

June 15, 2018

6718 Kenwood Forest Lane  
Bethesda, MD 20815 USA

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

Tel : +1 240 507 3392

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

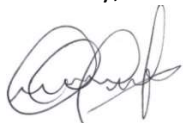
Dear Ms. Adair,

The International Federation of Inspection Agencies (“IFIA”) welcomes the opportunity to submit the following comments on the “The Internet of Things and Consumer Products Hazards”.

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 such as testing, inspection, certification, auditing, advisory and training across all stages of the supply chain. These services help manufacturers of all sizes to achieve compliance with national and international standards and regulations and gain global market access. Third-party conformity assessment delivers higher levels of assurance of compliance, and it is a cost-effective and preventive approach that protect consumer’s health and safety.

Thank you for the opportunity to provide comments. Should you have any questions, please don’t hesitate to contact Roberta Telles at +1 240 507-3392 / [rtelles@ifia-federation.org](mailto:rtelles@ifia-federation.org).

Sincerely,



Roberta Telles  
IFIA  
Executive Director Americas  
[rtelles@ifia-federation.org](mailto:rtelles@ifia-federation.org)



Hanane Taidi  
IFIA  
Director General  
[htaidi@ifia-federation.org](mailto:htaidi@ifia-federation.org)

**Introduction:**

IFIA congratulates the CPSC for the initiative to collect stakeholder input on “The Internet of Things and Consumer Products Hazards” during the hearing on May 16, 2018 and via written comments. Collaboration and engagement with the stakeholder community is key to leverage private sector expertise and ensure an effective approach to this challenging topic.

The independent third-party TIC industry is a key stakeholder group in this area, as there is a growing trend of companies outsourcing to independent third-party service providers. Manufacturers may not have the technical competence or test facilities as it may not make economic sense for them to invest in developing these in-house. Therefore, outsourcing to the independent third-party TIC sector can help manufacturers lower and optimize their in-house compliance costs.

Third-parties have economies of scale and the necessary technical expertise that can be leveraged more cost-effectively when developing software and hardware for their IoT products. Therefore, IFIA welcomes the opportunity to collaborate with the CPSC and would support a future exchange to discuss how the TIC sector experience and best practices in safety apply to security concerns.

IFIA provides below the TIC sector’s responses to the very well-thought questions that the CPSC raised in the Federal Register notice. In addition to the responses below, IFIA recommends the following:

- Continue ongoing collaboration with the stakeholder community
- Engagement at policy level with other federal agencies also working on IoT issues within their jurisdictions to ensure a coordinated approach (Federal Trade Commission, Federal Communications Commission, Food and Drug Administration, among others)
- Engagement and coordination with the National Institute of Standards and Technology (NIST) Cybersecurity efforts. The NIST Cybersecurity Framework’s favorable receipt and adoption by the private sector is attributable to a number of factors, including NIST’s ongoing reviews and engagement with the private sector, the Framework’s risk-based approach, the ability for the organizations to define the risk tolerance and the smart application of existing standards and industry practices.

- Engagement with foreign counterparts for a coordinated approach whenever possible. While IFIA recognizes the inherent differences in operating in the U.S. and other markets, there may be areas where countries can identify global solutions in order to avoid creating unique approaches that can burden industry with no added level to safety.
- When considering conformity assessment approaches:
  - Apply a risk-based approach. The determination of the method of conformity should be based on the objectives and confidence needs of the regulator to fulfill its mission. This will depend on various factors, such as: the risks associated with the object of compliance, how likely non-compliance is, what the industry's track record is, how much trust there is in the supply chain, the societal costs of non-compliance, the agency's resources and capabilities, among others. Please see Annex I for a draft IFIA paper on conformity assessment including some questions for federal agencies to consider when choosing a conformity assessment method.
  - 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.
  - Consider OMB A-119 policy to leverage private sector conformity assessment activities whenever possible:

