



Interim Report

TO THE EIGHTY-NINTH TEXAS LEGISLATURE

HOUSE SELECT COMMITTEE ON SECURING TEXAS
FROM HOSTILE FOREIGN ORGANIZATIONS

DECEMBER 2024

**HOUSE COMMITTEE ON SECURING TEXAS FROM HOSTILE FOREIGN
ORGANIZATIONS
TEXAS HOUSE OF REPRESENTATIVES
INTERIM REPORT 2024**

**A REPORT TO THE
HOUSE OF REPRESENTATIVES
89TH TEXAS LEGISLATURE**

**COLE HEFNER
CHAIRMAN**

**COMMITTEE CLERK
HARRISON SALTER**



Committee On
Securing Texas from Hostile Foreign Organizations

December 4, 2024

Cole Hefner
Chairman


P.O. Box 2910
Austin, Texas 78768-2910

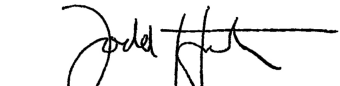
The Honorable Dade Phelan
Speaker, Texas House of Representatives
Members of the Texas House of Representatives
Texas State Capitol, Rm. 2W.13
Austin, Texas 78701

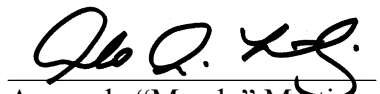
Dear Mr. Speaker and Fellow Members:

The Committee on Securing Texas from Hostile Foreign Organizations of the Eighty-eighth Legislature hereby submits its interim report including recommendations for consideration by the Eighty-ninth Legislature.

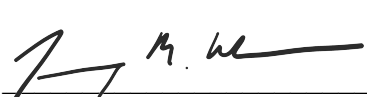
Respectfully submitted,


Cole Hefner


Todd Hunter


Armando "Mando" Martinez


Angie Chen Button


Terry Wilson


Cody Harris


Ray Lopez

TABLE OF CONTENTS

TABLE OF CONTENTS.....	3
OVERVIEW	4
BACKGROUND	5
SUMMARY OF COMMITTEE ACTION.....	6
<i>COMMITTEE HEARING ON JULY 24TH, 2024 – AUSTIN, TEXAS</i>	6
<i>COMMITTEE HEARING ON SEPTEMBER 10TH, 2024 – TYLER, TEXAS</i>	20
<i>COMMITTEE HEARING ON OCTOBER 16TH, 2024 – AUSTIN, TEXAS</i>	36
RECOMMENDATIONS.....	40
RELEVANT NON-COMMITTEE ACTIONS	48

OVERVIEW

Creation of Committee

By proclamation dated May 6, 2024, Dade Phelan, Speaker of the House of Representatives, formed the House Select Committee on Securing Texas from Hostile Foreign Organizations. Speaker Phelan appointed the following seven members to the House Select Committee on Securing Texas from Hostile Foreign Organizations (the Committee): Chair Cole Hefner, Todd Hunter, Armando “Mando” Martinez, Angie Chen Button, Terry Wilson, Cody Harris, and Ray Lopez.

Purpose and Jurisdiction

The Committee was created to:

- (1) Study the threat posed by hostile foreign organizations and related entities on the Texas economy, security, and values;
- (2) Evaluate the ways in which hostile foreign organizations acquire property, including real property, in Texas as well as the attendant risks. Recommend policy changes to mitigate the risks posed by ownership of Texas assets by hostile foreign organizations; and
- (3) Examine rates of intellectual property (IP) theft in the state and identify the industries most impacted. Make recommendations to better secure the IP of government and businesses operating in the state and ensure Texas remains competitive in the face of economic aggression by hostile foreign organizations.

Reporting

The Committee was directed to submit a final report in the same manner as an interim study committee under Rule 4, Section 61, Rules of the House of Representatives.

BACKGROUND

Objectives

In order to fulfill the intended purpose of this committee, several specific objectives were identified as necessary to complete:

- Identify hostile foreign countries and organizations that are actively taking actions to harm Texas
- Assess the current effectiveness of defense mechanisms currently in place to prevent this harm
- Identify existing vulnerabilities that are currently being exploited or may be exploited in the future by hostile foreign entities
- Conduct a risk-based prioritization of existing vulnerabilities
- Make legislative recommendations to address vulnerabilities presenting the highest risk and reduce or eliminate them

Committee Actions

Speaker Phelan created this Committee because the threat to Texas from hostile foreign nations is increasing rapidly. Threats to Texas' security are growing daily, most notably from foreign agents attempting to acquire land on behalf of hostile foreign governments and coordinated cyber attacks from hostile foreign actors on state and local systems. These may be the most visible, but many other threats exist. While the federal government is beginning to recognize this threat and is slowly taking action on this issue, Texas must act swiftly and decisively to form our own solutions and secure our state.

To swiftly assess these threats and identify effective solutions, the Committee held three public hearings during the interim. At these hearings, the Committee heard invited testimony from national security experts, cybersecurity experts, representatives of relevant associations, and the public. These hearings and the testimony during the process played a significant role in guiding the recommendations in the Committee's report.

The entirety of this Committee's work has been to identify areas of vulnerability and recommend specific actions to protect our state and her sovereignty. The actions recommended in this report are intended to protect against actions by foreign governments who seek to do harm to our state and our citizens. None of the recommendations within this report impugn a person on the basis of national origin. To the contrary, the recommendations herein are essential for the preservation of liberty and the rights of all persons in Texas to pursue the American dream. This committee welcomes people of all nationalities who immigrate to our country legally in pursuit of safety, security, and prosperity.

SUMMARY OF COMMITTEE ACTION

COMMITTEE HEARING ON JULY 24TH, 2024 – AUSTIN, TEXAS

The Committee held a public hearing on July 24th, 2024, with invited testimony.

The individuals listed below provided testimony to the Committee on this charge.

Public Hearing: July 24th, 2024

Witness List: July 24th, 2024 – Austin, Texas, Capitol Extension E2.016, at 10:00 AM

Panel 1

- Michael Lucci, State Armor
- Brian Cavanaugh, American Global Strategies
- Christopher Holton, Center for Security Policy

Panel 2

- David Alders, Texas Forestry Association
- JD Hale, Texas Association of Builders
- Mickey Edwards, Texas Farm Bureau

Panel 3

- Chuck Devore, Texas Public Policy Foundation
- Kenneth Nunnenkamp, Morgan, Lewis & Bockius LLP
- Gerald Klassen, Texas Real Estate Research Center at Texas A&M University

Panel 4

- Jef Conn, Texas Association of Realtors
- Mike Wong, Asian American Real Estate Association
- Aaron Day, Texas Land and Title Association

Panel 5

- Celeste Embrey, Texas Bankers Association
- Meredyth Fowler, Texas Mortgage Bankers Association

Panel 6

- Michael Lozano, Permian Basin Petroleum Association
- Cory Pomeroy, Texas Oil and Gas Association
- Mark Stover, Texas Solar Power Association

The information below is largely based on the oral and written testimony of the individuals and organizations above.

Michael Lucci, State Armor

Michael Lucci is the founder, CEO, and Chairman of State Armor, which he created to develop and enact state solutions to global security threats. State Armor advances state policies to protect state critical infrastructure, build the supply chains of freedom, and cease malicious foreign influence operations. At State Armor, Mr. Lucci synthesizes a unique understanding of global affairs with deep experience in state policymaking. For more than a decade, he has worked with both state and federal leaders to achieve State Armor's mission.

Mr. Lucci believes that a whole-of-government American response is needed to counter unprecedented global threats and ensure a free and peaceful 21st century. Accordingly, Mr. Lucci and State Armor work to advise states on policies to address growing international threats focused on infrastructure, building resilient supply chains, ending technological reliance on Chinese based companies, and ending adversarial influence operations. Mr. Lucci believes the Chinese Communist Party (CCP) represents the greatest international threat to the country, which most of his testimony was focused on.

Mr. Lucci discussed Chinese involvement in manufacturing chemical precursors for fentanyl-overdoses of which were the leading cause of death among those of military age. The US House Select Committee on the Chinese Communist Party's findings on the CCP's involvement in fentanyl trafficking which focused on the US, but also extended to other states they thought were threats- noting that the product is illegal to sell domestically while exports are subsidized by the government.

According to Mr. Lucci, the CCP is pre-positioning assets in the US to disrupt every normal function of civilian life if a conflict arose. Mr. Lucci emphasized, they the Chinese strategy of disruption is an "everything everywhere all at once" strategy. Mr. Lucci stated that the Chinese people were the chief victims of the CCP, both in China and abroad. Mr. Lucci described "Operation Fox Hunt," a CCP operation run in New York City where the Chinese government used fake police stations to detain and repatriate Chinese dissidents who had receive asylum. The CCP has shifted from a strategy of peaceful co-existence to one of attempting to become the leading global power.

Mr. Lucci discussed the Chinese government's strategy for influencing local and state governments in order to make them dependent on their companies as essentially client states. According to Mr. Lucci, a CNN article from 2022 demonstrated that nearly all of the communications grid in New England had been running on Huawei technology mostly near US nuclear missile silos which would allow them to intercept their military signals. Mr. Lucci explained that the same is true in Colorado and Wyoming. New England has decided to remove all equipment and has foregone federal replacement subsidies to do so faster. It is also important to note the CCP is attempting to create dependence on their companies for DNA sequencing technologies, drones, port cranes, connectivity devices for cars, and traffic cameras. Mr. Lucci believes that the CCP wants to dominate in areas where a technology has both civilian and military conflict involving China.

In 2017, a National Security law passed in China requiring all Chinese companies to collect data and transmit it back to government entities in Beijing, which is referred to as "spy and lie". Mr. Lucci explained the difference between laws adopted in Texas and those in other states is based on differences in economic drivers of those states.

Communist China is not the only country that threatens homeland security. Russia and North Korea are similar in nature, though they are considered disorganized and conducting most operation through organized crime groups. In addition to Russia and North Korea, Iran is a concern with regard to water infrastructure. Mr. Lucci explained an agreement active during the Cold War which was intended to allow the United States and the USSR to monitor the military activity of each other, but the USSR has begun to use the agreement for monitoring civilian infrastructure. It is important to note that foreign powers were not looking at surveillance traditionally but were mostly doing so through cybercrime.

Mr. Lucci noted that Texas has led on important issues related to security against Chinese influence. Specifically, he mentioned the Lone Star Infrastructure Protection Act (“LSIPA,”) passed in 2021, which he believes should be a national model. The LSIPA prohibits certain foreign governments, including Communist China, from connecting either physically or remotely into critical Texas infrastructure. The State of Texas has also adopted a cybersecurity plan that Mr. Lucci uses as a model for other states.

American Global Strategies

Brain J. Cavanaugh is the Senior Vice President at American Global Strategies LLC, an international strategic advisory firm. Mr. Cavanaugh focuses on critical infrastructure security and resilience, crisis management planning, continuity of operations, and disaster response and recovery operations.

Mr. Cavanaugh brings extensive experience from serving in the White House as the Special Assistant to the President for National Security Affairs and Senior Director for Resilience Policy on the National Security Council (NSC). During his three-year tenure at the NSC, Mr. Cavanaugh served as the National Continuity Coordinator, Deputy National Policy Coordinator for the Defense Production Act during the response to 2019 novel coronavirus (COVID-19) pandemic, and the White House representative to the President’s National Infrastructure Advisory Council.

Mr. Cavanaugh stated that the Chinese Communist Party represents an existential threat and is actively engaged in conflict with the United States, but their conflict is not traditional in nature. Mr. Cavanaugh concurred with Mr. Lucci that Chinese citizens are the greatest victims of their country’s authoritarian regime which included living in a surveillance state with social credit used to control behavior.

