy issues states addressed, the regulatory approaches they adopted, and the entities and sectors they chose to regulate. By analyzing all cybersecurity-related legislation enacted in 2025, this report provides lawmakers, practitioners, and researchers with a reliable snapshot of the current cybersecurity policy landscape in the U.S.

The analysis examines trends in (1) the types of cybersecurity rules being enacted into law and (2) the critical infrastructure sectors and entities subject to new requirements. Together, these patterns reveal emerging regulatory models, sectoral priorities, and practical lessons for other states. These insights informed recommendations that are presented in the conclusion for lawmakers considering cybersecurity legislation in 2026. The report also includes in-depth analysis of select states and state lawmakers driving cybersecurity policymaking.

The research identified 10 trends to describe the types of cybersecurity laws passed by states in 2025 and to characterize the entities and sectors being regulated. The results show that state legislatures:

- Built out leadership and governance structures, particularly within state cybersecurity offices and agencies;
- Expanded requirements for public and private organizations to implement baseline cybersecurity controls;
- Increased obligations for organizations to routinely report to oversight bodies on cybersecurity programs, projects, compliance, risks, and spending;
- Prioritized stronger cybersecurity incident preparedness and response across critical infrastructure sectors;

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

- Mandated the representation of cybersecurity experts within state decision-making and leadership; and
- Passed cybersecurity safe harbor laws to incentivize cybersecurity investment.

The analysis showed that state lawmakers passed legislation to address the needs of:

- State government systems, specifically state agencies, over all other entities;
- Education entities, paying special attention to K-12 schools;
- Cyber insurance policyholders; and
- High-risk, resource-constrained critical infrastructure sectors, such as water and wastewater systems and election systems.

Based upon CLTC's review of 2025's new cybersecurity laws, CLTC researchers recommend that state lawmakers:

1. Continue working on a bipartisan basis to pass cybersecurity bills, particularly as cybersecurity is an issue with relatively high levels of consensus across party lines;
2. Appropriate funding to accompany new cybersecurity mandates to ensure their successful implementation;
3. Be more prescriptive about required cybersecurity controls in legislation, rather than relying on undefined terms like "reasonable security measures";
4. Explore ways to support the monitoring and detection of cyber incidents; and
5. Require follow-up actions to reporting to ensure it translates to action.

In parallel to this report, CLTC has published a publicly accessible, searchable database of every cybersecurity-related bill enacted in 2025 across all 50 states. This database is meant to serve as a tool for researchers, practitioners, and lawmakers to quickly understand the legislative landscape in any given state, identify which local lawmakers are actively passing cybersecurity policy, and contact their offices if needed.

Introduction

States are often described as the “laboratories of democracy,” as they can serve as testbeds for policy experimentation and innovation at a pace the U.S. Congress struggles to match. This dynamic is especially pronounced in cybersecurity policymaking. By volume, most cybersecurity policymaking in the U.S. now occurs at the state level. Legislatures propose hundreds of cybersecurity-related bills every year, and dozens are enacted, creating a fragmented patchwork of state cybersecurity laws governing cyber defense across the country.

At the federal level, Congress continues to hold hearings and introduce cybersecurity legislation, but relatively few proposals become law. The U.S. still lacks a comprehensive national privacy law,¹ and efforts to pass healthcare cyber legislation to address ransomware attacks on hospitals have stalled for years.² Gridlock has also impeded renewal of established programs with demonstrated value, including the Cybersecurity Information Sharing Act of 2015 (CISA 2015), the State and Local Cybersecurity Grant Program (SLCGP), and the Tribal Cybersecurity Grant Program (TCGP), all of which expired on September 30, 2025. Only after great difficulty did Congress manage to temporarily reauthorize CISA 2015 and SLCGP through January 30, 2026; both authorities have since expired.^{3,4} Despite their broad support and contributions to improving national cyber defense, the long-term future of these programs remains uncertain.^{5,6,7}

At the same time, federal leadership on national cyber defense and capacity building is being redefined. The second Trump Administration is scaling back the federal government’s role and placing greater responsibility on state and local governments. This new direction was

1 Fazlioglu, Müge. (2025, October 25). [US Federal Privacy Legislation Tracker](#). International Association of Privacy Professionals.

2 Starks, Tim. (2025, December 5). [Bipartisan health care cybersecurity legislation returns to address a cornucopia of issues](#). CyberScoop.

3 Doubleday, Justin. (2025, November 13). [Congress extends CISA 2015, but path to long-term reauthorization remains murky](#). Federal News Network.

4 McCarter, Mickey. (2025, November 24). [Congress Revives State and Local Cyber Grants, But Funding Remains Unclear](#). StateTech Magazine.

5 Dowdall, S. (2025, June 17). [Support Reauthorization of the State and Local Cybersecurity Grant Program](#). National Association of Counties.

6 Alliance for Digital Innovation, Better Identity Coalition, Cybersecurity Coalition Information Technology Industry Council (ITI), & TechNet. (2025, September 2). [Re: Support for Reauthorization of the State and Local Cybersecurity Grant Program](#). Alliance for Digital Innovation.

7 The Protecting America’s Cyber Networks Coalition. (2025, September 24). [Letter to Congress on the Cybersecurity Information Sharing Act of 2015](#). U.S. Chamber of Commerce.

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

formalized in March 2025 through Executive Order (EO) 14239, *Achieving Efficiency Through State and Local Preparedness*, which asserts that cybersecurity “preparedness is most effectively owned and managed at the state [and] local” levels, with the federal role becoming more limited.⁸ Together, federal legislative stagnation and executive branch decentralization are accelerating the transfer of responsibility for cyber defense to states.

State legislatures have responded by filling regulatory gaps, particularly in data breach notifications, data protection, and cybersecurity requirements for state-managed critical infrastructure such as electric utilities, water systems, school districts, and healthcare. Cybersecurity also remains an area of bipartisan consensus in state legislatures, with many bills receiving bipartisan or unanimous support. While funding appropriations remain the largest barrier to passage,⁹ state legislatures have continued to pilot novel approaches and regulations to strengthen regional cyber defense and develop the cyber workforce, including state civilian cyber corps,¹⁰ student-led regional security operations centers (RSOCs), and state cyber commands.¹¹

As responsibility for cyber defense shifts toward states — and federal support and direction wane — state legislatures play an increasingly central role by controlling appropriations and establishing mandates that shape statewide cybersecurity strategy and capacity. However, despite the growing importance of states, there is limited analysis available related to what legislation they are actually enacting or of trends in laws passed across the country.

Several state-level cybersecurity law repositories and annual or mid-year analysis reports already exist. Since 2021, the National Conference of State Legislatures (NCSL) has annually published a list of all cybersecurity bills introduced in state legislatures and provided a high-level trend analysis of both proposed and enacted legislation.¹² The Consortium for School Networking published reports identifying broad trends in state and federal cybersecurity

8 [Exec. Order No.14239](#), 90, 3 C.F.R. 13267 (2025).

9 Pierson, Shannon. (2025, July). [Four Key Learnings from the 2025 Cyber Civil Defense Summit](#). UC Berkeley Center for Long-Term Cybersecurity.

10 Razeed, Michael. (2024, September 26). [Civilian Cyber Corps: A Model Law for States](#). New America.

11 Powazek, S. and Menna, G. (2025, June). [The Roadmap to Community Cyber Defense: A Path Forward from the Cyber Resilience Corps](#). UC Berkeley Center for Long-Term Cybersecurity.

12 National Conference of State Legislatures. (2025, October 10). [Cybersecurity 2025 Legislation](#).

TRACKING CYBERSECURITY POLICY DEVELOPMENTS ACROSS STATE LEGISLATURES

legislation for all of 2024 and the first half of 2025, with a focus on legislation related to the education sector.^{13,14}

However, CLTC researchers found no existing analysis focusing exclusively on enacted legislation that captures the substance of each new cybersecurity-related rule established, or that derives trends across critical infrastructure sectors in a given legislative session. Nor did CLTC find any publicly available dataset that categorizes and tags enacted state cybersecurity legislation by beneficiary sector, solution type, or sponsor.

In response to this gap, CLTC launched this project: a review of cybersecurity-related bills enacted in all 50 states during the 2025 legislative sessions, with the goal of examining nationwide patterns in the policy issues addressed and the types of interventions enacted. In tandem, CLTC published a publicly accessible, searchable database of every cybersecurity-related bill enacted in 2025 across all 50 states. This is a tool that researchers, practitioners, and lawmakers may use to quickly understand the legislative landscape in any given state, identify which local lawmakers are actively passing cybersecurity policy, and contact their offices if needed. This resource also provides template language from existing cybersecurity legislation that lawmakers can refer to or copy directly into their bills. This dataset is available at <https://cltc.berkeley.edu/publication/tracking-cybersecurity-policy-developments-across-state-legislatures/>.