*“Agencies should also design conformity assessment programs with the objectives of furthering outcomes that are closely aligned with market dynamics and otherwise maximize net benefits to society. In this context, agencies should recognize the possible contribution of private sector conformity assessment activities. When properly conducted, conformity assessments conducted by private sector conformity assessment bodies can increase productivity and efficiency in government and industry, expand opportunities for international trade, conserve resources, improve health and safety, and protect the environment”<sup>1</sup>.*

---

<sup>1</sup> [https://www.nist.gov/sites/default/files/revISED\\_circular\\_a-119\\_as\\_of\\_01-22-2016.pdf](https://www.nist.gov/sites/default/files/revISED_circular_a-119_as_of_01-22-2016.pdf)

**IFIA's responses to CPSC's questions:**

1. Do current voluntary standards and/or safety regulations address safety hazards specific to IoT-connected devices?

In some cases the answer is yes, if the hazard is already mitigated by the requirements. However, many of the hazards that are specific to IoT are not currently in scope for the existing safety regulations or adopted industry standards. As an example, an update to software/firmware could modify a safe product to unsafe, after it has gone through compliance assessment and is already in the market. 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 such connections may create if devices are not appropriately designed.

2. How can IoT-connected devices be subject to safety standards (or a set of design principles) to prevent injury?

There are two approaches that should be explored. The first is a general set of requirements to ensure that the IoT device and its related internet connected controller is not able to compromise the safety requirements currently in use. This general approach would be applied in addition to the applicable safety requirements, which will incur additional test cases to be utilized for 'general' foreseeable conditions of IoT use. (i.e. using an app and voice command to close a garage door while the obstruction beam indicates something is in the way). The second approach is to include specific requirements into the applicable safety regulations or standards that require the use of internet connected controllers for a given safety requirement. (i.e. update the safety standard for garage doors to includes tests for internet connected control systems).

3. What types of devices would need such controls or supervisory systems, and what type would not, if any?

IoT devices that pose injury to consumers when they malfunction should be subject to controls or supervisory systems. Devices may include products that could cause death or major injury if it fails during use or with vulnerable consumers, such as devices that have mechanical movement (physical injury), heating (fire hazard), etc. Connected devices that are unlikely to pose injury could be exempted, unless field data indicates injuries are occurring.

Every device that is covered by an existing safety standard and that becomes an IoT device due to its connectivity and whereby the connectivity allows the (remote) control and operation of the device shall remain functionally safe. Today's IoT devices may include software and or hardware-based controls and supervisory system to ensure essential (functional) safety. Any software-based control and supervisory system must comply with essential requirements as outlined in various international standards such as IEC 60730, IEC 62304, IEC 61508.

4. Who should develop such standards or create a set of design principles?

Regulators, standards organizations, business (including SMEs), conformity assessment bodies and consumer advocates must work collaboratively to develop a framework for best practices. In most cases, a voluntary industry approach is the best way to start development. Traditional standards development groups may need to recruit and include expertise in IoT device technologies. Expertise can come from organizations like CTIA, WiFi alliance, Bluetooth SIG, Zigbee, Z-wave, thread and others.

5. Should certification to appropriate standards be required before IoT devices are allowed in the marketplace?

As mentioned above and discussed in the Annex I, the choice of the appropriate conformity assessment method (testing, inspection, certification, auditing, etc.) should be risk-based and based on the objectives and confidence needs of the regulator to fulfill its mission. For high-risk products, such as medical devices or devices that can be controlled remotely and that, if not compliant, can result in serious hazards to health and safety, a more stringent requirement may be necessary. For a wider consumer products market, where the risk is determined to be lower, the regulator's confidence may be satisfied with various conformity assessment options. By monitoring adoption of the voluntary requirements and consumer injury data, a risk-based approach can be implemented to define which method of conformity is appropriate.

