Testimony from Karla Jones, Sr. Director, Federalism, Homeland Security and International Relations
American Legislative Exchange Council
Re: Maryland HB894

I am submitting this testimony on behalf of the American Legislative Exchange Council (ALEC), America's largest nonprofit, nonpartisan organization of state lawmakers dedicated to the principles of limited government, free markets and federalism to offer nonpartisan research and analysis on HB894, *An Act concerning Procurement – Scrutinized Entities Prohibition* which calls for a prohibition on state procurement contracts with entities owned, operated or controlled by the governments of countries that are subject to an embargo under the International Traffic in Arms Regulations (ITAR).

HB894 aims to protect the state from threats, infiltration, and influence posed by US adversaries such as the People's Republic of China (PRC). The PRC is widely recognized as America's greatest and most complicated national and homeland security challenge. And while there is a robust, although not infallible, federal national security infrastructure responsible for protecting the nation, the states, including Maryland, often lack such safeguards making them particularly vulnerable to PRC and other nations of concern's homeland security threats, interference, and influence. The states' lack of readiness compromises US national security as well their own.

In the case of technology equipment, U.S. state governments have purchased millions of dollars' worth of technology manufactured by companies beholden to Beijing to spy on Americans and seize data. Many of these companies have been banned outright by the US federal government or by U.S. military and intelligence agencies, in part because the PRC's 2017 National Intelligence Law obligates all Chinese companies to cooperate with any Chinese government directive to hand over information in their possession. That means that Beijing can demand any U.S. user data and sensitive knowledge—including health and financial data.

While federal policy directs information security for federal agencies, states determine their own information security standards. There is no central state or local vetting agency, so state and local governments lack the expertise and the infrastructure to mitigate the risk. Furthermore, the National Association of State Procurement Officers (NASPO), which is regarded as the "gate keeper" for state government purchasing across the United States, does not account for security vulnerabilities.

States have begun to recognize these vulnerabilities. In 2023, nine states passed laws prohibiting procurement contracts for technology manufactured by firms with ties to the PRC and this legislative session, approximately eight states are currently considering bills, many with broad, bipartisan support.

Earlier this year, FBI Director Chris Wray warned Congress (access his remarks here) about Chinese Communist Party (CCP) hackers targeting American infrastructure and preparing to "wreak havoc and cause real-world harm to American citizens and communities." In another new item, the *Washington Post* reported on China's strategy of targeting state and local officials to get around tensions in Washington. In March 2022, the *AP* reported that at least six state governments were hacked by the Chinese government. In July of the same year, the U.S. National Counterintelligence and Security Center issued a notice warning of the PRC's aggressive campaign to exert influence at the state and local levels. The notice provided specific detail on China's strategy to collect personal information on state and local leaders and their associates.

I am sorry that I am not able to be there as you consider these important policy ideas , however, I am happy that Maryland is working to address these security vulnerabilities and invite you to contact me with any questions at kjones@alec.org.