

**Commerce Committee  
Connecticut General Assembly  
TESTIMONY OF RAMESH SEPEHRRAD  
Vice President, National Governance, Risk and Compliance  
Comcast Cable  
February 26, 2015**

Good afternoon Chairwoman Hartley, Chairman Perone, and distinguished members of the Committee. My name is Ramesh Sepehrrad, and I am the Vice President of National Governance, Risk and Compliance at Comcast Cable. In my role, I oversee several security teams focusing on the protection of customer data, the security of Comcast's enterprise and service delivery networks, and all technology compliance- related activities.

I appreciate the opportunity to be here today to discuss SB 835 *An Act Concerning Cybersecurity*. The legislation aims to encourage the growth of a cybersecurity jobs pipeline and cybersecurity businesses in Connecticut. These are objectives that Comcast fully supports. Indeed, Comcast has worked hard over the last four years to develop and strengthen a partnership with the University of Connecticut designed to bolster cybersecurity research, training, and innovation.

I would like to briefly discuss our relationship with UConn, since I believe it highlights the value and benefits of partnerships between the private sector, academia and government that can help to bolster our local, state and national cyber defense capabilities, resources, and personnel.

With over 20 million residential and business broadband customers on one of the world's largest converged Internet Protocol-based voice, video, and data network, ensuring the safety and security of our network is one of Comcast's top priorities. Our customers depend on our network infrastructure to engage in commerce, access entertainment content, and conduct an increasingly wide range of activities and transactions. Deterring, detecting, and responding to cybersecurity threats and vulnerabilities is therefore a fundamental requirement for our continued business success.

Because of this, we have strong built-in incentives to utilize the most advanced tools, strategies, and protocols available today for preventing and addressing cybersecurity attacks. Our work with the Center of Excellence for Security Innovation at UConn is designed to help us identify those tools, strategies and protocols. It is an example of our strategic commitment to advancement of knowledge and preparation for future challenges for our workforce.

If I had to pick one word to encapsulate the key to sustaining a secure network environment at both the individual company level or the macro-sector level, that word would be *innovation*. Innovation signifies continuous effort, research, invention, creativity, and tenacity - and that is exactly what is needed to meet the challenges posed by today's dynamic and constantly-shifting cyber threat landscape.

Make no mistake: today's hackers, bot-masters, cyber criminals and other online malefactors are highly sophisticated technically. They are continuously innovating. We have to match or exceed their level of innovation, so that we are not constantly playing a game of catch-up or losing the initiative in the ongoing effort to preserve a safe and secure network environment.

The central importance of innovation is what drove Comcast to enter into its partnership on security matters with UConn - with a specific focus on hardware security. Beginning in 2011, UConn and Comcast teamed up on a number of special projects, spurring discussions on the issue of hardware security and the need for a more holistic approach to addressing the evolving challenges of cybersecurity.

These discussions coincide with the creation of UConn's Center for Hardware Assurance, Security, and Engineering ("CHASE"), a research consortium that brings together commercial, academic and government participants committed to enabling knowledge breakthroughs that shape future electronic systems. CHASE is one of only a select few cybersecurity research programs recognized at the national and government level. In 2013, Comcast and UConn began focusing more directly on hardware security vulnerabilities, initiating several special research projects in areas such as:

- Counterfeit Detection and Prevention
- Risk and Test Technology Assessment
- Development of Standard Tests and Measurements for Authentication
- Hardware Security and Trust
- Transistor-to-System Reliability Analysis
- Chip-to-system Level Test, Quality Analysis, Debug, and Diagnosis

Last year, Comcast expanded its relationship with UConn by establishing the Comcast Center of Excellence for Security Innovation (CSI). Launched as a joint venture between the UConn and Comcast, CSI is the country's first dedicated laboratory focusing on the research and testing of hardware security advancements. Comcast is currently the only company with a dedicated security innovation lab at a university in the United States.

CSI brings together the brightest minds from industry and academia to help develop cutting-edge security technologies, practices, and processes. CSI helps to provide training and education for the next generation of cyber professionals that will help Comcast and other organizations confront the cybersecurity risks and challenges of the future.

Through the CSI, Comcast draws students from UConn and other universities and engages them in research and training by, for example, sponsoring a series of challenges that address various parts of the computing infrastructure, including network architecture, software, and hardware. Like UConn and the participating schools, Comcast is focused on professional development and educating and grooming the cybersecurity workforce of the future.

CSI's dedicated research includes issues related to security assessments, hardware authentication, chip tampering, counterfeit detection, and chip agents. CSI illustrates the

mutually beneficial nature of partnership arrangements between the private sector and academia, as the acumen, expertise and resources of UConn's faculty, students and research facilities are brought to bear to help address real-world security issues. Students and faculty at the Center engage in vulnerability assessments of - and help design improvements for - hardware, software, and product platforms, providing them with first-hand exposure to cybersecurity issues and solutions in the marketplace.

“Security” encompasses a broad spectrum of techniques, tools, protocols, and practices. There is no one silver bullet or quick fix, especially because the risks and threats change so very frequently and dramatically as new technology is developed and as bad actors in cyberspace continue to adapt to the latest counter-measures and employ new techniques and tools. As a result, our security protections are never complete; we must continuously learn, invest, and work to improve and develop new capabilities to meet the ever-changing threats.

Effective cybersecurity can benefit immeasurably when government, industry, and academia work as partners to address cybersecurity problems and solutions in a cooperative and cross-disciplinary fashion. The Comcast-UConn relationship provides one example of how such partnerships can help develop new cyber defense tools, practices and protocols, and offer research and workforce training opportunities that address cutting-edge cyber issues.

By encouraging the development and expansion of a cybersecurity workforce here in Connecticut, SB 835 would help to forge new partnerships that can promote job training and expertise, boost the State's economy, and help provide a safe and secure network environment for Connecticut residents and businesses. The workforce training and business development program established under SB 835 can help lay the groundwork for the education and growth of the next generation of cyber professionals that will help Connecticut businesses and other companies and organizations across the country meet the cybersecurity risks and challenges of the future

Thank you for the opportunity to testify. I would be happy to answer any questions you might have.