

**Testimony for the Public Hearing before the Public Safety and Security
Committee of the Connecticut General Assembly on HB 6317
Tuesday, February 17, 11:30 AM, Room 2B, Legislative Office Building**

Good morning, Senator Larson, Representative Dargan, and distinguished members of the Public Safety and Security Committee.

My name is Joseph Tolisano, and I work at Board of Regents, Connecticut State Colleges and Universities as the Chief Information Officer.

I am submitting this testimony in relation to the general concept raised in House Bill 6317: An Act Establishing Public-Private Partnerships to Provide Internet Security Training to account for the rising threats and attacks to computers, networks, data, and programs, and reduce vulnerability to such attacks.

The main threats to the State College and University System are malware attacks, advanced persistent threats, denial of service attacks looking to steal confidential data.

The system in collaboration with the colleges and universities is designing security controls and standards based on the NIST (National Institute of Standards and Technology) framework with the first priority being a protective enclave. There are 17 areas within the NIST framework that will be further developed to enhance security, primarily around the protective enclave, those staff (50-150) at each campus that have access to confidential data. The enclave requires you to map and inventory how confidential data (paper and electronic) is processed to include; how the data enters the campus, how the data is stored and finally how the data gets transmitted from the campuses. Within the enclave, you set up a secured network or VLAN a virtual network restricted to these 50-150 staff and protect the servers and desktops. The desktops have a standard configuration or image, meaning they all have the same software and the staff member doesn't have administrative rights to the system. Servers are built to a secure specification. The systems are also protected by Application White Listing. White listing only allows know good programs to make changes to the system, significantly reducing the risk of malware being installed by hackers or a user error. The confidential data will be encrypted at rest and in transmission. The standard requires you to inventory all confidential data within the institution and the computer systems and applications where the data is processed. To do this the BOR has setup data stewards, data managers and data users. Essentially, a data steward is an area vice president; this individual is responsible for all confidential data within his/her area. The data stewards appoint a data manager who will inventory all the data with respect to who has access, what machines access the data, where the data resides and what applications or enterprise software processes the data. The overarching goal is to limit and reduce, to the greatest extent possible; access by staff, processing steps and number of systems accessing the data all on the secure

network.

The BOR is in various stages of setting these critical steps in motion and have entered into a number of partnerships with industry leaders to monitor our security posture and data traffic flows on the firewalls to ensure the data is going to the correct destinations. Steps have been taken to train staff using SANS Institute online security courses. The course includes a series of 30 or more short videos on operational data security, with a test at the end of each segment. All staff with access to confidential data must take a 2 hour course initially and a 45 minutes refresher annually.

On many levels, through councils and committees this is taking place. CHERIS is the Connecticut Higher Education Roundtable on Information Security, which is a consortium of institutions and private sector firms discussing the role of security at Colleges and Universities. BEST also currently holds a monthly meeting with the Information Security managers at state agencies, UConn and CSCU. A more formal coordinated and state sponsored commission would expedite the transfer of knowledge and best practices, while providing much need administration and logistics to this important endeavor.

I believe there is a lot of good work and best practices taking place within the state of Connecticut, the commission will provide an opportunity for these efforts to be shared amongst all stake holders.