April 26, 2019

The Honorable Floyd Prozanski
Chair
Committee on Judiciary
Oregon State Senate

The Honorable Kim Thatcher
Vice-Chair
Committee on Judiciary
Oregon State Senate

Subject: HB 2395, Security of Internet Connected Devices

Dear Chair Prozanski and Vice-Chair Thatcher,

On behalf of UL, I submit to you the following background for your review as you consider testimony on House Bill 2395.

UL is a global, independent, safety-science company that has championed progress and safety for 125 years. Guided by our mission, UL's 14,000 professionals promote safe working and living environments for all people. UL uses research, standards, and conformity assessment to continually advance and meet ever-evolving safety challenges, and partners with businesses, manufacturers, retailers, trade associations, and regulatory authorities to provide solutions and to address the risks of increasingly complex global supply chains. As both an American National Standards Institute (ANSI) accredited standards development organization and leading provider of testing, inspection and certification services, UL has unique and qualified expertise that can be leveraged by the Committee.

Grounded in science and collaboration, UL's work empowers trust in pioneering technologies, from electricity to the internet. We help innovators create safer, more secure products and technologies to enable their safe adoption, including cybersecurity of network-connected products and systems. UL supports efforts aimed at mitigating risks associated with the global ICT supply chain by enabling end-to-end security designed for our interconnected world. We possess a unique expertise in developing and assessing conformance to security frameworks for IoT and interconnected systems.

The intent of this background is to provide greater understanding of how consensus standards can and should be leveraged to enhance the cybersecurity posture of connected products. Additionally, it provides perspective on the importance of leveraging appropriate conformity assessment methods to ensure compliance to such standards.

What is a UL consensus standard and how is it developed?

Safety standards are written documents that outline the process by which a product is tested to help mitigate risk, injury or danger. UL is an ANSI accredited standards development organization, combining extensive safety research, scientific expertise and uncompromising focus on quality to help create a safer world. UL Standards are used to measure and validate not only safety, but also the performance, security, environmental health and sustainability of products and/or the systems in which they operate.

UL develops and maintains standards using the ANSI accredited consensus method utilizing consensus bodies, known as Standards Technical Panels (STPs) within UL. UL Standards are developed under the continuous maintenance method outlined in ANSI's Essential Requirements, versus developing standards under a periodic maintenance method. This enables UL to facilitate updates and revisions to its standards on a rolling basis based on technology developments or emerging hazards. UL's process complies with World Trade Organization (WTO) principles as outlined in the Technical Barriers to Trade (TBT) Committee Decisions and Recommendations to the TBT Agreement.

In this regard, the UL STP process is characterized by several guiding principles, including openness, lack of dominance, balance, consensus, and due process. To solicit participation in STPs, UL canvasses trade associations, consumer groups, inspection authorities, and government agencies that have oversight for the product(s) subject to the standard, and publicizes its standards activities in ANSI's *Standards Action* in an effort to reach persons materially affected. Through a UL outreach coordinator, we seek to balance the STPs to ensure the participation of a broad spectrum of potentially affected stakeholders.

UL Standards encompass UL's extensive safety research and scientific expertise. With over a century of experience in the development of more than 1,500 Standards, UL is an accredited standards developer in the US and Canada. In extending its global public safety mission, UL Standards partners with national standards bodies in countries around the world to build a safer, more sustainable world.

For further details, visit *ulstandards.ul.com*.

What are UL's cybersecurity standards?

In June 2015, UL established a task group to evaluate the complexities and challenges associated with cyber risk and develop an outline of investigation. This outline became the testable technical criteria for the UL 2900 Standard series. An STP was assembled to begin drafting the standard, which was published as a national standard for both the U.S. and Canada (ANSI/SCC) in July 2017.

UL Cyber Assurance Program (CAP) uses the UL 2900 series of standards to offer testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses, minimize exploitation, review security controls and increase security awareness. UL CAP is applicable for vendors looking for trusted support in assessing security risks while they continue to focus on product innovation to help build safer more secure products, as well as for purchasers of products who want to mitigate risks by sourcing products validated by a trusted third party.

CAP's purpose is to help manufacturers, purchasers and end-users, both public and private, a baseline of cybersecurity hygiene to mitigate those risks via methodical risk assessments and evaluations. These standards form a foundational set of technical requirements to measure, and thereby elevate, the security posture of products and systems. UL 2900 is designed to evolve and incorporate additional technical criteria as the security needs in the marketplace mature.

What is conformity assessment?

As a necessary complement to strong consensus standards, conformity assessment methods help demonstrate that the requirements in standards are actually being met. Third-party conformity assessment, one type of conformity assessment, can deliver additional trust through independent, impartial assessment to voluntary consensus standards.

Conformity assessment is the "demonstration that specified requirements relating to a product, process, system, person, or body are fulfilled." Conformity assessment refers to numerous activities, including testing, inspection and certification of products, management of systems and personnel. At its core, conformity assessment seeks to answer basic questions about product and service performance:

1. **Requirements** - What are the requirements and how should a product or service perform?
2. **Determination** – How do we know it performs?
3. **Attestation** – Who says its performance has been demonstrated?
4. **Surveillance** – What provides assurances about the product or service next week?

With respect to **"Attestation,"** there are three models:

- **First Party** – A seller, manufacturer, supplier or individual/organization with need for assurance that specified requirements are fulfilled;
- **Second Party** – A purchaser, user, or individual/organization with a need for assurance that specified requirements are fulfilled; and
- **Third Party** – An individual or organization whose interests are independent of transactions between the first and second parties.

These approaches all have merit and should be applied using a risk-based framework to understand risk and appropriate methods of conformity. In simple terms, the greater the risk presented by a connected product, the greater need for more rigorous conformity assessment.

We appreciate the opportunity to share our expertise and welcome additional questions or comments that you and other Committee members may have.

Sincerely,

Karen Grunstra

Karen Grunstra
Global Government Affairs Senior Associate
Karen.grunstra@ul.com
202.530.6166
UL LLC