Center for Security Policy

Christopher Holton is a Senior Analyst and Director for State Outreach Center for Security Policy. During Mr. Holton’s 20 plus years with the Center, he has directed the Center’s Divest Terror Initiative and Shariah Risk Due Diligence Program. He has been involved in education and outreach in more than two dozen states regarding divestment of taxpayer supported pension systems from foreign companies that do business with the Islamic Republic of Iran, the Islamic Republic of Sudan, and the Syrian Arab Republic. In addition, he has been involved in state level counterterrorism and coutershariah initiatives in dozens of states.

Mr. Holten was a co-author of *War Footing*, published by the US Naval Institute Press and co-author of *Shariah, Law and Financial Jihad: How Should America Respond?* In 2015, Mr. Holten co-authored the *Gulen Movement: Turkey's Islamic Supremacist Cult and Its Contribution to Civilization Jihad in America*.

In testimony regarding foreign adversary land ownership, Christopher Holton outlined the ways state legislatures are taking action to prevent foreign adversaries like Communist China, Russia, North Korea, and Iran from acquiring property, particularly near sensitive U.S. infrastructure. Noting that legislation varies across states, Holton emphasized initiatives targeting agricultural land and land near military installations to safeguard food security and national defense.

Holton highlighted several specific threats from Communist China, including rapid military expansion, state-sponsored espionage, and human rights abuses, stressing that Chinese investments in U.S. land could compromise national security. He pointed to the PLA doctrine of "Unrestricted Warfare," suggesting that Communist China uses economic and strategic land acquisitions as tactics to undermine U.S. interests. Cases like the attempted land purchase by a Chinese company near a North Dakota Air Force base exemplify the national security risks involved.

Effective legislation, according to Holton, can provide remedies like fines, voiding sales, and revoking licenses, ensuring due process while protecting U.S. infrastructure. He also advised against relying solely on federal measures, as state-level actions have historically played a critical role in land ownership regulations. Holton advocated for laws specifically targeting adversarial entities, with exemptions for foreign nationals with legitimate business ties, to balance security with international cooperation in agriculture.

Holton concluded by underscoring the need for vigilance in preserving U.S. food security and protecting critical infrastructure, suggesting that the U.S. must act to prevent adversarial encroachments on its land resources and strategic sites.

Texas Forestry Association

David Alders, President-Elect of the Texas Forestry Association testified before the Committee. Mr. Alders highlighted that the Texas forestry industry manages 64 million acres of rural property and 12 million acres of forests, while employing 70,000 Texans and contributing \$24 billion of economic impact to the state.

Mr. Alders emphasized the role of East Texas forests as critical natural resources, describing them as "the lungs of our state," with substantial contributions to Texas Parks and Wildlife Department (TPWD) revenue streams.

Mr. Alders characterized industry stakeholders as patriotic stewards of private property rights and expressed concerns over foreign investment, noting significant capital influxes from global entities into the forestry sector. He recommended that any legislative action targeting foreign adversaries be approached with a "first do no harm" principle to avoid unintended negative impacts.

Mr. Alders argued that broad restrictions on foreign ownership could reduce the value of timberland assets and deter potential investments. He suggested that industry challenges arose more from competition with similar industries in other states rather than from foreign adversaries.

Texas Association of Builders

The Texas Association of Builders represents approximately 10,000 builders, remodelers, and associates throughout Texas. The association's members contribute significantly to the state's economy, supporting around 758,000 jobs and generating roughly \$72 billion in economic activity.

In this testimony, J.D. Hale, Director of Government Affairs for the Texas Association of Builders, underscored the Association's commitment to securing and protecting our state and country from hostile threats. At the start of the 88th Legislative Session, Hale explained members expressed two primary concerns:

1. The need to focus on protecting state security and the homeland.
2. The potential impacts of legislation on single-family home purchases, and the range of transactions subject to regulation.

Hale stated from the outset, the Association is particularly concerned about legislation that may inadvertently target individuals and lead to unintended consequences.

Furthermore, Hale highlighted the protections under The Federal Housing Act of 1968. The Act prohibits discrimination by direct providers of housing including landlords, real estate companies, banks, lending institutions, insurance companies. The objective was to prohibit discrimination in sales and rentals of housing. These prohibitions include developers, builders, remodelers or any individual responsible for the design or construction of a home.

The act identifies discrimination in the form of:

- race or color
- religion
- sex
- national origin
- familial status, or
- disability.

Hale urged careful consideration of these concerns above to ensure state-level actions align with federal protections, while addressing security risks effectively.

In conclusion, the Texas Association of Builders supports state security initiatives, but calls for a balanced approach to avoid infringing on housing rights and creating legal conflicts. Hale added

that the Association looks forward to continued dialogue to address these important matters comprehensively and thoughtfully.

Texas Public Policy Foundation, Honorable Chuck DeVore

In his testimony, Chuck DeVore highlighted the increasing acquisition of U.S. real estate by Chinese nationals and corporations, citing strategic motivations and potential national security concerns. Mr. DeVore noted that Chinese interest in U.S. property surged by 2015, with America as the top destination for these investments. DeVore explained that, while Communist China imposed restrictions on residential and entertainment property investments, purchases of agricultural and industrial assets continued, signaling their strategic significance. Between 2020 and 2022, Chinese-led entities increased their foreign land transactions, with notable land holdings in Texas, North Carolina, and Missouri.

DeVore outlined three primary motivations behind these acquisitions:

1. *Food Security*: Communist China seeks to stabilize its food supply by owning U.S. farmland and food facilities, a hedge against potential domestic shortages.
2. *Intellectual Property (IP) Access*: By acquiring farmland and agricultural facilities, Chinese entities gain insights into U.S. agricultural practices, technologies, and IP, replicating previous approaches seen in other sectors.
3. *Espionage Opportunities*: The strategic location of some Chinese-owned U.S. properties near military installations raises concerns about espionage, surveillance, and even potential electronic interference. A recent example is the proposed Fufeng Group land purchase near Grand Forks, North Dakota, close to a U.S. Air Force Base. Chinese-owned agricultural land could theoretically serve as a conduit for biological attacks on U.S. food supply chains or for disruptive infrastructure, such as wind turbines, that might impact critical sites. A Chinese wind farm acquisition near Laughlin Air Force Base in Texas illustrates this concern, though state laws curbed the project.

DeVore also explained the People's Republic of China's 2017 National Intelligence Law, which mandates cooperation from Chinese citizens and companies in intelligence activities, increasing potential security threats from Chinese-owned U.S. land. He urged proactive measures to address risks posed by foreign land ownership near sensitive U.S. sites, citing recent FBI warnings about Communist China's covert intelligence operations across the United States.

Sources:

- Air Force Times. (2023). Chinese company's corn plant for North Dakota. Retrieved from [AirForceTimes.com](https://www.airforcetimes.com)
- National Agriculture Law Center. (n.d). Foreign Ownership of Agricultural Land. Retrieved from [NationalAgLawCenter.org](https://www.nationalaglawcenter.org).

-
- U.S. Government Accountability Office (GAO). (n.d). Foreign Investment in U.S. Agricultural Land, Raising National Security Concerns. Retrieved from GAO.gov.
 - Louisiana Legislature. (2023). Act 420. Retrieved from Legis.La.gov.
 - U.S. Department of Defense (DOD). (2023). Chinese Telecommunications Infrastructure Near Strategic U.S. Bases Retrieved from Defense.gov.

Kenneth Nunnenkamp

Kenneth Nunnenkamp is a 30-year attorney with specific expertise in the Committee on Foreign Investment in the United States (CFIUS), providing insights into the limitations and focus areas on CFIUS reviews.

Mr. Nunnenkamp explained that CFIUS does not review every transaction involving foreign entities, targeting only specific cases that impact critical infrastructure and sensitive technologies. Most foreign investment transactions, especially in real estate, fall outside CFIUS' scope unless they involve majority ownership or active control over critical assets. Mr. Nunnenkamp described this approach as "catch-and-release", which allows certain types of recurring transactions to proceed without CFIUS review.

Mr. Nunnenkamp noted that CFIUS oversight remains voluntary and does not typically apply to real estate, except in cases involving critical infrastructure or technologies. He emphasized that federal-state authority questions around CFIUS largely avoid preemption issues, often focusing instead on standing. Although national security is generally seen as a federal concern, he explained there is flexibility for states to intervene when no constitutional law governs the area, specifically in relation to economic security and land purchases.

Citing examples of sanctioned Russian nationals holding U.S. agricultural land, Mr. Nunnenkamp highlighted the need for transparency in CFIUS's decision-making process, which he described as a "black box." This secrecy limits states' understanding of when they can enforce independent restrictions. He suggested the possibility of Congress expanding CFIUS's authority to address economic security concerns at both the state and federal levels.

Texas Real Estate Research Center at Texas A&M University

Gerald Klassen is the Research Data Scientist at the Center. Mr. Klassen leads development of the Center's advanced data warehouse. Prior to joining the Center in 2008, Mr. Klassen spent 12 years managing and developing portfolio management systems in the investment industry. He worked at Wachovia Global Securities Lending during the collapse of Bear Stearns and Lehman Brothers in the Great Financial Crisis. Prior to that he worked at USAA supporting the Investment Management Company's trading and portfolio systems. Mr. Klassen has a deep understanding of financial markets and a passion for explaining the complexities so others can make informed business decisions. Mr. Klassen has a BBA in Accounting & Finance, MBA from University of Texas at San Antonio and a Master of Land Economics & Real Estate (MLERE) from Texas A&M University.

Mr. Klassen's research examines the complexities surrounding foreign property ownership in Texas, provides comparative insights into international practices, and offers policy considerations for the United States.

Texas Property Ownership Analysis

Two strategic locations were analyzed to illustrate the challenges in tracking property ownership:

- Dyess Air Force Base Region
 - 39,313 property tax accounts, 28,698 unique owner names, and total assessed value of \$6.3 billion across 89,436 acres.
- High Plains (Ogallala) Aquifer
 - 632,360 property accounts, 376,830 unique owner names, covering 36.9 million acres with an assessed value of \$93.3 billion.

While these figures provide insight into land use, they reveal significant limitations in the available data. Ownership records, primarily held in county registries, only contain names and addresses, often with inconsistent formatting or misspellings. There is no reliable method to determine an owner's county of origin, immigration status, or corporate affiliations, complicating efforts to enforce foreign property ownership restrictions.

International Property Ownership Systems

Mr. Klassen contrasts Texas' deeds registration system with the Torrens Title system used in countries such as Canada, Australia, and Japan.

Under Torrens systems:

- Governments act as custodians of all property titles and oversee title transfers.
- Identification of buyers and sellers is required during transactions, enabling governments to regulate foreign ownership more effectively.

In contrast, the United States deeds system allows title transfers to occur through private contracts with minimal government involvement. The structure presents obstacles for establishing and enforcing foreign ownership laws, potentially leading to delays and legal complexities.

Mr. Klassen explained that requiring identification for both buyers and sellers would improve transparency. This process would align with post-9/11 measures under the USA Patriot Act, which already mandates identity verification for financing. Adding that to a centralized data repository, similar to British Columbia's Land Ownership Transparency Registry, could aid law enforcement by tracking indirect ownership interests and activities by foreign organizations. Integrating such a registry with existing property databases would offer stronger monitoring capabilities.

Texas Association of Realtors

Jef Conn, Chairman of the Texas Association of Realtors, is the top officer of the association's leadership team. Mr. Conn is a recognized REALTOR® who specializes in all aspects of office, industrial, and investment properties since 2007. Additionally, Jef has held leadership positions on committees at the local, state and national levels. He is also a current member of the National Association of REALTORS® Board of Directors and has encouraged future leaders through his involvement with the Young Professionals Network (YPN).

