2022 BSA State Legislative Summary: CYBERSECURITY

- States enacted five times more cybersecurity legislation and twice as many states evaluated cybersecurity bills in 2022 than in 2021.
- Of the 293 cybersecurity bills considered, 100 were introduced in 2022.
- Despite the increase in the bill volume and state interest, fewer bills were enacted in 2022 (26) compared with 2021 (30); Only 12 percent of state cybersecurity legislation was enacted in 2022.
- California, Massachusetts, Maryland, New Jersey, and New York introduced half (146) of all the cybersecurity bills in 2022.
- Most of the cybersecurity legislation addressed public sector concerns, as it did in 2021.
- Other cybersecurity bill topics include private sector cyber incident and data breach regulation, ransomware, cybersecurity criminal penalties, and workforce development and training.

Due in large part to the global pandemic, and similar to 2021, the majority of state cybersecurity legislation this session focused on regulating data breaches and cybersecurity incidents in the public sector or improving the public sector's cybersecurity infrastructure. Private sector cybersecurity and data breach legislation accounted for less than 8 percent of all state cybersecurity bills. Unlike in 2021 sessions, the states examined cybersecurity legislation on a variety of subjects including public and private sector cybersecurity incident and data breach, building cybersecurity infrastructure, ransomware, public utilities' cybersecurity, and task forces. Bills relating to ransomware, cyberattacks as emergencies, and criminal penalties were among the least likely to be introduced and enacted. Bills relating to state and local oversight and requirements were the most common to be enacted this year; yet only 12 percent of state cybersecurity bills introduced in 2022 were enacted.

This year, there were five times as many states that introduced cybersecurity legislation compared to 2021. Despite that, 146 of the 293 bills were introduced in Illinois, Maryland, Massachusetts, New Jersey, and New York. Despite the increase in the number of introductions, states actually enacted fewer cybersecurity laws in 2022 than in 2021.

Although, no states enacted legislation seeking to address the cybersecurity workforce challenges, California, Iowa, Illinois, Maryland, New Jersey, and Virginia bills. Two states, Tennessee and West Virginia, passed laws to increase penalties for cybersecurity crimes; nine other states have proposed bills to modify or introduce penalties for cybersecurity crimes including ransomware. Maryland,

Illinois, and Arizona enacted cybersecurity infrastructure legislation, but a similar measure was vetoed in Mississippi. Republican controlled legislatures were more likely to pass legislation to specifically address public sector cybersecurity incidents, whereas Democratic controlled legislatures were more likely to pass public sector data breach legislation. Of the commissions and task forces established in 2022, of note are Utah's Cybersecurity Commission on best practices, Rhode Island's cybersecurity review board for election systems, and Louisiana's Cybersecurity Redhibition Task Force.

As BSA looks ahead to 2023, cybersecurity legislation will continue to be a priority of state legislatures especially as American Reinvestment Plan Act (ARPA) dollars continue to be spent by states and the value of increasing the percentage of state budgets spent of cybersecurity. Over one-third of introduced bills did not receive a committee hearing in 2021 or 2022 and only 14 percent of cybersecurity legislation will carry over into 2023. Many of 2022's bills are likely to be re-introduced in January. However, given the pattern of the past two years, much of that legislation is likely to be enacted the second year of the two-year legislative cycle.

FOR MORE INFORMATION CONTACT:
Tom Foulkes | Senior Director, State Advocacy | tomf@bsa.org
Abigail Wilson | Manager, State Advocacy | abigailw@bsa.org