13 Consortium for School Networking. (2025, August). [2025 State Cybersecurity Legislation Report](#). Consortium for School Networking.

14 Consortium for School Networking. (2025, January). [State and Federal Cybersecurity Policy and Education in 2024](#). Consortium for School Networking.

Methodology

CLTC researchers sourced this dataset using LegiScan, a real-time, nonpartisan legislative tracking service and text-based search engine monitoring all bills introduced in the 50 U.S. states and Congress since 2010.¹⁵ The researchers conducted keyword searches for bills introduced during the 2025 legislative sessions that contained the terms “cybersecurity” or “cyber security” across all 50 state legislatures. The results were exported and filtered to include only enacted legislation (i.e., statutes, resolutions), and each piece of legislation was then manually reviewed for inclusion. CLTC researchers based their inclusion criteria on CISA’s definition of cybersecurity: “*Protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.*”¹⁶

Based on this definition, researchers excluded legislation primarily focused on data privacy or the use or governance of artificial intelligence (AI) technologies. While these topics are closely related to cybersecurity, they fell outside the scope of this analysis unless a piece of legislation established concrete cybersecurity mandates, controls, or resource allocations. This decision reflects CLTC’s intention to focus on cybersecurity-specific legislation, rather than the broader data privacy or AI policy domains.

A more detailed description of CLTC’s methodology and coding procedures can be found in Appendix I.

¹⁵ Legiscan. (n.d.) [Legiscan GAITS](#).

¹⁶ Cybersecurity and Infrastructure Security Agency. (2021, February 1). [What is Cybersecurity?](#)

The analysis below identifies trends in (1) the types of cybersecurity rules being enacted into law and (2) the critical infrastructure sectors and entities subject to regulation. This analysis yielded many lessons for other states that informed recommendations presented in the conclusion for lawmakers considering cybersecurity legislation in 2026.

EMERGING THEMES IN 2025 STATE CYBERSECURITY LEGISLATION

What types of cybersecurity laws did state legislatures enact in the 2025, and what unique trends and regulatory models are emerging across states? To answer these questions, CLTC researchers conducted a close reading of each cybersecurity-related legislation passed in 2025 to extract and log each cybersecurity-specific provision, identifying 393 new rules.

CLTC researchers then mapped each rule to one of the six functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0.¹⁸ CLTC selected CSF 2.0 because it is widely recognized as the baseline framework for cybersecurity risk management in the U.S., and it aligns closely with the NIST standards used by U.S. federal agencies. Figures 2 and 3 show the distribution of the rules across the CSF 2.0's six functions: Govern, Identify, Protect, Detect, Respond, and Recover. Each rule was also categorized by policy action type to describe the kinds of solutions state lawmakers pursued. Figure 4 summarizes these issue areas, and Appendix IV provides definitions for each policy action category.

Analysis of the cybersecurity bills passed by states in 2025 identified six overarching themes that characterize the scope, focus areas, and policy approaches reflected across the statutory corpus:

- **Theme 1:** States built out leadership and governance structures, particularly within state cybersecurity offices and agencies.
- **Theme 2:** States expanded requirements for public and private organizations to implement baseline cybersecurity controls.
- **Theme 3:** States increased obligations for organizations and agencies to routinely report to oversight bodies on cybersecurity programs, projects, compliance, risks, and spending.
- **Theme 4:** States prioritized stronger cybersecurity incident preparedness and response across critical infrastructure sectors.

¹⁸ NIST Computer Security Resources Center. (2024, February 26). [The NIST Cybersecurity Framework \(CSF\) 2.0](#). National Institute of Standards and Technology.

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

NIST Cybersecurity Framework (CSF) 2.0 Core Functions	Govern oversight of risk management	Identify risk	Protect systems from threats and vulnerabilities	Detect cybersecurity events	Respond to cybersecurity events	Recover system operations	Outside of NIST
Description	Provisions that create leadership and governance structures to oversee cybersecurity risk management by defining and assigning oversight responsibilities, and developing standards and procedures to ensure effective management.	Provisions that help organizations identify, assess, and mitigate cybersecurity risk.	Provisions that aim to limit or contain the impact of a potential cybersecurity event.	Provisions that enable the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring.	Provisions that require organizations to prepare for and respond to cybersecurity incidents and to prevent and prepare for service disruptions.	Provisions that support the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.	Provisions that did not align with any of the CSF Core Functions.
Related Policy Action Types	<ul style="list-style-type: none"> ● Policy & Standards ● Reporting ● Coordination & Support ● Statewide Plans & Strategy ● Disclosure Exemptions ● Oversight ● Cyber Leadership & Representation ● Governance Bodies ● Statewide Plans & Strategies ● Funding 	<ul style="list-style-type: none"> ● Risk Assessment ● Vulnerability Assessment and Penetration Testing ● Asset Inventory 	<ul style="list-style-type: none"> ● Cybersecurity controls ● Awareness Training ● Vulnerability Disclosure Program (VDP) ● .gov Domain Adoption 	<ul style="list-style-type: none"> ● Information Sharing 	<ul style="list-style-type: none"> ● Incident Notification ● Incident Response Planning ● Incident Response Operations & Assistance ● Incident Response Teams ● Exercises, Drills, & Testing 	<ul style="list-style-type: none"> ● State Cyber Insurance Programs & Backstops ● Liability Safe Harbor ● Business Continuity & Disaster Recovery Planning 	<ul style="list-style-type: none"> ● Cyber Harms & Remedies
Number of Related Provisions	200 Provisions	27 Provisions	64 Provisions	6 Provisions	56 Provisions	37 Provisions	3 Provisions

Figure 2: Alignment of the 2025 State Cybersecurity Legislation Provisions to the the NIST Cybersecurity Framework (CSF) 2.0 Core Functions¹⁹

19 See Footnote 16.

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

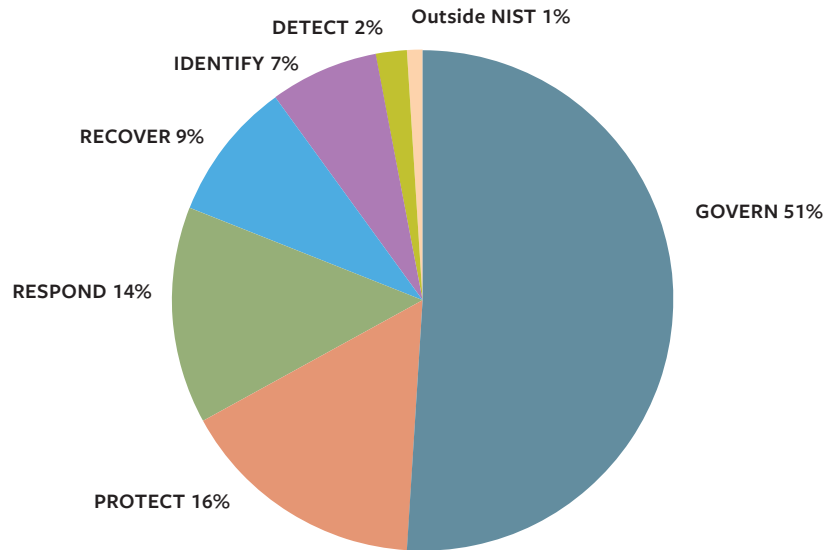


Figure 3: Share of 2025 State Cybersecurity Provisions by NIST CSF 2.0 Function

Rank	Actions	NIST CSF 2.0 Function	Count	Percentage
1	Cybersecurity Controls	PROTECT	40	10.2%
2	Policy & Standards	GOVERN	39	9.9%
3	Reporting	GOVERN	37	9.4%
4	Incident Notification	RESPOND	32	8.1%
5	State Cyber Insurance Programs & Backstops	RECOVER	27	6.9%
6	Coordination & Support	GOVERN	23	5.9%
7	Statewide Plans & Strategies	GOVERN	22	5.6%
8	Disclosure Exemptions	GOVERN	19	4.8%
9	Oversight	GOVERN	18	4.6%
	Awareness Training	PROTECT	18	4.6%
	Cyber Leadership & Representation	GOVERN	18	4.6%
10	Risk Assessment	IDENTIFY	17	4.3%

Figure 4: Top 10 Cybersecurity Policy Action Types in 2025 State Legislation, Ranked by Frequency²⁰

²⁰ See Appendix II for a full list of the cybersecurity action types in 2025 state legislation, ranked by frequency.

- **Theme 5:** States mandated cybersecurity expertise representation within state decision-making and leadership.
- **Theme 6:** States passed cybersecurity safe harbor laws to incentivize cybersecurity investment.

Theme 1: States built out leadership and governance structures, particularly within state cybersecurity offices and agencies.

