STATE OF KANSAS
HOUSE OF REPRESENTATIVES

STATE CAPITOL
TOPEKA, KANSAS 66612
(785) 296-7695
chris.croft@house.ks.gov

8909 W. 148TH TERRACE
OVERLAND PARK, KANSAS 66221

CHRISTOPHER D. CROFT
8TH DISTRICT

Thank you, Chairman, Ranking Member, and Members of the Committee, for giving me the opportunity to testify in support of HB 2293 today.

Modern warfare and surveillance have expanded beyond the physical, integrating advanced technologies such as drones into their core operations. While these devices offer significant benefits for civilian, law enforcement, and military applications, they also present a vulnerability when their critical components are sourced from nations with malicious intentions.

Countries of concern, as defined in HB 2293, including China, Russia, Iran, North Korea, Cuba, and Venezuela, have demonstrated a pattern of behavior that threatens the United States' security and technological sovereignty. Their efforts to dominate the technological sphere and gather intelligence through various means directly challenge our national security.

As we discuss in every conversation surrounding the issue, nations like China can demand that all data be turned over to the government. This puts our citizens at risk when advanced drone technology can have their data taken by an adversarial government with the stroke of a pen. Tools our agencies purchase to keep our citizens safe can and will suddenly become the way other nations collect our sensitive data.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have sounded the alarm on the risks tied to Unmanned Aircraft Systems (UAS) made in China. Bryan A. Vorndran, Assistant Director of the FBI's Cyber Division, put it bluntly: 'Without proper safeguards, the widespread use of Chinese-manufactured UAS across our nation's critical sectors poses a serious national security threat—opening the door to unauthorized access to sensitive systems and data.'

By acquiring critical drone technology components from these countries, we inadvertently expose ourselves to espionage, sabotage, and other forms of cyber warfare. This legislation aims to mitigate this risk by prohibiting state and local governments from purchasing,

acquiring, or using drones and related services or equipment with critical components produced or owned by any foreign principal from these nations.

This legislation is also consistent with President Trump's recently released America First Investment Policy, which warns of these threats and promises "the United States will reduce the exploitation of public and private sector capital, technology, and technical knowledge by foreign adversaries such as the PRC." It further highlights the numerous advantages of shifting U.S. investment away from those counties seeking to exploit and undermine the United States.

My testimony today is a call to action against a specific technological threat and a broader appeal for vigilance and resilience in our ongoing battle to safeguard our state and nation from foreign adversaries. The prudent measures outlined in HB 2293 represent another step forward in our collective defense, ensuring that the advancements we embrace today will not become the vulnerabilities our adversaries exploit tomorrow.

You may recall that we introduced a similar bill last year. To address some of the concerns raised during the last session, we've made a few key adjustments. First, this bill is prospective - allowing government agencies to continue using equipment acquired before July 1, 2025. However, going forward, agencies will be prohibited from purchasing new or replacement equipment and components from any foreign principal, unless that entity has already been vetted and cleared of security risks or has an active national security agreement in place as of July 1, 2025. The bill also explicitly includes software within the definition of critical components. Additionally, it still includes the carefully crafted exception process, managed by the Secretary of Administration in collaboration with the Adjutant General, to ensure that Kansas's safety and security remain our top priorities.

I urge the committee to support HB 2293 reinforcing our commitment to the security of our technological infrastructure for the safety and privacy of our citizens. Thank you again for the opportunity to testify on this critical issue.

Respectfully,

Representative Chris Croft

House Majority Leader