If CPSC decides to rely on certification, it is recommended that CPSC works to align, whenever possible, its program with other existing national and/or international schemes that may utilize the same consensus standards. This would help reduce duplicative efforts, overlap, or conflict with other conformity assessment schemes. CPSC should ensure that the existing schemes, or any new program that the CPSC may develop, have adequate accreditation requirements that satisfy its confidence needs and policy

objectives. It is highly encouraged that the agencies leverage existing schemes instead of creating new ones: in many markets high-risk products may already be covered by certification schemes, whereas lower risk-products may be regulated by other methods. Existing regulations and standards need to be updated to address the safety concerns related to connectivity, incl. software and software updates (patching).

6. What are the industry's best practices for predicting potential hazards caused by IoT-connected devices? What controls or supervisory systems are necessary to mitigate these potential hazards?

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. It is important that such evaluations are conducted during the total life time of the IoT-product. This should follow a similar approach to design evaluations and safety assessments used by industry's leading brands that utilize a certified quality management system.

7. What controls or supervisory systems are available to mitigate potential hazards caused by misuse of IoT-connected devices, such as preventing the disabling of a safety feature?

Warnings, alerts and notifications to consumers can be utilized where consumers have a choice to deactivate safety features. Such consumer communication should include a clear description of the potential for injury and what steps need to be followed to reduce risk (i.e. re-enable the safety feature). Where possible, such functionality which allows consumers to disable a safety feature should be discouraged.

IoT devices that pose injury to consumers when their software malfunctions shall obviously not provide consumer options to deactivate safety features. The IoT equipment itself shall provide protection against any attempts (whether unintentional or deliberate) from the outside over communication (e.g. WiFi, bluetooth, etc.) to modify or even-deactivate safety features.

8. What controls or supervisory systems on products are necessary to prevent injuries from unintended consequences of mis installation, failed update, and operational changes over time, or misuse of an Internet connection?

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

(Instructions, warnings, etc.). 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. Similar test cases can be developed to address operational changes and foreseeable misuse of an internet connection. The frequency and nature of the updates should be considered. For example, products that have frequent updates such as gaming IoT devices may need a different approach as opposed to a smart home IoT device that only updates once every couple of years. In any case, updates and patching have to be considered as a part of an IoT-device. Any certification schemes, and where applicable standards, shall consider these dynamics of changing product features.

9. Have IoT-related incidents and injuries already occurred? Please describe the injury scenario and the severity of any injuries. How would IoT-related incidents be distinguished from other incidents?

There have been numerous publicly available reports that detail a variety of incident and injuries. The following are a few examples. A self-driving vehicle has struck and killed a pedestrian. Batteries of many IoT devices have caught fire, exploded and resulted in burn injuries. Smart home devices such as switches, have been hacked, and can cycle on and off fast enough to short out an outlet and start a fire. A diesel generator was hacked and its circuit breakers were programmed to open and close out of sync, eventually leading to an explosion. A vehicle was shown to be vulnerable to allow control of critical operator and safety controls to remote hackers. 'IoT related' may be filtered based on the cause of an incident. Overheating of devices after a firmware update are well known from the press.

10. Are incident-collection systems set up to collect IoT-related incident data?

Not that we are aware of. Current incident-collection systems do not provide much insight into the root cause of the hazard, which would help to differentiate between classic issues and new IoT issues. For future data collection and analysis of IoT-device incidents it may be useful to point out IoT-related incidents in the data collection systems.

11. Are there ways CPSC can collaborate with other federal agencies to address potential safety hazards related to IoT?

Yes, collaboration with DOC, FDA, FTC and other federal agencies on topics regarding cyber-security will help reduce unauthorized remote access which can result in death or injuries. Although their focus may

be on data privacy protection, the same cyber security solutions, such as encryption, can benefit the safety of consumers for a wide range of IoT devices.

12. Are there ways CPSC can collaborate with outside stakeholders to address potential safety hazards related to IoT?

Yes, supporting the activity of standards development bodies that are building future requirements for IoT can help to align their focus on the safe operation of IoT devices from design, development, production, installation and updating. Collaboration with counterparts in key markets and international / regional organizations to share best practices can help the CPSC leverage resources and technical expertise and help ensure a coordinated global approach.