Over half of all provisions (51%) focused on centralizing cybersecurity authority by building up leadership and governance structures for cybersecurity risk management within public and private organizations. These measures primarily expanded the governance architecture, authority, and responsibilities of state cybersecurity offices, enabling them to more effectively coordinate cybersecurity activities statewide.

In practice, this entailed standing up new departments and offices, assigning authorities and duties, and establishing oversight structures. Lawmakers charged these bodies with developing cybersecurity policies, procedures, and statewide cybersecurity strategies and plans, and with coordinating cybersecurity efforts across state agencies and critical infrastructure sectors.

Example:

- Texas ([HB150](#)) established a command center to improve the state's ability to prevent and respond to cyber incidents affecting government entities and critical infrastructure, consolidating statewide cybersecurity and network security responsibilities previously housed under the Texas Department of Information Resources (DIR) into a standalone, independent institution within the University of Texas System, administratively attached to the University of Texas at San Antonio.

Theme 2: States expanded requirements for public and private organizations to implement baseline cybersecurity controls.

The most common cybersecurity policy action taken by state legislatures in 2025 was mandating the use of cybersecurity controls for critical infrastructure organizations. Such mandates accounted for 10.2% of all provisions. States specified, to varying degrees of detail, the safeguards required to protect systems and sensitive data from threats and vulnerabilities.

These requirements were applied to state agencies, financial services organizations, water and wastewater systems (WWS), state emergency services, and entities handling genetic sequencing data. Commonly cited controls included encryption, access controls, secure system configura-

tions (e.g., network segmentation), tamper-resistant hardware, and the establishment of comprehensive cybersecurity programs, though the bills often do not detail what such a program entails.

However, most provisions relied on broad, generic language, such as requiring “reasonable security measures” or “reasonable encryption” without defining what those terms entail and what organizations can do to achieve them. According to the Center for Internet Security (CIS), “there is not a national, statutory, cross-sector minimum standard of what constitutes reasonable cybersecurity.”²¹ Without clear definitions, organizations lack clarity on how to interpret and comply with the law and mitigate potential liability in the event of a data breach.²²

A smaller subset of the laws passed were more prescriptive, requiring specific technical controls such as phishing-resistant, multi-factor authentication (MFA), specific encryption protocols (e.g., AES-256), and alignment with cybersecurity frameworks (e.g., CISA’s Zero-Trust Model, SOC 2, and ISO 27001).

Examples:

- Idaho ([H0035](#)) required the use of phishing-resistant MFA for all staff in the state legislative, judicial, and constitutional branches when accessing state IT devices or services, including email, cloud storage accounts, and all web applications.
- Nebraska ([LB660](#)) required drone systems to enforce end-to-end encryption for data-at-rest and data-in-transit using AES-256 and transport-layer security protocols as a condition for state purchase approval.

Theme 3: States increased obligations for organizations and agencies to routinely report to oversight bodies on cybersecurity programs, projects, compliance, risks, and spending.

Reporting mandates were the third-most common cybersecurity policy action in 2025, accounting for 9.4% of the dataset. These provisions established new or expanded requirements for entities to submit periodic (e.g., annual or biennial) reports to executive leadership and/or legislative oversight bodies.

These mandates required reporting on topics such as: status updates on cybersecurity programs, compliance audits, and measuring adherence with cybersecurity policies and

21 Center for Internet Security. (n.d.) [Reasonable Cybersecurity](#).

22 Shackelford, S. J., Boustead, A., & Makridis, C. (2023). [Defining “Reasonable” Cybersecurity: Lessons From the States](#). *Yale Journal of Law & Technology*, 25, 86–143.

standards, cybersecurity expenditures and budget trends, and recommendations for improvements.

Reporting obligations most frequently fall on states' central IT/cybersecurity departments or offices. These mandates also place requirements on advisory boards, commissions, select state agencies (e.g., education, emergency services), and regulated private-sector entities (e.g., financial institutions, AI companies). Reports are primarily directed to governors, state legislatures, or joint committees focused on IT, cybersecurity, and the budget, although some provisions require reporting to internal governance bodies within organizations, such as executive management or boards of directors.

The intent behind reporting requirements is to increase transparency and situational awareness of an organization's cybersecurity posture and needs, enabling more informed decision-making about improvements and budget allocations.

Theme 4: States prioritized stronger cybersecurity incident preparedness and response across critical infrastructure sectors.

In total, 14% of all cybersecurity-related legislative provisions passed by states in 2025 focused on requiring critical infrastructure organizations to prepare for and respond to cybersecurity incidents to prevent and prepare for service disruptions.

The most common incident response policy lever was incident notification, ranking fourth among policy action types across the entire dataset. These laws require entities to report cybersecurity incidents, data breaches, and/or ransom payments to government agencies or other specified parties (e.g., leadership, insurers, consumers) within defined timelines, often 24 to 72 hours. Notification requirements targeted critical infrastructure sectors, including financial institutions, municipalities, state agencies, community WWS, airports, and election systems.

Examples:

- Florida ([S1662](#)) required commercial service airports to notify the Department of Transportation within 48 hours of discovering a potential cybersecurity breach.
- Maryland ([SB871](#)) obligated community water and sewerage systems to report cyber incidents to the Department of Information Technology (DoIT) State Security Operations Center.
- Rhode Island ([So603](#)) required licensed financial services firms to notify the state's Department of Business Regulation within three business days of determining that a

security event occurred, and to later provide detailed information and updates about the incident.

The second-most common incident response (IR) action was IR planning, which requires entities to develop, implement, and/or maintain written plans for responding to various types of cybersecurity incidents. This includes requirements to update, review, or file plans with an oversight body. Entities required to establish IR plans include financial institutions, state agencies, cities, and counties. States also required entities to test their IR plans and preparation through tabletop exercises.

Examples:

- New York ([So7672](#)) required all state agencies to conduct at least one exercise of its IR plan annually and to document the plan's successes and shortcomings in a written report.
- Texas ([SB75](#)) directed the Texas Grid Security Commission to conduct simulated or tabletop exercises with state providers of electric generation, transmission, and distribution services to mitigate and prepare for a cyberattack on a critical facility.

Three states formed incident response teams, including Arkansas ([HB1549](#)), Texas ([HB150](#)), and Nevada ([SB467](#)). Other states established obligations for the provision of IR assistance to municipalities, electric utilities, and water systems:

- New York ([So7672](#)) required its Division of Homeland Security and Emergency Services (DHSES) to acknowledge requests from municipalities and public authorities for cybersecurity incident advice or technical assistance within 48 hours and to provide support as soon as possible.
- Texas ([SB75](#)) required the Texas Grid Security Commission to engage the Texas National Guard for training as first responders to cybersecurity threats to Texas' electric grid and other critical infrastructure.
- Maryland ([SB871](#)) directed its Cyber Preparedness Unit to assist local governments in providing guidance to local emergency management organizations for incidents against water and wastewater facilities.

Theme 5: States mandated cybersecurity expertise representation within state decision-making and leadership.

Four states enacted statutes requiring entities or governing bodies to include or consult qualified cybersecurity professionals to ensure cybersecurity risk perspectives are incorporated into policy- and decision-making. Including a cybersecurity subject-matter expert at the decision-making table — to translate technical security risks into policy-relevant terms and

explain their implications for adjacent sectors or emerging technologies — can help ensure security considerations are integrated earlier and more consistently across state governance.

Examples:

- Utah ([HB0040](#)) required its Division of Technology Services CISO, or the chief's designee, to be part of the School Security Task Force.
- Georgia ([HB423](#)) required the board of directors of the Georgia Emergency Communications Authority to include one member with cybersecurity subject-matter expertise, appointed by the Governor.
- Maryland ([HB956](#)) appointed two cybersecurity representatives to the Workgroup on Artificial Intelligence Implementation, which will report findings and recommendations on AI regulation.

Maryland pursued a different approach. Instead of hiring cybersecurity experts into sector-specific bodies, SB294 expanded the Maryland Cybersecurity Council's membership to include representatives from key sectors and civil society, ensuring that sectoral risk perspectives inform statewide cyber policy. New participants included representatives from Maryland's bankers' association, hospital association, an electric company, and a water system serving customers in the state, as well as academics from think tanks such as the Center for Democracy and Technology.

Theme 6: States passed cybersecurity safe harbor laws to incentivize cybersecurity investment.

Four states enacted legal safe harbors for businesses that reduce or eliminate civil liability or penalties arising from cyber incidents or data breaches under certain conditions. Some statutes conditioned these protections on companies demonstrating the implementation of "reasonable" cybersecurity safeguards. These policies are intended to incentivize proactive cybersecurity investments by linking liability protection to baseline cybersecurity controls.

