Chairman Ghanbari, Vice Chairman Plummer, Ranking Member Thomas, and Members of the committee, thank you for the opportunity to testify on H.B. 472, groundbreaking legislation that adopts the highest cybersecurity certification standards and enhanced vendor risk assessment for voting systems in the country to include adoption of Blockchain digital ledger in our voter registration databases.

My name is Marcell Strbich, I live in Dayton and am a 20-year retired Air Force intelligence officer with varied operational, command and combat experience. My prior work assessing supply chain risk management and threat analysis for leading Air Force weapons systems informs my testimony. The views expressed in this testimony are mine alone and not those of the U.S. Air Force or Dept of Defense.

Before I begin, the core theme I want to raise to your attention in the bill is its attempt to drive at and solve specific solutions to 20-year systemic issues and security standard deficiencies ranging in key areas of election administration and voting systems. Whether you agree or not with our analysis or with Ohio SoS's assertion, "If you don't have an accurate voter list, your not going to have an honest election," it is vital that we take tangible steps to secure our election infrastructure and ensure only eligible electors by law vote in Ohio.

For Ohio to maintain or exceed its election "Gold Standard" reputation, this appropriately assigned committee can advance critical and long-standing election shortfalls in all the bill's main categories spanning *Voter Registration Data Validation, Independent Auditing of Voter Registration Databases, Identity and Citizenship Verification, Enhanced Vendor Cybersecurity Standards, Election Administration and the County Voting System Backup*. Today's proponents will cover each of these areas.

2024 Critical Transparency Gaps and Voting System Vulnerabilities

With that said the federal election just six months away. Targeting of voting system infrastructure by nation-state actors or rogue insiders remains a serious threat. Recently during an interview Sec of State Blinken noted evidence of Chinese attempts to influence and interfere with our 2024 elections. This claim is preceded by the FBI Director who briefed Congress and our State's own Butler County Sheriff that threat streams not seen since 9/11 are in play for 2024. With no ability to *independently verify voting system design, developer security practices and supply chain foreign ownership control and influence*, it is not possible to assess the degree of vulnerability of our election systems nor assert an acceptable risk posture for our upcoming elections.

Vendors Present Primary Points of Attack into Election Infrastructure

The **2018 U.S. Senate Intelligence Committee Report titled, "Russian Targeting of Election Infrastructure During the 2016 Election,"** detailed widespread attempts and instances of system breaches, with confirmed access into several State's voter registration databases. The 2018 Senate report highlighted the fact that private vendors play a central role in American elections and are considered a "prime target", yet there remains "very little insight into the cyber security practices of election vendors," A separate **2019 report by the Brennan Center for Justice titled "A Framework for Election Vendor Oversight,"** reinforces the U.S. Senate findings on vendor vulnerabilities by asserting voting system "vendors, unlike those in other sectors that the federal government has designated as critical infrastructure, receive little or no federal review."

Ohio's Review and Approval Process for Voting System Certification

Despite the evolved and elevated security threat, Ohio's election laws addressing voting systems certification requirements remain unchanged over 20 years. The focus for voting system certification is not based on identifying and correcting system vulnerabilities upfront, rather its emphasis is on functional capability and operability features. Since 2004, State law deferred responsibility and authority for testing specification and certification standards for voting machines, markers, and tabulators, to the Election Assistance Commission, a non-binding federal advisory agency with no enforcement authority over vendors that violate federal guidelines. All other voting system products or services in use across Ohio, to include *voter registration databases, ePollbooks or election reporting services, remain without federal or State certification standards*.

Ohio Certifying Election System "Critical Infrastructure" to a 2005 Security Standard Baseline

To date, because of a lack of election vendor oversight and enforcement mechanisms absent at the Federal and State-level, several voting system vendors when given the option to certify their systems to a 2021 security standard per Ohio law, chose to certify their election management software just two weeks prior to the EAC extended deadline-to a 2005 security standard in advance of the 2024 election. These circumstances raise doubt as to the oversight, accountability and seriousness for which those responsible for securing our election "critical infrastructure" assume their role. This Committee charged with protecting our Homeland must act to correct this security standard deficiency and pass expected vendor certifiability requirement standards detailed in H.B. 472.

How could Ohioan's have confidence in the integrity of their voting system knowing the system security test baseline originated two years before the first iPhone? Until we enact proven risk management framework standards for our voting systems, we cannot claim that our election systems infrastructure is secure.

The Solution Adopts All 5 Cyber Core Functions into Risk Management Framework

H.B. 472 establishes and applies across the board enhanced voting system vendor standards implements independent 3rd party reviews in the areas of design, security and test requirements planning and software development practices. *Ohio becomes the 1st State to incorporate all five core cyber functions* of 1.) Identifying 2.) Protecting 3.) Detecting 4.) Responding 5.) Recovering as part of its risk management framework. Currently, Ohio accomplishes three of these core cyber functions.

This legislation is another historic opportunity for Ohio to lead other States and reverse the 20-year trend of technology outpacing policy. **This committee must act to safeguard our election system "critical infrastructure" by approving independent security assessment reviews of voting systems to a military grade level review**. In doing so, Ohio will be the first State postured to realize industry's upcoming pivot toward open-source election software and capitalize on its benefits.