

MEMO TO: Senator Steve Casano, Chairman, GAE Committee
Representative Ed Jutila, Chairman, GAE Committee
Mr. Aaron Frankel, Governor's Office

FROM: Bruce Carlson
President, Connecticut Technology Council

DATE: March 22, 2015

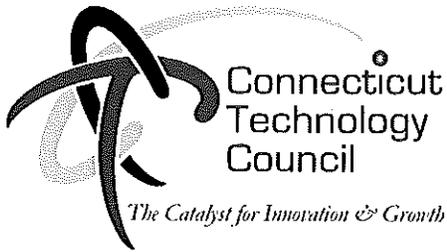
SUBJECT: SB 949 AN ACT IMPROVING DATA SECURITY AND AGENCY
EFFECTIVENESS

SB 949 addresses a number of issues and has great intentions of helping the public know when data breaches occur. We applaud the Governor and the General Assembly in their efforts to make the information more readily available.

Unfortunately, when SB 949 was on the agenda for the GAE Public Hearing, I was not aware of a few of the issues that negatively affect the Members of the Connecticut Technology Council (CTC). The CTC has nearly 300 members and represents the 3000 technology companies in Connecticut. Many of the members of the CTC are contractors to the State and would be affected by the provisions in Sec. 1 of SB 949. I am writing to you now with the hopes that as you consider the issues that have been raised in the public hearing and elsewhere, you can consider these points as well.

We live in a world where data breaches are increasingly common. To paraphrase the FBI Director, we have two types of business, those that know that they have been breached and those that haven't been made aware of it yet. Although stopping the data breaches would be the most desirable course of action, until that happens better managing the information concerning breaches is the best we can do. To that end, the CTC would recommend:

- Initial notice – We agree that the contracting agency and the Attorney General should be notified quickly if a data breach occurs. Within 24 hours raises a concern since there will be many moving parts at that moment trying to determine the extent of the breach, etc. It would be better if the bill allowed a little longer, 72 hours for notifications, so that such notification can appropriately be put into the data breach protocol of the companies.
- Detailed report within 72 hours – Experience is showing that in most cases the level of detail available concerning a data breach within 72 hours is vague and public notification at that point could lead to more problems than solutions. Sometimes it will take 3 weeks or more to understand the full extent of the breach, and what confidential information is affected. For instance, a breach could occur and the company would within 72 hours know that all of their customers were affected, but only through more thorough and forensic



examination determine that of those affected, only a small percentage had confidential information breached. We suggest a longer period of time, minimum 3 weeks, for the more detailed report,

- Penalties – As noted above, data being breached is becoming a fact of life. The “bad guys” have tools and knowledge that are staying steps ahead of the efforts to stop breaches from happening. We need to establish a minimum standard of data protection that any state contractor must have in place. If that state contractor has the minimum standard in place, and can show that the company has been rigorous in maintaining those standards, penalties should not apply. However, we fully support the idea of penalties for companies whose lax data management allows for confidential data to be accessed.

As you know other states have recently wrestled with or are currently wrestling with these same issues. I would be happy to provide you with information on how other states have addressed them.

Thank you for giving me the chance to let you know the concerns of the CTC members and I would be happy to work with you and the GAE Committee on developing language that results in better protecting the personal privacy of our citizens while recognizing the realities of the companies that serve as contractors to the State.