Example:

- Texas ([SB2610](#)) provided protection to small- to mid-sized businesses (SMB) with fewer than 250 employees from exemplary damages resulting from a data breach, if they demonstrated that, at the time of a breach, they had implemented and maintained a cybersecurity program. Programs must include administrative, technical, and physical safeguards that protect personal information and conform to an industry-recognized cybersecurity framework, with requirements scaled to business size. For example, firms

with 20 to 100 employees must implement CIS Controls Implementation Group 1 (the minimum standard for cyber hygiene for all enterprises),²³ whereas firms with 100 to 249 employees must maintain full compliance with an accepted industry framework, such as NIST CSF or ISO/IEC 27000.

Texas' approach is notable for its prescriptiveness and recognition of the resource constraints of SMBs. By tying liability protection to concrete, tiered controls or frameworks, the statute creates a clear risk-mitigation pathway that rewards cybersecurity investment while acknowledging that smaller firms likely cannot afford, and may not need, to stand up enterprise-grade cybersecurity programs.

In stark contrast, other states adopted far broader and less conditional safe harbors. For example, Nebraska ([LB241](#)) granted any private entity immunity from liability in class-action lawsuits arising from cybersecurity incidents, unless it can be proved that the incident was caused by the entity's willful, wanton, or gross negligence. While these kinds of provisions protect organizations, they may do less to encourage improved cybersecurity practices.

SECTORAL PRIORITIES IN 2025 STATE CYBERSECURITY LEGISLATION

CLTC researchers categorized each piece of legislation by its intended beneficiary to assess which entities and sectors lawmakers prioritized and where they concentrated new cybersecurity protections. Appendix III provides definitions for each beneficiary category.

CLTC identified four main themes in state cybersecurity legislation from 2025:

- **Theme 1:** Legislation primarily focused on state government systems like state agencies.
- **Theme 2:** Lawmakers paid heightened attention to K-12 schools and other education entities.
- **Theme 3:** Lawmakers addressed the cyber insurance industry by passing laws to modernize state insurance guaranty laws and establish state risk pools.
- **Theme 4:** Lawmakers passed a small but meaningful body of legislation to improve cybersecurity in high-risk, resource-constrained critical infrastructure sectors.

23 Center for Internet Security. (n.d.) [CIS Critical Security Controls Implementation Group 1](#).

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

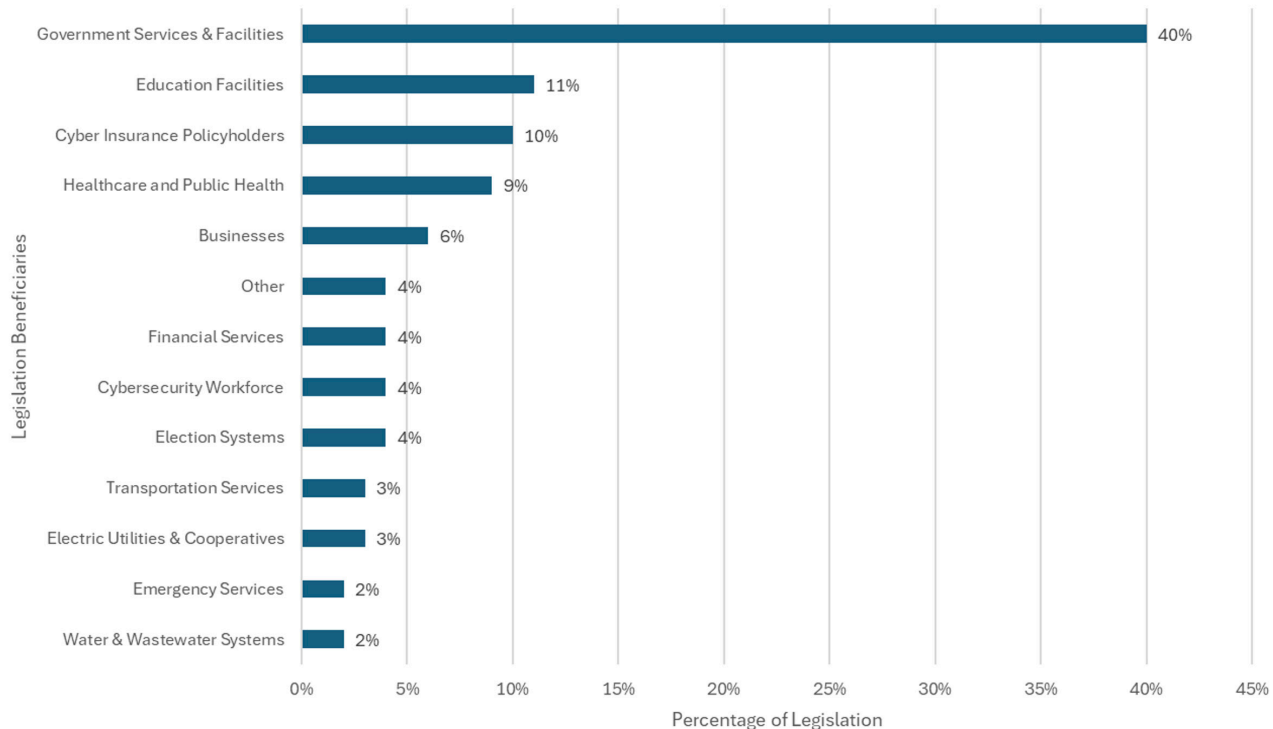


Figure 4: Intended Beneficiaries of 2025 State Cybersecurity Legislation²⁴

Theme 1: Legislation primarily focused on state government systems like state agencies.

Nearly half (40%) of the cybersecurity-related legislation focused on strengthening cybersecurity for state government services and facilities, including state agencies, courts, legislatures, and their support offices, as well as state, local, tribal, and territorial facilities. Most of these laws centralize responsibility for cybersecurity by creating or empowering statewide cyber offices to set and enforce cybersecurity standards across state government, audit agency compliance, report findings to the legislature, and coordinate statewide incident response activities.

Example:

- Arkansas ([HB1549](#)), Texas ([HB150](#)), and Nevada ([SB467](#)) established dedicated state cybersecurity offices or agencies to formalize coordination and management roles, and directed their state cybersecurity offices to form incident response teams.

24 Appendix III provides definitions for each beneficiary category.

- Maryland ([HB235](#)), Arkansas ([HB1557](#)), Nevada ([SB467](#)), and Alabama ([HB207](#)) assigned duties to their state IT and cybersecurity departments to develop and implement, on an annual or biennial basis, statewide strategic plans for the security of information systems.

Theme 2: Lawmakers paid heightened attention to K-12 schools and other education entities.

Education facilities — including pre-kindergarten through 12th-grade schools, higher education institutions, business and trade schools, and school libraries — were the second-most common beneficiaries of legislation in 2025 (11%).²⁵ These statutes created state-administered insurance programs, mandated the development of secure mechanisms for sharing student data, convened working groups to discuss cybersecurity challenges in the education sector, and required school districts to use template cybersecurity policies.

Examples:

- Indiana ([SBo472](#)) directed its Office of Technology to develop a uniform cybersecurity policy for K–12 school districts and public universities and colleges, making it mandatory for them to adopt the policy and conduct employee training on it. The law also requires schools and universities to submit their adopted cybersecurity policy to the Office of Technology every two years.
- Utah ([HB0040](#)) convened a School Security Task Force to craft recommendations for minimum cybersecurity standards for local education agencies. The statute required Utah’s State Chief Information Security Officer (CISO) to be part of the task force.
- Maine ([LD1404](#)) established a working group to study whether school and public libraries within the state have sufficient access to basic cybersecurity resources.
- Arkansas ([SB481](#), [HB1821](#)) directed the State Insurance Department to offer cybersecurity risk insurance to public K-12 schools, set reporting requirements, and provided coverage requirements.
- Oregon ([HB2508](#)) directed its Department of Education to establish a technical advisory committee to assist in the development and implementation of a standardized method for school districts, education service districts, and the department itself to electronically create, collect, use, maintain, disclose, transfer, and access student data from multiple platforms. The statute requires the department to incorporate the committee’s analysis and recommendations on cybersecurity issues that may affect student data.

25 Cybersecurity and Infrastructure Security Agency. (n.d.) [Government Services and Facilities Sector](#).

This legislative focus on cybersecurity for education facilities tracks with the sharp rise in ransomware attacks on K-12 schools and data breaches involving sensitive student information. A 2024 U.S. Department of Homeland Security threat assessment identified K-12 school districts as “a near constant ransomware target.”²⁶ The operational and financial costs of these incidents for K-12 schools are steep: in 2024, ransomware attacks caused schools to lose 12.6 days of downtime on average, each day costing nearly \$550K,²⁷ and recovery costs averaged over \$3.7 million, more than double the figure for 2023.²⁸ In December 2024, student information system provider PowerSchool suffered the largest known breach of K-12 student records in history, and stolen credentials were used to expose and steal sensitive data belonging to over 60 million students and teachers.²⁹

Theme 3: Lawmakers addressed the cyber insurance industry by passing laws to modernize state insurance guaranty laws and establish state risk pools.