Texas REALTORS® supports ensuring land ownership remains secure from entities or individuals associated with hostile foreign governments. Security concerns stem from the potential misuse of real property, particularly in areas close to critical infrastructure. Existing measures at federal and state levels offer some protections, but the REALTORS® community acknowledges that these may not be comprehensive.

However, Mr. Conn cautioned that restricting property ownership broadly based on nationality could infringe upon individuals' rights and impact the real estate market. Texas REALTORS® suggests focusing on entities with demonstrable ties to hostile foreign governments rather than broadly restricting foreign nationals, noting that strict enforcement procedures should apply post-purchase if any security risk is discovered.

Mr. Conn's testimony emphasizes the significant role foreign investments play in Texas' economy, particularly in commercial real estate and land development. Texas REALTORS® argues that an overly restrictive approach could deter investment in key projects, such as commercial development, which often requires initial land acquisition before attracting investors and securing necessary permits. Large-scale projects that involve agricultural land acquisition could suffer delays and financing obstacles under ambiguous regulations.

Real estate development, particularly in rural and underdeveloped areas, often relies on foreign investments for growth and infrastructure improvement. A chilling effect on foreign investment could limit growth and delay development, ultimately impacting Texas' economic prospects.

The association remains open to working with legislators on refining legal language that ensures Texas remains attractive to responsible investors while prioritizing state security. Texas REALTORS®' position encourages legislation that prevents hostile actors from owning land near critical infrastructure without broadly limiting foreign ownership.

Asian American Real Estate Association

Mike Wong is a full-time professional agent with Keller Williams Realty. Experienced agent, experienced investor, exceptional service. Mr. Wong specializes in commercial real estate, residential sales and leasing, as well as working with investors.

Mr. Wong is a member of the HAR Political Advisory Leadership Group, Asian American Real Estate Association Board of Directors Member. A community volunteer and contributor, and founding member of Caring Realtors to help fellow associates in need.

Immigration and investment in Texas real estate have recently come under scrutiny amid growing concerns about foreign ownership of critical infrastructure and land. In testimony, Mike Wong expressed concerns that security-based restrictions on real estate investments could unintentionally impact immigrant communities, particularly those fleeing hostile regimes. Wong, an Asian American Real Estate Association of America (AREAA) member, provided a perspective that emphasizes the importance of economic access for immigrant communities while advocating for targeted, secure pathways for property ownership.

Wong's testimony emphasized the positive contributions of immigrant communities to Texas' economy. Drawing from his own experience, he argued that allowing foreign nationals and

refugees, particularly those from conflict-prone regions, to own property facilitates economic stability and integration. For example, Taiwanese immigrants, who have fled Chinese aggression, have actively participated in the U.S. economy, finding stability through homeownership and investment. Restricting this access, Wong argues, risks excluding these communities from meaningful economic engagement.

Wong underscored his family's experience fleeing Taiwan as an example of why Texas should be cautious in its approach to security-related property restrictions. He expressed concerns that foreign powers, such as those that threatened Taiwan, might attempt to extend their influence in Texas through property ownership or covert investments. Thus, while Wong supports security measures, he argued for policies that would prevent hostile actors from exploiting Texas' open real estate market without harming vulnerable refugee communities.

His testimony reflects a broader trend where immigrants who fled hostile conditions are wary of seeing similar threats emerge in their new communities. Wong advocates for strategic protections to prevent foreign influence without broadly restricting immigrant and refugee communities from participating in the real estate market.

Texas Land Title Association

Aaron Day is Director of Government Affairs and Counsel for the Texas Land Title Association (TLTA). Aaron is TLTA's general counsel, and he directs the association's government affairs program. In addition to lobbying for TLTA during legislative sessions, Mr. Day manages the association's role and participation in Texas Department of Insurance regulatory activities, including rate hearings, rule hearings and other regulatory responsibilities.

Mr. Day testified before the Committee expressing concerns over the effectiveness and risks associated with proposed property databases and ownership reporting requirements. He argued that these methods could create substantial liability and would not be as effective in addressing security concerns as anticipated. Instead, Day recommended focusing on strengthening law enforcement processes rather than implementing blanket prohibitions on property ownership.

Mr. Day emphasized the challenges within the title industry regarding property transaction reversals, stating that title ownership often involves multiple third parties, making it challenging to unwind ownership without significant legal complications. He also recommended that any procedures for reversing property sales include provisions to protect lienholders, reflecting his concern for the stability and liability of all stakeholders in the title process.

Texas Bankers Association

Celeste Embrey, general counsel at the Texas Bankers Association (TBA), testified before the Committee. The Texas Bankers Association, established in 1885, represents nearly 400 banks in Texas that collectively employ over 230,000 Texans.

Texas Bankers Association expressed strong support for legislative efforts to protect Texans from hostile foreign organizations.

Furthermore, Ms. Embrey highlighted the extensive federal statutory and regulatory framework banks must follow, including:

- Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) Act of 2020:
 - Designed to combat money laundering and terrorism through risk-based programs and stringent record-keeping.
- Fair Lending Requirements:
 - Including the Equal Credit Opportunity Act (ECOA) and Regulation B, which prohibit discrimination in credit transactions based on race, national origin, and other protected characteristics. Ms. Embrey noted that while immigration status can be considered, it cannot lead to discrimination.

Recent joint statements by the DOJ and CFPB (Consumer Financial Protection Bureau) emphasize that financial institutions must ensure consideration of immigration status does not result in discriminatory practices.

The Texas Bankers Association and its members are dedicated to combating anti-money laundering and terrorism financing, while also upholding fair lending practices. Ms. Embrey underscored the organization's willingness to collaborate with the Committee and Legislature to meet federal and state obligations.

Texas Mortgage Bankers Association

Meredyth Fowler acts as general counsel to the Texas Mortgage Bankers Association, TMBA, and also leads their governmental affairs team.

Ms. Fowler presented TMBA's perspective on foreign ownership legislation, particularly concerning real estate transactions.

Representing a broad coalition of financial institutions, TMBA members voiced support for legislative measures to protect critical infrastructure from foreign entities tied to hostile governments, advocating for focused legislation that limits ownership only for organizations affiliated with adversarial governments rather than individuals.

TMBA emphasized that Texas' history of non-discrimination should guide this legislation, cautioning against measures that could inadvertently impact law-abiding residents or businesses and create conflicts with the Texas Constitution's non-discrimination protections (Article 1, Section 3a), as well as federal laws like the Fair Housing Act and the Equal Credit Opportunity Act. TMBA urged that any legislation focus solely on entities, not individuals, to maintain Texas' appeal for legitimate international investment and prevent conflicts with existing protections for equal access in real estate and finance.

- **Focus on Hostile Governments:** TMBA advocates targeting only entities controlled by hostile governments as identified by national intelligence agencies, to avoid discouraging legitimate foreign investment.
- **Exemptions for Individuals with Strong U.S. Ties:** TMBA suggested exemptions for U.S. citizens, green card holders, certain visa holders (e.g., professionals and victims of

trafficking), and non-citizen spouses to safeguard the rights of these individuals in real estate ownership and prevent discrimination.

- **Community Property Concerns:** TMBA noted that Texas' community property laws could inadvertently affect U.S. citizens married to non-exempt foreign individuals. Any restrictions should ensure such spouses' property rights remain protected.
- **Clarifying Property Interest and Control Definitions:** TMBA recommended that legislation include clear definitions of property interests and entity control. They proposed aligning definitions with Texas Business Organizations Code to avoid ambiguity regarding control thresholds.
- **Enforcement Over Void Transactions:** TMBA expressed concern about provisions making prohibited transactions "void" or "voidable," which could create downstream instability in the real estate market. Instead, they suggested authorizing the Texas Attorney General to manage cases of prohibited ownership through a receivership and divestiture process, providing structured protection for innocent third parties.
- **Collaborative Legislative Process:** TMBA offered to serve as a resource, committing to work with legislators on refining and advancing effective legislation that protects critical infrastructure without compromising Texas' reputation for economic inclusivity.

Permian Basin Petroleum Association

Michael Lozano, Director of Government Affairs & Communications with the Permian Basin Petroleum Association testified before the Committee. Mr. Lozano emphasized that the development of resources within the Permian Basin represents the largest operation of resource extraction in world history. He noted some existing security vulnerabilities in asset acquisition processes, attributed to delays in approval protocols. Mr. Lozano highlighted that these delays could potentially expose operations to risks.

Given the increasing complexity of technologies used in the industry, Mr. Lozano underscored that most industry members have adopted sophisticated cybersecurity measures to address these growing cybersecurity threats.

Mr. Lozano discussed the occurrence and impact of ransomware attacks targeting oil and gas operations. He stressed the importance of robust cybersecurity to protect critical infrastructure assets and operations.

Texas Solar Power Association

Mark Stover, Executive Director of the Texas Solar Power Association, testified before the Committee. Mr. Stover highlighted that solar energy is the fastest-growing generation type in the Electric Reliability Council of Texas, ERCOT, grid, representing approximately 10% of total generation capacity. Additionally, Mr. Stover described the role of solar power in supporting ratepayers, including aiding recovery efforts for those impacted by Hurricane Beryl.

Mr. Stover highlighted property security concerns, emphasizing the importance of protecting Texans and the ERCOT grid from foreign actors acquiring properties that could undermine grid security, while ensuring renewable generation remains integral in grid stability.

In regard to manufacturing and sourcing, Mr. Stover explained that many solar panels are manufactured in Asia, but noted a growing trend toward establishing manufacturing capacity in the United States, including a new facility in Houston, Texas. On other solar components, Mr. Stover confirmed that many transmission-related elements are foreign-made, though specifics on primary manufacturing locations were not available.

Mr. Stover stated that solar farms are primarily owned by independent power producers, with roughly 60% domestic ownership and 40% foreign ownership. The majority of the foreign ownership are countries such as the United Kingdom, France, and Germany. He clarified that most land used by solar farms is privately owned and leased, though some energy firms purchase properties from retiring ranchers.

In conclusion, Mr. Stover highlighted grid connection and security measures. He described ERCOT's interconnection process, which requires detailed ownership and asset disclosures to ensure that entities with potential security risks cannot connect to the grid without scrutiny. Mr. Stover expressed confidence in the process's capability to maintain grid security.

COMMITTEE HEARING ON SEPTEMBER 10TH, 2024 – TYLER, TEXAS

The Committee held a public hearing on September 10th, 2024, with both invited and public testimony.

The individuals listed below provided testimony to the Committee on this charge.

Public Hearing: September 10th, 2024

Witness List: September 10th, 2024 – The University of Texas at Tyler, Soules College of Business – Room COB 180, 3501 Liberty Lane, Tyler, TX 75701

Panel 1

- Colonel Steven McCraw, Department of Public Safety
- Tony Sauerhoff, Department of Information Resources
- Chad Seely, Electric Reliability Council of Texas

Panel 2

- David Dunmoyer, Texas Public Policy Foundation
- Dr. Tom Roberts, University of Texas at Tyler – Center for Cybersecurity and Data Analytics

Panel 3

- Thure Cannon, Texas Pipeline Association
- Scott Shtofman, Association for Uncrewed Vehicle Systems International

Public Testimony

- Bob Brewer
- Zhengang Cheng
- Mallika Choudhury, Asian Texans for Justice
- Holly Hayes
- Scott Hommel, Lamar County GOP
- Josh Joplin, Constables Office Smith County Precinct 4
- Robert Kecseg
- Clifton McCaleb
- Cebren O'bier
- Ann Pennington
- Sabrina Sha
- John Soules
- John Van Compernelle
- Alice Yi

The information below is largely based on the oral and written testimony of the invited individuals and organizations above.

