Summary Brief: Cybersecurity in Texas and the
Texas Cybersecurity, Education and Economic Development Council

Texas Cybersecurity, Education and Economic Development Council (TCEEDC)

TCEEDC Summary/Timeline:

- Council originally created and authorized in 2011 by the 82nd Texas Legislature SB 988
- Council Composition:
  - 9 Members appointed by Executive Director of Tx Department of Information Resources (DIR)
  - Legislation required representatives from:
    - DIR
    - Office of the Governor
    - Higher-Education with cybersecurity related programs
    - Public Junior College with a cybersecurity related program
    - State Military forces liaison experienced in cybersecurity
    - Chambers of commerce, organizations or businesses with cybersecurity background
- TCEEDC chartered to conduct study and provide recommendations to:
  - Improve the infrastructure of the state's cyber security operations with existing resources and through partnerships between government, business, and institutions of higher education
  - Examine specific actions to accelerate the growth of cyber security as an industry in the state.
  - Report delivered December 1, 2012: *Building a More Secure and Prosperous Texas*
- The 83rd Regular Legislative Session passed multiple bills strengthening Texas' Cybersecurity posture:
  - SB 1597 – Required proactive protection of the state against cybercrime/similar security threats.
  - SB 1101 – Extended the TCEEDC for additional 2 years to be effective through 8/31/2015.
  - SB 1102 – Required DIR to designate a state Cybersecurity Coordinator and permitted DIR to implement other recommendations from the Council report.
  - SB 1134 – Required DIR to establish a state framework for cybersecurity.

TCEEDC Report - 3 Areas of Focus

- State Cybersecurity Infrastructure
  - Identify improvements needed to state infrastructure
  - Assess ability to coordinate cyber-security efforts among non-governmental entities within state
- Cybersecurity Industry Within Texas
  - How the security of cyber assets in the state's industries could be improved
  - How more industry could be attracted to the state to increase economic development
- State's Cybersecurity Educational Needs
  - Identify formal degree and certification programs
  - Address general cybersecurity awareness for Texas citizens

TCEEDC Findings

- No state-wide coordination of cybersecurity strategy beyond state agencies
  - Policy, Response, Industry Economic Development, Citizen Awareness Programs
- Lack of coordinated cybersecurity effort allows cyber-crime to outpace the development of a cybersecurity infrastructure to effectively counter those activities

- Several examples of innovation and cyber excellence throughout Texas, but mostly localized rather than programs to expand to regional or statewide models
- Lack of qualified cybersecurity workforce is significantly impactful to both economic growth and the protection of the state's cyber infrastructure

TCEEDC Recommendations (Summary Overview)

- Create a Cybersecurity framework for the state including:
  - State-level coordinator for cybersecurity efforts
  - Formal partnership between public and private sector leaders and cybersecurity practitioners
  - State program to foster improvement of cyber resiliency in both private and public infrastructure by establishing a baseline for cyber operations
  - Cybersecurity education pipeline to introduce cybersecurity initiatives from K – PhD

Evolution of the TCEEDC and the Texas Cybersecurity Council

The Texas Cybersecurity Council

- Formed in 2013 as authorized by SB 1102.
- Council Chair is designated State Cybersecurity Coordinator (DIR)
- Members include TCEEDC's membership expanded from original 9 members:
  - TCEEDC members integrated within the Texas Cybersecurity Council
    - DIR
    - Office of the Governor
    - Higher-Education with cybersecurity related programs
    - Public Junior College with a cybersecurity related program
    - State Military forces liaison experienced in cybersecurity
    - Chambers of commerce, organizations or businesses with cybersecurity background
  - Expanded members include:
    - State agency stakeholders for key programs: Primary (K-12) education system, Higher education system, Adults - Veterans groups.
    - Other partner members from private industry including large and small organizations representing a variety of key Texas industries.
    - More diverse geographic representation – 4 Major Texas Cities - San Antonio, Dallas, Houston, Austin
    - Overall diversity in organizations, industries, and verticals
- Create alignment with the overall state cybersecurity efforts unified under the branding "Texas Cybersecurity Council".

TCEEDC Recommendations – Progress to Date

The following is the current status of the recommendations noted in the 2012 TCEEDC report:

1. **Establishing a Texas Coordinator of Cybersecurity within the Office of the Governor** to provide a strategic direction to bring government and business leaders together as partners in securing the state's infrastructures and developing a strategy and plan to promote the cybersecurity industry within the state.

a. Authorized by SB 1102
b. DIR designated the State CISO, Edward Block as the state Cybersecurity Coordinator.
c. Some progress towards building public/private partnerships between state agencies and industry.
d. Limited progress coordinating efforts to leverage best practices among organizations throughout the state.

