Testimony from Karla Jones, Vice President, ALEC Center for International Freedom
American Legislative Exchange Council
Re: Maryland HB188

Thank you for the invitation to offer testimony. I am Karla Jones, Vice President of the American Legislative Exchange Council's or ALEC's Center for International Freedom. This testimony is being submitted on behalf of 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 HB188, *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).

HB188's use of the ITAR list as a guide is a sound way to protect the state from threats, infiltration, and influence posed by US adversaries, including but not limited to the People's Republic of China (PRC). It is important to emphasize, however, that the threat posed by China is unique and more challenging than other ITAR countries of concern due to factors ranging from manufacturing and foreign direct investment (FDI) capabilities and China's already significant US market share for technology equipment. 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 homeland security threats, interference, and influence by the PRC and other nations of concern. 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. Ensuring that third party vendors are also vetted is important as well.

States have begun to address these vulnerabilities. In 2023, nine states passed laws prohibiting procurement contracts for technology manufactured by firms with ties to the PRC and in 2024, Maine, Nebraska, Utah and New Hampshire adopted similar legislation. Often the legislation got broad, bipartisan support, and in the case of Nebraska, the legislation was championed by a Democrat, Senator Eliot Bostar. States also recognize that not procuring questionable technology in the first place is less expensive than replacing it later when security

problems become apparent. The challenge is so pervasive that in the most recent National Defense Authorization Act (NDAA), $3 billion dollars was allocated just for telecommunications rip and replace programs. Over the last decade, the Pentagon had to replace Lexmark printers that it acquired as well as Lenovo laptops and the US Air Force required Raytheon to replace IBM servers following Lenovo's acquisition of the company.

In terms of the threat, last year, then FBI Director Christopher 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." Later in 2024 we learned about Salt Typhoon, which Virginia Senator Mark Warner described as "the worst telecommunications hack in US history." In late December the Foundation for Defense of Democracy released an alarming report about the PRC's subnational reach. 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 commend you for considering these important policy ideas, applaud Maryland for working to address these security vulnerabilities and invite your questions.