Col. Steve McCraw, Texas Department of Public Safety

Col. McCraw's testimony before the Committee is summarized below:

Steven C. McCraw became the Director and Colonel of the Texas Department of Public Safety in August 2009. Colonel McCraw began his law enforcement career with DPS in 1977 as a Trooper in the Texas Highway Patrol and later as a DPS Narcotics Agent until 1983 when he became a Special Agent with the FBI. He served in Dallas, Pittsburgh, Los Angeles, Tucson, San Antonio and Washington, DC.

Colonel McCraw's promotions included Supervisory Special Agent, United Chief of the Colombian/Mexican Organized Crime Unit, Assistant Special Agent in Charge in Tucson, Inspector-In-Charge of the South East Bomb Task Force, Inspector – Deputy Assistant Director, Special Agent in Charge of the San Antonio office, Assistant Director of the Office of Intelligence for which he was tasked to establish after the attacks on 9/11. He was also responsible for establishing the Foreign Terrorism Tracking Task Force under Office of the Attorney General.

In 2004, Colonel McCraw retired from the FBI to become the Texas Homeland Security Director in the Office of the Governor where he served until his appointment as DPS Director.

There is no greater responsibility of government than protecting its citizens. Texas faces the entire range of threats to its ever-increasing population of almost 30 million residents, who live throughout the states over 268,000 square miles of rural and urban communities and along 367 miles of coast line and 1,254 miles of international border with Mexico. Texas possesses a substantial amount of the nation's critical infrastructure and key resources and has over 313,000 miles of roadways with over 210,000 miles in the unincorporated areas of Texas.

These threats present daunting challenges for the state's leadership, Legislature, local officials, and agencies such as the Department charged with protecting people from harm. Constant vigilance and the timely and effective integration of effort across all jurisdictions and disciplines is absolutely essential because even one of these threats can quickly overwhelm entire cities, counties, and regions of the state. This is particularly important at a time when state and local governments are faced with decreasing revenue and resources to protect people from harm.

Currently, there are only 80,179 local and state commissioned officers in Texas working for 2,768 different local and state law enforcement agencies in 254 counties. While these departments are highly professional, over 50% have 10 or fewer officers, 78% have 20 or fewer officers and 91% have 50 or fewer officers. Regardless of their professionalism and dedication, it is not possible for most of these agencies to sustain around-the-clock operations for long periods of time or to invest in the types of capabilities needed to address significant threats. Fortunately, Texas is blessed with a strong sense of cooperation among law enforcement agencies and the support of the public, which serves as a force multiplier of these limited resources.

The State Legislature and Governor have provided DPS with essential public safety capabilities to address its many public safety responsibilities and to assist its law enforcement partners when needed. In recent years, the Department has been tasked with conducting major crime prevention operations along the international border with Mexico to address the substantial amount of drug and human smuggling into and throughout Texas and in other areas of the state threatened by escalating drug and gang related violence. The Department has also been directed to proactively

address threats to schools, mass attacks in public places, violent gangs, and the sex trafficking industry throughout the state. The amount and type of DPS assistance varies, and sometimes requires the integration of several of the below essential public safety capabilities that most law enforcement agencies in Texas either do not have or cannot sustain at the level and intensity needed.

Colonel McCraw's testimony provides insight into recent migrant trends, cartel activities, and the shifting dynamics of human trafficking along the Texas-Mexico border. The testimony highlights data on migrant origins, the rise of organized crime, and the role of law enforcement partnerships.

1. Migrant trends

- Increased Presence of Non-Mexican Migrants:
 - Migrants are increasingly coming from Russia, China, and Iran.
 - Venezuelans crossing the border have surged dramatically since 2021.
- Data on Foreign Nationals Detained Since 2021:
 - 8,954 Chinese nationals
 - 1,958 Russians
 - 219 Iranians
 - 0 North Koreans

Many of the detained Chinese nationals are military-age males, not females.

2. Cartel Activity and Organized Crime

- Cartels still control trafficking operations along the Texas-Mexico border.
- The Tren de Aragua (TdA), a Venezuelan gang, is gaining power and is expected to be classified as a Tier One criminal organization soon.
- Cartels are involved in manufacturing fentanyl and methamphetamine, with precursor chemicals coming from Communist China.

3. Human Trafficking and Smuggling Trends

- Decline in Human Smuggling:
 - Human smuggling has decreased by 49% over the last 8 months.
 - Texas is no longer the “center of gravity” for trafficking, with operations shifting to states west of Texas.
- Impact of Migrant Crime:
 - Since 2011, 320,000 migrants have been charged with criminal offenses in Texas.

4. Law Enforcement and Border Security Cooperation

- Federal-State Cooperation:
 - Partnerships between federal and state law enforcement agencies are critical for combating trafficking and cartel activities.
- Ongoing Border Threats:
 - Weapons, cash, and trafficked individuals continue to move through border crossings west of Texas, emphasizing the importance of Texas' role in national security efforts.

Colonel McCraw’s testimony emphasizes the shifting dynamics of migration and trafficking along the Texas border, with new patterns of migration and rising criminal organizations posing complex challenges. The data presented indicates the need for strong law enforcement cooperation to curb the influence of cartels and protect national security from emerging threats, including human trafficking, drug manufacturing, and cross-border financial flows.

Department of Information Resources

The Texas Department of Information Resources (DIR) delivers technology solutions to state and local government entities. Specifically, DIR is here to:

- Offer purchasing support and policy insights so organizations across all levels of Texas government can find and securely implement modern technology
- Set forth strategic direction for IT statewide through policies and guidance
- Analyze cybersecurity risks and solutions
- Empower state and local government entities with reliable and secure technology
- Assist with technology procurement/purchasing
- Collaborate with technology vendors
- Create a dynamic online community for knowledge sharing

The approximately 200 professionals who work at DIR are driven by a sincere desire to make governmental technology more secure, cost-effective, and forward-looking. DIR is honored to serve as the cornerstone of public sector technology in Texas.

Mr. Tony Sauerhoff is the Chief Information Security Officer (CISO) for the State of Texas. As State CISO, Mr. Sauerhoff oversees the team responsible for developing state agency security policies and standards, facilitating the statewide cybersecurity awareness training program, providing statewide incident response capabilities, collecting and analyzing security incidents from across the state, the coordination of security services, and promoting information sharing across the public and private sector cybersecurity communities.

Before moving into his current role, Mr. Sauerhoff served as the Senior Deputy CISO and the State Cybersecurity Coordinator. He also chaired the Texas Cybersecurity Council. Mr. Sauerhoff has over 30 years of experience in IT and cybersecurity in the public and private sectors and served in leadership positions with the United States Department of Defense and the federal judiciary prior to joining DIR in 2022.

Mr. Sauerhoff emphasized that foreign adversaries such as Communist China, Russia, North Korea, and Iran are the biggest threat to cybersecurity in Texas. These countries fund organizations to conduct cyber attacks on the United States. Though the goal of these countries is to infiltrate United States systems, the motive of each country varies. China, Russia, and Iran conduct information and misinformation campaigns to suppress certain social and political activities. North Korea mostly commits cyber crime to collect intelligence and create revenue to

fund their government. However, North Korea is becoming more involved in intellectual property (IP) theft.

Communist China is the biggest threat to intellectual property. They continue to engage in forced technology transfer and cyber espionage tactics aimed at leveraging advanced technology against their competitors, costing the United States economy billions of dollars annually.

In cybersecurity terminology, these well funded state sponsored groups are known as advanced persistent threats, or APTs. APTs activity is typically aimed at prolonged system intrusion and maintaining persistence in a target system or network. Their objectives include espionage, intellectual property theft, network or system disruption or destruction for financial gain.

Russia and APTs are believed to have worked with ransomware gangs in order to carry out attacks. A state sponsored APT may hire outside hackers to have a layer of deniability, or because they lack a specific skill set to carry out an attack. Most of these ransom groups are apolitical and financially motivated and thus will conduct cyber operations for the highest bidder.

These entities have been behind cybersecurity attacks such as the solar winds attack and the 2019 ransomware attack that affected 23 Texas governmental local entities.

Nation States also pose a threat to critical infrastructure in the State of Texas. In July of 2024, the United States Department sanctioned two members of a Russian activist group known as the Cyber Army of Russian Reborn for their involvement in attacks on water facilities in Abernathy and Muleshoe Texas.

According to the Office of the Director of National Intelligence, Communist China remains the most active persistent cyber threat to the private sector and critical infrastructure networks. Chinese sponsored state actors are seeking to preposition themselves on United States IP networks for destructive cyberattacks against critical infrastructure in the event of a major crisis or conflict with the United States.

Communist China is quietly infiltrating critical infrastructure networks across the United States and maintain their access without being noticed. If they believe that a major conflict with the US were imminent, they would consider using that access for aggressive cyber operations against the US critical infrastructure and military assets. Such a strike would be designed to deter US military action by impeding US decision making, inducing societal panic, and interfering with the deployment of US forces.

The United States government recently issued warnings about Iran based cyber actors conducting militia cyber operations aimed at multiple US sectors.

Mr. Sauerhoff explained that even though this information is frightening, there are steps that organizations can take to protect themselves. These steps are: implementing basic security controls and practices like multifactor authentication, regular software updates, firewalls, end point protection, and strong access controls.

The Department of Information Resources has cybersecurity training, monitors the dark web, and shares information with over 1,100 entities statewide.

These hostile foreign nations are not just attacking the United States online. DIR is aware that foreign governments, militaries, intelligence agencies and their high-ranking officials have

invested large amount of money into technology companies, which creates serious concerns that these products could be used to compromise the privacy of the public and the national security of the United States.

Mr. Sauerhoff stated that a good example of a dangerous technology company is TikTok, which Governor Abbott banned from being used on government issued state devices and networks in December of 2022. Governor Abbott directed DIR and the Department of Public Safety to work together to draft a statewide model plan to ban other technologies that are considered a threat, including products from Communist China and Russia. In the 88th Legislative Session, the legislature put the TikTok ban into state law through Senate Bill 1893 for state entities and local governmental entities. Senate Bill 1893 authorizes the governor to add additional applications or services to this prohibition.

With technology companies being privately held, it can be difficult to determine who the actual beneficial ownership of such companies. Due to this, DIR is currently in the process of hiring an audit firm to evaluate the ownership of products and services offered through their cooperative contract program, used by state and local governments.

The planned audit will examine approximately 200 contracts to determine whether any of those companies are either wholly or substantially owned by any foreign government, officials, or have business dealings with any such company to raise the same concerns. At the audit's conclusion, DIR will examine the findings and likely exclude those products from their program. DIR will share any such findings with relevant state leaders to help evaluate whether products originating with that vendor should be included in the states prohibited technologies policy.

Mr. Sauerhoff concluded his testimony by reiterating that the cyber attacks posed by hostile foreign organizations are many, the attacks are continuous and ever increasing in sophistication. He emphasized that Governor Abbott and the legislature are taking these threats seriously and that they have provided direction and funding for a number of programs. However, the protection of Texas' sensitive data and critical infrastructure is an ongoing effort. We must always stay up to date with the increasing and evolving threats of our adversaries.

Electric Reliability Council of Texas

Chad Seely is the Senior Vice President, General Counsel, and Corporate Secretary for Electric Reliability Council of Texas, also known as ERCOT.

Mr. Seely testified before the Committee, describing ERCOT's work to implement Senate Bill 2116 during the 87th Legislative Session and Senate Bill 2013 during the 88th Legislative Session. ERCOT has issued requests for information, RFIs, regarding foreign ownership of proposed resource projects and modified rules governing the connection of new projects to the grid, including registration of ownership.

