May 3, 2021

The Honorable Chris Paddie
Chair
House Committee on State Affairs
The Texas Capitol
1100 Congress Ave.
Austin, TX 78701

The Honorable Ana Hernandez
Vice Chair
House Committee on State Affairs
The Texas Capitol
1100 Congress Ave.
Austin, TX 78701

Internet Association Supports The Cybersecurity Modernization Efforts In Texas Through SB475E

Dear Chair Paddie and Vice Chair Hernandez:

Internet Association (IA) represents the world's leading internet companies and supports policies that promote and enable internet innovation, including commercial cloud solutions. Our member companies are global leaders in the drive to develop lower cost, more secure, and innovative digital government services, with a focus on protecting both the civil servants delivering those services and the residents receiving them.

On behalf of our members, IA thanks you for your consideration of Senate Bill 475E (SB475E), a bill that will ultimately result in a comprehensive information technology (IT) risk and authorization management effort that every Texan can trust. IA supports the state's push towards that goal and looks forward to working with the Department of Information Resources (DIR) to continue improving the program once started, helping it to become a model for other states and organizations in many ways.

With two relatively minor but ultimately significant tweaks to the bill, SB475E will become the legislative foundation that will help create that model program. Considering the pace of modernization that was spurred by the pandemic and will continue long after it is over, ensuring the state uses the most secure possible cloud solutions is paramount. To that end, giving the dedicated staff and contractors at DIR the ability to choose solutions that *exceed* currently established standards or programs as well as the ability to iteratively roll out the requirement in phases will maximize the ultimate impact of the program.

First, the constantly shifting cybersecurity environment should be accounted for when a solution can be proven to exceed existing requirements. The language in Section 2054.0593(b) that was amended to provide for a level of reciprocity with the federal government was a great step forward towards supporting a holistic national cybersecurity strategy and Texas state legislators are to be commended for their foresight.[1] Ensuring that the state is able to take advantage of its streamlined processes when the federal government is unable to act, however, will help spur that national strategy even further, as there are a number of instances when industry participants who are deeply involved in

[1] *See* SB 475 Engrossed version, Page 2, Lines 7-15, https://capitol.texas.gov/tlodocs/87R/billtext/pdf/SB00475E.pdf (April 19, 2021)

the development of cloud security standards are operating at a level beyond existing federal risk and authorization management programs.

Currently, for example, the FedRAMP program maps their certification process to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4, a standard that was first published on April 30, 2013 and was last updated on January 22, 2015.[2] On September 23, 2020, NIST SP 800-53 Rev. 4 was replaced with NIST SP 800-53 Rev. 5, which according to NIST's own analysis, included a total of 698 changes that were "[m]ore than editorial or administrative" in nature.[3] On November 24, 2020, two months after the release of the updated standard, FedRAMP announced their plans to make the transition so that they can support NIST Rev. 5.[4] Since then, there was an update on December 10, 2020 to the standard itself and updates to crucial supplemental material on January 22, 2021.[5]

In order to ensure Texas can take advantage of the latest in cybersecurity research, there are a few approaches the state can take to emphasize compliance with standards and programs or to incentivize exceeding requirements of existing programs. Such a change will help Texas maintain the strength of the current language while providing the state the flexibility necessary to do more - but never less - than the federal government.

Second, a phased implementation will help ensure the state creates an optimal process that will be scalable and replicable across all state agencies. While it is understandably important to improve cybersecurity hygiene as quickly as is technically feasible, it is important to consider the operational and administrative feasibility. For example, FedRAMP certification can take up to three years before an authorization is provided and the Cybersecurity Maturity Model Certification (CMMC) program is being implemented over five years - with the start time already delayed, as it was understood that the process to onboard every contractor in the Defense Industrial Base (DIB) at once is not feasible.