Of all cybersecurity laws enacted by states in 2025, nine percent introduced new protections for cyber insurance policyholders. These statutes most commonly updated state insurance guaranty laws to better equip state guaranty associations to handle cyber insurance claims.

Insurance guaranty associations (IGAs) are state-mandated nonprofit organizations that provide a financial backstop for policyholders in case an insurer does not have the resources to reimburse insured clients, also known as insolvency or bankruptcy. Every state has at least one or two IGAs. However, IGA systems were not built with cyber claims in mind. As cyber insurance becomes a mainstream insurance product, IGAs expect to receive cyber insurance-related claims in the future, which will inevitably raise questions about how these policies will be handled when insurers fail.³⁰

Seeing this problem on the horizon, representatives from the National Conference of Insurance Guaranty Funds (NCIGF) raised the issue at a September 2022 meeting of the National Association of Insurance Commissioners (NAIC). NCIGF supplied a model bill amending the widely adopted Property and Casualty Insurance Guaranty Association Model Act to help states

26 U.S. Department of Homeland Security. (2023, September 14). [The Department of Homeland Security \(DHS\) Intelligence Enterprise Homeland Threat Assessment](#).

27 Bischoff, P. (2024, August 27). [On average, US schools & colleges lose \\$500K per day to downtime from ransomware attacks](#). Comparitech.

28 Mahendru, Pujja. (2024, July 11). [The State of Ransomware in Education 2024](#). Sophos.

29 Langreo, L., & Prothero, A. (2025, May 8). [PowerSchool Paid a Hacker's Ransom. Now Cyber Criminals Are Threatening Schools](#). EducationWeek.

30 National Conference of Insurance Guaranty Funds. (2022, September 29). [Considerations for Insolvency Practitioners presented with Cyber Security Claims](#). National Association of Insurance Commissioners.

clarify how cyber insurance claims should be treated under guaranty fund statutes before an insurer fails and claims administration becomes urgent.³¹

Nine states passed legislation based on the newly updated model act, including Arkansas, Maine, Massachusetts, Mississippi, Nebraska, North Carolina, Oklahoma, Oregon, and Rhode Island. Statutes set caps on the liability of the IGAs between \$300,000 and \$500,000 per insured event for all first- and third-party claims under a cybersecurity insurance policy arising out of a single insured event, regardless of the number of claims or claimants. These caps prevent one ransomware incident from draining the guaranty fund. States also included provisions granting IGAs flexibility and discretion not to automatically cover very large or wealthy organizations when an insurer fails, enabling them to decide on a case-by-case basis whether to reimburse them.

Theme 4: Lawmakers passed a small but meaningful body of legislation to improve cybersecurity in high-risk, resource-constrained critical infrastructure sectors.

While statutes addressing the government services and facilities sector dominated the dataset, lawmakers also passed a targeted set of statutes addressing cybersecurity in healthcare, election systems, utilities, water systems, and emergency services.

These critical sectors deliver essential public services but are often ill-prepared in cybersecurity due to limited knowledge and investments in staff, tools, equipment, and incident response support. These organizations tend to prioritize public service delivery over managing cyber risk, and are increasingly targeted by cyberattacks from state and non-state actors. For example, U.S. water systems are increasingly targeted by criminal ransomware gangs and state-backed hacking groups, namely China's Volt Typhoon, which seeks to pre-position itself within water system networks to enable service disruption or facility damage.³²

Seven statutes addressed the healthcare and public health sector. Five statutes from Arkansas ([SB311](#)), Tennessee ([SBO318](#), [HBO395](#) [concurrent]), Texas ([HB130](#)), and Louisiana ([HB125](#)) established cybersecurity requirements for entities storing genetic sequencing data (i.e., medical facilities, research facilities, or companies and third parties). This included obligations

³¹ National Association of Insurance Commissioners. (2023). [Property and Casualty Insurance Guaranty Association Model Act \(#540\)](#).

³² Cybersecurity and Infrastructure Security Agency. (2024, February 7). [PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure](#).

to use reasonable encryption methods, restrictions on access, and other cybersecurity best practices.

Other statutes added protections for retirement communities and pharmacists:

- New Hampshire ([SB124](#)) mandated that continuing care retirement community (CCRC) providers applying for a certificate of authority to operate must certify that their IT platforms comply with all applicable cybersecurity requirements.
- Arkansas ([HB1620](#)) required benefits managers and healthcare payors to pay interest on payments owed to pharmacists or pharmacies that are delayed due to a cybersecurity breach or data security issue.

Three statutes addressed the digital security of election systems, including voter registration databases, voting systems, and other technology used to manage elections and to report and validate results.³³ These measures generally aim to protect election systems from cyber incidents by mandating the use of cybersecurity best practices, incident notification requirements, and reporting and auditing obligations to ensure compliance.

Examples:

- Washington ([SB5014](#)) imposed breach disclosure requirements on vendors supporting county or state election cyber assets, and on manufacturers, distributors, and contractors supporting the voter registration database system. Washington also required election offices to use “.gov” domains for all election-related websites and email communications. Additionally, the law required physical and electronic partitioning of election and voting infrastructure (e.g., internal government networks, servers, and other electronic equipment) from other county assets housed in the same location, and directed county auditors to monitor compliance with required cybersecurity measures for election systems.
- New Hampshire’s legislature ([HB626](#)) directed the state’s chief election officer to establish and operate a vulnerability disclosure program (VDP) for election systems that meets or exceeds the recommendations outlined in CISA’s *Guide to Vulnerability Reporting for America’s Election Administrators*.³⁴

33 Cybersecurity and Infrastructure Security Agency. (n.d.). [Election Security](#).

34 Cybersecurity and Infrastructure Security Agency. (2020, December 17). [Guide to Vulnerability Reporting for America’s Election Administrators](#).

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

Three statutes addressed electric utilities and cooperatives — in South Carolina ([H3309](#)), Virginia ([SB1239](#)), and Texas ([SB75](#)). These statutes established working groups to evaluate cybersecurity risks facing electric utilities and cooperatives and recommend actions when a cyber incident threatens the reliability or security of the broader electric grid.³⁵

Two statutes addressed community WWS, one in Maryland ([MD SB871](#)) and one in Indiana ([IN SB0459](#)). This legislation set incident-reporting and notification standards, established policies and procedures, required cyber awareness training, mandated vulnerability assessments and penetration tests, and mandated the appointment of a cyber lead.³⁶

Two statutes targeted the cybersecurity of emergency services, specifically 911 emergency response services. Both Georgia ([HB423](#)) and Maryland ([SB138](#)) enacted laws establishing minimum cybersecurity standards for providers of next-generation 911 services.

³⁵ For more information on the most comprehensive electric utility cybersecurity statute passed in 2025, see the Top State Champions section.

³⁶ For more information on the most comprehensive water system cybersecurity statute passed in 2025, see the Top State Champions section.

Top State Champions

Cybersecurity lawmaking in 2025 was widespread across state legislatures but unevenly distributed nationwide. While 74% of states enacted at least one cybersecurity-related bill in 2025, legislative activity was highly concentrated: three states accounted for roughly one-third of all enacted cybersecurity legislation nationwide. Maryland led with 14 statutes, followed by Texas (11) and Arkansas (9).

In total, 74 unique state lawmakers served as the primary sponsors of cybersecurity legislation in 2025. Excluding resolutions, three states—Maryland, Texas, and Arkansas—stood out for hosting the most prolific cybersecurity lawmakers of 2025, each with two enacted statutes. These legislative leaders included Maryland State Senator Katie Fry Hester (D–District 9),³⁷ Texas State Representative Giovanni Capriglione (R–98th district),³⁸ and Arkansas State Representative R. Scott Richardson (R–13th District).³⁹

Analysis of sponsor activity suggested that 2025 state cybersecurity policymaking was driven less by national momentum on cybersecurity topics, and more by sustained leadership and interest from a small number of highly engaged legislative champions with a particular passion for cybersecurity.

Arkansas, Maryland, and Texas ushered in some of the most exhaustive, forward-thinking legislation aimed at improving cybersecurity for public-interest organizations, namely laws focused on securing WWS, electric grids, and K-12 schools. The following sections spotlight and provide a deeper analysis of some of these landmark statutes.