Lone Star Infrastructure Protection Act

- Lone Star Infrastructure Protection Act
 - State of Texas regulations regarding access to and security of critical infrastructure.
- Originally adopted June 18, 2021
 - 87th Legislature via Senate Bill 2116
- Amended June 9, 2023
 - 88th Legislature via Senate Bill 2013

Senate Bill 2116, 87th Legislative Session

SB 2116 amended Chapter 117, Title 5, Business and Commerce Code. SB 2116 prohibits Texas businesses from entering into agreements relating to critical infrastructure with a company:

- If the company would be granted direct or remote access to or control of critical infrastructure in Texas.
 - Excludes access specifically allowed for product warranty and support purposes.
- And if it is known that the company is either:
 - Owned by or the majority of stock or other ownership interest is held or controlled by:
 - Citizens of, or directly controlled by the government of, China, Iran, North Korea, Russia, or a designated country, or
 - A company or other entity owned or controlled by citizens of or is directly controlled by the government of China, Iran, North Korea, Russia, or a designated country
 - Or headquartered in China, Iran, North Korea, Russia, or a designated country.
- Designated Country:
 - A country designated by the governor as a threat to critical infrastructure (See Section 117.003)
 - There are currently no additional designated countries
- Applies only to a contract or agreement entered into on or after the effective date of the Lone Star Infrastructure Protection Act, or LSIPA.

Senate Bill 2013, 88th Legislative Session

Senate Bill 2013 amended Section 39.360, Subchapter H, Chapter 39, Utilities Code

- An independent System Operator, ISO, may not register or maintain the registration of a business entity operating in the power region unless the business entity attests that they comply with the LSIPA.
- As a condition of operating in the power region, business entities must report to the ISO the purchase of any critical grid equipment or service from a company described by the LSIPA.

-
- For each reported purchase, business entity shall submit an attestation to the ISO that the purchase will not result in access to or control of its critical electric grid equipment by a company described by LSIPA.
 - ISO may immediately suspend or terminate a company's registration or access to any ISO systems if the ISO has reasonable suspicion that the company meet any of the criteria described by the LSIPA.
 - ISO may adopt guidelines or procedures relating to the requirements in this section, including the qualification of electric grid equipment or services as critical.
 - The commission shall adopt any rules necessary to administer this section of authorize ISO to carry out a duty imposed by this section.
 - The Texas Attorney General may conduct and prioritize periodic audits of the attestations required.

ERCOT Rules and Procedures Adopted to Meet Requirements Under Senate Bill 2013

- NPRR 1155, June 2023
 - Because NPRR1155 was adopted during SB 2013's passage, no new rules were needed to comply with SB 2013's passage, no new rules were needed to comply with SB 2013's requirements regarding Market Participant (MP) registration.
- NPRR 1199, May 2024
 - Addressed new requirements in SB 2013 regarding market participant reporting on the purchase of "critical electric grid equipment services."
 - Created definitions for Critical Electric Grid Equipment, CEGE, and Critical Electric Grid Services, CEGS.
 - Adopted procedures and created standard reporting form to comply with CEGE/CEGS reporting requirements.
- ERCOT Registration Policies
 - ERCOT purchased software providing reports on a Market Participant's corporate family tree.
 - ERCOT is implementing procedures for pulling random samples of existing and new market participants on a regular basis to run and analyze corporate family tree reports.
 - RFIs sent to Market Participants when questions arise regarding their attestation.
- ERCOT's Employment Policies
 - Reviewed and modified ERCOT hiring and contracting processes to identify relevant ERCOT employee and contractor positions that are deemed "critical to the security of the grid."

No other changes needed to existing employee/contractor background check policies due to current requirements.

Cybersecurity Impacts – Procurement/Contracting Policies for Vendors

- Supply Chain
 - Required Suppliers to identify ties to China, Iran, North Korea, Russia, or a designated country, consistent with LSIPA criteria.

Mr. Seely added that ERCOT has also adjusted its procurement processes to account for the origins of products used within its systems. Additionally, by the end of this year, ERCOT expects to receive reports from their market participants detailing the countries of origin for grid and software-related purchases.

Texas Public Policy Foundation

David Dunmoyer is the campaign director for Better Tech for Tomorrow, and initiative of the Texas Public Policy Foundation. Mr. Dunmoyer’s testimony frames the problem, survey the challenges posed to critical infrastructure in the age of digitalization and artificial intelligence (AI), highlight state and federal responses, and, ultimately, provide concrete policy recommendations to help Texas meet these challenges and be a national leader on critical infrastructure cybersecurity.

The Challenges Posed to Critical Infrastructure in the Age of Digitalization

As digitalization transforms critical infrastructure sectors, vulnerabilities increase, placing essential systems at risk. With 16 sectors identified by the Cybersecurity and Infrastructure Security Agency (CISA) as critical to U.S. economic, health, and national security, recent trends expose these systems to elevated risks from both rogue nation-states and cybercriminals (CISA, n.d.). Mr. Dunmoyer explains the impacts of digitalization, the rise of cyberattacks on critical infrastructure, and the increased sophistication of foreign state-sponsored threats, emphasizing the urgency of robust cybersecurity measures.

Critical infrastructure, including sectors such as energy, water, transportation, and emergency services, supports essential societal functions and underpins national security. As these systems integrate advanced digital technologies, they become susceptible to cyberattacks, particularly from state-sponsored actors who see an opportunity to compromise U.S. resilience (CISA, n.d.). Mr. Dunmoyer’s testimony examines the current threat landscape, highlighting recent attacks and the necessity for improved security postures to protect critical infrastructure.

The digital transformation of critical infrastructure marks a shift from isolated, “air-gapped” systems to interconnected, internet-based networks. This transformation has created significant vulnerabilities, particularly as the demand for remote access to operational technology (OT) systems grows in a post-pandemic work environment (Tufts, 2023). Previously, infrastructure operated on isolated networks, reducing cyber threats. However, digital interconnectivity has introduced new attack vectors, requiring modern cybersecurity defenses that can keep pace with this rapid change (DHS, n.d.).

The frequency of cyberattacks on U.S. critical infrastructure has risen sharply, with recent FBI data showing over 40% of 2023’s 2,825 ransomware incidents affecting this sector, up from one-third the previous year (Kapko, 2024; FBI, 2023). Notably, foreign adversaries, particularly from

Communist China, Russia, North Korea, and Iran, have been responsible for around 60% of these attacks (Security Magazine, 2023). Cybercriminals often leverage weak cybersecurity practices, including unprotected employee accounts and vulnerabilities in remote access systems, to infiltrate infrastructure networks (CISA & USCG, 2023). The attack methods include spearphishing, which accounted for 33% of successful intrusions in 2022, and unauthorized access through leftover employee accounts, highlighting the need for comprehensive account management and multi-factor authentication (MFA) (CISA & USCG, 2023).

A recent high-profile incident in Texas illustrates the severity of cyber threats. On January 18, 2024, Russian cyber operatives infiltrated Muleshoe, Texas' water infrastructure, causing a massive water loss. This attack, confirmed by the Cybersecurity and Infrastructure Security Agency (CISA), was orchestrated via a remote hack into the city's Supervisory Control and Data Acquisition (SCADA) system, a crucial component for monitoring water distribution systems (Miller, 2024). Other Texas towns experienced similar attacks, with Hale Center facing tens of thousands of infiltration attempts, suggesting a deliberate effort by state actors to evaluate weaknesses and refine offensive techniques against U.S. critical infrastructure.

These incidents reflect broader tactics by nation-states seeking not only immediate disruption but also intelligence gathering. In these attacks, Russia tested U.S. defenses and exploited gaps to prepare for future, potentially larger-scale operations. With data on vulnerabilities, attackers could coordinate with other cyber or physical tactics to disrupt water supplies or power grids, threatening public safety and economic stability (Miller, 2024; DHS, n.d.).

Artificial intelligence (AI) poses dual implications for critical infrastructure. While AI offers tools for enhanced threat detection and incident response, it also empowers cybercriminals with advanced automated attack capabilities. AI-driven spearphishing campaigns, sophisticated malware, and AI-enabled vulnerability scanning can help attackers identify and exploit weaknesses faster than traditional methods. The rise of AI thus raises the stakes, necessitating rapid adaptation within cybersecurity frameworks to prevent malicious AI applications (Security Magazine, 2023).

The digitalization of critical infrastructure necessitates robust cybersecurity policies and proactive defense strategies. Many successful intrusions result from simple lapses in basic cybersecurity measures, such as failing to enforce MFA or leaving default passwords unchanged. While Muleshoe, Texas, responded to recent attacks by implementing MFA and updating default passwords, the incident underscores a broader need for security protocols across all levels of critical infrastructure (Miller, 2024). Additionally, CISA and the Department of Homeland Security (DHS) urge enhanced public-private sector collaboration and adherence to cybersecurity best practices to combat state-sponsored cyber threats.

While digitalization brings efficiency gains, it also invites greater cybersecurity risks, especially from state-sponsored actors targeting U.S. critical infrastructure for both immediate disruption and intelligence gathering. As AI amplifies the potential scope of these threats, it becomes crucial for infrastructure sectors to adopt advanced security frameworks, conduct regular vulnerability assessments, and foster a culture of cybersecurity awareness. Government agencies, private companies, and critical infrastructure operators must work in tandem to safeguard national security in an era of unprecedented digital dependency.

Sources:

-
- Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). Critical Infrastructure Sectors. CISA.gov.
 - Department of Homeland Security (DHS). (n.d.). Critical Infrastructure Security.
 - Federal Bureau of Investigation (FBI). (2023). Cybersecurity Threat Assessment.
 - Kapko, M. (2024). Ransomware and Critical Infrastructure: Trends and Responses.
 - Miller, T. (2024). Cyber Intrusions in Texas Water Systems.
 - Security Magazine. (2023). State-Sponsored Cyber Attacks on U.S. Infrastructure.
 - Tufts, B. (2023). Digitalization of Critical Infrastructure: Risks and Rewards.

The Challenges Posed to Critical Infrastructure in the Age of AI

With digitalization transforming critical infrastructure, artificial intelligence (AI) is rapidly reshaping the landscape of cybersecurity. AI amplifies both defensive and offensive capabilities, offering tools for threat detection and adversarial advantages alike. This portion of Mr. Dunmoyer’s testimony reviews the emerging AI-enabled cyber threats, focusing on hostile applications by foreign actors, and explores the pressing security implications for U.S. infrastructure.

The proliferation of digitalization across critical infrastructure has introduced complex cybersecurity challenges, further complicated by the advent of AI. As AI models evolve, concerns mount over their potential misuse by adversaries to conduct advanced cyberattacks. AI enhances attack sophistication, enabling foreign and non-state actors to deploy targeted, efficient, and evasive malware attacks against U.S. systems (Reuters, 2024; DHS, 2023).

AI has become a double-edged sword, aiding defenders in identifying vulnerabilities and facilitating attackers in amplifying threats. The U.S. Department of Homeland Security (DHS) warns that AI-driven capabilities could scale up cyber threats, enabling faster and more evasive attacks against essential services, including transportation and water systems (DHS, 2023). Hostile actors utilize AI to create potent tools such as malware and AI-assisted vulnerability identification methods, creating a heightened threat to critical infrastructure that could devastate public safety and the economy (Reuters, 2024; DHS, 2023).

Foreign adversaries are increasingly deploying AI to refine their cyberattack techniques. According to Drew Hamilton of Texas A&M Cybersecurity Center, AI technologies support numerous malicious applications, including adversarial machine learning, deepfake evasion, and automated exploitation of critical systems (House Committee on Artificial Intelligence & Emerging Technologies, 2024). For instance, AI tools enable more precise social engineering tactics and spearphishing attacks, where attackers impersonate familiar figures to compromise sensitive systems (House Committee on Artificial Intelligence & Emerging Technologies, 2024). These applications underscore AI’s role in creating highly adaptive and scalable cyber threats, allowing even low-skilled attackers to perform sophisticated exploits.

