Response of UL LLC (Underwriters Laboratories)
National Institute of Standards and Technology
September 09, 2016

UL LLC respectfully submits these comments in response to the recent RFI: Information on Current and Future States of Cybersecurity in the Digital Economy

UL is an independent standards developer and product testing and certification organization dedicated to public safety. Since our founding in 1894, UL's engineers and staff have helped develop safety standards and product –testing protocols, conducted independent product safety testing and certification, and inspected manufacturing facilities around the world. UL is driven by our global safety mission, which promotes safe living and working environments through the application of safety science and hazard-based safety engineering. The application of these principles manifests itself in the evaluation of tens of thousands of products, components, materials and systems for compliance to specific requirements. Through these activities, UL actively engages the U.S. government in its development and administration of federal regulations and conformity assessment programs at the federal, state and local levels. Further, UL also participates in many international standards development technical committees as well as international conformity assessment schemes and national certification programs.

***What is UL's role in the Cyber-Industry?***

Each and every day, UL works collaboratively with manufacturers, retailers, trade associations, public interest groups and international regulatory authorities to advance safety, performance and security through applied science. Through our research, testing and certification, we help ensure that the products used every day, whether in the home, hospital, office, manufacturing plant or connected to the Internet, meet safety, interoperability and performance standards.

From our beginnings at the Chicago World's Fair in 1893 and the introduction of electricity to every technological innovation since, UL has been one of the most recognized and trusted resources for advancing safety. As technology has evolved, we have expanded our capabilities in key areas, broadening the definition of safety and moving from the physical realm to the virtual world. Throughout our history, UL has always understood the relationship between security and safety, and this is certainly true in today's connected world.

Powered by software embedded in devices, this new intersection between the "physical" and the "virtual" poses a new set of risks. UL has built up a knowledge base while working with everything from wearable devices to chip cards that gives us a special insight into the trends impacting these connected technologies. This insight has allowed us to view cybersecurity differently than other organizations, and establish a series of cybersecurity standards and a voluntary certification program.

***What is UL's CAP Program?***

Underwriters Laboratories Inc.
1850 M St. N.W., Suite 1000, Washington, DC 20036-5833 USA
T: 202.296.1435 / F: 202.872.1576 / W: UL.com

As the total universe of devices swells, it's paramount we understand the security risks to people and develop solutions to meet this challenge. Recognizing this need, in April of this year, UL launched the voluntary Cybersecurity Assurance Program — called CAP — that addresses the many risks associated with connected technologies. The CAP program was established with input from government, academia and industry groups. The CAP mission is simple and important: to help vendors identify security risks in products and systems, and help them address the foundational elements required for good cyber-hygiene.

We built CAP around defined technical criteria, providing innovators with a testable set of cybersecurity criteria for their network-connectable products and systems. Working with our customers, CAP accomplishes four things:

1. Reduces vulnerabilities – by requiring testing for vulnerabilities following the NVD.
2. Reduces malware – by requiring testing for known malware.
3. Addresses security controls – by requiring testing of security control implementations.
4. Increases overall public security awareness and preparedness – by getting certified products on the market where basic security information is publicly available in the UL certification database.

***What was UL's Approach When Developing UL 2900?***

UL views cybersecurity as a fundamental aspect of safety. We recognize that with critical product and system control structures being exposed to external tampering comes the potential for compromise to critical infrastructure. This results in the need for risk controls to be implemented where such external tampering could take place, and the UL CAP, among other things, addresses testing the implementation of such risk controls.

UL's approach in developing the technical requirements for UL 2900 was based on an extensive list of research studies, including the DoD SOAR Assessment, Verizon Data Breach Report, and multiple studies done on the common causes of security incidents. This led UL to focus on the technical requirements of the software within products and systems where a high number of security incidents are the result of:

1. The absence of a Software Bill of Materials (BOM), which would allow each item to be assessed for known software vulnerabilities (CWEs)
2. Improper management of known software weaknesses
3. Product shipped with malware
4. A lack of repeatable and reproducible testing to confirm the security controls in products

***The Value of Third-Party Certification:***

We encourage the government to leverage public-private partnerships in developing public policy by incorporating consensus-based standards, available accreditation schemes, and globally recognized practices to meet its compliance interests. By working with the private sector, government agencies can promote transparency, leverage private sector resources, and contribute to economic and job growth.