CASE STUDIES FROM KEY STATE LEGISLATION: MARYLAND AND TEXAS

Case Study 1: Maryland Protects Local Water and Wastewater Systems

Maryland ([SB871](#)) passed the most expansive community WWS statute in the country in 2025. This statute set new cybersecurity requirements for all WWS in the state, requiring

37 Maryland General Assembly. (n.d.). [Senator Katie Fry Hester](#).

38 Texas House of Representatives. (n.d.). [Rep. Capriglione, Giovanni - District 98](#)

39 State of Arkansas House of Representatives (n.d.). [R. Scott Richardson](#).

TRACKING CYBERSECURITY POLICY DEVELOPMENTS ACROSS STATE LEGISLATURES

them to meet new cybersecurity standards established by the Maryland Department of the Environment or to meet or exceed CISA's Cross-Sector Cybersecurity Performance Goals.⁴⁰

The bill also included actions to help WWS identify cybersecurity risks and protect themselves from threats and vulnerabilities. This came in the form of requirements for WWS to undertake annual cybersecurity awareness training and conduct operational technology (OT) and IT cybersecurity maturity assessments biennially. Maryland also included an oversight and enforcement component in the bill, requiring WWS to certify compliance with DoIT biennially and requiring DoIT to report to Maryland's legislature biennially on WWS' implementation progress.

The statute also strengthens water and wastewater system incident response by requiring systems to report cyber incidents to the state security operations center (SOC). DoIT is also required to publish an annual public summary of reported incidents from the prior calendar year without identifying individual WWSs. Given all these new obligations for DoIT, Maryland also bulked up its capacity to meet these new responsibilities by directing DoIT to hire staff with OT cybersecurity expertise to support water systems and other critical infrastructure. The law also tasks Maryland's Cyber Preparedness Unit with providing guidance to local emergency management organizations for incidents affecting water and wastewater facilities.

These new requirements are significant for several reasons. First, Maryland is stepping up its responsibility for WWS cybersecurity at a time when the federal entities that typically lead on this topic are stepping away. The Environmental Protection Agency (EPA) is the federal government's designated lead for managing cyber risk and ensuring the cyber resilience of America's water and wastewater infrastructure, but it is undergoing reorganization under the Trump Administration and has experienced the largest staffing cuts (25%) in its history,⁴¹ leaving behind a critical leadership vacuum on WWS cybersecurity.⁴²

Second, Maryland is taking some steps to bring its local water systems up to speed on cybersecurity, something desperately needed across the country. Only 20 percent of U.S. water

40 Cybersecurity & Infrastructure Sector Agency. (n.d). *Cybersecurity Performance Goals 2.0 (CPG 2.0)*.

41 Sellers, C., Blum, S., Kohl, E., Sullivan, M., Fredrickson, L., Stoll, S. L., Legefled, M., Barrett, K., Levy, A. (2025, September 3). *Burning Down the EPA: Documenting the Second Trump Administration's Historic Assault*. Environmental Data & Governance Initiative.

42 Pierson, Shannon. (2025, May). *Slashing EPA funding may have downstream cybersecurity impacts on an already vulnerable water sector*. Center for Long-Term Cybersecurity.

and wastewater systems currently maintain basic levels of cyber hygiene, and 70 percent of the water systems inspected by the EPA since 2023 have been found in violation of the mandatory cybersecurity standards established in Section 1433 of the federal Safe Drinking Water Act (SDWA).⁴³ Maryland is empowering both its Department of the Environment and DoIT to take up some of the EPA's role, leading efforts to protect the integrity and reliability of drinking water, including by protecting WWS's systems and networks from cyber threats.

Case Study 2: Texas Electric Utilities and Cooperatives

Texas ([SB75](#)) enacted the most sweeping cybersecurity law affecting electric utilities and cooperatives in 2025 by establishing the Texas Grid Security Commission, under the Texas Division of Emergency Management. This commission, composed of representatives from various state agencies and power generation and utility companies, is tasked with evaluating all hazards to the state's electric grid, including cyberattacks, as well as vulnerabilities to essential municipal service systems.

The commission is tasked with recommending cybersecurity resilience standards for municipalities and critical infrastructure of Texas' electric grid and micro-grids and reporting out estimated implementation costs, potential consequences of non-implementation, and prospective implementation timelines to the State Legislature. Additionally, the commission must develop a statewide critical infrastructure protection plan for the State Legislature by the end of 2026 that (1) evaluates whether proposed recommendations would induce cyber vulnerabilities and (2) includes recommendations for installing, replacing, or upgrading industrial control systems and associated networks, or for using compensating controls or procedures, to address cyber vulnerabilities in critical facilities.

The statute strengthens the ability of electric utilities and cooperatives to prepare for and respond to cyber incidents by requiring the commission to conduct tabletop exercises with providers of electric generation, transmission, and distribution service providers in the Texas power region. Moreover, the commission is tasked with engaging Texas universities with cybersecurity expertise and the Texas National Guard to strengthen statewide cybersecurity response capabilities.

43 U.S. Environmental Protection Agency. (2024, May). [Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities](#).

Analysis and Recommendations for 2026

CLTC researchers identified 10 trends to describe the types of cybersecurity laws state legislatures passed in 2025 and to characterize the entities and sectors being regulated. To summarize, states:

- Built out leadership and governance structures, particularly within state cybersecurity offices and agencies;
- Expanded requirements for public and private organizations to implement baseline cybersecurity controls;
- Increased obligations for organizations to routinely report on cybersecurity programs, projects, compliance, risks, and spending to oversight bodies;
- Prioritized stronger cybersecurity incident preparedness and response across critical infrastructure sectors;
- Mandated cybersecurity expertise representation within state decision-making and leadership; and
- Passed cybersecurity safe harbor laws to incentivize cybersecurity investment.

With the above directives, lawmakers sought legislation to address the needs of:

- State government systems, specifically state agencies, over all other entities;
- Education entities, paying special attention to K-12 schools;
- Cyber insurance policyholders; and
- High-risk, resource-constrained critical infrastructure sectors.

From these findings, a few trends particularly stood out to CLTC researchers, leading to the following recommendations:

Recommendation 1: Lawmakers should continue reaching across the aisle to pass cybersecurity bills, as bipartisan consensus on cybersecurity exists at the state level.

Recommendation 2: Lawmakers should attach accompanying funding to new cybersecurity mandates to ensure their successful implementation.

Recommendation 3: Lawmakers should be more prescriptive about required cybersecurity controls in legislation, rather than relying on undefined terms like “reasonable security measures.”

Recommendation 4: Lawmakers should explore ways to support states in detecting cyber incidents.

Recommendation 5: Lawmakers should require follow-up actions to ensure that reporting translates into action.

Recommendation 1: Lawmakers should continue reaching across the aisle to pass cybersecurity bills, as bipartisan consensus on cybersecurity exists at the state level.

Cybersecurity as a policy topic remained a bipartisan issue within state legislatures in 2025, though Republican-sponsored bills advanced to enactment at slightly higher rates than Democrat-sponsored measures. In total, 74 unique state lawmakers served as primary sponsors for enacted cybersecurity legislation during the year. Our review of primary bill sponsors indicates that Republicans led on cybersecurity lawmaking in 2025, introducing 61% of enacted bills compared to 39% by Democrats. While these results suggest Republicans were slightly more successful at advancing cybersecurity measures through to passage in 2025, the activity of both parties indicates that cybersecurity remains a topic of concern in state legislatures across the country. It also remains an area on which lawmakers are willing to work across the aisle: six percent of laws were passed by bipartisan co-sponsors.

Recommendation 2: Lawmakers should attach accompanying funding to new cybersecurity mandates to ensure their successful implementation.

While this study did not include an in-depth review of state budgets and appropriations bills, the researchers noted a high volume of unfunded mandates. The legislation passed in 2025 establish many new, expensive cybersecurity requirements — such as annual risk assessments, tabletop exercises, penetration testing, and the hiring of cybersecurity staff — yet the vast majority of legislation in this corpus lacks accompanying appropriations. The entities tasked with fulfilling cybersecurity requirements are frequently resource-constrained critical infrastructure organizations that may not have the resources to meet these new requirements. Cybersecurity regulation and funding must go hand-in-hand to set up regulated entities for success.

The absence of accompanying appropriations was likely due to funding obstacles. Funding remains one of the biggest hurdles to passing cybersecurity-related legislation. Because of this, lawmakers often are required to revise bills into unfunded mandates or have their bills outright rejected simply because they require appropriations.

Recommendation 3: Lawmakers should be more prescriptive about required cybersecurity controls in legislation, rather than relying on undefined terms like “reasonable security measures.”

The cybersecurity control requirements established by states in 2025 reflect a divide between generic and prescriptive requirements. Many laws rely on vague standards, such as “reasonable security measures” or “reasonable encryption.” While this gives entities flexibility in how they comply, it can also make requirements difficult to enforce and make it harder for entities to understand their liability. More prescriptive laws can make expectations clearer and drive faster improvements, but they are harder to keep up to date as technology evolves and may require future amendments that must be approved by a legislature.

Recommendation 4: Lawmakers should explore ways to support states in detecting cyber incidents.

