6718 Kenwood Forest Lane
Bethesda, MD 20815 USA

Tel : +1 240 507 3392

Submitted via: cpsc-os@cpsc.gov

May 02, 2018

Ms. Patricia Adair
Director, Risk Management Group
Office of Hazard Identification and Reduction
U.S. Consumer Product Safety Commission

Ref: Docket No. CPSC–2018–0007 "The Internet of Things and Consumer Products Hazards"

Dear Ms. Adair,

The International Federation of Inspection Agencies ("IFIA") requests the opportunity to present at the hearing "The Internet of Things and Consumer Products Hazards" on May 02, 2018.

IFIA is a trade federation that represents over 60 of the world's leading independent third-party testing, inspection and certification (TIC) companies. IFIA members offer conformity assessment services, including testing, inspection, certification, systems audits, advisory and training, technical and documentary support. These services help manufacturers gain global market access and help ensure that not only regulatory requirements are fulfilled, but also that reliability, economic value and sustainability are enhanced.

IFIA will be represented at the hearing by its member company Bureau Veritas, and the presentation will be delivered by Mr. Travis L. Norton, Technical Director, Hardlines, Electronics and Smart Products, Bureau Veritas.

We appreciate the opportunity to present. Should you have any questions, please don't hesitate to contact Roberta Telles at +1 240 507-3392 / rtelles@ifia-federation.org and Mr. Travis L. Norton at +1 716 505 3742 / travis.norton@us.bureauveritas.com.

Sincerely,

Roberta Telles
IFIA
Executive Director Americas
rtelles@ifia-federation.org
M: +1.240.507.3392

Hanane Taidi
IFIA
Director General
htaidi@ifia-federation.org
M: +32473629947

Written text of IFIA's presentation

a) Good morning and thank you for the opportunity to be here. My name is Travis Norton and I'm the Director of Technical Services for the Americas at Bureau Veritas, an active member of the International Federation of Inspection Agencies, also known as IFIA, who I speak for today.

b) I'll provide a brief overview of IFIA, our sector's view on IoT safety and some considerations for next steps in the ongoing assessment of IoT consumer products safety.

c) IFIA is the global trade association for the independent third-party testing, inspection and certification industry (TIC industry). IFIA members provide independent third-party conformity assessment services that help ensure quality, safety, performance and sustainability across a wide range of sectors: food, consumer products, petroleum, agriculture, medical device, infrastructure and many others; our sector is active in virtually all sectors of the economy

d) There is a growing trend of IoT companies outsourcing to third-party to lower their in-house compliance costs, as third-parties have economies of scales and technical expertise that can be leveraged more cost-effectively when developing software and hardware for their IoT products.

e) Our industry provides a wide range of conformity assessment services that go beyond testing and include inspection, certification, auditing, advisory and training across all stages of the supply chain, from the design stage to the post retail stage.

f) Third-party conformity assessment help manufacturers, importers, and distributors of all sizes to achieve compliance with international requirements and gain global market access, mitigate risks and protect reputation. Third-party delivers the highest levels of assurance of compliance, and it is a cost-effective and preventive approach that enhances consumer product safety.

g) Some standardization committees (e.g. IEC TC 61 - Safety of household and similar electrical appliances) are drafting requirements with regards to connected devices and the hazards created by such devices are not appropriately designed. However, many of the hazards that are specific to IoT are not currently in scope for the existing safety regulations or adopted industry standards.

h) There are two approaches that should be explored. The 1st is a general set of requirements to ensure that any IoT device and its related internet connected controller is not able to compromise the safety requirements currently in use. Essentially, adding the IoT control systems into the scope of the safety compliance assessments that are applicable to consumer products today. Regulators,

IFIA Americas Committee | 6718 Kenwood Forest Lane | Bethesda, MD 20815 USA | +1 240 507 3392 | ifia-federation.org

standards organizations, business and consumer advocate organizations must work collaboratively to develop frameworks for such generic functional safety requirements.

i) The 2nd approach is to include specific requirements into the applicable safety regulations or standards that require the use of internet connected controllers. This would mirror the approach of the IEC TC 61 committee, but for each of the other IoT sectors, they would be required to develop 'functional safety' requirements for their own product types that have unique challenges.

j) During design / development of IoT devices, manufacturers and their partners should conduct safety assessments that focus on the intended and foreseeable use of the devices and their related internet connected control systems. When updates to software / firmware are being rolled out, it should trigger a re-assessment under controlled conditions to see if the safety of the product has been compromised.

k) A review of the installation options prior to release to market can highlight where potential injuries may occur and can be used to update design, safety features, and software/firmware or consumer guidance such as instructions and warnings. Updates to software/firmware should include safety assessments that utilize test cases where intentional disruption of the update occurs, to assess how the device responds and if it results in a hazardous condition.

l) For leading tech companies, we have seen the utilization of test cases that evaluate the end use conditions created by new/changes in software with a focus on hazard detection. Similar to classic safety assessments, the device is evaluated for the potential to create hazardous conditions given a range of intended and foreseeable use test conditions after it is installed into the target device(s). Development methods for such companies also include software integrity verification at each development step to ensure that hazards have not been introduced.

m) With respect to recalls, in addition to traditional notices, IoT companies can push notifications into devices that display alerts to consumers (if supported by device), and/or establish software / firmware updates that mitigate the hazard or disable the product if a hazard is likely to occur.

n) The CPSC participation and support of the inclusion of 'functional safety' into the focus of standards development bodies that are building future requirements for IoT products can help to align their scope of to ensure the safe operation of such devices from design, development, production, installation and updating.

o) Thank you so much for the opportunity to provide the testing inspection and certification industry's views on IoT and consumer product hazards and I look forward to answering any questions.

IFIA Americas Committee | 6718 Kenwood Forest Lane | Bethesda, MD 20815 USA | +1 240 507 3392 | ifia-federation.org