To increase overall trust in the marketplace, we believe that it is essential that independent third-party organizations conduct testing and certification to provide a neutral validation of products. Third-party certification bodies use an existing network of laboratories that many manufacturers already partner with for other market requirements such as safety to ensure program compliance through independent technical verification and auditing of results and continued compliance monitoring through market surveillance programs. There have already been many examples of successful public private partnerships that emphasize this point, including: The U.S. Occupational Safety and Health Administration (OSHA) on the Safety of Products in the Workplace, The Consumer Product Safety Improvement Act on Toy Testing Requirements and the U.S. ENERGY STAR Program:

Highlighted:

1. **The U.S. Occupational Safety and Health Administration (OSHA) on the Safety of Products in the Workplace**
    a. OSHA's Nationally Recognized Testing Laboratory (NRTL) Program is an excellent example of how the Federal Government benefits from relying on private sector organizations to help carry out its mission, which in OSHA's case is to "promote the safety and health of America's working men and women."
    b. OSHA recognizes private sector NRTLs to test, certify, and monitor ongoing compliance with safety standards for certain products used in U.S. workplaces.
    c. It has been documented by OSHA that they see the following benefits arising out of this partnership with the private sector:
        i. Reducing Government Costs
        ii. Lessening OSHA's Market Surveillance Burdens
        iii. Positively Affecting the Development of Standards
        iv. Promoting International Trade

2. **U.S. ENERGY STAR Program**
    a. In March, 2010 the U.S. Government Accountability Office (GAO) published a report detailing a covert testing operation and review of the current practices under the ENERGY STAR program. The report highlighted that "GAO's investigation shows that Energy Star was for the most part a self-certification program vulnerable to fraud and abuse."
    b. As a result of this investigation, EPA launched a number of reforms to improve program oversight. First, they recognized a number of Accreditation Bodies that would determine whether or not laboratories were capable of conducting the tests called for in the ENERGY STAR criteria. Second, EPA put in place a qualification system for all products. This system requires product manufactures to test their products in accredited laboratories and then an EPA-recognized Certification Body would determine whether or not the product met the ENERGY STAR criteria. EPA did not stop there. The final part of their scheme included requiring Certification Bodies to conduct market surveillance activities on the products that they qualified on an annual basis to ensure that products that bear the ENERGY STAR label continue to meet the program's requirements.

***How Can CAP Strengthen Cybersecurity in Both the Public and Private Sectors?***

CAP addresses one of the biggest cybersecurity threats today: trust. By providing third-party certification, CAP strengthens overall cybersecurity in both public and private sectors. It accomplishes this in two distinct ways:

**First, by increasing public safety**. UL believes that it is important for industry to have products and systems that are safe, reliable, and secure; and as we become a more connected world, security is a concern for manufacturers and consumers alike. Third-party certification provides a trusted partner for manufacturers by leveraging the existing efforts of the private sector to instill consumer confidence that products certified by CAP, in fact, meet the program's stringent and standardized requirements.

**Second, by increasing innovation**. Cybersecurity overall should not be seen as a problem for innovators. It should be seen as an enabler of innovation, where by demonstrating that security risks have been addressed, manufacturers can continue to provide value and trust to the marketplace. The more that public-private sector cooperation works towards protecting innovation by addressing cybersecurity, the faster and more vibrant economies can grow and adopt cutting-edge capabilities to solve today's problems.

Based upon our experience with CAP, we believe that the government should collaborate with the private sector to:

1. Develop a scientific methodology for assessing software in products and provide metrics for identifying, measuring and addressing vulnerabilities. In addition, we believe that when independent third-party organizations conduct testing and certification it increases trust in the marketplace.

2. Use industry recognized supply chain controls such as certification programs as the basis for a framework that identifies a vendor's ability to execute on security objectives across the entire supply chain. This begins with manufacturers using established practices to develop, build and support products and systems for sale, and with system operators, maintainers and asset owners then having the ability to install, configure and support systems safely and securely.

**Conclusion**

UL applauds the Commission on Enhancing National Cybersecurity efforts and approaches regarding coordination and collaboration with the U.S. private sector to strengthen cybersecurity. Cybersecurity provides an ideal opportunity for a strong public-private partnership. CAP is well on its way to providing a framework that supports the Commission's objective to strengthen cybersecurity in both the public and private sectors, to better ensure public safety and enhance innovation.

If you have any questions or would like to discuss elements of this submission, please contact Abel Torres (abel.torres@ul.com).

Sincerely,

Abel Torres

UL, Global Government Affairs