



What Sid Miller Omits: Data Centers Are Vital to National Security and Public Safety

By Steven McCraw, TNSC Security Expert

Commissioner Sid Miller is one of the most vocal critics of data centers in Texas. While he raises some legitimate concerns, such as the potential strain on water resources, prime farmland, and the electric grid, his comments fail to address a larger issue.

What is missing from the Commissioner's criticism is any serious discussion about the consequences of *not* building data centers at the scale necessary to keep Texas and the United States competitive and our sensitive information and critical infrastructures safe. Even the Commissioner is dependent upon data centers to broadcast his public statements on his Facebook, Instagram, YouTube, and X accounts, including his criticism of data centers.

Miller also implies that he doesn't have confidence in the Governor or our Legislature to protect Texas or Texans. I am confident that Governor Greg Abbott and the Texas Legislature will provide the proper oversight needed to manage our natural resources and protect the electric grid.

Secure domestic data centers are essential for protecting our sensitive information, safeguarding critical infrastructure, including 911 systems and the electric grid, and maintaining America's technological edge against adversarial nations. These facilities process and store our daily digital transactions: emails, text messages, search histories, bank records, medical histories, addresses, Social Security numbers, and even the viewing habits of our children. Data centers operated outside the United States pose unacceptable risks to American information, and those within the United States that rely on hardware or software from adversarial nations, particularly China, also pose serious risks.

According to the 2026 Annual Threat Assessment of the U.S. Intelligence Community, China is the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks. Joint FBI and CISA reporting further documents how China state-sponsored actors have compromised U.S. telecommunications providers to steal subscriber information and network data. Russian ransomware groups and other cyber criminals have repeatedly targeted American organizations, stealing vast amounts of personally identifiable information. A successful cyber-attack on domestic data centers would undermine daily activities and threaten other vital sectors, including the electric grid, as demonstrated by the 2015 and 2016 Russian cyberattacks on Ukraine's power grid.

Texas has a unique opportunity to become the nation's premier hub for this critical technology. We benefit from abundant energy resources, land, a high-tech workforce, a robust cybersecurity network, and enabling state legislation. The 16th Air Force cyber warfare hub, the new Texas Cyber Command at UTSA, strong university cybersecurity programs, Texas's robust critical-infrastructure safeguards, and our own independent electric grid provide protections that simply do not exist in other states.

We are in a high-stakes AI arms race. Sufficient secure data-center capacity is a national security imperative. China has made clear its intention to become the global AI leader by 2030. Ceding ground in this strategic competition would hand adversaries dominance in military technology, intelligence, cyber capabilities, and economic growth.

By supporting responsible data-center development that fully complies with Senate Bill 6 and all applicable state requirements, which ensure adequate generation for Texas homes, cost allocation for grid upgrades, and environmental safeguards, Texas can strengthen national security, protect our families' information and infrastructure, and secure America's leadership in the technologies needed for a prosperous future.

Steven C. McCraw is the Former Director, Texas Department of Public Safety (2009–2024) and Former Assistant Director, FBI
