To: Senate Select Committee on Open Government
Senator Rodney Ellis, Chair
Senator Wendy Davis, Vice Chair
Senator Kevin Eltife
Senator Florence Shapiro
Senator Jeff Wentworth

From: Texas Cybersecurity, Education and Economic Development Council
Mr. Robert Butler, Chair
Dr. Gregory White, Vice Chair
Dr. David A. Abarca, CISSP
Dr. Frederick Chang
Mr. Angel Cruz
Ms. Mary Dickerson, CISSP
Mr. B. Keith Graff
Mr. Sam Segran, GIAC-GSLC
COL Timothy M. Smith, CISSP

Re: Texas Cybersecurity, Education and Economic Development Council Findings and Recommendations

Chairs and Committee Members:

The Texas Cybersecurity, Education and Economic Development Council (TCEEDC) offers the following written testimony as requested by the Senate Select Committee on Open Government relative to the Select Committee's Interim Charge 2: Examine the effectiveness of security measures used to protect electronic information held by state agencies and make recommendations for enhancing security, if needed.

With the advancement of technology and the proliferation of computer systems and networks, cyber security threats to Texas' government and industries are growing, evolving, and are outpacing Texas organizations' ability to provide effective protection for Texas' cyber environment. This includes putting the private information of Texas citizens, including our children, at risk.

In 2011, the Texas Legislature and the Governor, respectively, passed then signed S.B. 988 which authorized the creation of the Cybersecurity, Education, and Economic Development Council (TCEEDC). The Council was chartered to provide recommendations to the state of Texas regarding ways to 1) improve the infrastructure of the state's cyber security operations with existing resources and through partnerships between government, business, and institutions of higher education; and 2) examine specific actions to accelerate the growth of cyber security as an industry in the state.

In fulfilling its mandate, the Council examined three areas of importance: the State's cybersecurity infrastructure, the cybersecurity industry within Texas, and the State's

cybersecurity educational needs. Each of these areas yielded a number of findings with associated recommendations. The state's cybersecurity infrastructure was addressed in order to develop recommendations that could lead to both improving the state's own cyber security infrastructure as well as its ability to coordinate cyber security efforts among non-governmental elements within the state. Industry, a vital part of the cyber security environment, was examined from two standpoints – first, from the perspective of how the security of cyber assets in the state's industries could be improved and second, how more industry could be attracted to the state to increase economic development. Finally, the Council examined education from the perspective of both formal degree and certification programs as well as general cybersecurity awareness for Texas citizens.

Information Gathering

To arrive at a comprehensive understanding of the current cybersecurity environment in Texas, as well as determine consideration for recommendations, the Council utilized multiple approaches for gathering information including: public sector and industry surveys, interactive dialogues, public forums and discussions with cybersecurity experts, both within the state and throughout the nation.

Findings

The Council identified findings in several related areas. First, beyond state agencies, there is no statewide coordination of cybersecurity strategy (including policy, response, industry economic development, citizen awareness programs) nor widespread public-private partnerships in these areas. Subsequently, the lack of a coordinated cybersecurity effort allows cyber-crime activities to outpace the development of a cybersecurity infrastructure to effectively counter those activities. Second, while there are several examples of innovation and cyber excellence throughout the state, these efforts are mostly localized rather than programs to expand to regional or statewide models. Finally, the lack of a qualified cybersecurity workforce is significantly impactful to both economic growth and the protection of the state's cyber infrastructure.

Recommendations

The Council determined that the best way to accomplish the legislative mandate and create a sustainable cybersecurity environment for Texas would be to focus recommendations on the establishment of an appropriate cybersecurity framework for the State. Key components of the recommended framework include: creation of a state-level coordinator for cybersecurity efforts, establishment of a formal partnership between public and private sector leaders and cybersecurity practitioners, creation of a State program to foster improvement of cyber resiliency in both private and public infrastructure by establishing a baseline for cyberoperations, and the development of a cybersecurity education pipeline to introduce cybersecurity initiatives from K-PhD. Through its implementation, the framework is intended to provide a mechanism for the production of action plans that are timely and relevant to meet specific State needs. A critical factor for success, the recommended framework integrates participation from a wide-range of organization types throughout the State, including: state agencies, critical infrastructure industries, profit, non-profit and faith based organizations and public school districts providing

diverse perspectives in the areas of infrastructure, economic development and education. It is the Council's belief that the establishment of this framework is the most appropriate means for the State to effectively address cybersecurity concerns, both in the immediate timeframe and for the future.

State Agencies

As a component of the Council's information gathering efforts, the Council identified that all state agencies are required to maintain security best practices according to Texas Administrative Code (TAC) 202. While collaborative efforts within the State would strengthen the overall security posture of state agencies, the Council recognized that state agency compliance with TAC 202 requirements form a good foundation for ensuring basic protection of State of Texas information assets. Additionally, the Council identified the need to increase the number of cybersecurity practitioners throughout the State, not only to provide the expertise needed to grow cyber security investment in Texas, but also to protect the state's cyber assets.

Next Steps

The Council will present the details of each of our findings and recommendations in a report to the Governor, Leadership in the Texas Legislature, and other stakeholders titled, Building a More Secure and Prosperous Texas, on December 1, 2012.

Thank you for the opportunity to submit testimony.