A notable case highlights the risks posed by deepfake technology in corporate cybersecurity. In early 2024, a multinational corporation fell victim to a sophisticated AI-driven scam where

deepfake video and audio impersonated the company's CFO, convincing an employee to transfer \$25.6 million under false pretenses (Chen & Magramo, 2024). This incident reveals AI's potential to exploit vulnerabilities in authentication processes, raising concerns about critical infrastructure, where a similar breach could allow unauthorized access to essential systems. Such deepfake scams cost Americans \$2.6 billion in 2022 alone, illustrating the widespread implications of this threat vector (Karimi, 2023).

Spearphishing, a prevalent attack vector in critical infrastructure, demonstrates AI's ability to facilitate cybercrimes with precision and scale. Spearfishers exploit personal details to convince victims of their legitimacy, a technique bolstered by AI models that can replicate speech patterns, create tailored content, and translate languages fluently (DHS, 2023). AI tools like ChatGPT streamline this process, enabling attackers to generate convincing messages rapidly, intensifying the threat to critical sectors and demanding more sophisticated countermeasures (DHS, 2023).

Sources:

- Chen, L., & Magramo, K. (2024). AI-Driven Deepfake Scams on the Rise.
- Cybersecurity and Infrastructure Security Agency (CISA). (2023). Critical Infrastructure Sectors Overview.
- Department of Homeland Security (DHS). (2023). Homeland Threat Assessment 2024.
- House Committee on Artificial Intelligence & Emerging Technologies. (2024). Texas Cybersecurity Testimonies.
- Karimi, S. (2023). Financial Impacts of AI-Enabled Scams.
- Reuters. (2024). Concerns Over AI's Dual Use in Cybersecurity.

Using AI as a Proactive and Reactive Tool in Cybersecurity for Critical Infrastructure

The surge in AI technologies has catalyzed advancements across critical infrastructure sectors, from water treatment facilities to nuclear surveillance. However, it has also introduced significant cybersecurity vulnerabilities. Following Executive Order 14110, the Department of Homeland Security (DHS) released guidelines in 2024 identifying risks linked to the design and deployment of AI tools within critical infrastructure systems, underscoring the need for cybersecurity frameworks that address these evolving threats (DHS, 2024). Mr. Dunmoyer highlights these vulnerabilities and explores AI's potential to enhance security protocols and reduce detection times for cyber incidents.

DHS has identified several risk factors in the AI application across critical infrastructure, citing potential for malfunctions or unintended operational disruptions stemming from design flaws in AI systems (DHS, 2024). Given the rapid pace of digitalization without proportional investment in cybersecurity, the vulnerabilities of AI-integrated systems could be exploited by adversarial actors. These include deficiencies in AI planning, system design, and implementation, which expose infrastructure to malfunctions that impact essential services (DHS, 2024).

AI has demonstrated its value in nuclear facility surveillance through the International Atomic Energy Agency (IAEA), which operates over 1,300 cameras globally to monitor sensitive materials and activities. AI-enabled review software facilitates the efficient monitoring of extensive footage, thus minimizing human error and improving compliance verification (Wagman & Nicula-Golovei, 2022). This surveillance model showcases the benefits of AI in mitigating errors in critical infrastructure, suggesting its utility for other sectors, including water treatment and power grids, to proactively flag unusual patterns before they cause disruptions.

AI not only offers defensive capabilities but also enables more responsive measures to cyber incidents. Data breaches, which historically take up to 322 days to detect, could be identified more rapidly through AI-based monitoring systems. By analyzing network traffic for anomalies and implementing machine learning-driven pattern recognition, these systems can detect and address cyber threats faster than traditional methods (Yehoshua, 2023). An example of this utility is seen in recent Chinese hacking campaigns against U.S. transportation hubs, where AI detection tools could significantly reduce the duration of unauthorized access and mitigate potential damage (Lyngaas, 2024).

One key benefit of AI is in accelerating recovery from ransomware attacks. AI-powered diagnostics enable faster assessments of the scope and impact of breaches, providing actionable insights that can streamline response times for organizations with limited resources. For example, some institutions, such as independent school districts, may opt to pay ransoms due to high recovery costs; AI-based solutions can reduce reliance on such measures by automating critical recovery processes (Blinder & Perloth, 2018; Bovbjerg, 2023). This is especially beneficial for rural providers, where budget constraints limit recovery options.

The dual-use nature of AI in cybersecurity is both a tool and a threat, necessitating a multifaceted policy approach. As AI technologies evolve, securing critical infrastructure will depend on balancing innovation with robust oversight to prevent exploitation by hostile entities. In line with DHS guidelines, policies should prioritize risk assessment in AI design, ensuring systems are resistant to adversarial attacks while remaining adaptable to emerging threats.

Sources:

- Blinder, A., & Perloth, N. (2018). *The Economic Costs of Ransomware and Cyberterrorism*.
- Department of Homeland Security (DHS). (2024). *Guidelines to Mitigate AI Risks to Critical Infrastructure*.
- Lyngaas, S. (2024). *Foreign Cyber Threats Against U.S. Transportation Infrastructure*.
- Wagman, R., & Nicula-Golovei, G. (2022). *Artificial Intelligence and Machine Learning in Nuclear Surveillance*.
- Yehoshua, S. (2023). *Advances in Data Breach Detection and Containment Through AI*.

University of Texas at Tyler – Center for Cybersecurity and Data Analytics

Dr. Tom Roberts is a Professor of Information Systems for the Computer Science Department in the College of Business & Technology at the University of Texas at Tyler. He was formerly the Director of the Center of Information Assurance, Information Systems Coordinator and Clifford R. King Professor of Information Systems at Louisiana Tech University. He received his MBA and Ph.D. in Information Systems from Auburn University and BA degree from the University of Oklahoma.

At Louisiana Tech, Dr. Roberts was the Project Lead for the university's pursuit of NSA/DHS National Center of Excellence (CAE) in Cyber Defense Education and NSA/DHS National Center of Excellence in Cyber Defense Research (CAE-R). Currently, Louisiana Tech is one of only 35 universities in the United States to achieve both designations.

Dr. Roberts explained that the state of Texas can make a difference in cybersecurity by having all of the employees in all organizations to perceive cybersecurity as safety, not just for them personally, but for the organization. Something that creates a safety guideline that employees can follow to enhance cybersecurity.

Dr. Roberts went on to discuss the ransomware attack at UT Health East Texas in November of 2023. According to Dr. Roberts, they are still working to recover from the attack. This attack happened due to an employee downloading a file onto their computer, which was the ransomware file. In this particular case, Dr. Roberts' first thought was "lives are imbalanced". UT Health East Texas was forced to redirect patients to different hospitals because the cyber attack led to them not having access to patient records, including patients not being able to have their prescription filled. Dr. Roberts emphasized that hospitals are a major target to these foreign adversaries.

Texas Pipeline Association

Thure Cannon serves as president of the Texas Pipeline Association (TPA). Prior to joining TPA in 2010, Mr. Cannon worked in the Texas Legislature for over 12 years serving as chief of staff for a state representative. Before his legislative tenure, Mr. Cannon consulted on numerous political campaigns and interned for members of the Texas House and Texas Senate.

Mr. Cannon holds a Master of Public Affairs degree from the Lyndon B. Johnson School of Public Affairs at the University of Texas. He has been a guest lecturer on Texas campaigns at the Lyndon B. Johnson School of Public Affairs and has been a speaker at conferences and service clubs on the Texas Legislature and politics.

Mr. Cannon discussed the industry's resiliency efforts and investments in controls and firewalls. Mr. Cannon explained that systems have improved since the Colonial pipeline hack of 2021. The "vast majority" of attacks are stopped, but attacks are becoming more sophisticated.

Association for Uncrewed Vehicle Systems International

Scott Shtofman is a policy and operations advocate with a focus on uncrewed systems and is the Senior Manager of Grassroots Advocacy at the Association for Uncrewed Vehicle System International (AUVSI). His work at AUVSI, the largest nonprofit dedicated to the advancement of uncrewed systems, is focused on advocacy at the state and federal levels through management of their vast member and chapter network. Mr. Shtofman knows how to navigate the complexities of advanced drone operations from inception to implementation while gaining public acceptance along the way and simultaneously considering sales and go-to market strategies. This experience stems from his drone service and consulting business, Quad Axis LLC, which he founded and ran for more than 6 years. Mr. Shtofman has passionately advocated for the safe integration of drones into the National Airspace System (NAS) through his work on the Beyond Visual Line of Sight (BVLOS) Aviation Rulemaking Committee (ARC) and various state committees. That work has ranged from small systems to traditional aviation and to Advanced Air Mobility (AAM) and electric Vertical Takeoff and Landing (eVTOL) platforms. Mr. Shtofman's state specific work is seen in Drone Prepared, a national campaign focused on industry vetted, common sense model legislation, to enable the future of advanced aviation technology around the country. Mr. Shtofman is a licensed attorney in Texas, a Part 107 certificated remote pilot, OSHA 30 certified, and a member of multiple standards setting organizations in the uncrewed space. He provides insightful industry commentary and analysis through participation in conference programs, publishing articles, and working directly with regulators on crafting new legislation. Mr. Shtofman holds a JD from the University of Texas, an MBA from Indiana University, and a BSBA from Indiana University.

The uncrewed systems industry in the United States, encompassing drones and other autonomous technologies, faces significant competition and security challenges. These challenges are exacerbated by hostile foreign entities, particularly from the People's Republic of China (PRC), which dominates the uncrewed aircraft systems (UAS) market through aggressive state subsidies and extensive cyber capabilities. The Texas State government has taken proactive measures, such as banning PRC-made drones from government use, reflecting a growing awareness of national security risks associated with foreign UAS technology (Cybersecurity Guidance, 2024).

Foreign dominance in the UAS market, primarily led by Communist China's DJI, poses both economic and security threats to the United States economy and critical infrastructure. Supported by PRC subsidies, DJI drones have captured the majority of the global market, raising concerns about potential cyber espionage, data security, and the integrity of U.S. infrastructure (Select Committee on the CCP, 2024). As the U.S. House of Representatives acknowledged in its passage of the Countering CCP Drones Act, future PRC drones could soon be banned from U.S. airwaves, marking a step toward limiting these foreign incursions (Countering CCP Drones Act, 2024).

The "Made in China 2025" initiative represents a coordinated effort by the Chinese government to dominate strategic sectors, including UAS. Intellectual property theft from U.S. companies alone costs the economy billions annually, and the PRC's policy of systematic theft stifles U.S. innovation by dissuading investment and reducing competitiveness in the market (FBI, 2019; PBS, 2021). The UAS sector's vulnerability to these practices is notable as it involves rapid technological advancements, including drone delivery services, which have drawn investments from both large corporations and small businesses alike.

At the federal level, Executive Orders from the Trump and Biden administrations have acknowledged the risks associated with PRC-manufactured drones, implementing measures to restrict procurement and investment in such technologies (Executive Order on UAS, 2020). In addition, the Federal Communications Commission (FCC) and the Cybersecurity and Infrastructure Security Agency (CISA) have issued advisories highlighting potential security risks posed by Chinese-made UAS (CISA, 2024).

State actions have similarly reflected these concerns. Texas, for example, recently placed DJI on its prohibited technologies list, aiming to mitigate risks by blocking procurement of these drones by state agencies (Texas DIR, 2024). Texas' economic prominence and strategic infrastructure make it a priority for robust defenses against cyber and economic espionage.

Amid these threats, the United States UAS industry has significant opportunities for growth. Domestic investment in UAS manufacturing, training, and maintenance facilities could strengthen supply chains and foster a competitive edge. State initiatives, particularly in Texas, can drive innovation and reinforce national values of security and entrepreneurship while positioning Texas as a leader in UAS technology (AUVSI White Paper, 2024). With policies that balance security and support for entrepreneurship, Texas and other states can mitigate risks posed by foreign actors while promoting American leadership in uncrewed technologies.