CLTC researchers noticed a lack of attention to improving critical infrastructure entities’ ability to detect cybersecurity events in a timely manner, aside from the information-sharing provisions, which accounted for 1.5% of the dataset. Very few statutes strengthen a state’s ability to continuously monitor systems, detect intrusions, or analyze indicators of compromise. This matters because detection enables organizations to identify risks and intrusions early on, before they escalate into major disruptions. The lack of detection is especially concerning given the loss of federal support for shared services like the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (E-ISAC) in 2025.^{44 45} As federal involvement on cyber defense continues to roll back, states will increasingly need to build or fund their own detection and monitoring capabilities.

Recommendation 5: Lawmakers should require follow-up actions to ensure that reporting translates into action.

CLTC noted a high volume of new reporting requirements. While reporting can improve transparency and oversight, it is only effective when someone is clearly responsible for reviewing the reports, following up, and enforcing compliance. In absence of these pieces, reports risk sitting unused and becoming a paperwork exercise that consumes staff time without improving cybersecurity outcomes. In 2026 and beyond, lawmakers should ensure that their cybersecurity legislation includes explicit review and follow-on actions to enable action on the findings of reports.

44 Wood, Colin. (2025, September 29). [CISA confirms it’s ending MS-ISAC support](#). CyberScoop.

45 Wood, Colin. (2025, February 20) [Federal cuts to election security concern secretaries of state](#). CyberScoop.

Conclusion

In conclusion, 2025 was a banner year for state cybersecurity policymaking. States are increasingly taking legislative action on cybersecurity by setting standards, allocating resources, and assigning responsibility to better protect critical infrastructure and consumers of digital services connected to essential services.

In 2026, CLTC expects states to continue their high-volume production of cybersecurity policy and innovation.

This analysis of states' cybersecurity legislation represents the first step in a broader research agenda. In future work, CLTC plans to publish a deeper analysis of the most important models emerging across states. Future work will seek to analyze state funding and appropriations for cybersecurity through a review of state budgets and appropriations bills, and aim to quantify funding amounts, identify distinct funding models, and highlight funding priorities.

Appendices

APPENDIX I — METHODOLOGY

CLTC researchers sourced this dataset using LegiScan, a real-time, nonpartisan legislative tracking service and text-based search engine monitoring all bills introduced in the 50 U.S. states and Congress since 2010.⁴⁶ The researchers conducted keyword searches for bills introduced during the 2025 legislative sessions that contained the terms “cybersecurity” or “cyber security” across all 50 state legislatures. The results were exported and filtered to include only enacted legislation (i.e., statutes, resolutions), and each piece of legislation was then manually reviewed for inclusion.

CLTC researchers based their inclusion criteria on CISA’s definition of cybersecurity: *“Protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.”*⁴⁷

Based on this definition, researchers excluded statutes primarily focused on data privacy or the use or governance of artificial intelligence (AI) technologies. While these topics are closely related to cybersecurity, they fell outside the scope of this analysis unless a statute established concrete cybersecurity mandates, controls, or resource allocations. This decision reflects CLTC’s intention to focus on cybersecurity-specific legislation, rather than the broader data privacy or AI policy domains.

For this legislative analysis, CLTC researchers:

1. **Calculated the timeline of passage by tracking each bill’s introduction and enactment dates;**
2. **Identified each bill’s primary sponsors and their party affiliations; and**
3. **Identified the statute’s intended beneficiaries.**

“Intended beneficiary” refers to the identified sectors, critical infrastructure operators, or technology stakeholders that lawmakers intend to support or protect through a given piece of cybersecurity legislation. When creating these categories, researchers referred to the 16 critical infrastructure sectors and subsectors, as defined in the February 2013 revision of the National

⁴⁶ Legiscan. (n.d.) [Legiscan GAITS](#).

⁴⁷ Cybersecurity and Infrastructure Security Agency. (2021, February 1). [What is Cybersecurity?](#)

Infrastructure Protection Plan.⁴⁸ In addition, researchers included supplementary categories (e.g., cyber insurance policyholders, cybersecurity workforce, businesses, etc.) to account for groups that fall outside of the critical sectors but are nonetheless intended beneficiaries of cybersecurity legislation. Next, the researchers:

4. **Conducted a close reading of each cybersecurity-related legislation to extract and log each cybersecurity-specific provision, identifying 393 new rules;**
5. **Coded each cybersecurity rule according to six Functions of the National Institute of Standards and Technology Cybersecurity Framework (NIST) Framework.**

CLTC researchers then mapped each rule to one of the six functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0⁴⁹ CLTC selected CSF 2.0 because it is widely recognized as the baseline framework for cybersecurity risk management in the U.S., and it aligns closely with the NIST standards used by U.S. federal agencies. Figures 2 and 3 show the distribution of the rules across CSF 2.0's six functions: Govern, Identify, Protect, Detect, Respond, and Recover.

The NIST CSF 2.0 is the national baseline for how government agencies, industry, and nonprofits manage cybersecurity risk. CLTC researchers chose to use this framework for this analysis because it (1) aligned with how federal agencies evaluate state cyber capabilities and (2) enabled us to segment cybersecurity-related legislative actions into six distinct categories, making it easier to compare states and evaluate where they placed their emphasis.

To design this methodology, CLTC researchers drew inspiration from a recent Government Accountability Office (GOA) framework used to summarize projects funded by different states using the State Local Cybersecurity Grant Program (SLCGP).⁵⁰

6. **Categorized each provision by policy action type to describe the kinds of solutions state lawmakers pursued.**

To provide greater granularity to the actions, the authors grouped each cybersecurity rule into an even more specific category. Overall, this approach gave a clear and consistent way

48 Cybersecurity and Infrastructure Security Agency. (2013). *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*.

49 NIST Computer Security Resources Center. (2024, February 26). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology.

50 Hinchman, D. B. & Sherman, T. W. (2025, April) *DHS Implemented a Grant Program to Enable State, Local, Tribal, and Territorial Governments to Improve Security*. Government Accountability Office.

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

to assess how states prioritized cybersecurity in the 2025 legislative session, and it made comparisons more grounded and meaningful. Figure 4 summarizes these issue areas, and Appendix IV provides definitions for each policy action category.

APPENDIX II — CYBERSECURITY POLICY ACTION TYPES IN 2025 STATE LEGISLATION, RANKED BY FREQUENCY

Rank	Actions	NIST CSF 2.0 Function	Count	Percentage
1	Cybersecurity Controls	PROTECT	40	10.2%
2	Policy & Standards	GOVERN	39	9.9%
3	Reporting	GOVERN	37	9.4%
4	Incident Notification	RESPOND	32	8.1%
5	State Cyber Insurance Programs & Backstops	RECOVER	27	6.9%
6	Coordination & Support	GOVERN	23	5.9%
7	Statewide Plans & Strategies	GOVERN	22	5.6%
8	Disclosure Exemptions	GOVERN	19	4.8%
9	Oversight	GOVERN	18	4.6%
	Awareness Training	PROTECT	18	4.6%
	Cyber Leadership & Representation	GOVERN	18	4.6%
10	Risk Assessment	IDENTIFY	17	4.3%
11	Governance Bodies	GOVERN	16	4.1%
12	Incident Response Planning	RESPOND	10	2.5%
	Funding	GOVERN	10	2.5%
13	Vulnerability Assessment and Penetration Testing	IDENTIFY	7	1.8%
	Incident Response Operations & Assistance	RESPOND	7	1.8%
14	Information Sharing	DETECT	6	1.5%
16	Liability Safe Harbor	RECOVER	6	1.5%
15	Incident Response Teams	RESPOND	4	1.0%
	Business Continuity and Disaster Recovery Plan	RECOVER	4	1.0%
16	Exercises, Drills, & Testing	RESPOND	3	0.8%
18	Asset Inventory	IDENTIFY	3	0.8%
18	Cyber Harms & Remedies	Outside of NIST	3	0.8%
17	Vulnerability Disclosure Program (VDP)	PROTECT	2	0.5%
20	.gov Domain	PROTECT	2	0.5%

APPENDIX III — DEFINITIONS OF INTENDED BENEFICIARY CODING CATEGORIES

Beneficiary Code	Definition
Businesses	Small-, medium-, and large-sized businesses across all industries.
Cybersecurity Workforce	The present and future cybersecurity workforce, for which opportunities are being created via investments in education, training, and workforce development programs.
Cyber Insurance Policy Holders	Insured entities and affected third-party claimants.
Education Facilities	Pre-kindergarten through 12th-grade schools, higher-education institutions, and business and trade schools.
Electric Utilities and Cooperatives	Public and privately-owned utilities that provide electricity to local communities.
Emergency Services	Emergency management, emergency medical services, fire and rescue services, law enforcement, and public works.
Financial Services	“Depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions.” ⁵¹
Government Services and Facilities	State agencies, courts, legislatures, and their support offices, as well as state, local, tribal, and territorial facilities.
Healthcare and Public Health Sector	Hospitals, clinics, pharmacies, and labs.
Transportation Services	Aviation, highway and motor carrier, maritime transportation systems, mass transit and passenger rail, pipeline systems, freight rail, and postal and shipping.
Water and Wastewater Systems (WWS)	Public and privately-owned facilities that treat drinking water to make it safe for consumption and manage wastewater to remove pollutants before discharge or reuse.
Other	Entities that fall outside of the above listed categories.

