

Alaska SB258, introduced by Sen. Jesse Kiehl, is currently pending before the Senate Committee on Community and Regional Affairs. The bill language reads:

(a) A contract entered into by the state or a political subdivision of the state to license a software application designed to run on generally available desktop or server hardware may not limit the state's or political subdivision of the state's ability to install or run the software on desktop or server hardware of the state's or political subdivision of the state's choosing.

What is the purpose of SB258, and what problem does it address?

The purpose of SB258 is to ensure that when a state agency buys software, the contract doesn't artificially restrict where or how the software can be used. This means the agency should be free to run the software on whatever computer systems or cloud services work best for its needs, without being locked into one specific setup.

The need for this legislation arises out of growing concern among IT leaders, procurement offices, and regulators around the country (and the world) that restrictive licensing practices are leading to wasteful government spending, creating unnecessary cybersecurity vulnerabilities, and hindering technology modernization efforts. Restrictive licensing practices also lead to what's become known as "vendor-lock," in which purchasers of software are effectively prevented from switching between technology service providers as circumstances necessitate.

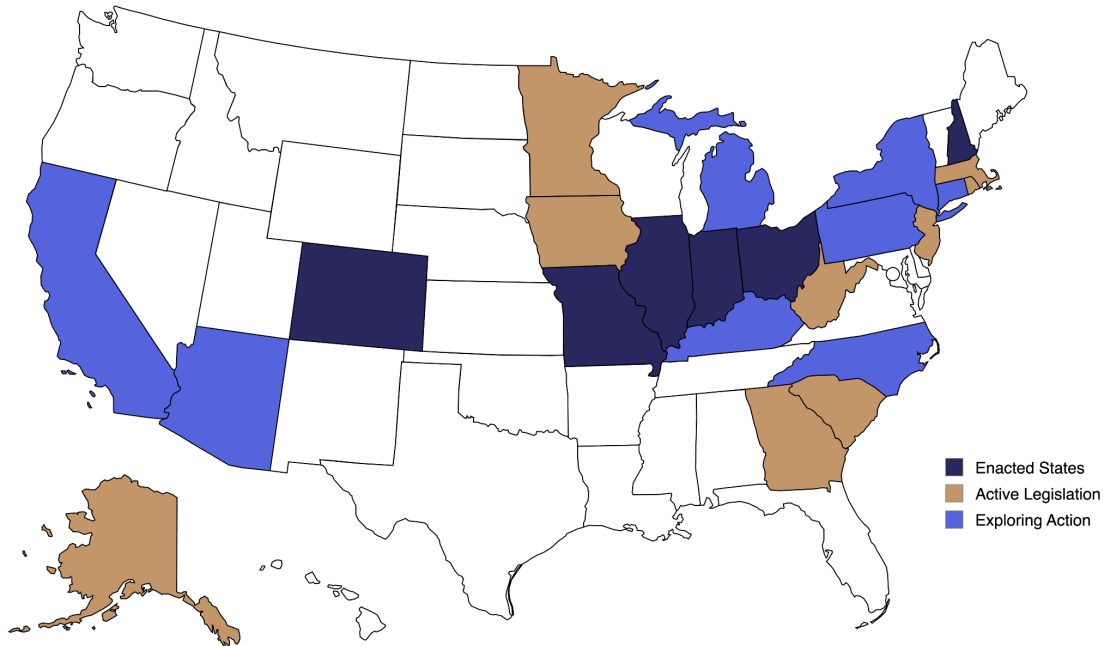
What are the benefits of passing SB258?

SB258 is a technology procurement good housekeeping bill:

- It applies only to future public procurement contracts.
- It does not constrain the state in its choice of software OR of cloud providers, instead empowering agencies to select the software vendors and hardware environments that best meet their business needs.
- It incentivizes vendor diversification, which strengthens cybersecurity.
- It does not ask the state to pick winners and losers— rather, it fosters healthy competition in the public cloud, which spurs innovation and lowers cost to taxpayers.
- It prioritizes the needs of the state over the preference of the software vendor.