2. **Establishing the Business Executives for Texas Security (BETS) partnership** to bring public and private sector leaders and cybersecurity practitioners together to form a framework for knowledge sharing and collaboration, making non-proprietary and industry recognized best practices and solutions readily available for the collective improvement of cybersecurity across the state.
    a. Some efforts made towards creating partnerships through the Texas Cybersecurity Council and through individual efforts
    b. Engagement with the Texas CISO Council, a security intelligence and resource sharing initiative consisting of over 20 Texas security leaders from public/private organizations.
3. **Establishing a "Cyber Star" program** to foster improvement of cyber resiliency in both private and public infrastructures across the state and to increase public trust by establishing a baseline for responsible cyber operations.
    a. Not started – longer term initiative requiring a foundation from other recommendations
4. **Adopting the Community Cyber Security Maturity Model as a statewide guide** for developing a viable and sustainable cybersecurity program and fostering a culture of cybersecurity throughout the state.
    a. Not started
    b. UTSA is recognized as a national leader in this area – yet their expertise does not seem to be significantly utilized by entities in Texas. This is a good example of a local resource that could be better leveraged to the betterment of the state.
5. **Increasing the number of cybersecurity practitioners in Texas** to provide the expertise needed to grow cybersecurity investment and to protect the cyber assets of the state
    a. The Texas Cybersecurity Council education members are working to identify potential strategies
    b. Efforts have been made to work with federal and state military representatives regarding transition plans for veterans.
6. **Providing a consistent voice for industry** regarding cybersecurity policies in order to facilitate communication between the state and industry.
    a. Some efforts have been made toward creating partnerships through Texas Cybersecurity Council and individual efforts
7. **Continuing investment in higher education cybersecurity programs** in order to attract students to the cybersecurity field, spur research and development, and encourage institutions of higher education to become leaders in cybersecurity within their own communities.
    a. No new specific strategies, initiatives or additional funding currently identified
8. **Promoting collaboration, innovation, and entrepreneurship in cybersecurity** to facilitate the commercialization of university research and development and encourage the development of new businesses with innovative products and services in cybersecurity.
    a. No new specific initiatives currently identified at state level
9. **Developing a comprehensive cybersecurity education pipeline through the BETS partnership** to introduce cybersecurity initiatives from K-PhD**.**

a. The Texas Cybersecurity Council education members are working to identify potential strategies
b. Current initiatives to promote statewide participation in national events include:
    i. Cisco Networking Challenge, a public-private venture
    ii. Nationwide CyberAces and CyberPatriot programs.
    iii. CyberPatriot education/promotion - DIR facilitated events throughout the state in Fall 2013 to encourage participation by local school districts and has been working to promote cyber-focused summer camps at new venues.
c. DIR is facilitating the identification of key collaboration opportunities through various state agencies including the following: Texas Workforce Commission, Texas Education Agency, Texas Veterans Commission, and the Higher Education Coordinating Board.

10. **Reviewing and sharpening the leadership role of the Texas Department of Information Resources (DIR)** in establishing a sustainable Cybersecurity Awareness Program for all Texans.
    a. Texas CISO currently serving dual role as state Cybersecurity Coordinator and Chair, Texas Cybersecurity Council.
    b. No full-time/dedicated staff or additional funding allocated to state cybersecurity coordination or state awareness efforts
    c. Current awareness efforts include an electronic newsletter and partnership with DHS for National Cybersecurity Month events

84th Legislature – Interim Committee Charges related to Cybersecurity

Senate – Business and Commerce

- Cyber-security/Storage: Examine cyber-security efforts undertaken by state entities and study the legal, policy and privacy implications of the trend toward storage of personal, private and business confidential information in network attached storage, cloud storage and other developing data storage options rather than on local devices. Make recommendations on how to best protect Texans' financial and personal information.

House Committee on Economic and Small Business Development:

- Evaluate Texas's competitiveness with other states in recruiting and cultivating high-growth, high-tech industries, fostering economic development, and creating new jobs. Examine if current incentives and regulations assist or hinder the state's ability to compete with other states for economic growth and sustainability.

House Committee on Government Transparency and Operation

- Identify and address potential gaps in the state's cybersecurity policies and ensure personal information held by state agencies is secure. Address whether industry-accepted cybersecurity standards have been met by state agencies and state data centers and determine ways to promote a culture of cybersecurity awareness among users of state information resources.

- Study the use of commercial cloud computing by state agencies and institutions of higher education, including efficiencies surrounding a utility-based model, security impacts of transitioning to cloud computing, and cost-savings achieved by the utilization of commercial cloud computing services

- Study the impact of emerging technologies used by law enforcement and issues related to appropriate dissemination of the data provided by those technologies, including the impact of technologies on the operation of law enforcement agencies, the operation of the Public Information Act, and any appropriate safeguards for citizens and law enforcement officers who interact with those technologies or whose data is recorded. (Joint charge with the House Select Committee on Emerging Issues in Texas Law Enforcement)

House Committee on House Administration

- Identify and address potential gaps in the Legislature's cybersecurity policies and ensure the governmental and personal information held by the legislative or legislative service agencies is secure. Address whether industry-accepted cybersecurity standards have been met by the legislative and legislative service agencies and determine ways to promote a culture of cybersecurity awareness among users of legislative resources.

House Committee on Investments and Financial Services

- Study the current state of cybersecurity of financial institutions in Texas. Review state and federal laws, and evaluate what additional steps need to be taken to make financial institutions in Texas more secure.

House Committee on Public Education

- Examine the accessibility to broadband services for schools, libraries, and institutions of higher education. Study the feasibility and affordability of providing scalable broadband to schools and other public institutions. Research federal and state funding opportunities to support increased access to broadband. Review innovative efforts by school districts to integrate technology in the classroom. Explore ways to enhance high-tech digital learning opportunities in the classroom to improve student achievement and fulfill future workforce demands.

- Examine partnerships between higher-education institutions, public school districts and workforce that promote postsecondary readiness. Provide coordination recommendations to ensure vocational, career and technical education programs are more accessible. Determine the most effective ways to invest in these partnerships and programs to direct at-risk students to stable career paths. Examine current rules and laws limiting employers from providing meaningful internships, apprenticeships, and other opportunities. Consider new methods to finance workforce training programs and associated assets in high schools and postsecondary schools, including ways to reduce or eliminate these costs and options to incentivize businesses to invest in training equipment for schools. (Joint charge with the House Committee on Economic and Small Business Development)

House Committee on Urban Affairs

- Identify and address potential gaps in cities' cybersecurity policy and ensure that personal information held by cities and other municipal entities is secure