51 Cybersecurity & Infrastructure Security Agency. (n.d.) [Financial Services Sector](#).

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

APPENDIX IV — DESCRIPTION OF CYBERSECURITY POLICY ACTION CODING CATEGORIES

Policy Action Code	NIST CSF Function	Definition
Cybersecurity Controls	PROTECT	Provisions that require entities to implement cybersecurity safeguards within their organization to protect information systems and data. These controls include: adopting standards set by governance bodies (e.g., state agencies), establishing cybersecurity programs, encryption methods, access controls, secure system configurations (e.g., network segmentation), and the use of tamper-resistant hardware.
Policy & Standards	GOVERN	Provisions requiring authorized entities to develop, adopt, implement, and/or periodically update written cybersecurity and technology governance materials, such as policies, standards, guidelines, governance models, and frameworks. This includes requirements to issue guidance or define minimum standards for cybersecurity, oversight, and accountability.
Reporting	GOVERN	Provisions that require entities to submit periodic cybersecurity-related reports or specific information to executive and legislative oversight authorities (e.g., the governor, legislative committees, general assembly, state agencies), or to make them publicly available. Reporting obligations may include: cybersecurity program status and compliance, audit results, incident preparedness assessments, spending and funding allocations, project performance metrics, implementation guidelines, required notifications or disclosures to authorities about cyber insurance coverage or involvement in cyber assessments, and recommendations for improvements.
Incident Notification	RESPOND	Provisions requiring entities to report or disclose cybersecurity incidents (including data breaches and ransom payments) to government agencies or other specified parties (e.g., leadership, insurers, consumers) within defined timelines (e.g., 24 to 72 hours).
State Cyber Insurance Programs & Backstops	RECOVER	Provisions creating state cyber insurance or reimbursement programs to improve access to affordable coverage for eligible entities (e.g., public schools), and/or authorizing state guaranty associations to cover cybersecurity insurance claims in the event of insurer insolvency, including payout caps and eligibility limits.
Coordination & Support	GOVERN	Provisions that assign a governance body (e.g., agencies, boards, councils, working groups) responsibility to manage, coordinate, and facilitate cybersecurity activities across the state, including interagency collaboration, mutual aid mechanisms, operational support, and stakeholder partnerships. This includes duties to provide cybersecurity resources or assistance (e.g., technical guidance, direct response support, shared services) to specific stakeholders, such as public agencies, utilities, service providers, academic institutions, nonprofits, or small- to mid-sized businesses (SMBs).

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

Statewide Plans & Strategies	GOVERN	Provisions requiring government IT and cybersecurity agencies to prepare and publicly release statewide strategic plans for securing state information systems, often including requirements for periodic updates or new plans.
Disclosure Exemptions	GOVERN	Provisions exempting entities from public disclosure obligations and imposing confidentiality protections for sensitive cybersecurity information (e.g., incident details, security measures, policies, contracts, network schematics, hardware/software configurations, encryption information, cyber insurance coverage limits and deductible amounts, or incident response practices) when disclosure could enable unauthorized access or jeopardize security. Shields information from open meetings and public records requests.
Oversight	GOVERN	Provisions that require cybersecurity activities or decisions to be subject to formal oversight by an authorized entity (e.g., via review, approval, certification, testing, or audit) to verify compliance with required cybersecurity controls, governance standards, or cybersecurity frameworks.
Awareness Training	PROTECT	Provisions that require entities to provide cybersecurity awareness training, often with requirements to regularly update it.
Cyber Leadership & Representation	GOVERN	Requires entities to appoint or designate qualified cybersecurity personnel to oversee, implement, and enforce cybersecurity programs and/or serve as the primary point of contact (POC) for cybersecurity incidents or issues with relevant authorities. Also includes provisions requiring entities or governing bodies (e.g., offices, agencies, boards, councils, working groups) to appoint, include, or hire qualified cybersecurity personnel to ensure cybersecurity subject-matter expertise and risk perspectives are incorporated into decision-making.
Risk Assessment	IDENTIFY	Provisions that require entities to conduct cybersecurity risk or maturity assessments to identify risks to the security of information systems.
Governance Bodies	GOVERN	Establishes governance bodies (e.g., offices, agencies, boards, councils, working groups) or convenes work groups, advisory committees, councils, and boards to provide oversight, coordination, strategy, and standards development on cybersecurity risk of an organization or sector.
Incident Response Planning	RESPOND	Requires entities to develop, implement, and/or maintain written incident response plans for cybersecurity incidents, including requirements to update, review, or file plans with an oversight body.
Funding	GOVERN	Provisions that allocate, authorize, collect, or retain financial resources to support cybersecurity programs, services, upgrades, insurance, or workforce development. This includes appropriations, dedicated funds, expanding allowable uses of existing funds, cost-sharing mechanisms, and fee authorization.
Vulnerability Assessment and Penetration Testing	IDENTIFY	Provisions that require entities to complete cybersecurity vulnerability assessments and/or perform penetration tests, often on a periodic basis, to perform technical testing to discover exploitable weaknesses.

TRACKING CYBERSECURITY POLICY DEVELOPMENTS
ACROSS STATE LEGISLATURES

Incident Response Operations & Assistance	RESPOND	Requires entities, or permits the use of certain entities, to review and respond to reported cyber incidents by providing guidance, technical assistance, coordination, and other support.
Information Sharing	DETECT	Provisions that direct entities to establish, participate in, or support cybersecurity information sharing mechanisms (e.g., ISACs) to disseminate cyber threat information among relevant stakeholders.
Liability Safe Harbor	RECOVER	Provisions that create legal protections for entities or individuals that reduce, limit, or eliminate civil liability and penalties resulting from a cyber incident or data breach; exemptions or immunity applying when certain conditions are met (e.g., implementing “reasonable” cybersecurity safeguards, the absence of willful misconduct / gross negligence).
Incident Response Teams	RESPOND	Provisions that establish or require the creation of cybersecurity incident response teams or units responsible for coordinating state incident response and recovery efforts.
Business Continuity and Disaster Recovery Plan	RECOVER	Provisions that require entities to establish written business continuity and/or disaster recovery plans to ensure the continuity of operations and restore services following disruptions caused by cybersecurity incidents.
Exercises, Drills, & Testing	RESPOND	Provisions that require or encourage entities to conduct tabletop exercises or test their incident response plans to improve preparedness for cyberattacks.
Asset Inventory	IDENTIFY	Provisions that require entities to create and maintain an inventory of their information assets, such as systems, software, hardware, and/or related technology resources.
Cyber Harms & Remedies	Outside of NIST	Provisions that designate specific online activities as illegal or criminal offenses and establish corresponding penalties.
Vulnerability Disclosure Program (VDP)	PROTECT	Provisions that require organizations to set up and operate vulnerability disclosure programs (VDP) to enable security researchers to document and submit security vulnerabilities to them.
.gov Domain	PROTECT	Provisions that require government entities to host official websites using a .gov domain to strengthen the credibility and trustworthiness of government services and reduce impersonation-based cyberattacks, including typosquatting/typesquatting.

About the Authors

Shannon Pierson serves as the Senior Fellow of Public Interest Cybersecurity at UC Berkeley's Center for Long-Term Cybersecurity, where she conducts flagship research on defending low-resource organizations like nonprofits, municipalities, and schools from cyber attacks. Shannon also organizes the annual Cyber Civil Defense Summits, mission-based gatherings of cybersecurity academics, policymakers, state and federal government officials, hackers, and industry experts working to protect the nation's critical infrastructure from cyber attacks. She previously worked on Meta's Integrity, Investigations, and Intelligence (i3) team and has consulted for Microsoft and other major technology companies. She has also conducted cybersecurity and technology policy research at leading think tanks and research institutions, including the Helmholtz Center for Information Security, the German Marshall Fund, the Wilson Center, and the University of Cambridge's Minderoo Centre for Technology & Democracy.

Sree Varsha Bhanoor is a graduate student at the University of California, Berkeley, pursuing a Master's degree in Nutritional Sciences and Dietetics. Her research interests include health policy, digital health, and comparative analysis of state-level legislation of both technology and public health. She brings an interdisciplinary background spanning clinical nutrition, public health, and policy research.



CLTC

Center for Long-Term
Cybersecurity

UC Berkeley