Setting Standards for Excellence

June 15, 2018

ONLINE VIA: https://www.regulations.gov/

Patricia Adair
Director, Risk Management Group
Office of Hazard Identification and Reduction
Consumer Product Safety Commission
Room 813
4330 East-West Highway
Bethesda, MD 20814

Re: NEMA Comments on Request for Written Comments the Internet of Things and Consumer Product Hazards

Docket Number: CPSC–2018–0007

Dear Ms. Adair,

As the leading trade association representing the manufacturers of electrical and medical imaging equipment, the National Electrical Manufacturers Association (NEMA) provides the attached comments on the CPSC Request for Written Comments the Internet of Things and Consumer Product Hazards. These comments are submitted on behalf of NEMA Member companies.

The National Electrical Manufacturers Association (NEMA) represents nearly 350 electrical equipment and medical imaging manufacturers that make safe, reliable, and efficient products and systems. Our combined industries account for 360,000 American jobs in more than 7,000 facilities covering every state. Our industry produces $106 billion shipments of electrical equipment and medical imaging technologies per year with $36 billion exports. Please find our detailed comments attached.

Our Member companies count on your careful consideration and we look forward to an outcome that meets their expectations. If you have any questions on these comments, please contact Alex Boesenberg of NEMA at 703-841-3268 or alex.boesenberg@nema.org.

Sincerely,
Joseph Eaves
Head (Acting) NEMA Government Relations
National Electrical Manufacturers Association

National Electrical Manufacturers Association
1300 North 17th Street, Suite 900 - Rosslyn, VA 22209

NEMA Comments on CPSC Request for Written Comments the Internet of Things and Consumer Product Hazards

Answers to Specific CPSC Questions:

The Commission is interested in discussion about consumer product hazards enabled by an internet connection. The areas for discussion include:

- Do current voluntary standards and/or safety regulations address safety hazards specific to IoT-connected devices?
  NEMA Comment: with respect to connected lighting products, an internet connection does not introduce any new hazards in the lighting segment because a standard light switch was already "remote", and products are designed to be safe even if they are unexpectedly turned on by another person. This is one reason why exposure to live parts is an important part of current safety standards.

  A wide variety of residential and consumer appliances are becoming internet connected devices, and industry is not creating a separate category for IoT devices. We do not believe at this point that IoT and Internet connected appliances are vastly different and in need of special treatment with respect to safety.

- How can IoT-connected devices be subject to safety standards (or a set of design principles) to prevent injury?
  NEMA Comment: See our comment for question #1. For lighting, the use of IoT does not add new hazards.

  Residential consumer devices or appliances should continue to be certified against the standing safety standards available for the United States. We recommend in the case of an Internet connected device or appliance that in addition to already-required safety testing additional testing be performed for the Internet connected portion of the device or appliance. We do not recommend a separate category of IoT safety certifications.

  Inexperienced parties might be tempted to say that the connectivity capability of IoT products has created a new category of risk, by virtue of the connectivity. However, while the rate of connection is certainly increasing, this is not a new phenomenon; rather the rate of occurrence is larger than it was historically. Remote operation and connection have existed for upwards of 30 years in some product categories, thus their safety concerns and risks have already been addressed and incorporated into design and management. Ensuring proper/safe operation of appliances or systems following loss of connectivity has been incorporated into industry standards and practices for many years as a result. The risk of malicious interaction with connected equipment veers into cybersecurity territory quickly, and we agree that the CPSC should defer to those agencies addressing cyber risks. The CPSC can and should stay abreast of these proceedings, even participate, but there is no need to duplicate this work.

- What types of devices would need such controls or supervisory systems, and what type would not, if any?
  NEMA Comment: Supervisory systems may be needed in the case of unexpected events, but it is difficult to say when and where they might be necessary. The presence of IoT systems, internet connected devices or appliances do not make existing devices more or less safe, though they may make them vulnerable to unexpected outcomes. An example of unexpected events in connected appliances is a situation involving multiple high current devices, such as a stove, air conditioning and heating, and dryer in a residence cycling on at the same time due to a connected signal. The worst case outcome, if the proper electrical panel is available and the devices are properly fused or the proper circuit breakers are available, is that a circuit breaker trips. Tripping may be a whole-house event, or an individual circuit breaker

on a panel. This leaves the consumer uninformed about what caused the circuit breaker(s) to trip, though the condition is not unsafe, strictly speaking.

We note that lighting products already covered by UL1993, UL8750, and UL1598 should not need additional standards or system requirements.

- Who should develop such standards or create a set of design principles?
  NEMA Comment: we agree with commenters/panelists at the May 16th public meeting at CPSC who recommended that industry-led consensus standards should be the basis for any future requirements, best practices, design principles and other guidance related to IoT product consumer safety. Industry representatives know their products best and are ideally suited to contribute deeply to any related requirements for those products and systems.

