# THE INTERNET OF THINGS (IOT) AND CONSUMER PRODUCTS HAZARDS

## IFIA's Recommended Guidelines for Ensuring the Safety of Connected Devices

The International Federation of Inspection Agencies ("IFIA") provides below the testing, inspection and certification industry's recommended guidelines for the consumer product market to ensure the safety of IoT products:

IoT devices and/or their connected controllers must not:

- Compromise safety compliance to the applicable rules, bans or standards
- Introduce a hazard to the consumer as a result of being connected or updated
- Disable, disarm or otherwise impair effectiveness of a safety control mechanism

IoT devices and/or their connected controllers should include:

- Safety controls/supervisory systems if impaired use can result in death or major injury (high-risk)
- Safety controls/supervisory systems if intended for use with vulnerable consumers (children, elderly)
- Notifications, cautionary warnings or alerts if consumers disable safety controls, since it might not be feasible to prohibit consumers from disabling safety controls, including warnings against the use of unauthorized apps
- Consumer warnings of potential for injury and steps to mitigate known hazards
- The ability of software to be updated for a safety patch, to eliminate hazards (i.e. send a fix remotely)
- Option(s) enabling user(s) to disconnect / deactivate devices, stopping a hazard

IoT Device Manufacturers / Importers / Retailers should:

- Apply the safety-by-design principle including a default 'safe mode' whenever possible
- Conduct safety assessments of connected control systems and software updates
- Test firmware/software updates on devices to assess safety impact, prior to releasing
- Utilize safety standards for products and provide input to voluntary standards development

- Identify, capture and share IoT hazard incident data (item, hazard, cause, etc.) with the CPSC

Regulators should:

- Continue engagement and participation in the voluntary standard development process
- Continue engagement and participation at the international level to share best practices
- Outreach and coordinate with other government agencies/departments who have already developed industry guidelines on IoT within their jurisdiction[1]
- Engagement with foreign counterparts for a coordinated approach whenever possible in order to avoid creating unique approaches that can burden industry with no added level to safety
- Consider updating incident reporting systems to effectively track IoT related injuries and incidents
- When considering different conformity assessment approaches, use a risk-based approach and leverage private sector conformity assessment
- Rely, whenever possible and applicable, on international or regional systems for conformity assessment, as well as sectorial schemes in order to facilitate recognition of conformity assessment results

## About the International Federation of Inspection Agencies - IFIA

IFIA is the international trade association representing the independent testing inspection and certification (TIC) sector globally. IFIA represents the world's leading international testing, inspection and certification bodies active in over a hundred and sixty countries around the world with a combined turnover of roughly €25 billion and a highly qualified work force of over 300,000 employees.

In the consumer product field specifically, IFIA members provide technical expertise during all stages of the value chain: from the design of a product to the sourcing of materials, auditing of suppliers, production, distribution and post-retail—ensuring products placed on the market meet safety, quality, performance and sustainability standards.

[1] For example, NTIA in the U.S.: https://www.ntia.doc.gov/files/ntia/publications/draft-communicating_iot_security_update_0426.pdf

Furthermore, IFIA members implement the IFIA Compliance code: a rigorous business code of conduct reviewed by independent auditors and covering 5 key principles: Integrity, Conflicts of Interest, Confidentiality, Anti-bribery, Fair marketing.