13. How can CPSC educate consumers on the proper use of IoT-connected devices?

Web based guidance (pages, downloads, videos, etc.) can be developed to share safety insights to IoT consumers. Sharing examples of IoT device case studies where safety issues have occurred can raise awareness for the need to be vigilant when buying, using or gifting IoT devices. As injuries occur with IoT devices, additional insights or safety tips may be apparent and the CPSC can post these online to promote safe use of devices. In today's world of apps, that may not be provided and/or authorized by the manufacturer, it should be made clear to consumers that they carry the responsibility for potential negative implications arising from the use of such apps.

14. Some of the consumer hazards that could conceivably be created by IoT devices are: fire, burn, shock, tripping or falling, laceration, contusion, and chemical exposure. Are there other hazards that could be introduced into consumer products through enabling an Internet connection?

The listed hazards appear to be the primary concerns. Additionally, exposure to all sorts of hazardous radiation (e.g. acoustic / sound pressure, light, laser, EMF, ionizing radiation) is possible.

15. For products whose remote operation could create a hazard to consumers, should Internet connectivity specifically prevent remote operation?

If remote operation is the intended function of the product, it may be difficult to impose internet connectivity as the solution to injury prevention without sophisticated software. However, a 'kill switch' could be included on connected devices that pose risk of injury. This would allow local users of a device



to over-ride the internet triggered commands. Local controls on products shall prevail over control commands via remote communication channels. Products with optional remote operation shall require to be set by the user to allow this remote operation.

16. How do IoT software development methods address potential product failures that may create hazards to consumers?

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 should not only focus on evaluation of end equipment (validation) but should also include verification of each software development step (e.g. architecture design, modules design, etc.). Only testing of software on end equipment (black box testing) will never reveal all software bugs.

17. What steps should be taken to prevent an Internet connection from creating a hazard to consumers after a product's purchase (or lease) and installation?

If there are known hazards with the product misuse, consumers should be warned and given guidance how to avoid them. If software/firmware releases are planned, they should be tested with a representative range of devices to ensure that no new or worse hazardous conditions have been created using safety assessments for intended and foreseeable use cases. Several of the above discussed measures shall prevent internet connections or other remote communication channels from creating a hazard on the product concerned.

18. What role should safety standards or design guidelines play in keeping IoT devices from creating new hazards to consumers? Should these standards be voluntary or mandatory?

Safety standards / design guidelines establish minimum requirements that devices should incorporate. Their adoption into the wider market is how they actually end up detecting and eliminating hazards.

Based on the level of risk, and the need for confidence that a product complies, various types of standards and methods of conformity assessment will be required. Some may be determined to be mandatory to insure the necessary levels of protection desired. Therefore, understanding of potential risk should be the key guide for policy makers in ascertaining whether voluntary or mandatory standards should apply.

19. What role should government play in keeping consumers safe regarding IoT devices?

Collaboration with all stakeholders is key. Governments should stimulate the industry, including SMEs, as well as consumer groups, to come together to build consensus standards, share data/trends/insights on where hazards are being reported, and intervene with regulations only when data shows that industry efforts are not being sufficient to address the hazards.

20. Will policies to prevent hazardization of IoT products require or benefit from strong international cooperation?

Yes, CPSC will benefit from awareness of best practices and/or developments that occur internationally. Other countries' efforts can often provide insights on what to avoid or pursue and may lead to a more coordinated approach to address global issues such cybersecurity issues. Hazardization is an example of a global issue we all need to solve, and strong international cooperation and the sharing of best practices provide benefits to industry and consumers.

21. For recalls involving IoT devices, what are different ways companies can communicate notice to consumers who own the IoT devices?

In addition to traditional notices, companies can consider using consumer contact information from warranty registration to notify individuals, push notifications into devices that alert consumers (if supported by device) and establish software / firmware updates that mitigate the hazard or disable the product if a hazard is likely to occur.