What are other jurisdictions doing about restrictive software licensing?

To date, six states – Colorado, Missouri, Illinois, Indiana, Ohio, and New Hampshire – have enacted fair software licensing legislation. Three more – Massachusetts, New Jersey, and Georgia – have active fair software licensing bills pending before their legislatures. Other states are exploring action.



Is restrictive software licensing just a state issue?

No. This is an issue that has also generated notable attention at the federal level.

- In November of 2024, the [FTC launched](#) a broad investigation into one legacy software provider's licensing practices in its cloud business.
- In December of 2025, the [House of Representatives passed](#) the bipartisan SAMOSA Act, which directs agencies to assess current software inventory and management of contracts and licenses.
- In 2024, the [GAO issued a report](#) recommending federal agencies implement policies to lessen the effect of restrictive software practices, estimating *annual savings of over \$750M*.

[Amdt. 2167](#) of the 2023 National Defense Authorization Act (NDAA) called for an investigation into the impact of restrictive software licensing on the Defense Department.

Who supports Fair Software Licensing legislation?

FSL is supported by numerous technology industry associations, including:



**Computer & Communications
Industry Association**
Open Markets. Open Systems. Open Networks.



MYTH vs. FACT

ALASKA SB258 Fair Software Licensing (FSL)

MYTH: Alaska SB258, fair software licensing (FSL), legislation will reduce flexibility and negotiating power in state procurement contracts.

FACT: To the contrary, the very purpose of FSL is to allow the state greater flexibility in the way it deploys its software, and the hardware vendors— whether for on premises or cloud services— it chooses.

MYTH: SB258 prevents software vendors from differentiating pricing between public and private sector customers.

FACT: For many years, enterprise software vendors have created different pricing schemes to accommodate the frequently constrained budgets of their public sector customers. Nothing in FSL changes that. Rather, FSL prevents software vendors from penalizing customers who choose to run its software on third party hardware by imposing higher fees.

MYTH: SB258 dictates the type of contracts into which a software vendor may enter with its private sector customers.

FACT: FSL is narrowly tailored, and applies only to software licensing contracts entered into by “state agencies.” Similar to a multitude of other procurement requirements, FSL is meant to empower the agencies and protect taxpayer funds.

MYTH: SB258 will increase the cost of software and related services.

FACT: FSL fosters competition amongst the state’s infrastructure hardware vendors— whether on premises or in the cloud. More competition means: better services and lower prices. When state agencies are free to choose the software that best fit their needs, vendors are incentivized to offer high quality goods and services at competitive prices.

MYTH: SB258 will require the state to review existing vendor contracts for compliance.

FACT: Again, the scope of SB258 is narrowly tailored, and applies only to the execution of future contracts between state agencies and their software vendors. Moreover, the language only applies to software “designed to run on generally available desktop or service hardware” — a limited class of the state’s vendor contracts. Nothing in the legislative language implicates existing contracts or requires retroactive review of previously executed agreements.

MYTH: FSL prevents states from realizing efficiencies by streamlining software and infrastructure contracts with single providers.

FACT: FSL empowers the state to run the software it pays for on the hardware of its choice. State agencies are free to streamline or differentiate providers, according to their business needs. Importantly, the State makes these decisions, not a software provider.

MYTH: FSL raises serious cybersecurity concerns, because it forces customers to use multiple vendors instead of a single, trusted partner.

FACT: The opposite is true. Dependence on any single software provider can be perilous for cyberresiliency. FSL frees the state to choose the software and hardware combinations that make the most sense for the security of their constituents.

MYTH: FSL is aimed at penalizing specific technology providers to the benefit of others, rather than toward establishing industry standards.

FACT: FSL creates a level playing field for all cloud providers to offer their services.