Chairman Prozanski and Vice-Chair Thatcher, thank you for the opportunity to share the Sub-Zero Group, Inc.'s viewpoint in how Oregon bill HB2395 can be modified and receive our full support to provide the strong cybersecurity protections that the people of Oregon deserve.

Sub-Zero share's the goals of the Attorney General and the authors of the bill to prevent future events like the catastrophic Mirai botnet attack of October 12th, 2016 that crippled the internet of the majority of the United States for an extended period of time. However, this bill is ineffective in achieving that goal for two reasons:

- The definition of reasonable security provides for the use of passwords – a basic element the Mirai vulnerability, and is not dynamic enough, nor clear enough to prevent future attacks as cybersecurity evolves.
- The current definition of manufacturers allows the class of devices that caused the Mirai botnet to be exempted

While we are appreciative of the authors efforts to provide flexibility within the bill to address future cybersecurity threats through the "reasonable security efforts" language, and included safe harbors, the current language and safe harbors open Oregon to significant cyberattacks. Passwords as a security measure, even unique per device, are already considered compromised as a security measure in practice today. Hardcoded passwords were the basis of the Mirai attack, and continuing to offer safe harbor for the use of passwords is not reflective today's state, let alone the evolving nature of cybersecurity. To appropriately provide a strong, clear measure by which products can be designed to, which can evolve at a rapid pace, we respectfully request that language be included to use National Consensus Standards as a reasonable security effort and remove passwords as a reasonable measure. This will result in a stronger bill that will be able to adapt to the changing landscape of cybersecurity. This specific type of standard brings together an open, rigorous process, and stakeholders from broad reach to ensure a level of strength and expertise not found through other approaches. Furthermore, this will provide manufacturers with the certainty at the time of manufacture that they have met the rigor required of the bill, rather than face uncertainty in the future that may be settled in the courtroom.

The current definition of manufacturers is defined as "a person that **makes** a connected device and sells or offers to sell the connected device in this state." However, a common class of devices to suffer security vulnerabilities are devices that are manufactured overseas and sold through additional channels and then labeled under another brand for sale in the US – therefore not meeting the "make" portion of the clause. In the case of the Mirai event, numerous video recorders, routers, and webcams sold specifically in this manner were the backbone of the attack. We request this language be modified to be more inclusive of other manufacturing and distribution models. This modification is necessary as exempting these highly vulnerable devices continues to leave Oregon open to significant cyberattacks.

Our goal is to advanced strong, clear security in all cases for our appliances. We believe Oregon Bill HB2395 should as well. The current bill as written does not set a strong standard, provides loopholes that are subject to security breaches that have already been exploited to catastrophic effect, and does not leverage the best tools available for ensuring strong security implementation. It is critical that we heed calls to strengthen security when we have the opportunity to do so. Oregon is ahead of the nation with this effort, and we ask that you strengthen this bill by including all device manufacturers, and defining reasonable security through the use of National Consensus Standards.

Thank you for your efforts and this opportunity.

Steve Nackers | Corporate Manager – Electronic Controls
Sub-Zero Group, Inc. | Madison, WI
608-661-5767 | steve.nackers@subzero.com