- Should certification to appropriate standards be required before IoT devices are allowed in the marketplace?
  NEMA Comment: this solution seems impractical, given the high degree of connectivity already present in the consumer market and homes. A more feasible approach may lie in voluntary best practices for product types and sectors viewed as high risk.

- 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?
  NEMA Comment: Such controls/supervisory systems should already be built-in, since the "potential hazards" being addressed here do not seem to be new or previously unforeseeable with non-IoT devices, and could exist regardless of IoT-capabilities. Please see our answers to question 3.

  Industry does not assume or believe that IoT or Internet connected devices or appliances are safety hazards in and of themselves simply by being connected to the Internet.

  Speaking again for lighting products only, Energy Management Systems have been in use for commercial buildings for decades. IoT is a simpler, potentially cheaper method to make the adoption of energy management systems more widespread by reducing the capital requirements, as well as adding some new features that did not previously exist (i.e. color changing lamps). However, none of this adds any new safety risks that the older technology did not already have, which have been addressed.

- 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?
  We have no comment on this item

- What controls or supervisory systems on products are necessary to prevent injuries from unintended consequences of misinstallation, failed update, operational changes over time, or misuse of an internet connection?
  NEMA Comment: while built-in protections already exist in products with selectable performance features, at some point there are consumer/owners who accept responsibility and risk by making adjustments or modifications to settings, meaning risk is no longer influenced exclusively by factory settings and software. The CPSC should acknowledge the existence of this threshold and establish conditions whereby manufacturer risk and responsibility can be lessened to some degree.

- 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?
  NEMA Comment: At this time NEMA Members do not know any injuries directly attributable to an Internet connected device or appliance, for which the failure mode involved being connected to the Internet.

- Are incident-collection systems set up to collect IoT-related incident data?
  NEMA Comment: we agree with comments during the May 16th public meeting expressing concern that expansion of the fields for public reporting may reduce public participation. One way to mitigate this while still providing additional information may be to review all public reporting templates and see if any fields/items can be eliminated (i.e. zero sum). A second point we would make is there is no specific definition or discrimination between an Internet connected appliance or device, and a non-Internet connected appliance or device. Many legislative proposals have been made, and the challenge always focuses on the scope and definition of "IoT" and "Connected".

- Are there ways CPSC can collaborate with other federal agencies to address potential safety hazards related to IoT?
  NEMA Comment: The recently proposed House Smart IoT Bill Act is relevant.

  CPSC should also collaborate with FTC during reports of data privacy and data security breaches that do not implicate physical property damage or personal injury.

- Are there ways CPSC can collaborate with outside stakeholders to address potential safety hazards related to IoT?
  NEMA Comment: the CPSC should seek to participate in industry-led standards and best practices mentioned in item 4 above. CPSC should also seek to engage with the standards development organizations (SDO) and consortiums or alliances that are working on best practices/guidelines for IoT devices:

  (Known draft standards noted. This is not an exhaustive list.)

  - Joint Technical Committee 1 (JTC1, ISO/IEC) SC 27
  - Open Fog Consortium
  - Trusted Platform Module (TPM)
  - Industrial Internet Consortium (IIC)
  - European Telecommunications Standards Institute (ETSI)
  - HiTrust Alliance
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Telecommunications Industry Association / Electronic Industries Alliance (TIA/EIA
  - ZigBee Alliance
  - GSM Association (GSMA)
  - Underwriters Laboratories (UL 2900, UL 5500)
  - International Organization for Standardization (ISO)

- International Electrotechnical Commission (IEC)
- Alliance for Internet of Things Innovation (AIOTI)
- National Institute of Standards and Technology (NIST)
- IoT Security Foundation (IoTSF)
- European Committee for Electrotechnical Standardization (CENELEC)

- How can CPSC educate consumers on the proper use of IoT-connected devices?
  NEMA Comment: This is ongoing – most of the quality complaints received by NEMA members relayed to NEMA staff anecdotally are about improper use or installation, and the consequences for such conditions relate to performance, not safety.

- 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?
  NEMA Comment: Not in the lighting segment. None of these listed hazards are novel and could exist regardless of whether a product or device is IoT-capable, nor does connectivity in and of itself appear to present a safety hazard in our view.

  We also note that CPSC's scope is focused primarily on physical personal injury and property damage as opposed to cyber-security, data collection/security, or data privacy issues, as stated on the public notice on its website ("We do not consider personal data security and privacy issues that may be related to IoT devices to be consumer product hazards that CPSC would address"). However, the RFI divides potential hazards into two categories of "product safety challenges" which touch on software and data encryption, as well as whether or not a device could be manipulated.