In Texas, there are at least 100 vendors that state agencies work with who will be required to comply with this provision, many of whom provide critical and essential services to the state. Many of them focus their work to serve Texas and having them go through such a certification process and program, whether it is implemented by the state or through another entity, will often take more time and cost more in funding than is originally anticipated. Similarly, as the process to verify and maintain compliance with this program is implemented throughout the state, there will be a number of lessons learned and pain points felt that, when scaled or addressed, will make for an even better outcome than expected.

In order to ensure Texas can operate an optimal cybersecurity program, a phased roll-out that would provide contractors up to two years after the effective date to obtain certifications or prove compliance with existing standards, should be considered. This approach will provide benefits to the industry participants serving the state and the government employees tasked with overseeing their compliance.

[2] *See* NIST SP 800-53 Rev. 4, https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final (January 22, 2015)
[3] *See* NIST, "Analysis of updates between 800-53 Rev. 5 and Rev. 4", https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r4-to-r5-comparison-workbook.xlsx (January 22, 2021)
[4] *See* FedRAMP, "FedRAMP's NIST Rev5 Transition Plan", https://www.fedramp.gov/FedRAMP-NIST-Rev5-Transition-Plan/ (November 24, 2020).
[5] *See* NIST SP 800-53 Rev. 5, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (January 22, 2021)

By incentivizing the use of cloud solution providers that meet or exceed existing standards and programs while also using a phased roll-out to optimize and streamline the verification process, the state of Texas can position itself to have a cybersecurity program that serves as a national model.

This is a rare opportunity to provide every state, local, tribal, and territorial government as well as every educational organization an example of how each of these entities can address their unique security needs while still ensuring that a national approach to the safety and security of our data is supported.

With your support and inclusion of these suggested changes or additional clarification in the final version of SB475E, everyone in the Lone Star State will be able to trust that their most sensitive information is secure when in the hands of a state agency. We appreciate your time in considering our feedback and look forward to the opportunity to discuss the benefits of the bill and the proposed changes in further detail.

Most sincerely,

James Hines
Director, Government Affairs, Southern Region

Omid Ghaffari-Tabrizi,
Director, Cloud Policy

Cc: The Honorable Joe Deshotel
The Honorable Sam Harless
The Honorable Donna Howard
The Honorable Todd Hunter
The Honorable Phil King
The Honorable Eddie Lucio III
The Honorable Will Metcalf
The Honorable Richard Peña Raymond
The Honorable Matt Shaheen
The Honorable Shelby Slawson
The Honorable John T. Smithee

Enc: Suggested Redlines

Suggested Redlines From Internet Association

As was outlined in the first suggestion of the accompanying letter, there are ways Texas can provide state agencies with the ability to use tools that *exceed* existing federal risk and authorization management programs (RAMPs) while still supporting and maintaining a holistic national strategy.

Option 1 - Compliance with a standard, such as NIST SP 800-53 Rev. 5 or NIST SP 800-171 Rev. 2
Suggested edits to Sec. 2054.0593(b)

(b) The department shall establish a state risk and authorization management program to provide a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency. The program must allow a vendor to demonstrate compliance by submitting documentation that shows the vendor's compliance with a **standard or** risk and authorization management program of:

(1) the federal government; or

(2) another state that the department approves.

Option 2 - Ability to prove meeting or exceeding the requirements of existing RAMPs
Suggested edits to Sec. 2054.0593(b)

(b) The department shall establish a state risk and authorization management program to provide a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency. The program must allow a vendor to demonstrate compliance by submitting documentation that shows the vendor~~'s~~ ~~compliance with~~ meets or exceeds the security requirements of a risk and authorization management program of:

(1) the federal government; or

(2) another state that the department approves.

Option 3 - Flexibility for universities to research and use emerging and advanced technologies
Suggested edits to Sec. 2062.001(2)

(2) "State agency" means a department, commission, board, office, council, authority, or other agency in the executive, legislative, or judicial branch of state government~~, including a university system or institution of higher education as defined by Section 61.003, Education Code,~~ that is created by the constitution or a statute of this state.