## ANNEX I

### **DRAFT: CONSIDERATIONS IN SELECTING METHODS OF CONFORMITY AS PART OF REGULATORY SCHEME FRAMEWORK**

#### **1. Questions for agencies to consider when deciding on a method of conformity that best meet their confidence needs**

When a decision has been made to regulate (or recognize/reference standards) to address a specific hazard or risk, how to choose the appropriate method of conformity? How does the role of government change under each method?

In general, the requirement for a particular level of rigor in the conformity assessment process is determined by the risks associated with the product, process, or service and its scope of use. The appropriate conformity assessment mechanism is also determined by other market factors, such as the legal system and the general philosophy of pre-market conformity assessment versus a fully funded post-market surveillance system. The confidence level needed is based on the risk of non-compliance and what market-driven mechanisms exist as mitigation tools for non-compliance. Part of a full analysis would include the pre-market and post-market structure that would be required. The choice of that structure has implications for costs of related government infrastructure, socio-economic costs, costs of establishing and sustaining technical competency levels, and capacity of those providing the service.

Below is a table that summarizes a few questions that agencies should consider when deciding on a method of conformity that best meet their confidence needs with the answers depending on the method of conformity. The answers below are not always this clear cut but represents what is generally the case for each method of conformity.

QUESTIONS:	FIRST-PARTY	THIRD-PARTY
1. Is a high level of confidence required?	No	Yes
2. Is the perceived risk high?	No	Yes
3. Are products regulated primarily manufactured in countries with a history of risk factors and other issues?	No	Yes
4. Are products manufactured in complex and fragmented supply chains?	No	Yes
5. Is there a documented history of industry compliance?	Yes	No
6. Is there a documented history of industry non-compliance?	No	Yes
7. Is there evidence that product liability is an effective deterrent?	Yes	No
8. Do regulatory authorizing/statutory provisions provide severe penalties and an effective deterrent?	Yes	No
9. How strong is the need for impartiality and independence?	Low	High
10. Are there voluntary, market driven schemes that address confidence needs?	Yes	No
11. Are there relied upon accepted international schemes that can be leveraged?	Yes, and sufficient to meet confidence needs	Yes, but insufficient
12. What are the societal risks of non-compliant products?	Low	High
13. Who bears the costs of market surveillance?	Primarily governments	Private sector
14. How likely is the need for recall or corrective action?	More likely	Less likely

## 2. Methods of conformity agencies can choose to satisfy their confidence needs

In general, there are three approaches to conformity assessment: **First-Party** (manufacturer), **Second-Party** (purchaser or user) and **Third-Party** (independent entity).

**First-Party Conformity Assessment:** “Performed by the person or organization that provides the object”<sup>2</sup>, that is, the supplier or manufacturer demonstrates that a product or service fulfils specified requirements, and it is typically used when there is a lower level of risk associated with non-compliance and with the product. In First Party Conformity Assessment, the resulting statement of conformity is commonly referred to as the Supplier’s Declaration of Conformity (SDoC).

For a First-Party conformity assessment model to work:<sup>3</sup>

- The risk of noncompliance must be low;
- The risk of the product must be low;
- There is confidence that manufacturers understand the technical, regulatory and market requirements and has satisfactory control over their supply chain;
- There are adequate penalties for placing noncompliant products in the market, which include - but are not limited - to:
  - civil and criminal penalties
  - product recall, and/or
  - product bans; and

---

<sup>2</sup> <https://www.iso.org/standard/29316.html>

<sup>3</sup> ACIL: <https://c.ymcdn.com/sites/www.acil.org/resource/resmgr/imported/ACILsDoCPositionPaper.pdf>

- There is a **fully-funded** post market surveillance system in place that quickly and effectively removes noncompliant products from the market in order to avoid injury and societal costs. A post market surveillance system should consist of:
  - mechanism for customer complaints,
  - marketplace surveillance and testing,
  - factory surveillance and testing, and
  - regular independent audits of individual manufacturers' declarations of conformity.