Sources:

- Cybersecurity Guidance on Chinese-Manufactured UAS. (2024). Cybersecurity and Infrastructure Security Agency.
- Select Committee on the CCP. (2024). March 19, 2024, Letter on PRC UAVs.
- Executive Order on Protecting the U.S. from Certain Unmanned Aircraft Systems. (2020).
- FBI. (2019). China: The Risk to Corporate America.
- AUVSI White Paper. (2024). Partnership for Drone Competitiveness.
- PBS. (2021). Made in China 2025: The Industrial Plan.

COMMITTEE HEARING ON OCTOBER 16TH, 2024 – AUSTIN, TEXAS

The Committee held a public hearing on October 16th, 2024, with both invited and public testimony.

The individuals listed below provided testimony to the Committee on this charge.

Public Hearing: October 16th, 2024

Witness List: October 16th, 2024 – Austin, Texas, Capitol Extension E2.010, at 10:00 a.m.

Panel 1

- Adam Klein, University of Texas at Austin - Robert Strauss Center for International Security & Law

Panel 2

- Chris Wolski, Applied Security Convergence LLC
- Brooks Lobingier, Port of Corpus Christ

Public Testimony

- Hugh Li, Austin Chinese American Network
- Sabrina Sha, Asian Texans for Justice
- Alice Yi, Asian Pacific Islander American Public Affairs

Registered but did not testify:

- Adam Savit, The American First Policy Institute

The information below is largely based on the oral and written testimony of the invited individuals and organizations above.

University of Texas at Austin – Robert Strauss Center for International Security & Law School

Adam Klein is with the Strauss Center at the University of Texas at Austin and also a professor of Law at UT Law. The Strauss Center advises national and state policy makers on intelligence, counter terrorism, foreign policy national defense, cybersecurity, artificial intelligence (AI) and other emerging technologies.

Additionally, the Texas Cybersecurity Clinic at the Strauss Center provides free cybersecurity services to Texas-based nonprofits, small businesses, and state and local government entities. The Strauss Center also provides UT Austin undergraduate and graduate students with career-launching experience, building our state's cybersecurity workforce while leveraging cybersecurity leadership at UT Austin and advisors from public and private sector organizations to foster robust resilience in Texas.

Professor Klein explained, foreign actors pose various threats to our state, which can be categorized into four main types: espionage, cyber-crime, subversion, and Iran's efforts to support certain protest movements.

Espionage involves covert operations to gather information about individuals, facilities, or technologies of interest to foreign governments. These operations can occur in the physical world, with reports of Chinese citizens using drones to fly over sensitive sites in the United States. Additionally, espionage also takes place in cyberspace, with hackers targeting computer networks to steal intellectual property and personal data.

Cyber-crime specifically focuses on ransomware attacks that can disrupt schools, hospitals, and critical infrastructure. The Texas Cyber Security Clinic by the Strauss Center offers free assistance to Texas organizations and small governmental bodies such as school boards following ransomware attacks.

Subversion involves tactics such as cognitive warfare and clandestine efforts to influence Americans and erode trust in institutions. TikTok poses a primary threat in this category. The algorithm that chooses which content users see is opaque and is controlled and updated from Beijing.

The final category is something that the federal Director of National Intelligence has recently warned of and that is Iran's efforts to support certain protest movements and other activities since the October 7th attacks of Israel. State authorities should likewise be concerned about activities in preparation of armed conflict, particularly with Communist China. Texas facilities would be a crucial part of the United States response in a potential conflict with China, including energy facilities, ports, military bases, and intelligence facilities. China could target these facilities through cyber attacks, hacking traffic systems, disrupting ports, and using online cognitive warfare tactics to sow fear and undermine national unity. The massive amounts of user data collected by apps like TikTok, especially considering the fact that the data is stored on servers accessible to personnel based in China, poses significant risks.

Additionally, there is a possibility of physical sabotage, similar to what Russia has done in Europe. While the government is becoming increasingly aware of these threats, more action needs to be taken to address them effectively.

Professor Klein emphasizes the importance of local cyber security measure in the state of Texas. While international targets like NSA and Microsoft have their own defenses, the focus should be on protecting local systems. Hostile actors could disrupt traffic systems or school districts, impacting workforce indirectly. In order to counter such threats, Texas should identify vulnerable areas within its responsibility, such as school districts, electrical grids, and traffic systems. Legislative action at the state level can significantly increase resilience against cyber attacks by making these non-traditional targets more challenging for adversaries. Professor Klein believes that we must think like an intelligence officer and anticipate how adversaries would exploit the state's most sensitive and weakest points to enhance overall cyber security.

Applied Security Convergence LLC

Mr. Wolski, with Applied Security Convergence LLC, was with the Port of Houston during a nation-state cyber attack four years ago. Mr. Wolski recounted that the attack occurred rapidly, with the aggressor taking control of the server within seconds of hitting it. Mr. Wolski emphasized that maritime and energy small and medium enterprises are vulnerable to such attacks, as staff may not immediately notice the breach. However, the Port of Houston was able to detect and halt the attack within 10 minutes, an unusually quick response that prevented further damage.

Due to lack of resources, small/medium enterprises struggle to conduct necessary cyber security due to diligence and maintenance. To address this issue, a Maritime Cyber Security Center of Excellence is being established in collaboration with the University of Houston and other organizations. This initiative aims to provide mutual support among regional entities for cyber security efforts.

Port of Corpus Christi

The Port of Corpus Christi is the number one crude export gateway in the United States, number two United States port for LNG exports, and the third largest exporter for crude oil in the entire world. Mr. Brooks Lobingier, Director of Information Technology, Port of Corpus Christi explained that the Port of Corpus Christi has a significant economic impact in Texas, creating over 95,000 jobs in the state. Capital investments in the Coastal Bend region have reached \$65B in the past decade.

The port has implemented strategies to protect its assets from cyber threats, including advanced persistent threats from countries like China, Russia, North Korea, and Iran. These threats target not only the port's information systems, but also vulnerabilities within customers and third-party suppliers to gain access to secured data.

The trends indicate we are on track to see the highest number of cyber attempts since we began tracking these metrics in 2020, Mr. Lobingier said, citing a 28% increase in cyber attacks per year. The Port of Corpus Christi is prioritizing information security to combat these increasing cyber threats. The Port, which has two security certifications, adheres to the highest industry standards in cyber risk management, following the National Institute of Standard Technology and the International Organization for Standardization 2701 framework. These frameworks are known for establishing best practices for information security systems.

RECOMMENDATIONS

Create a Statewide List in Statute of Designated Hostile Foreign Countries and Organizations

In order to craft meaningful and effective legislation that will protect Texas against hostile foreign actors and enhance state security, the state should create and maintain a list of designated hostile foreign countries and designated hostile foreign organizations.

A similar statutory list was created, known as the Lone Star Infrastructure Protection Act, or (“LSIPA”), in 2021. This list allows the Governor – in consultation with the public safety director of the Department of Public Safety and the Homeland Security Council – to identify countries that present threat to critical infrastructure in Texas.

A statutory list modeled after the existing LSIPA will enable the state to identify threats and craft solutions based on these threats.

Conduct a Statewide Pacific Conflict Stress Test

Communist China has conducted multiple simulated exercises preparing for an invasion and blockade of Taiwan. Should Communist China choose to move beyond exercises and execute an actual invasion of Taiwan or conflict in the Pacific theater on an even larger scale, the State of Texas must be prepared to minimize the disruption to our supply chains and critical infrastructure.

In order to be prepared for this possibility, Texas should conduct a Statewide Pacific Conflict Stress Test that will provide a detailed assessment of state preparedness. During this stress test, prioritized attention should be paid to our supply chain and critical infrastructure cybersecurity, as Communist China has been already executing probing attacks on these systems.

Protect Texas Land

Texas should act to prohibit hostile foreign actors, who intend to do us harm, from owning land in the state. This prohibition should extend to hostile foreign governments, entities controlled by hostile foreign governments, and persons living in countries with hostile foreign governments.

Care should be taken to ensure that the rights of American citizens and lawful permanent residents are not infringed upon. All efforts to protect Texas lands should be made in good faith without regard to a person’s immutable characteristics.

The legislature may consider prioritizing agricultural land, land adjacent to or within close proximity to military installations, and land adjacent to or within close proximity to critical infrastructure.

Diversify Supply Chains

Regardless of potential future conflict that may be instigated by hostile nations and disrupt our supply chains, diversification of our supply chains should be prioritized.

Texas should work to recruit companies to Texas that manufacture critical infrastructure components, pharmaceuticals including active pharmaceutical ingredients (API) and antibiotics, and other products that are critical to the health, safety, and welfare of Americans.

Enhance Foreign Agent Registration Act and Apply to Advocacy in Texas

Create a state-level process requiring registration of foreign agents who are engaged in political activity. A state-level FARA will address existing loopholes with the federal registration process and ensure that lobbying and advocacy on behalf of foreign agents is disclosed for the benefit of the public and of the policymakers.

Ban Sister Cities Arrangements with Cities Located in Countries on Hostile Foreign Country or Organization List

Sister City partnerships foster international engagement and cultural exchange at the local level. While these agreements can promote mutual understanding, they also present risks. Foreign adversaries, such as Communist China, have used Sister City agreements to disseminate propaganda, manipulate city officials, and promote policies aligned with their geopolitical goals. Despite Communist China's ongoing human rights abuses and efforts to undermine U.S. interests, many U.S. states and cities still maintain active agreements with Chinese municipalities.

Texas should prohibit Sister City agreements with foreign adversaries to protect against undue influence and propaganda efforts. These partnerships can serve as entry points for coercion and the spread of narratives that undermine U.S. interests. Texas, along with other states, should reassess and sever ties with foreign adversaries that pose national security risks.

In 2024, Indiana and Utah both passed legislation regarding Sister City partnerships.

- Indiana
 - Passed House Bill 1120 with strong bipartisan support (73-21 in the House; unanimous in the Senate).
 - This legislation prohibits Sister City agreements with foreign adversaries to mitigate risks of external influence.
- Utah
 - Enacted House Bill 404, banning partnerships with municipalities involved in forced labor.
 - The bill passed unanimously in the House and 25-2 in the Senate, reflecting broad legislative consensus on the importance of ethical international engagement.

To safeguard local governments from foreign influence and ensure alignment with national interests, Texas should follow Indiana and Utah’s example by prohibiting Sister City agreements with foreign adversaries. Such measures enhance transparency, limit the spread of propaganda, and reinforce ethical governance at the local level.

Revoke and Prohibit Future Business Licenses and Certifications for Individuals and Entities Convicted of Intellectual Property Theft

In order to protect the intellectual property of Texans and their businesses, the Legislature should consider a process to revoke a business registration of an entity who is finally adjudicated to have committed a violation of the Texas Uniform Trade Secrets Act. Upon a country finding of a violation, the Secretary of State could notate on a business registration that the registrant has a pending conviction against them. Upon a final conviction, the Secretary of State would revoke the business license of the offending entity. Alternatively, a judge could order the revocation of the business license as a means of relief for the claimant.

Unmanned Aerial Vehicle Security

The market for unmanned aerial vehicles (UAV) – also known as drones – is dominated by drone manufacturers located in Communist China. This presents a significant security threat, especially when the unmanned aerial vehicles are deployed in pursuit of law enforcement and other first responder objectives.

Da-Jiang Innovations (DJI), in many states, provides the government with more than 90% of all drones. The United States Department of Defense has classified DJI as a Chinese Military Company operating within the U.S. and the Treasury Department has sanctioned DJI for human rights abuses.

