Texas Public POLICY FOUNDATION
BETTER TECH FOR TOMORROW

TEXAS CYBER COMMAND: STRATEGICALLY POSITIONING TEXAS FOR THE FUTURE OF WARFARE

21ST CENTURY WARFARE: THE GROWING NEED FOR A DEVOTED CYBER DIVISION

Texas is the envy of the world with its critical assets. In energy, health, communications, and high tech sectors, the Lone Star State's prowess with critical infrastructure makes it a remarkably hot target for hostile foreign adversaries like Russia, China, and Iran. Notably, there has been a 5,220% increase in cyberattacks in the US over the last two decades, with nearly 2/3 of critical infrastructure attacks levied by state-affiliated, hostile actors. The frequency and sophistication of attacks continues to grow as society becomes more digital, and the emergence of new AI tools enhances the capability, motivation, and opportunity for threat actors to successfully infiltrate targets.

The Texas Cyber Command aims to:

- Establish a purpose-built, standalone cyber agency
- Position Texas as a global leader for cyber response and resilience
- Leverage regional strengths of San Antonio - UTSA, private sector, Air Force, FBI, and more - to perpetually refine and bolster operational posture of Texas Cyber Command

Last year, the West Texas town of Muleshoe had a water tower attacked by Russian cyberterrorists, concluding that the fear of nations remotely poisoning our water supply is no longer a far cry. The aftermath of this attack revealed a common theme: uncertainty as to which authority serves as point of contact for rapid response and clean up. After attacks, critical infrastructure systems often work with more than a half-dozen agencies, receiving conflicting advice and costing more taxpayer dollars as a result of duplicative work. This phenomenon, called stovepiping, has historically resulted in compartmentalization, inefficient data sharing, and, importantly, reactivity rather than proactivity.

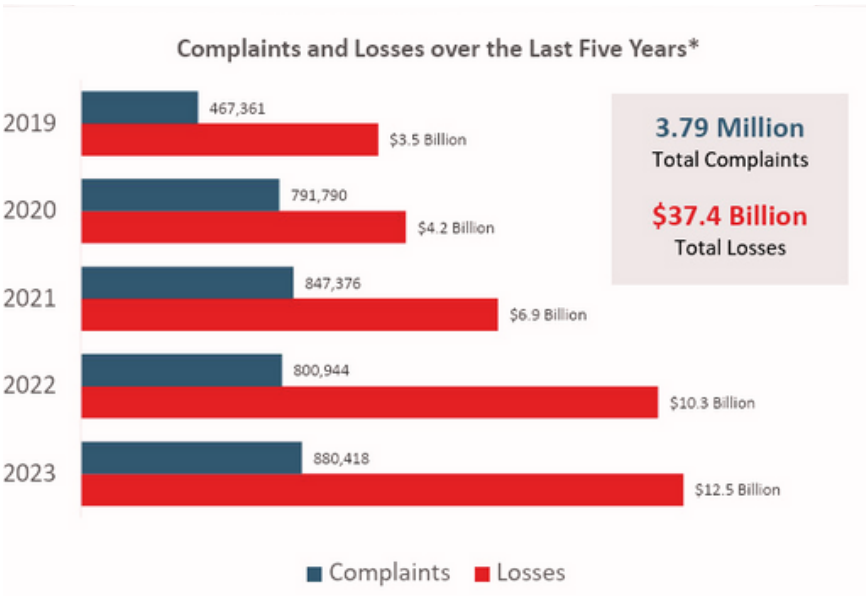
In 2018, the Trump Administration took decisive action to address this problem at the federal level, creating the Cybersecurity and Infrastructure Security Agency (CISA). With Gov. Greg Abbott's emergency declaration to establish a Texas Cyber Command, the Lone Star State can take similar action to create symbiosis between cyber authorities and specialists and more cost-effectively secure our critical assets.

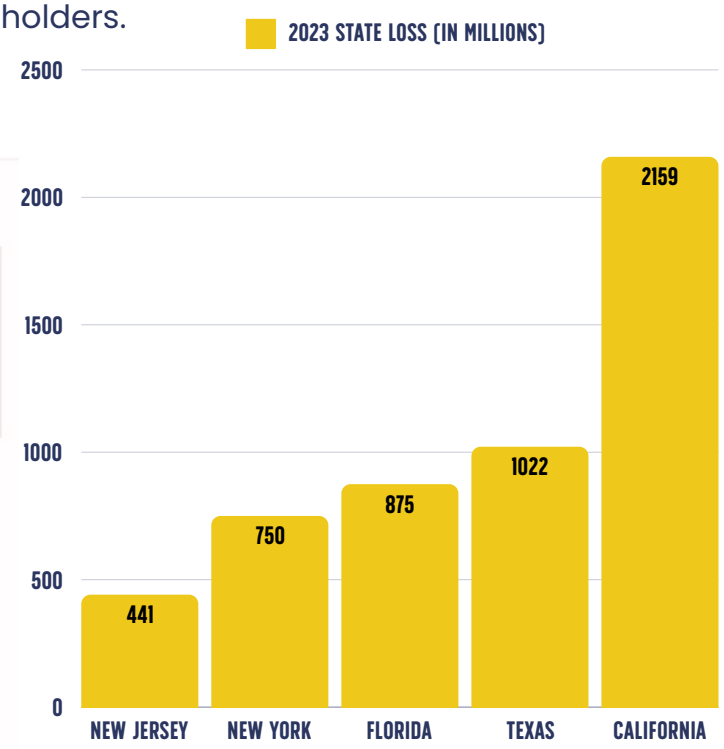
THE CASE FOR A NEW TEXAS CYBER COMMAND

- Historically, as new military capabilities are in their infancy, they are housed under existing branches. It was not until after WWII - after America initially struggled to compete with the German Luftwaffe - that the Air Force left the purview of the Army and was established as its own branch. We are at a similar inflection point with cyber warfare, and it is time for Texas to create a standalone, singular state cyber authority.
- Critical infrastructure operators throughout the state have requested more resources and support to prevent and respond to cyber incidents. The Texas Cyber Command will leverage state universities, Regional Security Operations Centers, the private sector, and government authorities to strengthen and streamline Texas' cyber mission.
- With the rapid digitalization of government and critical infrastructure, agencies like the Department of Information Resources (DIR) have stepped into the breach absent a singular state cyber authority. This has resulted in Texas agencies expanding their scope of responsibilities, sometimes at the expense of core functions given resource and personnel limitations. Having the Texas Cyber Command will both allow agencies to fixate on perfecting their core functions, while providing support and institutional knowledge where appropriate.

LEGISLATIVE APPROACH

- Rep. Giovanni Capriglione and Sen. Tan Parker's bill will establish key functions of the Texas Cyber Command, clarify the collaborative model, and equip the agency with the appropriate resources to protect and defend Texas from rogue outlets across the globe.
- San Antonio will serve as the hub, leveraging the incredible capabilities of the University of Texas at San Antonio and other local stakeholders.





These charts represent cyber crimes reported to the FBI's Internet Crime Complaint Center. Of note, actual numbers are likely significantly higher due to underreporting.