  CPSC should clarify whether it believes FTC or a different agency will handle these.

- For products whose remote operation could create a hazard to consumers, should internet connectivity specifically prevent remote operation?
  NEMA Comment: No, there are a wide variety of appliance that are already remote controlled, such as garage door openers, and these already have sufficient safety standards, practices and features such as physical and electric/electronic interlocks. For example, garage door openers already facilitate activation from a remote in a vehicle or from a consumer on a cell phone, in the near area or from an IoT connection. There are a variety of safety mechanisms built into modern garage door openers that prevent actuation, when something, usually people or animals, are in the path of the garage door. This is the best example of why it is unnecessary or unreasonable to prevent remote actuation of an Internet connected appliance or device. We expect that other examples with respect to ovens, stoves, or other appliances are available to the CPSC.

- How do IoT software development methods address potential product failures that may create hazards to consumers?
  NEMA Comment: Again, in the lighting world, these concerns are addressed via UL1993, UL8750, and UL 1598. It is not immediately apparent that software development methods different than those for appliance or device software development methods are necessary to prevent some dim possibility of a consumer hazard.

- 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?
  NEMA Comment: Acceptable security practices would need to be incorporated into IoT products throughout the product development lifecycle, and regularly kept updated via software development patches and system upgrades, similar to update practices already in place today.

- 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?
  NEMA Comment: It is not readily apparent to us that there are "new hazards" as safety concerns already exist for many products regardless of IoT-features that may be added later.

  If/when developed, these safety standards or guidelines should be voluntary. In many cases complex, connected products may involve multiple safety categories which generally require selecting appropriate sections of safety standards to assure coverage of hazards identified in development of that particular device. Many of these IoT devices blur the lines of the categories for which that the appliance or device are tested for safety. Voluntary standards allow the manufacturer to appropriately administer tests when a hazard is identified in the development process.

- What role should government play in keeping consumers safe regarding IoT devices?
  NEMA Comment: Please see our comment to item 8 above.

- Will policies to prevent hazardization of IoT products require or benefit from strong international cooperation?
  NEMA Comment: Almost all safety standards are consensus-based and international. Hazards are not the exclusive domain of the United States.

- How should the Commission consider responsibilities for hazards or injuries among the various contributors to an internet-connected product associated with an incident?
  NEMA Comment: We are not certain it is possible to segregate IoT, Internet connected appliances or devices, and the hazards or injuries directly attributable to these devices, as opposed to non-Internet connected appliances or devices. We support CPSC in their efforts to determine whether a method for segregating injuries and/or potential hazards caused due to being connected to the Internet is possible.

- How should the Commission consider responsibilities for hazards or injuries resulting from interdependencies between products (e.g., communications protocol between networked alarm and smart home hub)?
  NEMA Comment: In the lighting segment, product performance consequences (lights not working) are potentially impacted by interdependencies, but darkness (in the event that the lighting is not energized and "on" because of a product performance issue) is not a new hazard introduced by IoT-enabled devices.

- For recalls involving IoT devices, what are different ways companies can communicate notice to consumers who own the IoT devices?
  NEMA Comment: While using apps as a communication method for recalls might sound appealing, the lack of standards in operating systems (especially in the world of Android, where every device maker can, and often does, create a customized

version) creates a real risk that any single solution favored by the CPSC may not work across all platforms. This is especially true in the case of customers who decline to update their OS for various reasons and continue to run older, possibly unsupported versions. For this reason, automated communication should be considered in augmentation to the standard methods of communicating recalls, and not a replacement for them.
Companies already transmit electronic notices to customers via e-mail or via their websites. If any changes contemplated in this regard, CPSC should consider data privacy concerns.

If such standards are adopted, manufacturers will need clarity from CPSC as to whether a companies' section 15(b) reporting duties of a "substantial product hazard" and accompanying analysis would need to be altered in any respect, and whether CPSC would consider extending its existing 10-day investigation and reporting rule for incidents relating to IoT devices, given their technical complexity and the assessment required to distinguish between IoT-features and non-IoT features in various "smart" products.

A potential benefit to maintaining contact with consumers, and thus the CPSC's goals, is the fact that IoT devices generally require registration in order to activate the operation of the device. This should provide industry with much better visibility into customers. However it is worth pointing out that many jurisdictions are implementing privacy rules, which could potentially limit industries visibility into consumers or residences to communicate notices regarding IoT device hazards. Numerous industry representatives expressed concern in European Union proceedings in the past few years that privacy rulemaking could limit or inhibit safety related essential communications, or even warranty related information to consumers or residences. For example, the practice of the "right to be forgotten" includes contact information and warranty registration, leaving responsible industry actors unable to inform those forgotten consumers of newly discovered risks.