In 2023, the State of Florida adopted drone scrutiny imposing various levels of use restrictions on state agencies with rule 60GG-2.0075. These levels are as follows:

- Tier One;
 - Drones that do not collect or transmit data during flight (Example: Pre-programmed drones).
 - Used primarily for instructional purposes.
- Tier Two:
 - Drones that collect or transmit flight control data, but not visual or auditory data.
- Tier Three:
 - Drones that collect and transmit any type of data, including visual and auditory data.
- Research Exemption:
 - Drones used by educational institutions for research are exempt from certain requirements, but must balance research goals with security risks.

The legislature should amend procurement law to prohibit future purchase of unmanned aerial vehicles by first responder agencies.

The legislature should also consider standing up a grant program to phase out unmanned aerial vehicles manufactured in hostile foreign countries currently in use by first responders.

University Gifts/Grants/Research

The risks posed by foreign adversaries exploit vulnerabilities within state higher education systems. Universities, as hubs of innovation, research, and global collaboration, may inadvertently expose themselves to espionage, coercion, or undue influence. Implementing enhanced security measures across multiple domains will help protect these institutions from becoming gateways for foreign interference and ensure national security remains intact.

There are four key threats to higher education.

1. Foreign Gifts and Contracts

- Foreign governments and entities may leverage large donations or contracts to influence university operations, including academic programs, hiring decisions, or research agendas.
- Insufficient transparency around the source and conditions of foreign funding creates opportunities for undue influence that can undermine institutional integrity.

2. Foreign Researchers and Talent Recruitment Programs.

- Some adversarial nations use foreign researchers or recruitment programs (such as China's Thousand Talents Program) to gain access to sensitive technologies and intellectual property.
- These individuals, while contributing academically, may pose risks by transmitting research findings or technology back to their home governments.

3. Carelessness While Traveling Abroad

- Faculty, students, and researchers traveling internationally are at risk of being surveilled, coerced, or having their devices compromised.
- Laptops and research data may be exposed to cyber threats or espionage if insufficient precautions are taken.

4. Exploited Research Partnerships

- Collaborative research with foreign institutions can expose universities to risks when partnerships are not properly vetted.
- Foreign adversaries may exploit joint research projects to gain access to classified information, cutting-edge technologies, or intellectual property.

Policy Recommendations to Protect National Security

- Increased Scrutiny of Foreign Gifts and Contracts:
 - Mandating full disclosure and monitoring of foreign contributions to universities will help prevent undue influence.
- Enhanced Screening of Foreign Researchers:
 - Universities should adopt vetting procedures for visiting scholars and foreign researchers, especially in sensitive research areas.
- Travel Security Protocols:
 - Institutions must educate faculty and students on cybersecurity practices and protocols when traveling to high-risk areas.
 - Encrypted devices and virtual private networks (VPNs) should be provided to protect sensitive research data.
- Evaluating Research Collaborations:
 - Research partnerships should undergo thorough risk assessments to ensure they align with national security interests.
 - Government-university partnerships can help develop frameworks for managing international collaborations more effectively.

Foreign influence, espionage, and coercion within higher education systems present significant challenges to national security. Universities must balance the pursuit of academic collaboration with the need to protect sensitive research from foreign exploitation. Increased scrutiny and security measures across domains such as foreign funding, travel, research partnerships, and foreign researchers are essential to safeguarding public universities and preventing them from inadvertently undermining national interests.

Divestment of State Pension Funds from Companies Headquartered in Hostile Foreign Countries or Organizations List

States have invested heavily in China, with recent estimates showing \$68 billion allocated to Chinese assets, including billions from Texas. [1]

Allowing public funds to be invested in foreign adversaries presents risks to national security and fiduciary responsibility.

The first key concern is the lack of transparency. A report from the House Select Committee on the Chinese Communist Party (CCP) highlights the risks of United States capital flowing into China without clarity on how the funds are being used. This lack of information compromises market integrity and investor protection. [2]

The second key concern is the violation of fiduciary duty. Experts like Roger Robinson, from President Reagan's National Security Council, argue that investing in China inherently breaches fiduciary responsibility, given the national security risks. [3] Texas hedge fund manager Kyle Bass echoes this concern, urging that such investments undermine financial accountability.

Lastly, the third key concern is human rights and financial risk. Missouri Treasurer Vivek Malek spearheaded efforts to divest the state's pension fund from Chinese assets, citing poor financial performance, national security concerns, and involvement in human rights abuses.

State-level legislation in states such as Tennessee and Indiana have introduced laws to restrict or prohibit investments in Chinese assets. Governors from Iowa, Texas, Mississippi, and South Dakota have urged Vanguard to provide investment options that exclude Chinese market exposure. [4]

Policy Recommendations are as follows:

1. Prohibit Public Investments in Foreign Adversaries:
 - Enact state-level legislation to prevent public funds from being allocated to Chinese or other adversarial markets.
2. Increase Transparency in State Pension Funds:
 - Require detailed disclosures on how public investments align with national security interests and fiduciary duties.
3. Divest from Risky Foreign Assets:
 - Follow Missouri's lead by divesting from Chinese markets and reallocating to safer investments.
4. Promote Alternative Investment Options:
 - Work with financial institutions to develop emerging market funds without exposure to adversarial nations.

References:

- [1] [Future Union: Pensions](#)
[2] [House Select Committee on CCP Report](#)
[3] [CECC Hearing on Corporate Complicity](#)
[4] [Joint Governors' Letter to Vanguard](#)

K-12 Curriculum and Data Protection

Adversary-controlled entities have made inroads into the United States K-12 education system, creating risks through curriculum control, tutoring services, and data collection. The presence of companies connected to foreign adversaries within K-12 education introduces potential pathways for undue influence, data exploitation, and long-term ideological manipulation. To safeguard children's education, states must enact policies that ban adversary-controlled entities and closely scrutinize contracts, gifts, and exchanges with foreign nations.

Foreign-owned tutoring services are an area of concern. Tutor.com and Princeton Review, two prominent tutoring platforms, are owned by China's Primavera Capital. Primavera also holds investments in ByteDance, the parent company of TikTok, raising concerns about the control influence such entities may wield over student data and educational materials.

The second area of concern is cultural and educational exchanges. Adversary-controlled cultural exchanges and financial gifts to school systems may serve as avenues for infiltration. Through these means, adversaries could embed narratives or collect data in ways that circumvent local oversight, influencing curricula and fostering dependency on external educational providers.

The third area of concern is the risk of data exploitation. The involvement of foreign adversaries in education, particularly those with connections to companies managing sensitive student data, creates vulnerabilities. Without strict oversight, student information may be harvested for purposes beyond educational use, raising privacy concerns and national security risks.

-
1. Ban Contracts with Adversary-Controlled Entities
 - States should explicitly prohibit contracts with foreign-controlled education services such as Tutor.com and Princeton Review. Additionally, they should extend this prohibition to any vendor with ties to nations identified as adversaries, ensuring no indirect channels remain open for influence.
 2. Increased Oversight and Scrutiny
 - State education departments should implement stricter monitoring mechanisms for financial gifts, partnerships, and contracts with foreign entities. An auditing process, modeled on federal CFIUS (Committee on Foreign Investment in the United States) reviews, could help mitigate risks.
 3. Precedent for Action

Florida has taken proactive steps by issuing a warning to school districts against using services from Tutor.com and Princeton Review. This initiative underscores the importance of prompt intervention to protect the education system from foreign influence.

Lone Star Infrastructure Protection Act (LSIPA) and Public Utility Regulatory Act (PURA)

1. Add a financial penalty in PURA for Market Participants who provide false or incomplete information to ERCOT on LSIPA attestations and reports regarding: a) citizenship, ownership, or headquarters; or b) purchases of critical electric grid equipment or services. [Amending Tex. Util. Code Sec. 15.023]
 - The penalty could be set up to \$1 million per violation or some other appropriate amount.
 - The Texas Utilities Code already authorizes up to \$1M penalties for violations of other important obligations like weather preparedness. *See* Tex. Util. Code Sec. 15.023(b-1)(permitting fines of \$1M per violation for violating weather preparedness rules).
 - The Public Utility Commission of Texas (PUCT) enforcement division, supported by the ERCOT Reliability Monitor, already monitors all reliability rules in the ERCOT Region.
 - Adding this increased penalty amount should enhance due diligence and compliance of all Market Participants and create more confidence in the accuracy of the information given to ERCOT.
2. Add language in PURA authorizing ERCOT to request additional information from Market Participants regarding their responses in LSIPA attestations or reports regarding: a) citizenship, ownership, or headquarters; or b) purchases of critical electric grid equipment or services. [Amending Tex. Util. Code Sec. 39.360]
 - Allowing ERCOT specific authority in the statute will streamline any potential disputes with Market Participants that may argue additional information is not necessary or confidential in nature.

3. Add language in PURA that gives ERCOT clear authority to proactively hand over information to the Texas Office of the Attorney General (OAG) regarding suspicious LSIPA attestations or any other additional information and OAG can provide ERCOT and PUC with new information obtained as part of any investigation to protect critical infrastructure. [Amending Tex. Util. Code Sec. 39.360]

- ERCOT currently has very limited ability to research or investigate the truthfulness or accuracy of LSIPA attestations (outside of publicly available information).
- OAG currently has authority to audit LSIPA attestations regarding purchases of critical electric grid equipment or services but not attestations relating to citizenship, ownership, or headquarters. *See* Tex. Util. Code Sec. 39.360(i).
- OAG (or another appropriate agency) might leverage investigatory resources or authority, including relationships with other state or federal agencies, to investigate Market Participant ties to China, Russia, Iran, or North Korea.

This proposal would establish a clear state agency partner for ERCOT to collaborate with when there are suspicious circumstances regarding LSIPA attestations and expand the investigatory resources available to ERCOT.

RELEVANT NON-COMMITTEE ACTIONS

In November 2024, Governor Greg Abbott issued four directives to state agencies that overlap with the jurisdiction of this Committee.

On November 18, 2024, Governor Abbott issued an executive order requiring the Texas Department of Public Safety to identify any persons engaged in harassment or coercion against Chinese dissidents and bring appropriate criminal charges, to work with local and federal law enforcement partners in assessing incidents of transnational repression by foreign adversaries within the state, and to expand avenues for the reporting of such activity. Additionally, GA-47 requires the Department to provide recommendations to the Legislature on countering such threats.

The following day, the Governor issued two executive orders: GA-48, prohibiting certain state agencies from entering into new contracts or extending existing contracts with companies from certain hostile countries, and GA-49, ordering the Texas Division of Emergency Management to convene, in coordination with relevant state agencies, a task force to survey state and local government vulnerabilities and to recommend policies and best practices for addressing them. Further, GA-49 directs agencies to conduct an annual tabletop exercise simulating a cybersecurity attack by a foreign entity. Additionally, the order requires the Public Utility Commission to conduct an annual tabletop exercise on how the state will respond to a “black start event” in the event of, or as a result of, an overseas conflict.

On November 21, 2024, Governor Abbott issued a letter directing state agencies to divest any existing investments in China and prohibiting new investments of state funds in China. Governor Abbott concluded his letter by writing that “Texas will defend and safeguard itself and our public treasury from any potential threat, including those posed by the CCP.”

Each of these actions taken by Governor Abbott addresses threats posed by hostile foreign governments to the economy and security of our state, issues that this committee was charged with studying. Further, each order issued by the Governor, as well as his letter, aim to achieve similar objectives as recommendations provided in this report.

Governor Abbott’s directives, and the recommendations in this report, make clear that protecting Texas from hostile foreign organizations requires a whole of government response. The Legislature should consider codifying the Governor’s policies to ensure that these requirements continue. Because the Governor is limited in who he can provide direction to in these orders, the Legislature should ensure these orders are expansive so that all facets of state government are on guard against nefarious actions by hostile foreign governments.