A **fully-funded** post market surveillance system is a key requirement for a first-party conformity assessment model to be successful and avoid a high incidence of non-compliant products on the market that can contribute to health and safety issues and other socio-economic costs.

**Second-Party Conformity Assessment:** “Performed by a person or organization that has a user interest in the object”<sup>4</sup>, that is, the end user or entity acting in the interests of the end user, or an individual or group whose primary interest is in fulfilment of requirements demonstrates for itself that specified requirements are fulfilled.

Second parties may not always have business models that allow them to maintain the infrastructure, processes and technical competence to cost-effectively take advantage of this approach. Also, costs of goods and services can increase if suppliers face a high number of demands from individual second parties each carrying out their own conformity assessment. Therefore, second parties often rely on third-party conformity assessment to fulfil their confidence needs in a cost-effective manner.

**Third-Party Conformity Assessment:** Performed “by a person or body whose interests in the product are independent from those of first parties and whose interests in fulfilment of requirements are independent from those of second parties.”<sup>5</sup>

---

<sup>4</sup> <https://www.iso.org/standard/29316.html>

<sup>5</sup> <https://www.iso.org/standard/29316.html>

Independent third-party conformity assessment bodies (CABs) may be accredited and regularly assessed by accreditation bodies as proof of qualification (competence) to provide services as a result of accreditation to international ISO/CASCO standards such as: ISO/IEC 17025 for testing, ISO/IEC 17020 for inspection and ISO/IEC 17065 for certification. This accreditation also includes an in-depth review of their documented management systems used to assure ongoing compliance with these international standards. The accreditation bodies may be either government bodies, recognized accreditation bodies operating under international guides, or a combination of both.

Third-party is widely relied upon in many markets when<sup>6</sup>:

- There may be a **higher risk associated with non-compliance**;
- There may be a **higher risk from products**;
- There is need for an **independent** demonstration to the supply and demand chain such as consumers, manufacturers and regulators that a product fulfils specified requirements;
- There is need for **higher levels of confidence and assurance of compliance** with safety, health or environmental requirements;
- Manufacturers seek to **reduce in-house compliance costs** or apply third-party as an added value to their own quality and conformity assessment procedures to gain global market access and protect their brands and reputation; and/or
- There are **limited government resources to fully fund market surveillance systems**.

### 3. Third-party conformity assessment

Within third-party there are various options; in some cases, there will be a need for a full certification and others third-party testing only. Sometimes the agency may need only facility audits or inspections or a combination of different procedures. Again, it will depend on various factors and the levels of confidence

---

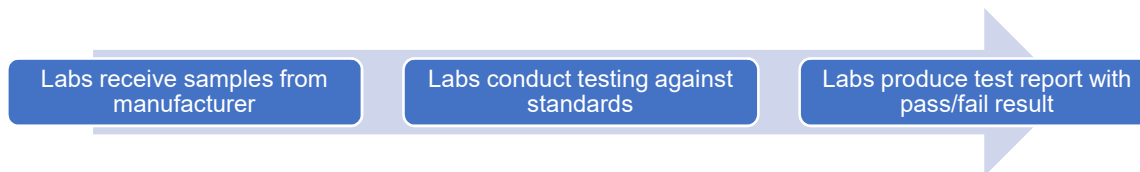
<sup>6</sup> ACIL:

<http://c.ymcdn.com/sites/www.acil.org/resource/resmgr/imported/The%20Value%20of%20Third%20Party%20Certification.pdf>

needed will drive the decision. For instance, if the agency has no resources for funding post-market surveillance and the risks associated with the product and with non-compliance are high, the agency might consider full certification. If the risks of non-compliance are low, there are liability laws and penalties that function as effective deterrents, and there is adequate post-market surveillance, then the agency might consider SDoC. If the situation is somewhere in between, perhaps third-party testing requirements might be an effective tool.

