Response of UL
National Institute of Standards and Technology
NISTIR 8074 Volume 1
September 23, 2015

Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity

UL respectfully submits these comments in response to the recently published draft Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity.

UL is an independent safety science 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.

UL Cybersecurity Assurance Program and Standards Development

UL is developing a cybersecurity assurance program that includes the development of voluntary standards that aggregate current industry standards, best practices and appropriate new industry specific requirements into a single program, applicable across industries, for the assessment and testing of network-connectable devices for known vulnerabilities and software security weaknesses using a baseline of verification activities.

UL's core competencies in writing standards; conducting testing, inspection and audits; and architecting successful certification programs are coming together to meet needs for the 21st century – cybersecurity. Society is becoming much more interconnected globally. And, as we become more interconnected, the risks also increase. UL is uniquely positioned as a trusted third party organization – trusted for the highest levels of quality and integrity by customers and governments alike. Our product evaluation and testing capabilities have responded to the connected, software-enabled smart revolution with the incorporation of functional safety, reliability and systems level approaches. Additionally, our broadening portfolio of services expands our capabilities that are trusted by financial institutions to review and validate their transaction processing systems for security and compliance.

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

Security of connected devices is a major concern for governments, manufacturers and consumers alike. There is growing awareness across multiple industries that helping ensure improved levels of cybersecurity will enable connected technology to move forward faster and in a safer manner. The intent of UL's cybersecurity assurance program is to assist governments, vendors and the public in mitigating cyber risks.

The Cybersecurity Assurance Program will include pilot testing to engage industry in the development of industry specific requirements and the standardization process; and will focus on medical and industrial equipment but the program will be applicable across other industries with connectable products. UL looks forward to continued consultation and collaboration with industry, government and other stakeholders to help ensure the program evolves to meet government, market and consumer needs and demands. UL's extensive experience in standards development and evaluating the safety of products in critical applications provides us with the background, knowledge and perspective required for the appropriate application of standards, testing and certification in the cybersecurity space. Furthermore, our collaborative approach to developing the cybersecurity assurance program and its application embraces the wide spectrum of stakeholders needed for a robust solution.

General Observations

In general, UL believes that the NIST Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity serves as a significant and meaningful basis to begin outlining the strategic objectives for pursuing the development and use of international standards for cybersecurity. In particular, UL applauds NIST's recognition that, "Cybersecurity relies upon a diverse set of standards including standards whose scopes are specific to one or more attributes of cybersecurity and standards from other domains that are relevant to cybersecurity."

UL appreciates NIST's recommendations that the U.S. Government (USG) collaborate with the private sector in order to develop and use new standards that are technically sound and suitable for the purposes of USG. In addition, UL welcomes NIST's encouragement of USG participation in the private sector standards development process and believes USG expertise serves as an important input to the consensus process.

Lastly, UL seeks to encourage NIST to consider the importance of conformity assessment schemes to overall standardization efforts. Conformity assessment is a demonstration that specified requirements relating to a product, process, system, person or body are fulfilled. Such demonstration can include sampling and testing, inspection, supplier's declaration of conformity, certification and management system assessment and registration. Activities can also include accreditation by a third party of the competence of the bodies performing the above activities. Recognition (usually by a government agency) of an accreditation body's capability is also a

conformity assessment activity if it involves a demonstration of fulfillment of specified requirements related to capability.

UL's additional comments on the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity are organized below pursuant to the formatting request made by NIST.

#	Source	Type	Page; Line #	Rational for Change	Proposed Change
1	UL	Major	3; 101-105	PERFORMANCE STANDARDS – Design includes both functional and non-functional requirements, whereas "performance" tends to be associated with functional requirements. . Both performance and design are needed in the case of cybersecurity.	Add - DESIGN VERIFICATION STANDARDS
2	UL	Major	4; 150-152	Definition of conformity assessment is incomplete.	Conformity assessment is a demonstration that specified requirements relating to a product, process, system, person or body are fulfilled. Such demonstration can include sampling and testing, inspection, supplier's declaration of conformity, certification and management system assessment and registration. Activities can also include accreditation by a third party of the competence of the bodies performing the

					above activities. Recognition (usually by a government agency) of an accreditation body's capability is also a conformity assessment activity if it involves a demonstration of fulfillment of specified requirements related to capability.
3	UL	Major	6; 250-264	Acknowledge UL standard development efforts.	Inclusion of UL 2900 standards development aimed at leveraging current industry best practices and general requirements for connectable devices; healthcare devices & systems; industry control systems; organization & process assessment.
4	UL		9; 311-321	Public private partnerships are critical in advancing the state of cybersecurity.	Add public-private partnerships
5	UL	Major	12; 494-498	In the spirit and intent of OMB A-119, federal agencies can effectively carry out their mandates by providing guidance to, and the framework for, private sector conformity programs that help to demonstrate and validate compliance. Frameworks	Federal agencies should support and coordinate the timely development of private sector conformity assessment schemes (including international schemes)

				may set minimum thresholds while preserving the right of companies to choose and offer other conformity programs of higher rigor. Federal procurement requirements must provide equitable recognition of products leveraging all acceptable conformity paths.	or activities.

Conclusion

UL applauds the National Security Council Cyber Interagency Policy Committee's International Cybersecurity Standard Working Group's efforts in pursuing the development and use of international standards for cybersecurity, and general recommended approaches regarding coordination and collaboration with the U.S. private sector in the development and execution of a comprehensive United States standardization strategy.

UL appreciates the opportunity to provide these initial comments on the report and looks forward to providing additional, more detailed approaches to the working group, as these recommendations are developed and implemented. In the meantime, if UL can be of further assistance or if you would like to discuss elements of this submission, please contact Abel Torres (abel.torres@ul.com).

Sincerely,

Abel Torres

Manager, Global Government Affairs