Below are a few examples to illustrate third-party testing and third-party certification:

**Third-party Testing:**



When conducting testing only, the laboratory role is limited to receiving samples, testing against standards and reporting pass/fail results. Labs have no control of, nor information about:

- a. Whether manufacturers are testing “golden samples”;
- b. Any material changes by the manufacturers when receiving a request from manufacturers to transfer data from old test reports or from reports issued by other labs;
- c. Whether the sample is representative of the entire production;
- d. Whether manufacturers have reasonable testing programs in place;
- e. Whether labs meet the applicable accreditation requirements when receiving test results from reports issued by other labs;
- f. Whether manufacturers’ supply chains ensure traceability and there are documentation controls in place; and
- g. Whether there is a system to offer testing to maintain continuing compliance



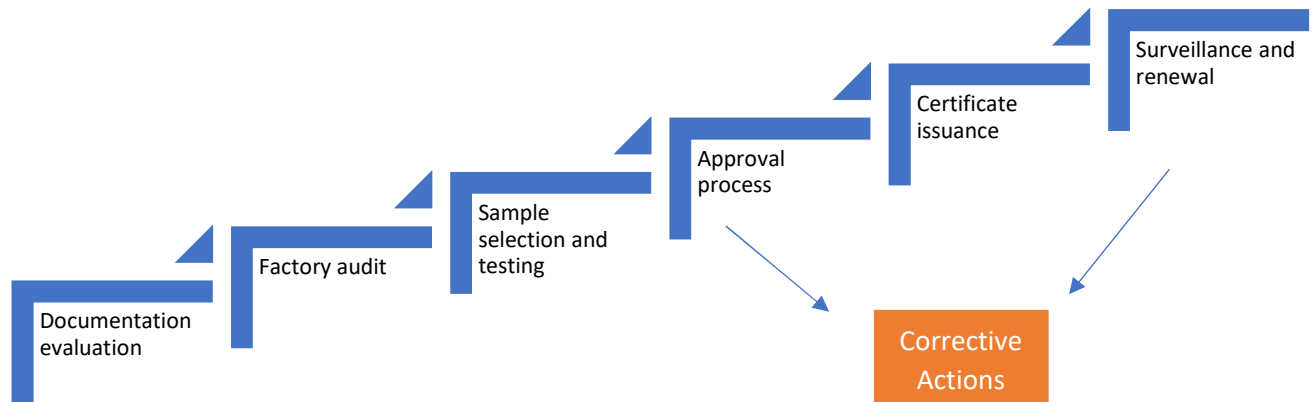
The U.S. Consumer Product Safety Commission (CPSC) third-party testing requirements for children's products is an example of the use of third-party testing as one of the tools in the regulator's toolbox to ensure products are safe. It is used in combination with other non-compliance deterrence measures, such as civil and criminal penalties, market and import surveillance, education of the supply chain on CPSC requirements, and a product recall system. Other market-driven aspects such as product liability and retailers' programs also provide further incentive for compliance.

### **Third-party Certification:**

Certification bodies conduct extensive review of a product's manufacturing process and make a determination that the product (or system, process, person) complies with applicable standards. The certification process includes periodic testing, inspection and factory auditing. It provides higher levels of assurance of ongoing compliance throughout the entire production process with corrective actions in place if non-conformities or issues are identified during the process.

The Environmental Protection Agency (EPA) Energy Star program is an example of a voluntary public-private partnership that relies on independent third-party certification to help ensure ongoing compliance and the integrity of the Energy Star label. Third-party requirements were introduced after high levels of non-compliance were identified by an investigation from the Government Accountability Office (GAO). Reliance on third-party certification helps maintain consumer trust in the Energy Star designation and improve oversight of the program while allowing the agency to save scarce resources since evaluation and market surveillance is performed by the private sector.

Below is an overview of the certification process:



### 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.

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.